Advanced Master's Degree
Senior Cybersecurity Management

tech technological university

Advanced Master's Degree
Senior Cybersecurity Management

- Modality: **online**
- Duration: **2 years**
- Certificate: **TECH Technological University**
- Dedication: **16h/week**
- Schedule: **at your own pace**
- Exams: **online**

Website: www.techtitute.com/in/information-technology/advanced-master-degree/advanced-master-degree-senior-cybersecurity-management

Index

01 Introduction p. 4

02 Objectives p. 8

03 Skills p. 16

04 Course Management p. 20

05 Structure and Content p. 28

06 Methodology p. 48

07 Certificate p. 56

01
Introduction

In today's world, cybersecurity is a fundamental element for individuals and companies, which are more exposed than ever to attacks. This is due to the continuous development of new technologies and the digitalization process, which has brought about transformations in all types of companies, streamlining numerous activities but also leading to the emergence of new vulnerabilities. For this reason, one of the most sought-after profiles today is that of the cybersecurity manager, a booming figure with numerous career opportunities. This program explores this figure in depth, and prepares the computer scientist to effectively and comprehensively address all the current challenges in this field, where management skills and a business perspective are also required. In addition, the program is developed in a 100% online format, making it perfect for combining it with work, allowing the professional to study whenever they wish.

This program will prepare you to meet all the challenges of the present and future in the field of cybersecurity, allowing you to specialize in leadership in this important area of IT"

Banking processes, online shopping, internal communications in different organizations, administrative procedures.. Nowadays, digitalization has transformed the way individuals and companies operate on a daily basis. It has streamlined numerous activities and has made it unnecessary to make certain trips, improving the quality of life of the population and saving costs for companies. However, these advantages have brought, collaterally, other disadvantages in terms of cybersecurity.

Many of the digital technologies and tools currently in use are under continuous development and are therefore open to attack. As the use of digital applications and devices has become widespread, a failure in them is critical, as it can affect the development of the organization, not only in terms of marketing and sales, but in its own internal functioning, which also depends on these utilities.

For this reason, companies need cybersecurity experts who can respond to the different problems that may arise in this area. One of the most sought-after profiles is that of Cybersecurity Manager, a position that entails a global vision of this field, and for which this Advanced Master's Degree fully prepares you. Therefore, this program is a great opportunity for the computer scientist, since it will bring them closer to all the novelties in this field, preparing them, at the same time, to face managerial decisions, which require the best knowledge and leadership skills.

All this, based on an online learning methodology that will be adapted to the professional circumstances of the student, while being accompanied by a teaching staff of great prestige in this area of computer science. You will also have at your disposal the best educational technology and the latest teaching resources: interactive summaries, videos, master classes, case analysis or complementary readings.

This **Advanced Master's Degree in Senior Cybersecurity Management** contains the most complete and up-to-date program on the market. The most important features include:

- The development of practical cases presented by experts in computer science and cybersecurity
- The graphic, schematic, and practical contents with which they are created, provide scientific and practical information on the disciplines that are essential for professional practice
- Practical exercises where the self-assessment process can be carried out to improve learning
- Special emphasis on innovative methodologies in cybersecurity management
- Theoretical lessons, questions to the expert, debate forums on controversial topics, and individual reflection assignments
- The availability of access to content from any fixed or portable device with an Internet connection

With this Advanced Master's Degree you will be able to delve into IoT security, cloud computing, blockchain and learn how to perform high-level audits for all types of companies and organizations"

Cybersecurity management is a booming professional profile and this program offers you the option, based on TECH's online methodology, to access the best opportunities in this field"

You will enjoy the support of a prestigious teaching staff, who will ensure that you learn all the necessary skills in the field of cybersecurity management.

You will have at your disposal the latest teaching resources to guarantee a fast and efficient learning process.

The teaching staff includes professionals from the cybersecurity sector, who bring their experience to this educational program, as well as 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 an immersive learning experience designed to prepare for real-life situations.

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

02

Objectives

The main objective of this Advanced Master's Degree is to turn the computer scientist into a great specialist in this field, allowing them to access the best professional opportunities. And, to this end, it will not only abound in all the latest developments in the field of cybersecurity, but will provide you with the best tools to get a global perspective of the business needs in this area. Therefore, you will be able to work managing the security of companies at all times, knowing the best methods to proceed in each case.

