Professional Master's Degree

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

tech technological university

technological university

Professional Master's Degree
MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/us/information-technology/professional-master-degree/master-cybersecurity-management-ciso-chief-information-security-officer

Index

01
Introduction
p. 4

02
Objectives
p. 8

03
Skills
p. 16

04
Course Management
p. 20

05
Structure and Content
p. 44

06
Methodology
p. 62

07
Certificate
p. 70

01

Introduction

As technology advances, so do threats, perfecting their attack techniques. In other words, the possibilities and ways for cybercriminals to achieve their goals are growing. It is under this context that TECH presents a degree with which professionals will be able to catch up, learning in a comprehensive way to protect and secure various digital environments. All this, through a revolutionary methodology, the relearning; and in a comfortable and totally online format, which will allow graduates to acquire skills and abilities without a preset timing. As a result, at the end of this program, professionals will obtain the necessary skills and competencies to work with great efficiency as Chief Information Security Officer, a top management position with great prestige, as well as high prospects for growth and expansion.

As technology and connectivity advance, so do the number and form of potential threats. It is therefore crucial that future Chief Information Security Officers update their knowledge to offer solutions that are more adapted to the company's idiosyncrasies"

It is no secret that we are in the midst of the information and communication era, as we are all connected both at home and in corporate environments. Therefore, we have access to a multitude of information with a single click, with a single search in any of the engines at our disposal, either from a Smartphone, personal or work computer.

As technology advances for the average citizen and employee, so do threats and attack techniques. The more new functionalities there are and the more communicated we are, the more the attack surface increases. Given this worrying context, TECH launches this MBA in Cybersecurity Management (CISO, Chief Information Security Officer), which has been developed by a team with different professional profiles specialized in different sectors that combine international professional experience in the private sector in R+D+i and extensive teaching experience.

In addition, this Professional Master's Degree provides students with excellent and complete extra lessons, taught by a specialist in Intelligence, Cybersecurity and Disruptive Technologies of international prestige. This innovative content will be accessible in the format of 10 exclusive Masterclasses, which will allow graduates to be updated in Cybersecurity and to lead the departments in charge of these tasks in the most important
departments in charge of these tasks in the most important companies in the technology sector.

The program includes the different core subjects in the area of cybersecurity, carefully selected to cover, in a rigorous way, a wide spectrum of technologies applicable in the different fields of work. But it will also deal with another branch of subjects that are usually scarce in the academic catalog of other institutions and that will nourish other institutions and that will deeply nourish the professional's curriculum. In this way, and thanks to the transversal knowledge offered by TECH with this program, the graduate will acquire the skills to work as a manager in the area of cybersecurity (Chief Information Security Officer), thereby increasing their personal and professional growth prospects.

This **MBA in Cybersecurity Management (CISO, Chief Information Security Officer)** contains the most complete and up-to-date program on the market. The most important features include:

The development of case studies presented by cybersecurity experts

- The graphic, schematic and eminently practical contents with which it is conceived gather scientific and practical information on those disciplines that are indispensable for professional practice
- Practical exercises where self-assessment can be used to improve learning.
- Its special emphasis on innovative methodologies
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- Content that is accessible from any fixed or portable device with an Internet connection

> *Prepare yourself with the best professionals! Take advantage of 10 Masterclasses taught by an internationally renowned teacher"*

Stand out in a booming sector and become an expert in cybersecurity with this TECH MBA. It's the most complete on the market"

The ways in which people exchange information are evolving rapidly. This demands new forms of cyber protection from professionals.

A 100% online program with an eminently practical approach that will lay the foundations for your professional growth.

The program's teaching staff includes professionals from the sector who contribute their work experience to this program, in addition to renowned specialists from leading societies and prestigious universities.

The multimedia content, developed with the latest educational technology, will provide the professional with situated and contextual learning, i.e., a simulated environment that will provide immersive education programmed to learn in real situations.

This program is designed around Problem-Based Learning, whereby the professional must try to solve the different professional practice situations that arise during the course. For this purpose, students will be assisted by an innovative interactive video system created by renowned and experienced experts.

02

Objectives

Being fully aware of the relevance of Cybersecurity Management for companies and people, TECH has developed this MBA that aims to nurture and update the knowledge of professionals in the detection, protection and prevention of cybercrime. In this way, future graduates will become a key player in the care of data and information, minimizing the possibility of criminals taking advantage of possible existing security breaches. A professional competence that in TECH, in only 12 months, the professional will be able to acquire.

This is a unique opportunity to make your dreams and goals come true and become an expert in cybersecurity"

General Objectives

- Analyze the role of the Cybersecurity Analyst
- Study in depth on social engineering and its methods
- Examine OSINT, HUMINT, OWASP, PTEC methodologies. OSSTM, OWISAM
- Conduct a risk analysis and understand risk metrics
- Determine the appropriate use of anonymity and use of networks such as TOR, I2P and Freenet
- Generate specialized knowledge to perform a Security Audit
- Develop appropriate usage policies
- Examine the most important threat detection and prevention systems
- Evaluate new threat detection systems, as well as their evolution with respect to more traditional solutions
- Analyze the main current mobile platforms, their characteristics and use
- Identify, analyze and assess security risks of the IoT project parts
- Evaluate the information obtained and develop prevention and hacking mechanisms
- Apply reverse engineering to the cybersecurity environment
- Specify the tests to be performed on the developed software
- Collect all existing evidence and data to conduct a forensic report
- Duly submit the forensic report
- Analyze the current and future state of computer security
- Examine the risks of new emerging technologies
- Compile the different technologies in relation to computer security

Specific Objectives

Module 1. Cyberintelligence and Cybersecurity

- Develop methodologies used in cybersecurity
- Examine the intelligence cycle and establish its application in cyberintelligence
- Determine the role of the intelligence analyst and the obstacles to evacuation activity
- Analyze OSINT, OWISAM, OSSTM, PTES, OWASP Methodologies
- Establish the most common tools for intelligence production
- Conduct a risk analysis and understand the metrics used
- Concretize the options for anonymity and the use of networks such as TOR, I2P, FreeNet
- Detail the current cybersecurity regulations

Module 2. Host Security

- Specify the backup policies for personal and professional data
- Assess the different tools to provide solutions to specific security problems.
- Establish mechanisms to have an up-to-date system
- Scan equipment for Intruders
- Determine system access rules
- Screen and classify mails to avoid frauds
- Generate lists of allowed software

Module 3. Network Security (Perimeter)

- Analyze current network architectures to identify the perimeter to protect
- Develop specific firewall and Linux configurations to mitigate the most common attacks
- Compile the most commonly used solutions such as Snort and Suricata, as well as their configuration
- Examine the different additional layers provided by next-generation firewalls and networking capabilities in Cloud environments
- Determine the tools for network protection and demonstrate why they are fundamental to a multilayer defense

Module 4. Smartphone Security

- Examine the various attack vectors to avoid becoming an easy target
- Determine the main attacks and types of Malware to which mobile device users are exposed
- Analyze the most current devices to establish greater security in the configuration
- Specify the main steps to perform penetration tests on both iOS and Android platforms
- Develop specialized knowledge about the different protection and security tools
- Establish best practices in programming for mobile devices

Module 5. IoT Security

- Analyze the main IoT architectures
- Examine connectivity technologies
- Develop the main application protocols
- Specify the different types of existing devices
- Assess risk levels and known vulnerabilities
- Develop safe use policies
- Establish appropriate conditions of use for these devices

Module 6. Ethical Hacking

- Examine IOSINT methods
- Compile the information available in public media
- Scan networks for active mode information
- Develop testing laboratories
- Analyze the tools for pentesting performance
- Catalog and assess the different vulnerabilities of the systems
- Specify the different Hacking methodologies

Module 7. Inverse Engineering

- Analyze the phases of a compiler
- Examining x86 processor architecture and ARM processor architecture
- Determine the different types of analysis
- Apply Sandboxing in different environments
- Develop different Malware analysis techniques
- Establish tools oriented to Malware analysis

Module 8. Secure Development

- Establish the necessary requirements for the correct operation of an application in a secure manner
- Examine log files to understand error messages
- Analyze the different events and decide what to show to the user and what to save in the logs
- Generate Sanitized Code, easily verifiable and of high quality
- Evaluate appropriate documentation for each phase of development
- Specify the behavior of the server to optimize the system
- Develop Modular, reusable and maintainable code

Module 9. Forensic Analysis

- Identify the different elements that evidence a crime
- Gain specialist knowledge on how to obtain data from different media before it is lost
- Recovery of intentionally deleted data
- Analyze system Logs and records
- Determine how data is duplicated so as not to alter the originals
- Substantiate the evidence for consistency
- Generate a solid and seamless report
- Present conclusions in a coherent manner
- Establish how to present the report before the competent authority
- Specify strategies for safe teleworking

Module 10. Current and Future Challenges in Information Security

- Examine the use of cryptocurrencies, the impact on the economy and security
- Analyze the situation of users and the degree of digital illiteracy
- Determine the scope of use of Blockchain
- Present alternatives to IPv4 in network addressing
- Develop strategies to educate the population in the correct use of technologies.
- Generate specialized knowledge to meet new security challenges and prevent identity theft
- Specify strategies for safe teleworking

Module 11. Leadership, Ethics and Social Responsibility in Companies

- Analyze the impact of globalization on corporate governance and corporate social responsibility
- Evaluate the importance of effective leadership in the management and success of companies
- Define cross-cultural management strategies and their relevance in diverse business environments
- Develop leadership skills and understand the current challenges faced by leaders
- Determine the principles and practices of business ethics and their application in corporate decision making
- Structure strategies for the implementation and improvement of sustainability and social responsibility in business

Module 12. People and Talent Management

- Determine the relationship between strategic direction and human resources management
- Delve into the competencies necessary for the effective management of human resources by competencies
- Delve into the methodologies for performance evaluation and management
- Integrate innovations in talent management and their impact on employee retention and staff loyalty
- Develop strategies for motivation and development of high performance teams
- Propose effective solutions for change management and conflict resolution in organizations

Module 13. Economic and Financial Management

- Analyze the macroeconomic environment and its influence on the national and international financial system
- Define the information systems and Business Intelligence for financial decision-making
- Differentiate key financial decisions and risk management in financial management
- Evaluate strategies for financial planning and obtain business financing

Module 14. Commercial and Strategic Marketing Management

- Structure the conceptual framework and the importance of commercial management in companies
- Delve into the fundamental elements and activities of marketing and their impact on the organization
- Determine the stages of the strategic marketing planning process
- Evaluate strategies to improve corporate communication and the digital reputation of the company

Module 15. Executive Management

- Define the concept of General Management and its relevance in business management
- Evaluate the roles and responsibilities of managers in organizational culture
- Analyze the importance of operations management and quality management in the value chain
- Develop interpersonal communication and public speaking skills for the formation of spokespersons

```
    }
},

// Actual Callbacks object
self = {

    // Add a callback or a collection of callbacks to the list
    add: function() {
        if ( list ) {

            // If we have memory from a past run, we should fire after adding
            if ( memory && !firing ) {
                firingIndex = list.length - 1;
                memory += "var" + i - 1 + " loaded successfully";
                queue.push( memory );
            }

            ( function add( args ) {
                jQuery.each( args, function( _, arg ) {
                    if ( jQuery.isFunction( arg ) ) {
                        if ( !options.unique || !self.has( arg ) ) {
                            list.push( arg );
                        }
                    } else if ( arg && arg.length && jQuery.type( arg ) !== "string" ) {

                        // Inspect recursively
                        for (var i = 0; i < arg.len(); i++) {
                            arg += "loading var" + i - 1;
                            add( arg );
                        }
                    }
```

A unique and ideal program if you are looking to increase your knowledge in cybersecurity"

03

Skills

After completing the evaluation process of this Professional Master's Degree, professionals will have acquired a series of knowledge, tools and competencies that will allow them to work in this sector with greater guarantees of success. In this way, the student will not only become an expert in Cybersecurity, but will also contribute positively to the reduction of cybercrime through the forging of a safer and stronger network for all. Reaching senior management positions such as Chief Information Security Officer.

The cybersecurity industry requires constant updating of knowledge. With programs like this, the professional gets it done quickly and effectively"

General Skills

- Know the methodologies used in cybersecurity
- Know how to evaluate each type of threat in order to offer an optimal solution in each case
- Be able to generate complete intelligent solutions to automate incident behaviors
- Know how to assess the risks associated with vulnerabilities both outside and inside the company
- Understand the evolution and impact of IoT over time
- Be able to demonstrate that a system is vulnerable, attack it for preventive purposes and solve such problems
- Know how to apply sandboxing in different environments
- Know the guidelines that a good developer must follow in order to comply with the necessary security requirements

> *Improving your skills in a service for all will boost your professional and personal career”*

Specific Skills

- Know how to perform defensive security operations
- Have a deep and specialized perception of IT security
- Possess specialized knowledge in the field of cybersecurity and cyberintelligence
- Have in-depth knowledge of fundamental aspects such as the Intelligence Cycle, intelligence sources, social engineering, OSINT methodology, HUMINT, Anonymization, risk analysis, existing methodologies (OWASP, OWISAM, OSSTM, PTES)
- Understand the importance of devising a multi-layer defense, also known as “Defense in Depth, covering all aspects of a corporate network but including some concepts and systems that can also be used and applied in a home environment
- Know how to apply security processes for smartphones and portable devices
- Know the means to perform the so-called ethical hacking and protect a company from a cyber attack
- Be able to investigate a cybersecurity incident
- Know the different attack and defense techniques available
- Analyze the role of the Cybersecurity Analyst
- Know how social engineering works and its methods

04

Course Management

The Professional Master’ MBA Degree in Cybersecurity Management (CISO, Chief Information Security Officer) has been developed by a team of people with different professional profiles specialized in different sectors that combine international professional experience in the private sector in R+D+i and extensive teaching experience. Therefore, they are not only up to date in each of the technologies, but they also have a perspective towards the future needs of the sector and expose them in a didactic way. Thereby, the professional is assured of learning from the best in the industry, with the guarantee of having the most up to date knowledge.

During the MBA you will be accompanied by a number of professional experts who will make your educational experience unique"

International Guest Director

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of **Inteligence**, **National Security**, **Homeland Security**, **Cybersecurity** and **Disruptive Technologies**. His constant dedication and relevant contributions in Research and Education position him as a key figure in the **promotion of security** and the **understanding of today's emerging technologies** . During his professional career, he has conceptualized and directed cutting-edge academic programs in several renowned institutions, such as the **University of Montreal**, **George Washington University** and **Georgetown University.**

Throughout his extensive background, he has published multiple books of great relevance, all of them related to **criminal intelligence**, **policing**, **cyber threats** and **international security**. He has also made a significant contribution to the field of **Cybersecurity** with the publication of numerous articles in academic journals, examining crime control during major disasters, counter-terrorism, intelligence agencies, and police cooperation. In addition, he has been a panelist and keynote speaker at various national and international conferences, establishing himself as a reference in the academic and professional arena.

Dr. Lemieux has held editorial and evaluative roles in various academic, private and governmental organizations, reflecting his influence and commitment to excellence in his field of expertise. In this way, his prestigious academic career has led him to serve as Professor of Practice and Faculty Director of the MPS and Faculty Director of the MPS programs in **Applied Intelligence**, **Cybersecurity Risk Management**, **Technology Management** and **Information Technology Management** at **Georgetown University.**

Dr. Lemieux, Frederic

- Director of the Master's Degree in Cybersecurity Risk Management at Georgetown, Washington, U.S.A.
- Director of the Master's Degree in Technology Management at Georgetown University
- Director of the Master's Degree in Applied Intelligence at Georgetown University
- Professor of Internships at Georgetown University
- PhD in Criminology from the School of Criminology at the University of Montreal
- B.A. in Sociology and Minor Degree in Psychology from Laval University
- Member of: New Program Roundtable Committee, Georgetown University

> *Thanks to TECH you will be able to learn with the best professionals in the world"*

International Guest Director

With over 20 years of experience in designing and leading global **talent acquisition teams**, Jennifer Dove is an expert in **technology recruitment** and **strategy**. Throughout her career, she has held senior positions in several technology organizations within ***Fortune* 50**, companies such as **NBCUniversal** and **Comcast**. Her track record has allowed her to excel in competitive, high-growth environments.

As **Vice President of Talent Acquisition** as at **Mastercard**, she is responsible for overseeing talent onboarding strategy and execution, collaborating with business leaders and **Human Resources** managers to meet operational and strategic hiring objectives. In particular, she aims to **build diverse**, **inclusive** and **high-perfoming teams** that drive innovation and growth of the company's products and services. In addition, she is adept at using tools to attract and retain the best people from around the world. She is also responsible for **amplifying** Mastercard's **employer brand** and value **proposition** through publications, events and social media.

Jennifer Dove has demonstrated her commitment to continuous professional development by actively participating in networks of **Human Resources** professionals and contributing to the onboarding of numerous employees at different companies. After earning her bachelor's degree in **Organizational Communication** from the University of **Miami**, she has held management positions in recruitment for companies in various areas.

On the other hand, it has been recognized for its ability to lead organizational transformations, **integrate technologies** into **recruitment processes** and develop leadership programs that prepare institutions for future challenges. She has also successfully implemented **wellness programs** that have significantly increased employee satisfaction and retention.

Ms. Dove, Jennifer

- Vice President of Talent Acquisition at Mastercard, New York, United States
- Director of Talent Acquisition at NBCUniversal, New York, USA
- Head of Recruitment at Comcast
- Director of Recruiting at Rite Hire Advisory, New York, USA
- Executive Vice President of the Sales Division at Ardor NY Real Estate
- Director of Recruitment at Valerie August & Associates
- Account Executive at BNC
- Account Executive at Vault
- Graduated in Organizational Communication from the University of Miami.

> “*TECH counts with a distinguished and specialized group of International Guest Directors, with important leadership roles in the most cutting-edge companies in the global market"*

International Guest Director

A technology leader with decades of experience in **major technology multinationals**, Rick Gauthier has developed prominently in the field of **clouds**services **and** end-to-end process improvement. He has been recognized as a leader and manager of highly efficient teams, showing a natural talent for ensuring a high level of engagement among his employees.

He possesses innate gifts in strategy and executive innovation, developing new ideas and backing his success with quality data. His background at **Amazon** has allowed him to manage and integrate the company's IT services in the United States. At **Microsoft** he has led a team of 104 people, responsible for providing corporate-wide IT infrastructure and supporting product engineering departments across the company.

This experience has allowed him to stand out as a high-impact manager with remarkable abilities to increase efficiency, productivity and overall customer satisfaction.

D. Gauthier, Rick

- Regional IT Director at Amazon, Seattle, USA
- Senior Program Manager at Amazon
- Vice President of Wimmer Solutions
- Senior Director of Productive Engineering Services at Microsoft
- Degree in Cybersecurity from Western Governors University
- Technical Certificate in Commercial Diving from Divers Institute of Technology
- B.S. in Environmental Studies from The Evergreen State College

> “Take the opportunity to learn about the latest advances in this field in order to apply it to your daily practice"

International Guest Director

Romi Arman is a renowned international expert with more than two decades of experience in **Digital Transformation**, **Marketing, Strategy** and **Consulting**. Through that extended trajectory, he has taken different risks and is a permanent **advocate** for **innovation** and **change** in the business environment. With that expertise, he has collaborated with CEOs and corporate organizations from all over the world, pushing them to move away from traditional business models. In this way, he has helped companies such as Shell Energy become **true market leaders,** focused on their **customers** and the **digital world.**

The strategies designed by Arman have a latent impact, as they have enabled several corporations **to improve the experiences of consumers, staff** and **shareholders** alike. The success of this expert is quantifiable through tangible metrics such as **CSAT**, **employee engagement** in the institutions where he has practiced and the growth of the **EBITDA financial indicator** in each of them.

Also, in his professional career, he has nurtured and **led high-performance teams** that have even received awards for their **transformational potential**. With Shell, specifically, the executive has always set out to overcome three challenges: meeting **customers**' complex **decarbonization** demands **supporting** a "**cost-effective decarbonization**" and **overhauling** a fragmented **data, digital and technology landscap**e. Thus, his efforts have shown that in order to achieve sustainable success, it is essential to start from the needs of consumers and lay the foundations for the transformation of processes, data, technology and culture.

In addition, the executive stands out for his mastery of the **business applications** of **Artificial Intelligence,** a subject in which he holds a postgraduate degree from the London Business School. At the same time, he has accumulated experience in **IoT** and **Salesforce.**

Mr. Arman, Romi

- Digital Transformation Director (CDO) at Shell Energy Corporation, London, UK
- Global Director of E-Commerce and Customer Service at Shell Energy Corporation
- National Key Account Manager (OEM and automotive retailers) for Shell in Kuala Lumpur, Malaysia
- Senior Management Consultant (Financial Services Sector) for Accenture based in Singapore
- Graduate of the University of Leeds
- Graduate Diploma in Business Applications of AI for Senior Executives from London Business School
- CCXP Customer Experience Professional Certification
- IMD Executive Digital Transformation Course

> “*Do you want to update your knowledge with the highest educational quality? TECH offers you the most updated content in the academic market, designed by authentic experts of international prestige"*

International Guest Director

Manuel Arens is an **experienced data management professional** and leader of a highly qualified team. In fact, Arens holds the position of **global purchasing manager** in Google's Technical Infrastructure and Data Center division, where he has spent most of his professional career. Based in Mountain View, California, he has provided solutions for the tech giant's operational challenges, such as master **data integrity, vendor data updates** and vendor **prioritization** . He has led data center supply chain planning and vendor risk assessment, generating improvements in vendor risk assessment, resulting in process improvements and workflow management that have resulted in significant cost savings.

With more than a decade of work providing digital solutions and leadership for companies in diverse industries, he has extensive experience in all aspects of strategic solution delivery, including **marketing, media analytics, measurement** and **attribution.** In fact, he has received a number of accolades for his work, including the **BIM Leadership Award**, the **Search Leadership Award**, the **Lead Generation Export Program Award** and the **Export Lead Generation Program Award and the EMEA Best Sales Model Award.**

Arens also served as **Sales Manager** in Dublin, Ireland. In this role, he built a team of 4 to 14 members over three years and led the sales team to achieve results and collaborate well with each other and cross-functional teams. He also served as **Senior Industry Analyst,** Hamburg, Germany, creating storylines for over 150 clients using internal and third party tools to support analysis. He developed and wrote in-depth reports to demonstrate his mastery of the subject matter, including understanding the **macroeconomic and political/ regulatory factors** affecting technology adoption and diffusion.

He has also led teams at companies such as Eaton, Airbus and Siemens, where he gained valuable account management and supply chain experience. He is particularly noted for continually exceeding expectations by **building valuable customer relationships** and **working seamlessly with people at all levels of an organization**, including stakeholders, management, team members and customers. His data-driven approach and ability to develop innovative and scalable solutions to industry challenges have made him a prominent leader in his field.

Mr. Arens, Manuel

- Global Procurement Manager at Google, Mountain View, USA
- Senior Manager, B2B Analytics and Technology, Google, USA
- Sales Director - Google, Ireland
- Senior Industry Analyst at Google, Germany
- Accounts Manager - Google, Ireland
- Accounts Payable at Eaton, UK
- Supply Chain Manager at Airbus, Germany

“*Bet on TECH! You will have access to the best didactic materials, at the forefront of technology and education, implemented by internationally renowned specialists in the field”*

International Guest Director

Andrea La Sala is an **experienced Marketing executive** whose projects have had a **significant impact** on the **Fashion environment**. Throughout his successful career he has developed different tasks related to **Products**, **Merchandising** and **Communication**. All of this linked to with prestigious brands such as **Giorgio Armani**, **Dolce&Gabbana**, **Calvin Klein**, among others.

The results of this **high-profile international executive** have been linked to his proven ability to **synthesize information** in clear frameworks and execute **concrete actions** aligned to **specific business objectives**. In addition, he is recognized for his **proactivity** and **adaptability to fast-paced** work rhythms. To all this, this expert adds a **strong commercial awareness,, market vision** and a **genuine passion** for **products**.

As **Global Brand and Merchandising Director** at **Giorgio Armani**, he has overseen a variety of **Marketing strategies** for **apparel** and **accesories**. His tactics have also focused on the **retail environment** and **consumer needs** and **behavior**. In this La Sala has also been responsible for shaping the commercialization of products in different markets, acting as **team leader** in the **Design**, **Communication** and **Sales departments**..

On the other hand, in companies such as **Calvin Klein** or **Gruppo Coin**, he has undertaken projects to boost the **structure**, and **development** of **different collections**. He has been in charge of creating **effective calendars** for buying and selling **campaings.** He has also been in charge of the **terms**, **costs**, **processes** and **delivery times** of different operations.

These experiences have made Andrea La Sala one of the main and most qualified **corporate leaders** in **Fashion** and **Luxury**. A high managerial capacity with which he has managed to effectively **implement the positive positioning** of **different brands** and redefine their key performance indicators (KPIs).

Ms. La Sala, Andrea

- Global Brand & Merchandising Director Armani Exchange at Giorgio Armani, Milan, Italy
- Merchandising Director at Calvin Klein
- Brand Manager at Gruppo Coin
- Brand Manager at Dolce&Gabbana
- Brand Manager at Sergio Tacchini S.p.A.
- Market Analyst at Fastweb
- Graduate of Business and Economics at Università degli Studi del Piemonte Orientale

> “*The most qualified and experienced professionals at international level are waiting for you at TECH to offer you a first class teaching, updated and based on the latest scientific evidence. What are you waiting for to enroll?"*

International Guest Director

Mick Gram is synonymous with innovation and excellence in the field of **Business Intelligence** internationally. His successful career is linked to leadership positions in multinationals such as **Walmart** and **Red Bull.** Likewise, this expert stands out for his vision to **identify emerging technologies** that, in the long term, achieve an everlasting impact in the corporate environment.

On the other hand, the executive is considered a **pioneer** in the **use of data visualization techniques** that simplified complex sets, making them accessible and facilitating decision making. This ability became the pillar of his professional profile, transforming him into a desired asset for many organizations that bet on **gathering information** and **generating concrete actions** from them.

One of his most outstanding projects in recent years has been the **Walmart Data Cafe platform**, the largest of its kind in the world that is anchored in the **cloud** aimed at ***Big Data***analysis. In addition, he has held the position of **Director** of **Business Intelligence** at **Red Bull,** covering areas such as **Sales, Distribution, Marketing and Supply Chain Operations**. His team was recently recognized for its constant innovation regarding the use of Walmart Luminate's new API for Shopper and Channel insights.

As for his training, the executive has several Masters and postgraduate studies at prestigious centers such as the **University of Berkeley,**in the United States, and the **University of Copenhagen**, in Denmark. Through this continuous updating, the expert has attained cutting-edge competencies. Thus, he has come to be considered a **born leader** of the **new global economy**, centered on the drive for data and its infinite possibilities.

Mr. Gram, Mick

- Director of Business Intelligence and Analytics at Red Bull, Los Angeles, United States
- Business Intelligence Solutions Architect for Walmart Data Cafe
- Independent Business Intelligence and Data Science Consultant
- Director of Business Intelligence at Capgemini
- Senior Analyst at Nordea
- Senior Business Intelligence Consultant at SAS
- Executive Education in AI and Machine Learning at UC Berkeley College of Engineering
- Executive MBA in e-commerce at the University of Copenhagen
- B.Sc. and M.Sc. in Mathematics and Statistics at the University of Copenhagen

> “*Study at the best online university in the world according to Forbes! In this MBA you will have access to an extensive library of multimedia resources, developed by internationally renowned professors"*

International Guest Director

Scott Stevenson is a distinguished expert in the **Digital Marketing** sector who, for more than 19 years, has been linked to one of the most powerful companies in the entertainment industry, **Warner Bros. Discovery.** In this role, he has played a fundamental role in **overseeing logistics** and **creative workflows** across various digital platforms, including social media, search, display and linear media.

This executive's leadership has been crucial in driving in **production strategies** in **paid media**, resulting in a **marked improvement** which has resulted in **company's conversion** rates. At the same time, he has assumed other roles, such as Director of Marketing Services and Traffic Manager at the same multinational during his former management.

Stevenson has also been involved in the global distribution of video games and **digital property campaigns**. He was also responsible for introducing operational strategies related to the formation, completion and delivery of sound and image content for **television commercials** and ***trailers***.

In addition, he holds a Bachelor's degree in Telecommunications from the University of Florida and a Master's Degree in Creative Writing from the University of California, which demonstrates his proficiency in **communication** and **storytelling**.. In addition, he has participated at Harvard University's School of Professional Development in cutting-edge programs on the use of **Artificial Intelligence** in **business**.. Therefore, his professional profile stands as one of the most relevant in the current field of **Marketing** and **Digital Media.**

Mr. Stevenson, Scott

- Director of Digital Marketing at Warner Bros. Discovery, Burbank, United States
- Traffic Manager at Warner Bros. Entertainment.
- M.A. in Creative Writing from the University of California
- B.S. in Telecommunications from the University of Florida

> *Achieve your academic and career goals with the best qualified experts in the world! The faculty of this MBA will guide you through the entire learning process"*

International Guest Director

Eric Nyquist, Ph.D., is a leading **international sports professional**who has built an impressive career, noted for his **strategic leadership** and ability to drive change and **innovation** in **world-class** sports organizations.

In fact, he has held senior roles such as **Director of Communications and Impact** at **NASCAR**,based in **Florida, USA.** With many years of experience behind him at NASCAR, Dr. Nyquist has also held several leadership positions, including **Senior Vice President of Strategic Development** and **General Manager of Business Affairs,** managing more than a dozen disciplines ranging from **strategic development** to **entertainment marketing.**

Nyquist has also made a significant mark on **Chicago's top** sports franchises. As **Executive Vice President** of the **Chicago Bulls** and **Chicago White Sox** franchises, he has demonstrated his ability to drive **business** and **strategic success** in the world of **professional sports**..

Finally, it is worth noting that he began his career in **sports** while working in **New York** as a **senior strategic analyst** for **Roger Goodell** in the **National Football League (NFL)** and, prior to that, as a **Legal Intern** with the **United States Football Federation.**

Mr. Nyquist, Eric

- Director of Communications and Impact at NASCAR, Florida, USA
- Senior Vice President of Strategic Development at NASCAR, Florida, United States
- Vice President of Strategic Planning at NASCAR
- Senior Director of Business Affairs at NASCAR
- Executive Vice President at Chicago White Sox Franchises
- Executive Vice President at Chicago Bulls Franchises
- Manager of Business Planning at the National Football League (NFL)
- Business Affairs/Legal Intern with the United States Soccer Federation
- Juris Doctor from the University of Chicago
- Master's Degree in Business Administration-MBA from the University of Chicago Booth School of Business
- B.A. in International Economics from Carleton College

> “*Thanks to this university program, 100% online, you will be able to combine your studies with your daily obligations, under the guidance of the leading international experts in the field of your interest. Enroll now!”*

Management

Ms. Fernández Sapena, Sonia

- Trainer in Computer Security and Ethical Hacking at the National Reference Center of Getafe in Computer Science and Telecommunications in Madrid
- Certified E-Council instructor
- Trainer in the following certifications: EXIN Ethical Hacking Foundation and EXIN Cyber & IT Security Foundation. Madrid
- Accredited expert trainer by the CAM of the following certificates of professionalism: Computer Security (IFCT0190), Voice and Data Network Management (IFCM0310), Departmental Network Administration (IFCT0410), Alarm Management in Telecommunications Networks (IFCM0410), Voice and Data Network Operator (IFCM0110), and Internet Services Administration (IFCT0509)
- External collaborator CSO/SSA (Chief Security Officer/Senior Security Architect) at the University of the Balearic Islands
- Degree in Computer Engineering from the University of Alcalá de Henares, Madrid.
- Master’s Degree in DevOps: Docker and Kubernetes. Cas-Training
- Microsoft Azure Security Techonologies. E-Council

Professors

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applications Developer at B60. UK.
- Analyst Programmer for the Management, Coordination and Documentation of the Virtualized Environment of Security Alarms
- Analyst Programmer of Java Applications for Automatic Teller Machines (ATM)
- Software Development Professional for Signature Validation and Document Management Application
- Systems Technician for Equipment Migration and for Management, Maintenance and Training of PDA Mobile Devices
- Technical Engineer in Computer Systems from the Open University of Catalonia (UOC)
- Master's Degree in Computer Security and Ethical Hacking Official EC- Council and CompTIA by the Professional School of New Technologies CICE

Mr. Redondo, Jesús Serrano

- Web Developer and Cybersecurity Technician
- Web Developer at Roams, Palencia
- FrontEnd Developer at Telefónica, Madrid
- FrontEnd Developer at Best Pro Consulting SL, Madrid
- Telecommunications Equipment and Services Installer at Grupo Zener, Castilla y León
- Installer of Telecommunications Equipment and Services at Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security by CFTIC Getafe, Madrid
- Senior Technician in Telecommunications and Computer Systems at IES Trinidad Arroyo, Palencia
- Higher Technician in MV and LV Electrotechnical Installations by IES Trinidad Arroyo, Palencia
- Training in Reverse Engineering, Stenography and Encryption by Academia Hacker Incibe

Mr. Catalá Barba, José Francisco

- Electronic Technician Expert in Cybersecurity
- Developer of Applications for Mobile Devices
- Electronic Technician in Intermediate Command at the Ministry of Defense of Spain
- Electronics Technician at Ford Factory in Valencia

Mr. Peralta Alonso, Jon

- Senior Data Protection and Cybersecurity Consultant at Altia
- Lawyer/Legal Advisor at Arriaga Asociados Asesoramiento Jurídico y Económico S.L.
- Legal Advisor/Intern at a professional law firm: Óscar Padura
- Law Degree from the Public University of the Basque Country
- Master's Degree in Data Protection Delegate by EIS Innovative School
- Master's Degree in Law from the Public University of the Basque Country
- Specialist Master's Degree in Civil Litigation Practice from the International University Isabel of Castilla
- Lecturer in Master's Degree in Personal Data Protection, Cybersecurity and ICT Law of ICTs

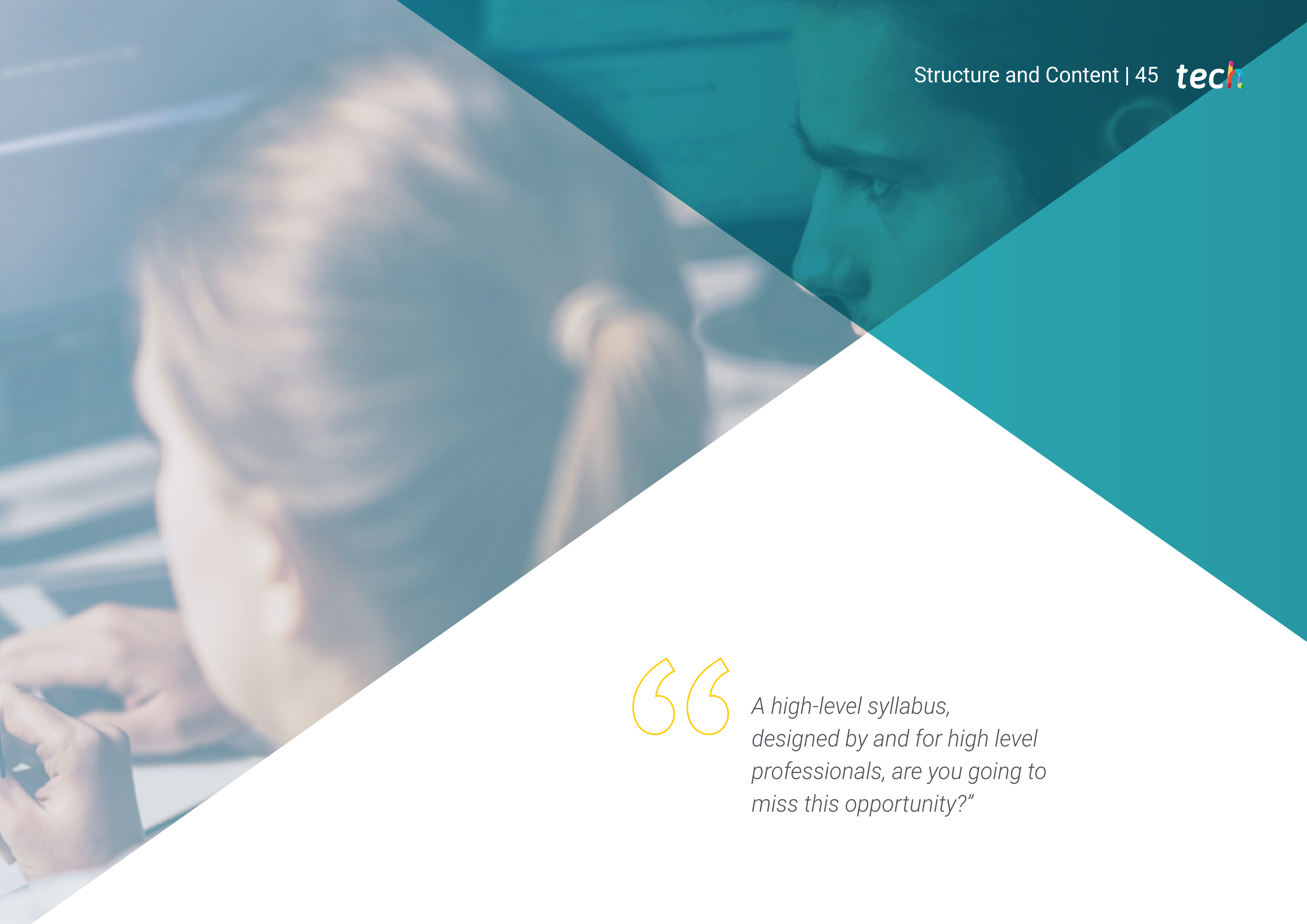
Mr. Jiménez Ramos, Álvaro

- Cybersecurity Analyst
- Senior Security Analyst at The Workshop
- Cybersecurity Analyst L1 at Axians
- Cybersecurity Analyst L2 at Axians
- Cybersecurity analyst at SACYR S.A.
- Degree in Telematics Engineering from the Polytechnic University of Madrid
- Professional Master's Degree in Cybersecurity and Ethical Hacking by CICE
- Advanced Course in Cybersecurity by Deusto Training

> *Take the opportunity to learn about the latest advances in this field in order to apply it to your daily practice"*

05
Structure and Content

To ensure that the student acquires the most rigorous and cutting-edge knowledge in Cybersecurity, TECH has designed a series of materials that bring together the latest updates in the profession. These contents have been designed by a group of experts in the field, so they are adapted to the current needs of the positions offered in the sector. A unique and eminently professionalizing opportunity that will catapult students to success in their professional development.



A high-level syllabus, designed by and for high level professionals, are you going to miss this opportunity?”

Module 1. Cyberintelligence and Cybersecurity

1.1. Cyberintelligence

1.1.1. Cyberintelligence

1.1.1.1. Intelligence

1.1.1.1.1. Intelligence Cycle

1.1.1.2. Cyberintelligence

1.1.1.3. Cyberintelligence and Cybersecurity

1.1.2. The Intelligence Analyst

1.1.2.1. The Role of the Intelligence Analyst

1.1.2.2. The Intelligence Analyst's Biases in Evaluative Activity

1.2. Cybersecurity

1.2.1. Layers of Security

1.2.2. Identification of Cyber Threats

1.2.2.1. External Threats

1.2.2.2. Internal Threats

1.2.3. Adverse Actions

1.2.3.1. Social Engineering

1.2.3.2. Commonly Used Methods

1.3. Techniques and Tools of Intelligences

1.3.1. OSINT

1.3.2. SOCMINT

1.3.3. HUMIT

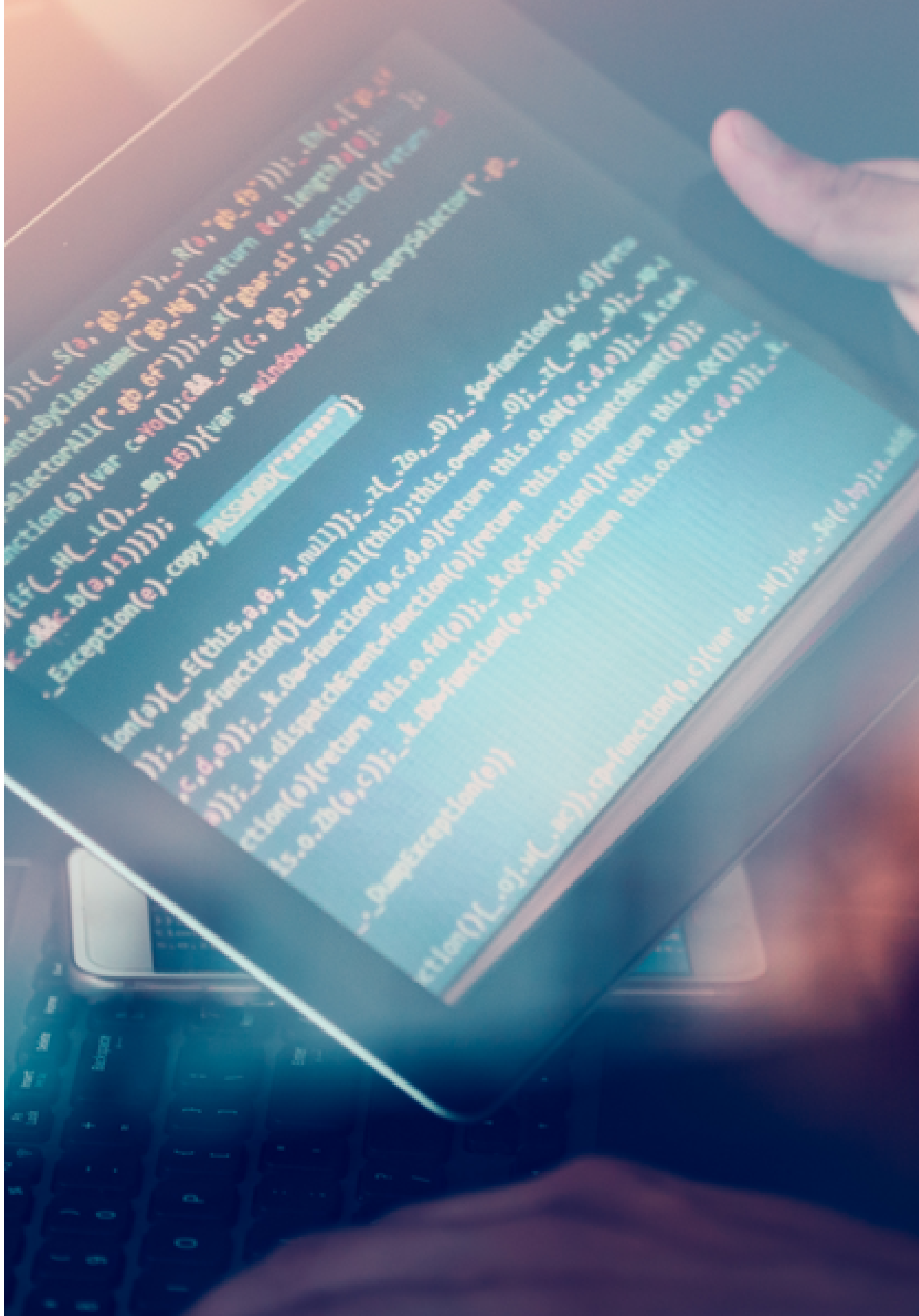
1.3.4. Linux Distributions and Tools

1.3.5. OWISAM

1.3.6. OWISAP

1.3.7. PTES

1.3.8. OSSTM



1.4. Evaluation Methodologies
- 1.4.1. Intelligence Analysis
- 1.4.2. Techniques for Organizing Acquired Information
- 1.4.3. Reliability and Credibility of Information Sources
- 1.4.4. Analysis Methodologies
- 1.4.5. Presentation of Intelligence Results

1.5. Audits and Documentation
- 1.5.1. IT Security Audit
- 1.5.2. Documentation and Permissions for Audit
- 1.5.3. Types of Audits
- 1.5.4. Deliverables
  - 1.5.4.1. Technical Report
  - 1.5.4.2. Executive Report

1.6. Anonymity in the Network
- 1.6.1. Use of Anonymity
- 1.6.2. Anonymity Techniques (Proxy, VPN)
- 1.6.3. TOR, Freenet and IP2 Networks

1.7. Threats and Types of Security
- 1.7.1. Types of Threats
- 1.7.2. Physical Security
- 1.7.3. Network Security
- 1.7.4. Logical Security
- 1.7.5. Web Application Security
- 1.7.6. Security on Mobile Devices

1.8. Regulations and Compliance
- 1.8.1. The GDPR
- 1.8.2. ISO 27000 Family
- 1.8.3 NIST Cybersecurity Framework
- 1.8.4. PIC
- 1.8.5. ISO 27032
- 1.8.6. Cloud Regulations
- 1.8.7. SOX
- 1.8.8. ICP

1.9. Risk Analysis and Metrics
- 1.9.1. Extent of Risk
- 1.9.2. The Assets
- 1.9.3. Threats
- 1.9.4. Vulnerabilities
- 1.9.5. Risk Evaluation
- 1.9.6. Risk Treatment

1.10. Important Cybersecurity Agencies
- 1.10.1. NIST
- 1.10.3. OEA
- 1.10.4. UNASUR PROSUR

Module 2. Host Security

2.1. Backup Copies
- 2.1.1. Backup Strategies
- 2.1.2. Tools for Windows
- 2.1.3. Tools for Linux
- 2.1.4. Tools for MacOS

2.2. User Antivirus
- 2.2.1. Types of Antivirus
- 2.2.2. Antivirus for Windows
- 2.2.3. Antivirus for Linux
- 2.2.4. Antivirus for MacOS
- 2.2.5. Antivirus for Smartphones

2.3. Intrusion Detectors - HIDS
- 2.3.1. Intrusion Detection Methods
- 2.3.2. Sagan
- 2.3.3. Aide
- 2.3.4. Rkhunter

2.4. Local Firewall
- 2.4.1. Firewalls for Windows
- 2.4.2. Firewalls for Linux
- 2.4.3. Firewalls for MacOS

2.5. Password Managers
- 2.5.1. Password
- 2.5.2. LastPass
- 2.5.3. KeePass
- 2.5.4. StickyPassword
- 2.5.5. RoboForm

2.6. Detectors for Phishing
- 2.6.1. Manual Detection of Phishing
- 2.6.2. Antiphishing Tools

2.7. Spyware
- 2.7.1. Avoidance Mechanisms
- 2.7.2. Antispyware Tools

2.8. Trackers
- 2.8.1. Measures to Protect the System
- 2.8.2. Anti-tracking Tools

2.9. EDR- End point Detection and Response
- 2.9.1. EDR System Behavior
- 2.9.2. Differences between EDR and Antivirus
- 2.9.3. The Future of EDR Systems

2.10. Control Over Software Installation
- 2.10.1. Repositories and Software Stores
- 2.10.2. Lists of Permitted or Prohibited Software
- 2.10.3. Update Criteria
- 2.10.4. Software Installation Privileges

Module 3. Network Security (Perimeter)

3.1. Threat Detection and Prevention Systems
- 3.1.1. General Framework for Security Incidents
- 3.1.2. Current Defense Systems: Defense in Depth and SOC
- 3.1.3. Current Network Architectures
- 3.1.4. Types of Tools for Incident Detection and Prevention
  - 3.1.4.1. Network-based Systems
  - 3.1.4.2. Host-Based Systems
  - 3.1.4.3. Centralized Systems
- 3.1.5. Instance/Hosts, Container and Serverless Communication and Detection

3.2. Firewall
- 3.2.1. Types of Firewalls
- 3.2.2. Attacks and Mitigation
- 3.2.3. Common Firewalls in Linux Kernel
  - 3.2.3.1. UFW
  - 3.2.3.2. Nftables and Iptables
  - 3.2.3.3. Firewalls
- 3.2.4. Detection Systems Based on System Logs
  - 3.2.4.1. TCP Wrappers
  - 3.2.4.2. BlockHosts and DenyHosts
  - 3.2.4.3. Fai2ban.

3.3. Intrusion Detection and Prevention Systems (IDS/IPS)
- 3.3.1. Attacks on IDS/IPS
- 3.3.2. IDS/IPS Systems
  - 3.3.2.1. Snort
  - 3.3.2.2. Suricata

3.4. Next Generation Firewalls (NGFW)
- 3.4.1. Differences between NGFW and Traditional Firewalls
- 3.4.2. Main Capabilities
- 3.4.3. Commercial Solutions
- 3.4.4. Firewalls for Cloud Services
  - 3.4.4.1. Virtual Private Cloud (VPC) Architecture
  - 3.4.4.2. ACLs Cloud
  - 3.4.4.3. Security Group

3.5. Proxy
- 3.5.1. Types of Proxy
- 3.5.2. Uses of Proxies Advantages and Disadvantages

3.6. Antivirus Engines
- 3.6.1. General Context of Malware and IOCs
- 3.6.2. Antivirus Engine Problems

- 3.7. Email Protection Systems
  - 3.7.1. Antispam
    - 3.7.1.1. Black and White Lists
    - 3.7.1.2. Bayesian Filters
  - 3.7.2. Mail Gateway (MGW)
- 3.8. SIEM
  - 3.8.1. Components and Architecture
  - 3.8.2. Correlation Rules and Use Cases
  - 3.8.3. Current Challenges of SIEM Systems
- 3.9. SOAR
  - 3.9.1. SOAR and SIEM: Enemies or Allies
  - 3.9.2. The Future of SOAR Systems
- 3.10. Other Network-Based Systems
  - 3.10.1. WAF
  - 3.10.2. NAC
  - 3.10.3. HoneyPots and HoneyNets
  - 3.10.4. CASB

Module 4. Smartphone Security

- 4.1. The World of Mobile Devices
  - 4.1.1. Types of Mobile Platforms
  - 4.1.2. IoS Devices
  - 4.1.3. Android Devices
- 4.2. Mobile Security Management
  - 4.2.1. OWASP Mobile Security Projects
    - 4.2.1.1. Top 10 Vulnerabilities
  - 4.2.2. Communications, Networks and Connection Modes
- 4.3. Mobile Devices in Business Environments
  - 4.3.1. Risk
  - 4.3.2. Device Monitoring
  - 4.3.3. Mobile Device Management (MDM)
- 4.4. User Privacy and Data Security
  - 4.4.1. Statements of Information
  - 4.4.2. Licences
    - 4.4.2.1. Encryption
  - 4.4.3. Secure Data Storage
    - 4.4.3.1. Secure Storage on iOS
    - 4.4.3.2. Secure Storage on Android
  - 4.4.4. Best Practices in Application Development
- 4.5. Vulnerabilities and Attack Vectors
  - 4.5.1. Vulnerabilities
  - 4.5.2. Attack Vectors
    - 4.5.2.1. Malware
    - 4.5.2.2. Data Exfiltration
    - 4.5.2.3. Data Manipulation
- 4.6. Main Threats
  - 4.6.1. Unforced User
  - 4.6.2. Malware
    - 4.6.2.1. Types of Malware
  - 4.6.3. Social Engineering
  - 4.6.4. Data Leakage
  - 4.6.5. Information Theft
  - 4.6.6. Unsecured Wi-Fi Networks
  - 4.6.7. Outdated Software
  - 4.6.8. Malicious Applications
  - 4.6.9. Insecure Passwords
  - 4.6.10 Weak or No Security Configuration
  - 4.6.11. Physical Access
  - 4.6.12. Loss or Theft of the Device
  - 4.6.13. Identity Theft (Integrity)
  - 4.6.14. Weak or Broken Cryptography
  - 4.6.15. Denial of Service (DoS)

4.7. Main Attacks
- 4.7.1. Phishing Attacks
- 4.7.2. Attacks Related to Communication Modes
- 4.7.3. Smishing Attacks
- 4.7.4. Criptojacking Attacks
- 4.7.5. Man in The Middle

4.8. Hacking
- 4.8.1. Rooting and Jailbreaking
- 4.8.2. Anatomy of a Mobile Attack
    - 4.8.2.1. Threat Propagation
    - 4.8.2.2. Malware Installation on the Device
    - 4.8.2.3. Persistence
    - 4.8.2.4. Payload Execution and Information Extraction
- 4.8.3. Hacking on iOS Devices: Mechanisms and Tools
- 4.8.4. Hacking on Android Devices: Mechanisms and Tools

4.9. Penetration Testing
- 4.9.1. iOS PenTesting
- 4.9.2. Android PenTesting
- 4.9.3. Tools

4.10. Safety and Security
- 4.10.1. Security Configuration
    - 4.10.1.1. On iOS Devices
    - 4.10.1.2. On Android Devices
- 4.10.2. Safety Measures
- 4.10.3. Protection Tools

Module 5. IoT Security

5.1. Devices
- 5.1.1. Types of Devices
- 5.1.2. Standardized Architectures
    - 5.1.2.1. ONEM2M.
    - 5.1.2.2. IoTWF
- 5.1.3. Application Protocols
- 5.1.4. Connectivity Technologies

5.2. IoT Devices. Areas of Application
- 5.2.1. SmartHome
- 5.2.2. SmartCity
- 5.2.3. Transportation
- 5.2.4. Wearables
- 5.2.5. Health Sector
- 5.2.6. IioT

5.3. Communication Protocols
- 5.3.1. MQTT
- 5.3.2. LWM2M.
- 5.3.3. OMA-DM
- 5.3.4. TR-069.

5.4. SmartHome
- 5.4.1. Home Automation
- 5.4.2. Networks
- 5.4.3. Household Appliances
- 5.4.4. Surveillance and Security

5.5. SmartCity
- 5.5.1. Lighting
- 5.5.2. Meteorology

5.6. Transportation
- 5.6.1. Localization
- 5.6.2. Making Payments and Obtaining Services
- 5.6.3. Connectivity

5.7. Wearables
- 5.7.1. Smart Clothing
- 5.7.2. Smart Jewelry
- 5.7.3. Smart Watches

5.8. Health Sector
- 5.8.1. Exercise/Heart Rate Monitoring
- 5.8.2. Monitoring of Patients and Elderly People
- 5.8.3. Implantables
- 5.8.4. Surgical Robots

5.9. Connectivity
- 5.9.1. Wi-Fi/Gateway
- 5.9.2. Bluetooth
- 5.9.3. Built-in Connectivity

5.10. Securitization
- 5.10.1. Dedicated Networks
- 5.10.2. Password Managers
- 5.10.3. Use of Encrypted Protocols
- 5.10.4. Tips for Use

Module 6. Ethical Hacking

6.1. Work Environment
- 6.1.1. Linux Distributions
  - 6.1.1.1. Kali Linux - Offensive Security
  - 6.1.1.2. Parrot OS
  - 6.1.1.3. Ubuntu
- 6.1.2. Virtualization Systems
- 6.1.3. Sandbox
- 6.1.4. Deployment of Laboratories

6.2. Methods
- 6.2.1. OSSTM
- 6.2.2. OWASP
- 6.2.3. NIST
- 6.2.4. PTES
- 6.2.5. ISSAF

6.3. Footprinting
- 6.3.1. Open-Source Intelligence (OSINT)
- 6.3.2. Search for Data Breaches and Vulnerabilities
- 6.3.3. Use of Passive Tools

6.4. Network Scanning
- 6.4.1. Scanning Tools
  - 6.4.1.1. Nmap
  - 6.4.1.2. Hping3.
  - 6.4.1.3. Other Scanning Tools
- 6.4.2. Scanning Techniques
- 6.4.3. Firewalland IDS Evasion Techniques
- 6.4.4. Banner Grabbing
- 6.4.5. Network Diagrams

6.5. Enumeration
- 6.5.1. SMTP Enumeration
- 6.5.2. DNS Enumeration
- 6.5.3. NetBIOS and Samba Enumeration
- 6.5.4. LDAP Enumeration
- 6.5.5. SNMP Enumeration
- 6.5.6. Other Enumeration Techniques

6.6. Vulnerability Analysis
- 6.6.1. Vulnerability Scanning Solutions
  - 6.6.1.1. Qualys
  - 6.6.1.2. Nessus
  - 6.6.1.3. CFI LanGuard
- 6.6. 2 Vulnerability Scoring Systems
  - 6.6.2.1. CVSS
  - 6.6.2.2. CVE
  - 6.6.2.3. NVD

- 6.7. Attacks on Wireless Networks
    - 6.7.1. Methodology of Hacking in Wireless Networks
        - 6.7.1.1. Wi-Fi Discovery
        - 6.7.1.2. Traffic Analysis
        - 6.7.1.3. Aircrack Attacks
            - 6.7.1.3.1. WEP Attacks
            - 6.7.1.3.2. WPA/WPA2 Attacks
        - 6.7.1.4. Evil Twin Attacks
        - 6.7.1.5. Attacks on WPS
        - 6.7.1.6. Jamming
    - 6.7.2. Tools for Wireless Security
- 6.8. Hacking of Web Servers
    - 6.8.1. Cross Site Scripting
    - 6.8.2. CSRF
    - 6.8.3. Hijacking Session
    - 6.8.4. SQLinjection
- 6.9. Exploiting Vulnerabilities
    - 6.9.1. Use of Known Exploits
    - 6.9.2. Use of Metasploit
    - 6.9.3. Use of Malware
        - 6.9.3.1. Definition and Scope
        - 6.9.3.2. Malware Generation
        - 6.9.3.3. Bypass of Antivirus Solutions
- 6.10. Persistence
    - 6.10.1. Rootkits Installation
    - 6.10.2. Use of Ncat
    - 6.10.3. Use of Programmed Tasks for Backdoors
    - 6.10.4. User Creation
    - 6.10.5. HIDS Detection

Module 7. Inverse Engineering

7.1. Compilers
- 7.1.1. Types of Codes
- 7.1.2. Phases of a Compiler
- 7.1.3. Table of Symbols
- 7.1.4. Error Manager
- 7.1.5. GCC Compiler

7.2. Types of Analysis in Compilers
- 7.2.1. Lexical Analysis
  - 7.2.1.1. Terminology
  - 7.2.1.2. Lexical Components
  - 7.2.1.3. LEX Lexical Analyzer
- 7.2.2. Parsing
  - 7.2.2.1. Context-free Grammars
  - 7.2.2.2. Types of Parsing
    - 7.2.2.2.1. Top-down Analysis
    - 7.2.2.2.2. Bottom-up Analysis
  - 7.2.2.3. Syntactic Trees and Derivations
  - 7.2.2.4. Types of Parsers
    - 7.2.2.4.1. LR (Left To Right) Analyzers
    - 7.2.2.4.2. LALR Analyzers
- 7.2.3. Semantic Analysis
  - 7.2.3.1. Attribute Grammars
  - 7.2.3.2. S-Attributed
  - 7.2.3.3. L-Attributed

7.3. Data Structures in Assembler
- 7.3.1. Variables
- 7.3.2. Arrays
- 7.3.3. Pointers
- 7.3.4. Structures
- 7.3.5. Objects

7.4. Assembler Code Structures
- 7.4.1. Selection Structures
  - 7.4.1.1. If, else if, Else
  - 7.4.1.2. Switch
- 7.4.2. Iteration Structures
  - 7.4.2.1. For
  - 7.4.2.2. While
  - 7.4.2.3. Use of Break

7.5. X86 Architecture Hardware
- 7.5.1. x86 Processor Architecture
- 7.5.2. x86 Data Structures
- 7.5.3. x86 Code Structures
- 7.5.3. x86 Code Structures

7.6. ARM Hardware Architecture
- 7.6.1. ARM Processor Architecture
- 7.6.2. ARM Data Structures
- 7.6.3. ARM Code Structures

7.7. Static Code Analysis
- 7.7.1. Disassemblers
- 7.7.2. IDA
- 7.7.3. Code Rebuilders

7.8. Dynamic Code Analysis
- 7.8.1. Behavioral Analysis
  - 7.8.1.1. Monitoring
- 7.8.2. Linux Code Debuggers
- 7.8.3. Windows Code Debuggers

7.9. Sandbox
- 7.9.1. Sandbox Architecture
- 7.9.2. Sandbox Evasion
- 7.9.3. Detection Techniques
- 7.9.4. Avoidance Techniques
- 7.9.5. Countermeasures
- 7.9.6. Sandbox and Linux
- 7.9.7. Sandbox and Windows
- 7.9.8. Sandbox on MacOS
- 7.9.9. Sandbox on android

7.10. Malware Analysis
- 7.10.1. Malware Analysis Methods
- 7.10.2. Malware Obfuscation Techniques
  - 7.10.2.1. Executable Obfuscation
  - 7.10.2.2. Restriction of Execution Environments
- 7.10.3. Malware Analysis Tools

Module 8. Secure Development

8.1. Secure Development
- 8.1.1. Quality, Functionality and Safety
- 8.1.2. Confidentiality, Integrity and Availability
- 8.1.3. Software Development Life Cycle

8.2. Requirements Phase
- 8.2.1. Authentication Control
- 8.2.2. Role and Privilege Control
- 8.2.3. Risk-oriented Requirements
- 8.2.4. Privilege Approval

8.3. Analysis and Design Phases
- 8.3.1. Component Access and System Administration
- 8.3.2. Audit Trails
- 8.3.3. Session Management
- 8.3.4. Historical data
- 8.3.5. Proper Error Handling
- 8.3.6. Separation of Functions

8.4. Implementation and Coding Phase
- 8.4.1. Ensuring the Development Environment
- 8.4.2. Preparation of Technical Documentation
- 8.4.3. Secure Codification
- 8.4.4. Communications Security

8.5. Good Secure Coding Practices
- 8.5.1. Input Data Validation
- 8.5.2. Coding of Output Data
- 8.5.3. Programming Style
- 8.5.4. Change Log Management
- 8.5.5. Cryptographic Practices
- 8.5.6. Error and Log Management
- 8.5.7. File Management
- 8.5.8. Memory Memory
- 8.5.9. Standardization and Reuse of Security Functions

8.6. Server Preparation and Hardening
- 8.6.1. Management of Users, Groups and Roles on the Server
- 8.6.2. Software Installation
- 8.6.3. Server Hardening
- 8.6.4. Robust Configuration of the Application Environment

8.7. DB Preparation and Hardening
- 8.7.1. DB Engine Optimization
- 8.7.2. Create Your Own User for the Application
- 8.7.3. Assigning the Required Privileges to the User
- 8.7.4. Hardening of the Database

8.8. Testing Phase
- 8.8.1. Quality Control in Security Controls
- 8.8.2. Phased Code Inspection
- 8.8.3. Checking Configuration Management
- 8.8.4. Black Box Testing

8.9. Preparation of the Production Step
- 8.9.1. Perform Change Control
- 8.9.2. Carry out Production Changeover Procedure
- 8.9.3. Perform Rollback Procedure
- 8.9.4. Pre-production Testing

8.10. Maintenance Phase
- 8.10.1. Risk-based Assurance
- 8.10.2. White Box Security Maintenance Testing
- 8.10.3. Black box Safety Maintenance Tests

Module 9. Forensic Analysis

- 9.1. Data Acquisition and Duplication
  - 9.1.1. Volatile Data Acquisition
    - 9.1.1.1. System Information
    - 9.1.1.2. Network Information
    - 9.1.1.3. Volatility Order
  - 9.1.2. Static Data Acquisition
    - 9.1.2.1. Creating a Duplicate Image
    - 9.1.2.2. Preparation of a Chain of Custody Document
  - 9.1.3. Methods for Validation of Acquired Data
    - 9.1.3.1. Methods for Linux
    - 9.1.3.2. Methods for Windows
- 9.2. Evaluation and Defeat of Antiforensic Techniques
  - 9.2.1. Objectives of Antiforensic Techniques
  - 9.2.2. Data Deletion
    - 9.2.2.1. Deletion of Data and Files
    - 9.2.2.2. File Recovery
    - 9.2.2.3. Recovery of Deleted Partitions
  - 9.2.3. Password Protection
  - 9.2.4. Steganography
  - 9.2.5. Secure Device Wiping
  - 9.2.6. Encryption
- 9.3. Operating System Forensics
  - 9.3.1. Windows Forensics
  - 9.3.2. Linux Forensics
  - 9.3.3. Mac Forensics
- 9.4. Network Forensics
  - 9.4.1. Logs Analysis
  - 9.4.2. Data Correlation
  - 9.4.3. Network Research
  - 9.4.4. Steps to Follow in Network Forensic Analysis
- 9.5. Web Forensics
  - 9.5.1. Investigation of Web Attacks
  - 9.5.2. Attack Detection
  - 9.5.3. IP Address Location
- 9.6. Forensic Database Analysis
  - 9.6.1. Forensic Analysis in MSSQL
  - 9.6.2. MySQL Forensic Analysis
  - 9.6.3. PostgreSQL Forensic Analysis
  - 9.6.4. Forensic Analysis in MongoDB
- 9.7. Cloud Forensic Analysis
  - 9.7.1. Types of Crimes in the Cloud
    - 9.7.1.1. Cloud as Subject
    - 9.7.1.2. Cloud as an Object
    - 9.7.1.3. Cloud as a Tool
  - 9.7.2. Challenges of Cloud Forensics
  - 9.7.3. Research on Cloud Storage Services
  - 9.7.4. Forensic Analysis Tools for Cloud
- 9.8. Investigation of Email Crimes
  - 9.8.1. Mailing Systems
    - 9.8.1.1. Mail Clients
    - 9.8.1.2. Mail Server
    - 9.8.1.3. SMTP Server
    - 9.8.1.4. POP3 Server
    - 9.8.1.5. IMAP4 Server
  - 9.8.2. Mailing Crimes
  - 9.8.3. Mail Message
    - 9.8.3.1. Standard Headers
    - 9.8.3.2. Extended Headers
  - 9.8.4. Steps for the Investigation of these Crimes
  - 9.8.5. E-Mail Forensic Tools

9.9. Mobile Forensic Analysis
- 9.9.1. Cellular Networks
  - 9.9.1.1. Types of Networks
  - 9.9.1.2. CDR Contents
- 9.9.2. Subscriber Identity Module (SIM)
- 9.9.3. Logical Acquisition
- 9.9.4. Physical Acquisition
- 9.9.5. File System Acquisition

9.10. Forensic Report Writing and Reporting
- 9.10.1. Important Aspects of a Forensic Report
- 9.10.2. Classification and Types of Reports
- 9.10.3. Guide to Writing a Report
- 9.10.4. Presentation of the Report
  - 9.10.4.1. Prior Preparation for Testifying
  - 9.10.4.2. Deposition
  - 9.10.4.3. Dealing with the Media

Module 10. Current and Future Challenges in Information Security

10.1. Blockchain Technology
- 10.1.1. Scope of Application
- 10.1.2. Confidentiality Guarantee
- 10.1.3. Non-Repudiation Guarantee

10.2. Digital Money
- 10.2.1. Bitcoins
- 10.2.2. Cryptocurrencies
- 10.2.3. Cryptocurrency Mining
- 10.2.4. Pyramid Schemes
- 10.2.5. Other Potential Crimes and Problems

10.3. Deepfake
- 10.3.1. Media Impact
- 10.3.2. Dangers to Society
- 10.3.3. Detection Mechanisms

10.4. The Future of Artificial Intelligence
- 10.4.1. Artificial Intelligence and Cognitive Computing
- 10.4.2. Uses to Simplify Customer Service

10.5. Digital Privacy
- 10.5.1. Value of Data in the Network
- 10.5.2. Use of Data in the Network
- 10.5.3. Privacy and Digital Identity Management

10.6. Cyberconflicts, Cybercriminals and Cyberattacks
- 10.6.1. The Impact of Cybersecurity on International Conflicts
- 10.6.2. Consequences of Cyber-attacks on the General Population.
- 10.6.3. Types of Cybercriminals. Protective Measures

10.7. Telework
- 10.7.1. Remote Work Revolution during and post COVID-19
- 10.7.2. Access Bottlenecks
- 10.7.3. Variation of the Attacking Surface
- 10.7.4. Workers' Needs

10.8. Emerging Wireless Technologies
- 10.8.1. WPA3.
- 10.8.2. 5G.
- 10.8.3. Millimeter Waves
- 10.8.4. Trend of “Get Smart” instead of “Get More”

10.9. Future Addressing in Networks
- 10.9.1. Current Problems with IP Addressing
- 10.9.2. IPv6.
- 10.9.3. IPv4+
- 10.9.4. Advantages of IPv4+ Over IPv4
- 10.9.5. Advantages of IPv6 Over IPv4

10.10. The Challenge of Raising Awareness of Early and Continuing Education in the Population
- 10.10.1. Current Government Strategies
- 10.10.2. Resistance of the Population to Learning
- 10.10.3. Training Plans to be Adopted by Companies

Module 11. Leadership, Ethics and Social Responsibility in Companies

11.1. Globalization and Governance

11.1.1. Governance and Corporate Governance

11.1.2. The Fundamentals of Corporate Governance in Companies

11.1.3. The Role of the Board of Directors in the Corporate Governance Framework

11.2. Leadership

11.2.1. Leadership A Conceptual Approach

11.2.2. Leadership in Companies

11.2.3. The Importance of Leaders in Business Management

11.3. Cross Cultural Management

11.3.1. Cross Cultural Management Concept

11.3.2. Contributions to Knowledge of National Cultures

11.3.3. Diversity Management

11.4. Management and Leadership Development

11.4.1. Concept of Management Development

11.4.2. Concept of Leadership

11.4.3. Leadership Theories

11.4.4. Leadership Styles

11.4.5. Intelligence in Leadership

11.4.6. The Challenges of Today's Leader

11.5. Business Ethics

11.5.1. Ethics and Morality

11.5.2. Business Ethics

11.5.3. Leadership and Ethics in Companies

11.6. Sustainability

11.6.1. Sustainability and Sustainable Development

11.6.2. The 2030 Agenda

11.6.3. Sustainable Companies

11.7. Corporate Social Responsibility

11.7.1. International Dimensions of Corporate Social Responsibility

11.7.2. Implementing Corporate Social Responsibility

11.7.3. The Impact and Measurement of Corporate Social Responsibility

11.8. Responsible Management Systems and Tools

11.8.1. CSR: Corporate Social Responsibility

11.8.2. Essential Aspects for Implementing a Responsible Management Strategy

11.8.3. Steps for the Implementation of a Corporate Social Responsibility Management System

11.8.4. CSR Tools and Standards

11.9. Multinationals and Human Rights

11.9.1. Globalization, Multinational Companies and Human Rights

11.9.2. Multinational Corporations and International Law

11.9.3. Legal Instruments for Multinationals in the Area of Human Rights

11.10. Legal Environment and Corporate Governance

11.10.1. International Rules on Importation and Exportation

11.10.2. Intellectual and Industrial Property

11.10.3. International Labor Law

Module 12. People and Talent Management

12.1. Strategic People Management

12.1.1. Strategic Human Resources Management

12.1.2. Strategic People Management

12.2. Human Resources Management by Competencies

12.2.1. Analysis of the Potential

12.2.2. Remuneration Policy

12.2.3. Career/Succession Planning

12.3. Performance Evaluation and Performance Management

12.3.1. Performance Management

12.3.2. Performance Management: Objectives and Process

12.4. Innovation in Talent and People Management

12.4.1. Strategic Talent Management Models

12.4.2. Talent Identification, Training and Development

12.4.3. Loyalty and Retention

12.4.4. Proactivity and Innovation

- 12.5. Motivation
    - 12.5.1. The Nature of Motivation
    - 12.5.2. Expectations Theory
    - 12.5.3. Needs Theory
    - 12.5.4. Motivation and Financial Compensation
- 12.6. Developing High Performance Teams
    - 12.6.1. High-Performance Teams: Self-Managed Teams
    - 12.6.2. Methodologies for the Management of High Performance Self-Managed Teams
- 12.7. Change Management
    - 12.7.1. Change Management
    - 12.7.2. Type of Change Management Processes
    - 12.7.3. Stages or Phases in the Change Management Process
- 12.8. Negotiation and Conflict Management
    - 12.8.1. Negotiation
    - 12.8.2. Conflict Management
    - 12.8.3. Crisis Management
- 12.9. Executive Communication
    - 12.9.1. Internal and External Communication in the Corporate Environment
    - 12.9.2. Communication Departments
    - 12.9.3. The Person in Charge of Communication of the Company The Profile of the Dircom
- 12.10. Productivity, Attraction, Retention and Activation of Talent
    - 12.10.1. Productivity
    - 12.10.2. Talent Attraction and Retention Levers

Module 13. Economic and Financial Management

- 13.1. Economic Environment
    - 13.1.1. Macroeconomic Environment and the National Financial System
    - 13.1.2. Financial Institutions
    - 13.1.3. Financial Markets
    - 13.1.4. Financial Assets
    - 13.1.5. Other Financial Sector Entities
- 13.2. Executive Accounting
    - 13.2.1. Basic Concepts
    - 13.2.2. The Company's Assets
    - 13.2.3. The Company's Liabilities
    - 13.2.4. The Company's Net Worth
    - 13.2.5. The Income Statement
- 13.3. Information Systems and Business Intelligence
    - 13.3.1. Fundamentals and Classification
    - 13.3.2. Cost Allocation Phases and Methods
    - 13.3.3. Choice of Cost Center and Impact
- 13.4. Budget and Management Control
    - 13.4.1. The Budget Model
    - 13.4.2. The Capital Budget
    - 13.4.3. The Operating Budget
    - 13.4.5. Treasury Budget
    - 13.4.6. Budget Monitoring
- 13.5. Financial Management
    - 13.5.1. The Company's Financial Decisions
    - 13.5.2. Financial Department
    - 13.5.3. Cash Surpluses
    - 13.5.4. Risks Associated with Financial Management
    - 13.5.5. Financial Administration Risk Management

13.6. Financial Planning
- 13.6.1. Definition of Financial Planning
- 13.6.2. Actions to be Taken in Financial Planning
- 13.6.3. Creation and Establishment of the Business Strategy
- 13.6.4. The Cash Flow Table
- 13.6.5. The Working Capital Table

13.7. Corporate Financial Strategy
- 13.7.1. Corporate Strategy and Sources of Financing
- 13.7.2. Financial Products for Corporate Financing

13.8. Strategic Financing
- 13.8.1. Self-Financing
- 13.8.2. Increase in Equity
- 13.8.3. Hybrid Resources
- 13.8.4. Financing Through Intermediaries

13.9. Financial Analysis and Planning
- 13.9.1. Analysis of the Balance Sheet
- 13.9.2. Analysis of the Income Statement
- 13.9.3. Profitability Analysis

13.10. Analyzing and Solving Cases/Problems
- 13.10.1. Financial Information on Industria de Diseño y Textil, S.A. (INDITEX)

Module 14. Commercial and Strategic Marketing Management

14.1. Commercial Management
- 14.1.1. Conceptual Framework of Commercial Management
- 14.1.2. Business Strategy and Planning
- 14.1.3. The Role of Sales Managers

14.2. Marketing
- 14.2.1. The Concept of Marketing
- 14.2.2. Basic Elements of Marketing
- 14.2.3. Marketing Activities of the Company

14.3. Strategic Marketing Management
- 14.3.1. The Concept of Strategic Marketing
- 14.3.2. Concept of Strategic Marketing Planning
- 14.3.3. Stages in the Process of Strategic Marketing Planning

14.4. Digital Marketing and e-Commerce
- 14.4.1. Digital Marketing and E-commerce Objectives
- 14.4.2. Digital Marketing and Media Used
- 14.4.3. E-Commerce General Context
- 14.4.4. Categories of E-commerce
- 14.4.5. Advantages and Disadvantages of E-commerce Versus Traditional Commerce

14.5. Digital Marketing to Reinforce a Brand
- 14.5.1. Online Strategies to Improve Your Brand's Reputation
- 14.5.2. Branded Content and Storytelling

14.6. Digital Marketing to Attract and Retain Customers
- 14.6.1. Loyalty and Engagement Strategies through the Internet
- 14.6.2. Visitor Relationship Management
- 14.6.3. Hypersegmentation

14.7. Managing Digital Campaigns
- 14.7.1. What is a Digital Advertising Campaign?
- 14.7.2. Steps to Launch an Online Marketing Campaign
- 14.7.3. Mistakes in Digital Advertising Campaigns

14.8. Sales Strategy
- 14.8.1. Sales Strategy
- 14.8.2. Sales Methods

14.9. Corporate Communication
- 14.9.1. Concept
- 14.9.2. The Importance of Communication in the Organization
- 14.9.3. Type of Communication in the Organization
- 14.9.4. Functions of Communication in the Organization
- 14.9.5. Elements of Communication
- 14.9.6. Communication Problems
- 14.9.7. Communication Scenarios

14.10. Digital Communication and Reputation
- 14.10.1. Online Reputation
- 14.10.2. How to Measure Digital Reputation?
- 14.10.3. Online Reputation Tools
- 14.10.4. Online Reputation Report
- 14.10.5. Online Branding

Module 15. Executive Management

15.1. General Management
- 15.1.1. The Concept of General Management
- 15.1.2. The Role of the CEO
- 15.1.3. The CEO and their Responsibilities
- 15.1.4. Transforming the Work of Management

15.2. Manager Functions: Organizational Culture and Approaches
- 15.2.1. Manager Functions: Organizational Culture and Approaches

15.3. Operations Management
- 15.3.1. The Importance of Management
- 15.3.2. Value Chain
- 15.3.3. Quality Management

15.4. Public Speaking and Spokesperson Education
- 15.4.1. Interpersonal Communication
- 15.4.2. Communication Skills and Influence
- 15.4.3. Communication Barriers

15.5. Personal and Organizational Communications Tools
- 15.5.1. Interpersonal Communication
- 15.5.2. Interpersonal Communication Tools
- 15.5.3. Communication in the Organization
- 15.5.4. Tools in the Organization

15.6. Communication in Crisis Situations
- 15.6.1. Crisis
- 15.6.2. Phases of the Crisis
- 15.6.3. Messages: Contents and Moments

15.7. Preparation of a Crisis Plan
- 15.7.1. Analysis of Possible Problems
- 15.7.2. Planning
- 15.7.3. Adequacy of Personnel

15.8. Emotional Intelligence
- 15.8.1. Emotional Intelligence and Communication
- 15.8.2. Assertiveness, Empathy, and Active Listening
- 15.8.3. Self-Esteem and Emotional Communication

15.9. Personal Branding
- 15.9.1. Strategies for Personal Brand Development
- 15.9.2. Personal Branding Laws
- 15.9.3. Tools for Creating Personal Brands

15.10. Leadership and Team Management
- 15.10.1. Leadership and Leadership Styles
- 15.10.2. Leader Capabilities and Challenges
- 15.10.3. Managing Change Processes
- 15.10.4. Managing Multicultural Teams

> *Your future starts here. Enroll today and become the Chief Information Officer of large companies"*

06
Methodology

This academic program offers students a different way of learning. Our methodology uses a cyclical learning approach: **Relearning.**
This teaching system is used, for example, in the most prestigious medical schools in the world, and major publications such as the **New England Journal of Medicine** have considered it to be one of the most effective.

Discover Relearning, a system that abandons conventional linear learning, to take you through cyclical teaching systems: a way of learning that has proven to be extremely effective, especially in subjects that require memorization"

Case Study to contextualize all content

Our program offers a revolutionary approach to developing skills and knowledge. Our goal is to strengthen skills in a changing, competitive, and highly demanding environment.

> *At TECH, you will experience a learning methodology that is shaking the foundations of traditional universities around the world"*

You will have access to a learning system based on repetition, with natural and progressive teaching throughout the entire syllabus.

The student will learn to solve complex situations in real business environments through collaborative activities and real cases.

A learning method that is different and innovative

This TECH program is an intensive educational program, created from scratch, which presents the most demanding challenges and decisions in this field, both nationally and internationally. This methodology promotes personal and professional growth, representing a significant step towards success. The case method, a technique that lays the foundation for this content, ensures that the most current economic, social and professional reality is taken into account.

> *Our program prepares you to face new challenges in uncertain environments and achieve success in your career"*

The case method has been the most widely used learning system among the world's leading Information Technology schools for as long as they have existed. The case method was developed in 1912 so that law students would not only learn the law based on theoretical content. It consisted of presenting students with real-life, complex situations for them to make informed decisions and value judgments on how to resolve them. In 1924, Harvard adopted it as a standard teaching method.

What should a professional do in a given situation? This is the question that you are presented with in the case method, an action-oriented learning method. Throughout the course, students will be presented with multiple real cases. They will have to combine all their knowledge and research, and argue and defend their ideas and decisions.

Relearning Methodology

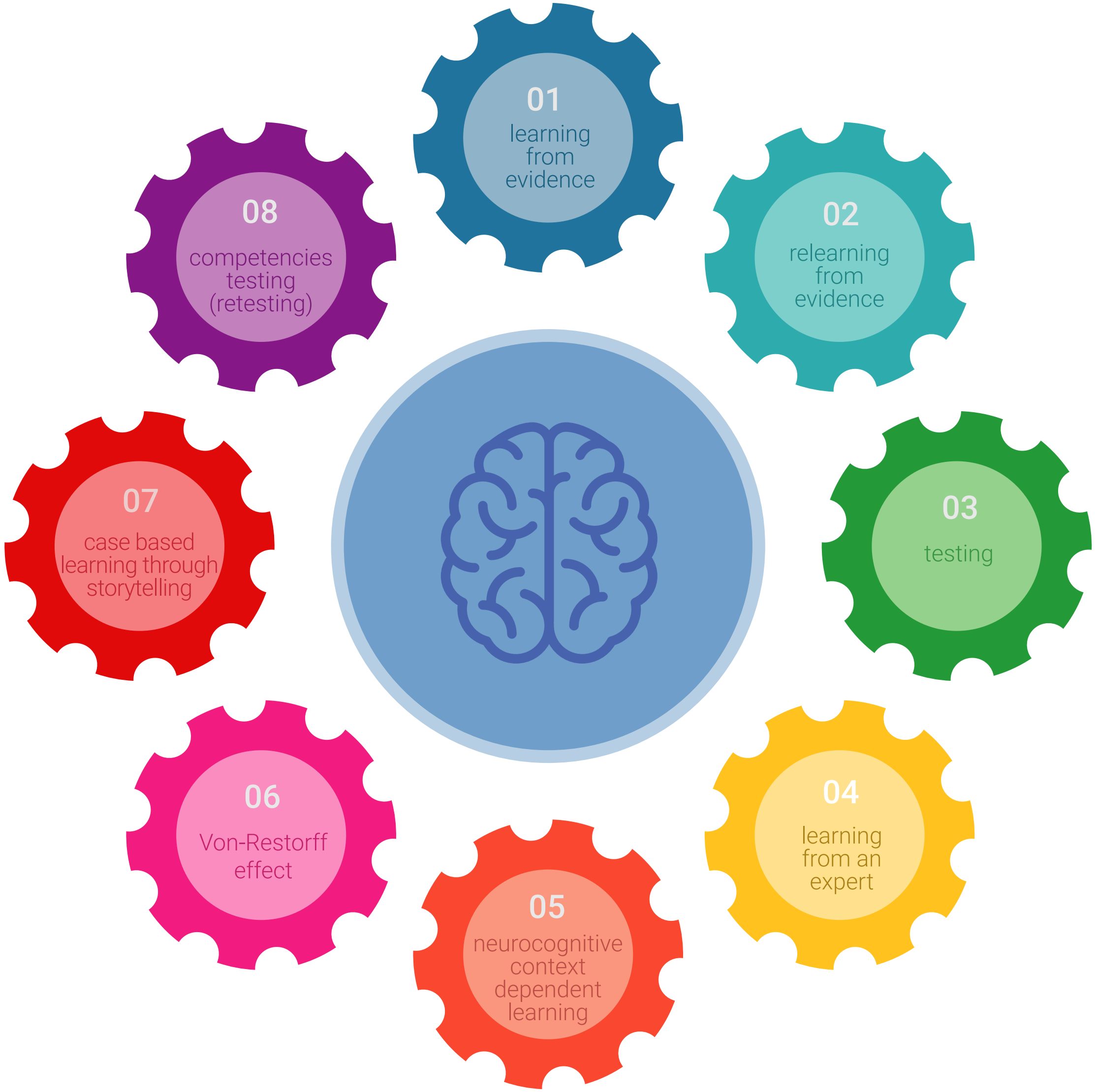
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

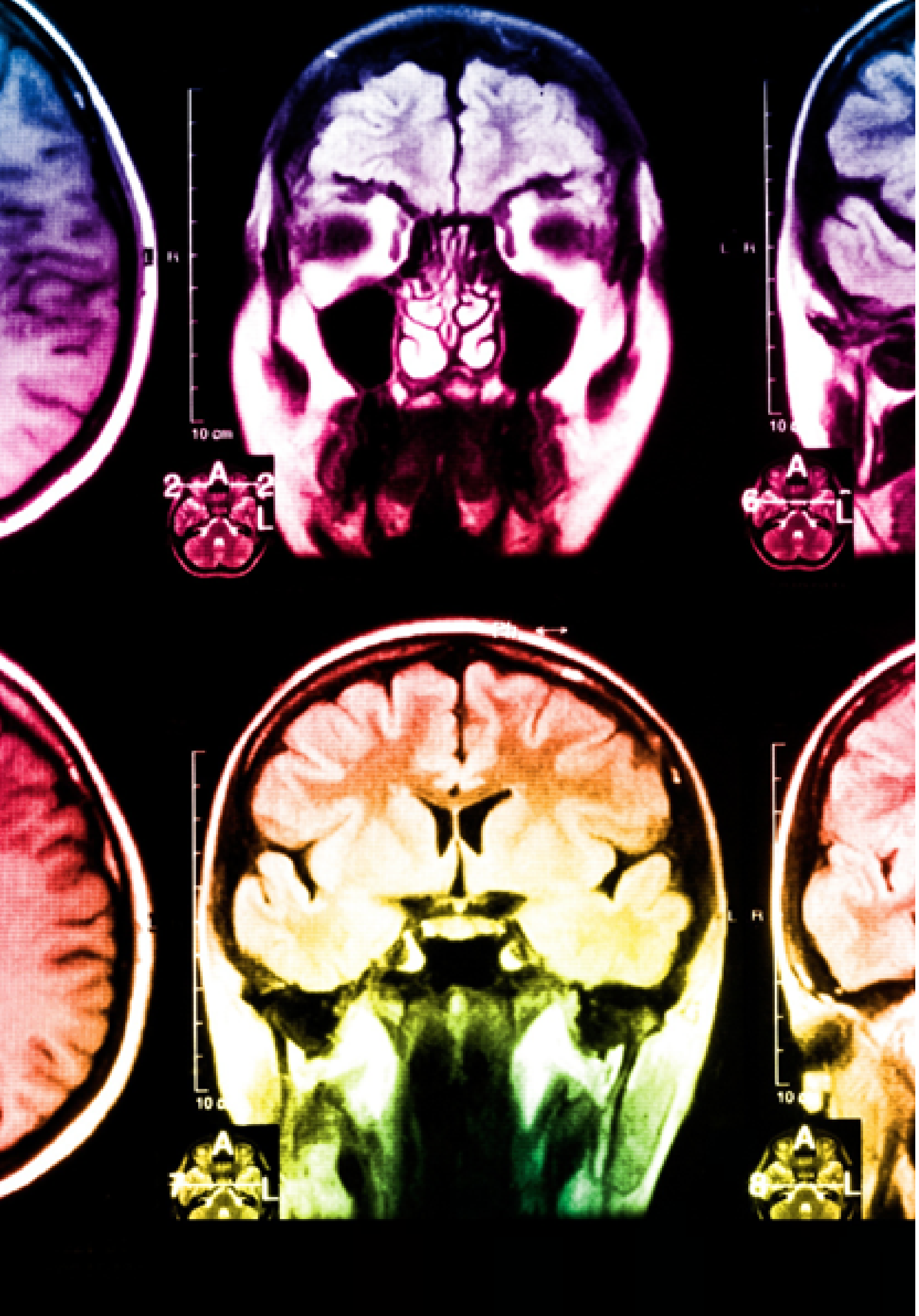
We enhance the Case Study with the best 100% online teaching method: Relearning.

In 2019, we obtained the best learning results of all online universities in the world.

At TECH you will learn using a cutting-edge methodology designed to train the executives of the future. This method, at the forefront of international teaching, is called Relearning.

Our university is the only one in the world authorized to employ this successful method. In 2019, we managed to improve our students' overall satisfaction levels (teaching quality, quality of materials, course structure, objectives...) based on the best online university indicators.


01
learning from evidence
02
relearning from evidence
03
testing
04
learning from an expert
05
neurocognitive context dependent learning
06
Von-Restorff effect
07
case based learning through storytelling
08
competencies testing (retesting)



In our program, learning is not a linear process, but rather a spiral (learn, unlearn, forget, and re-learn). Therefore, we combine each of these elements concentrically. This methodology has trained more than 650,000 university graduates with unprecedented success in fields as diverse as biochemistry, genetics, surgery, international law, management skills, sports science, philosophy, law, engineering, journalism, history, and financial markets and instruments. All this in a highly demanding environment, where the students have a strong socio-economic profile and an average age of 43.5 years.

Relearning will allow you to learn with less effort and better performance, involving you more in your training, developing a critical mindset, defending arguments, and contrasting opinions: a direct equation for success.

From the latest scientific evidence in the field of neuroscience, not only do we know how to organize information, ideas, images and memories, but we know that the place and context where we have learned something is fundamental for us to be able to remember it and store it in the hippocampus, to retain it in our long-term memory.

In this way, and in what is called neurocognitive context-dependent e-learning, the different elements in our program are connected to the context where the individual carries out their professional activity.

This program offers the best educational material, prepared with professionals in mind:

Study Material

All teaching material is produced by the specialists who teach the course, specifically for the course, so that the teaching content is highly specific and precise.

These contents are then applied to the audiovisual format, to create the TECH online working method. All this, with the latest techniques that offer high quality pieces in each and every one of the materials that are made available to the student.

Classes

There is scientific evidence suggesting that observing third-party experts can be useful.

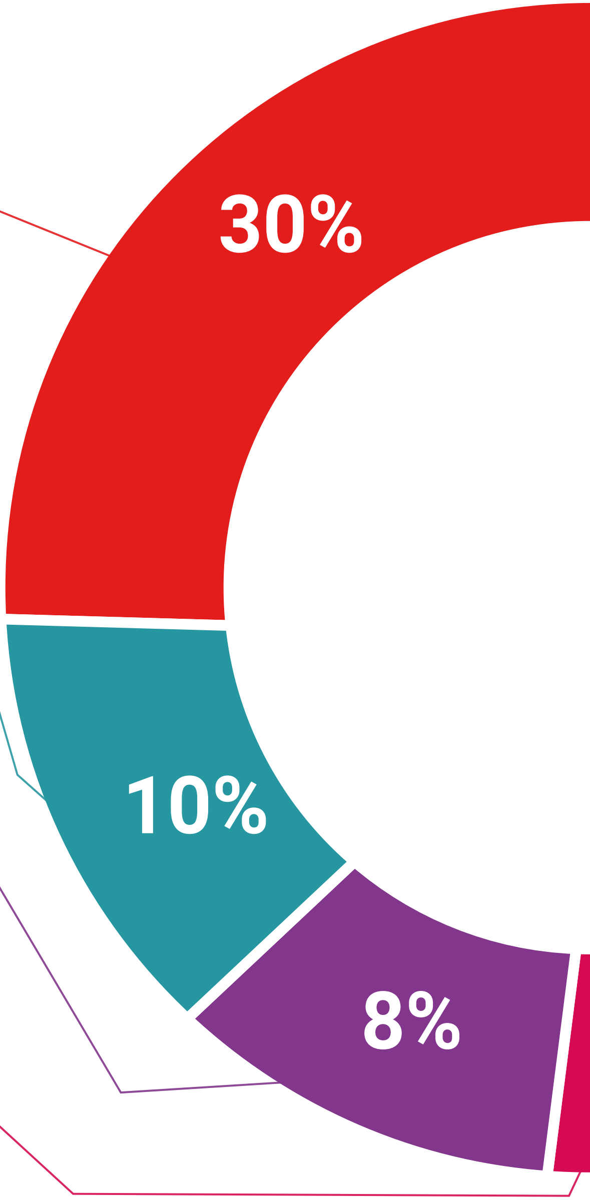
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

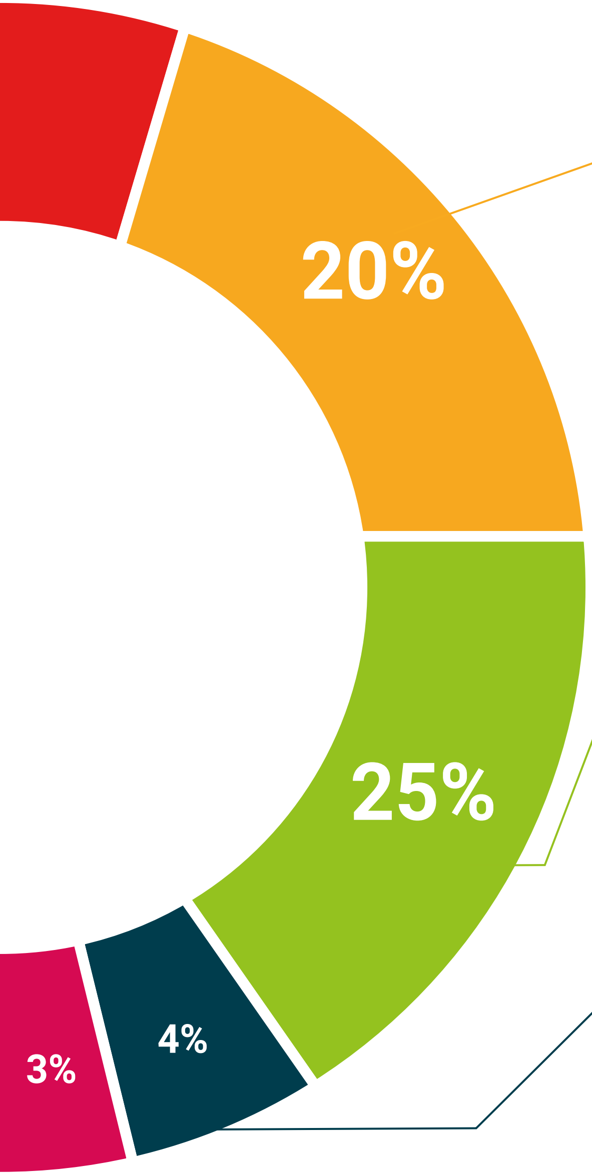
Practising Skills and Abilities

They will carry out activities to develop specific skills and abilities in each subject area. Exercises and activities to acquire and develop the skills and abilities that a specialist needs to develop in the context of the globalization that we are experiencing.

Additional Reading

Recent articles, consensus documents and international guidelines, among others. In TECH's virtual library, students will have access to everything they need to complete their course.





Case Studies

Students will complete a selection of the best case studies chosen specifically for this program. Cases that are presented, analyzed, and supervised by the best specialists in the world.

Interactive Summaries

The TECH team presents the contents attractively and dynamically in multimedia lessons that include audio, videos, images, diagrams, and concept maps in order to reinforce knowledge.

This exclusive educational system for presenting multimedia content was awarded by Microsoft as a "European Success Story".

Testing & Retesting

We periodically evaluate and re-evaluate students' knowledge throughout the program, through assessment and self-assessment activities and exercises, so that they can see how they are achieving their goals.

07

Certificate

The MBA in Cybersecurity Management (CISO, Chief Information Security Officer) guarantees, in addition to the most rigorous and up-to-date education, access to a Professional Master's Degree issued by TECH Technological University.

> Successfully complete this program and receive your university qualification without having to travel or fill out laborious paperwork"

This **MBA in Cybersecurity Management (CISO, Chief Information Security Officer)** contains the most complete and up-to-dated program on the market.

After the student has passed the assessments, they will receive their corresponding **Professional Master's Degree** issued by **TECH Technological University** via tracked delivery*.

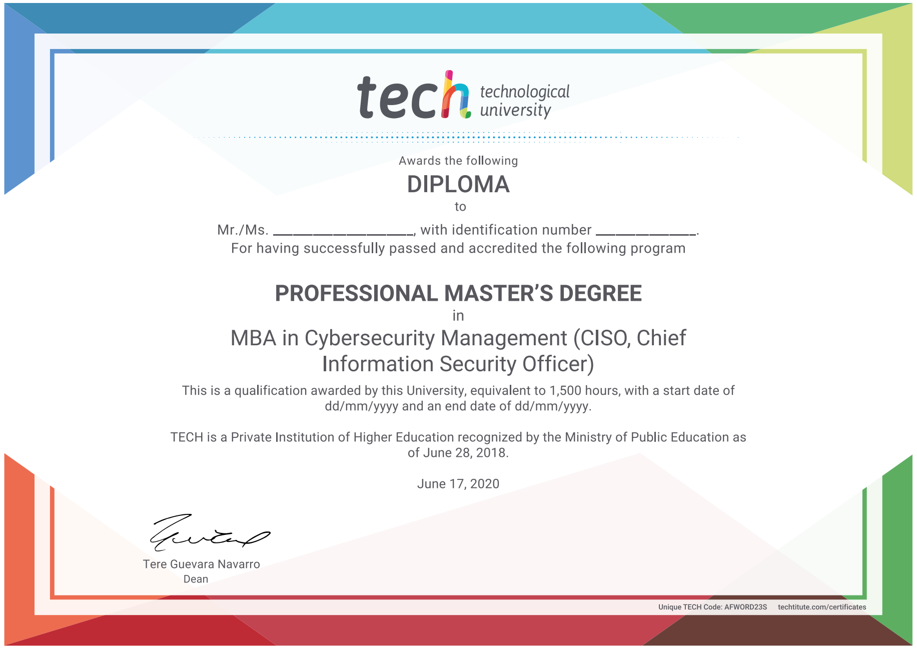
The diploma issued by **TECH Technological University** will reflect the qualification obtained in the Professional Master's Degree, and meets the requirements commonly demanded by labor exchanges, competitive examinations, and professional career evaluation committees.

Title: **Professional Master's Degree MBA in Cybersecurity Management (CISO, Chief Information Security Officer)**

Official Nº of hours: **1,500 h.**

Modality: **online**

Duration: **12 months**



tech technological university

Awards the following

DIPLOMA

to

Mr./Ms. _________________, with identification number ____________.
For having successfully passed and accredited the following program

PROFESSIONAL MASTER'S DEGREE

in

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

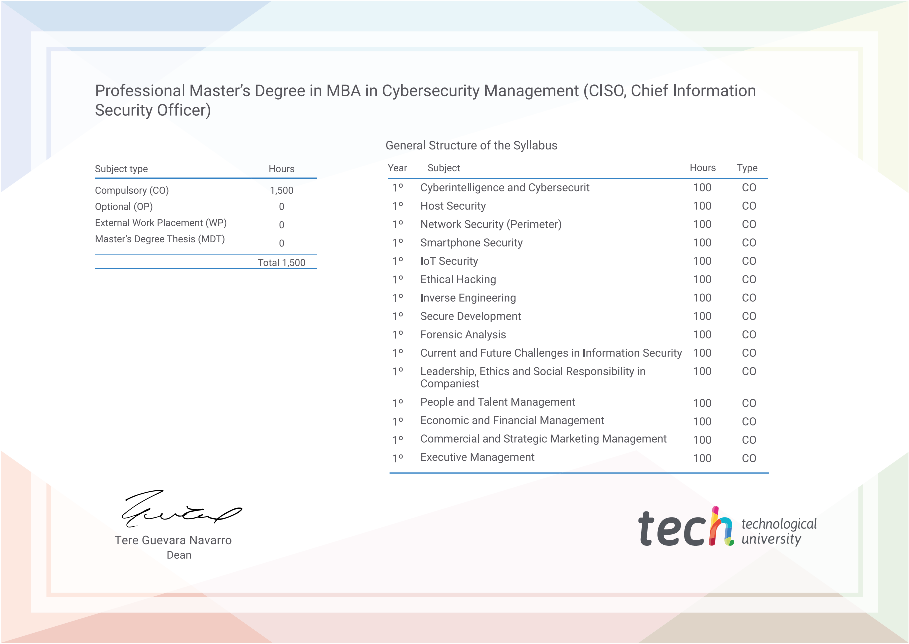
This is a qualification awarded by this University, equivalent to 1,500 hours, with a start date of dd/mm/yyyy and an end date of dd/mm/yyyy.

TECH is a Private Institution of Higher Education recognized by the Ministry of Public Education as of June 28, 2018.

June 17, 2020

Tere Guevara Navarro
Dean

Unique TECH Code: AFWORD23S techtitute.com/certificates



Professional Master's Degree in MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

Subject type	Hours
Compulsory (CO)	1,500
Optional (OP)	0
External Work Placement (WP)	0
Master's Degree Thesis (MDT)	0
	Total 1,500

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	Cyberintelligence and Cybersecurit	100	CO
1º	Host Security	100	CO
1º	Network Security (Perimeter)	100	CO
1º	Smartphone Security	100	CO
1º	IoT Security	100	CO
1º	Ethical Hacking	100	CO
1º	Inverse Engineering	100	CO
1º	Secure Development	100	CO
1º	Forensic Analysis	100	CO
1º	Current and Future Challenges in Information Security	100	CO
1º	Leadership, Ethics and Social Responsibility in Companiest	100	CO
1º	People and Talent Management	100	CO
1º	Economic and Financial Management	100	CO
1º	Commercial and Strategic Marketing Management	100	CO
1º	Executive Management	100	CO

Tere Guevara Navarro
Dean

tech technological university

*Apostille Convention. In the event that the student wishes to have their paper diploma issued with an apostille, TECH EDUCATION will make the necessary arrangements to obtain it, at an additional cost.

Professional Master's Degree
MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

- Modality: **online**
- Duration: **12 months**
- Certificate: **TECH Technological University**
- Schedule: **at your own pace**
- Exams: **online**

Professional Master's Degree

MBA in Cybersecurity Management (CISO, Chief Information Security Officer)

tech technological university