This Advanced Master's Degree will help you achieve the career advancement you are looking for, thanks to its comprehensive and up-to-date content, and its prestigious faculty composed of active cybersecurity experts"

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 detection and prevention systems for the most relevant threats
- 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
- Examining the risks of new emerging technologies
- Compile the different technologies in relation to computer security
- Generate specialized knowledge about an information system, types and security aspects that must be taken into account
- Identify the vulnerabilities of an information system
- Develop legal regulations and the criminalization of crime attacking on an information system
- Evaluate the different models of security architecture to establish the most suitable model for the organization
- Identify the regulatory frameworks of application and their regulatory bases
- Analyze the organizational and functional structure of an information security area (the CISO's office)
- Analyze and develop the concept of risk and uncertainty within the environment
- In which we live
- Examine the Risk Management Model based on ISO 31.000
- Examine the science of cryptology and the relationship to its branches: cryptography, cryptanalysis, steganography and stegoanalysis
- Analyze the types of cryptography according to the type of algorithm and according to its use
- Examine digital certificates
- Examining the Public Key Infrastructure (PKI)
- Develop the concept of identity management
- Identify authentication methods
- Generate specialized knowledge about the IT security ecosystem
- Assessing knowledge in terms of cybersecurity
- Identify the areas of cloudsecurity
- Analyze the services and tools in each of the security areas
- Develop the security specifications of each LPWAN technology
- Analyze comparatively the security of LPWAN technologies

Specific Objectives

- 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
- Establishing 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
- 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
- Analyze current network architectures to identify the perimeter we need 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 network functionalities in *cloud* environments
- Determine the tools for network protection and demonstrate why they are fundamental to a multilayer defence
- Examine the various attack vectors to avoid becoming an easy target
- Determine the main attacks and types of malware to which users of mobile devices are exposed
- Analyze the latest devices to establish greater security
- In the configuration
- Specify the main steps to perform a penetration test on
- both iOS and Android platforms
- Develop specialized knowledge about different protection and security tools
- Establish best practices in programming for mobile devices
- Analyze the main IoT architectures
- Examine connectivity technologies
- Develop the main application protocols
- Specify the different types of existing devices
- Assessing risk levels and known vulnerabilities
- Develop safe use policies
- Establishing appropriate conditions of use for these devices
- 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

- Concretize the various methodologies of hacking
- 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 malware analysis oriented tools
- Establish the necessary requirements for the correct operation of
- an application in a secure manner
- ExamineLog files to understand error messages
- Analyze the different events and decide what to show to the user and what to keep 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
- Identify the different elements that evidence a crime
- Generate specialized knowledge to obtain data from different media before they are 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 defend the report before the competent authority
- Specify strategies for safe teleworking
- Know the main syntax of graphic language and apply its rules to clearly and precisely describe objects and ideas
- Know the origin of letters and their historical importance
- Recognize, study and apply typography to graphic processes in a coherent way
- Know and apply the fundamental aesthetics of typography
- Know how to analyze the layout of texts in the design object
- Be able to carry out professional work starting from typesetting
- Assess the security of an information system in all its components and layers
- Identify current security threat types and trends
- Establish security guidelines by defining security policies and contingency plans
- Analyze strategies and tools to ensure the integrity and security of information systems
- Apply specific techniques and tools for each type of attack or security vulnerability
- Protect sensitive information stored in the information system
- Have the legal framework and typification of the crime, completing the vision with the typification of the offender and his victim
- Align the Safety Master Plan with the organization's strategic objectives
- Establish a continuous risk management framework as an integral part of the Master Security Plan
- Determine appropriate indicators for monitoring ISMS implementation
- Establish a policy-based security strategy
- Analyze the objectives and procedures associated with
- the employee, supplier, and partner awareness plan
- Identify, within the regulatory framework, the regulations, certifications and laws applicable to each organization
- Develop the fundamental elements required by the ISO 27001:2013 standard
- Implement a privacy management model in line with the European regulation GDPR
- Identify the different structures that an information security area can have
- Develop a security model based on three lines of defense
- Present the different periodic and extraordinary committees in which the cybersecurity area is involved
- Specify the technological tools that support the main functions of the security operations team (SOC)
- Evaluate vulnerability control measures appropriate to each scenario
- Develop the security operations framework based on the NIST CSF
- Specify the scope of the different types of audits (Red Team, Pentesting, Bug Bounty, etc.)
- Propose the activities to be carried out after a security incident
- Set up an information security command center encompassing
- all relevant actors (authorities, customers, suppliers, etc.)
- Examine, with a holistic view, the environment in which we operate
- Identify the main risks and opportunities that may affect the achievement of our objectives
- Analyze the risks based on the best practices at our disposal
- Evaluate the potential impact of these risks and opportunities
- Develop techniques that will enable us to address risks and opportunities in a way that

maximizes our value contribution

- Examine in depth the different risk transfer and valuation techniques
- Generate value from the design of proprietary models for agile risk management
- Examine the results to propose continuous improvements in project and process management based on *risk-driven* management models
- Innovate and transform general data into relevant information for risk-based decision-making
- Compile the fundamental operations (XOR, large numbers, substitution, and transposition) and the various components (One-Way functions, Hash, random number generators)
- Analyze cryptographic techniques
- Develop the different cryptographic algorithms
- Demonstrate the use of digital signatures and their application in digital certificates
- Assess key management systems and the importance of cryptographic key lengths
- Examine key derivation algorithms
- Analyze key life cycle
- Evaluate block cipher and stream cipher modes
- Determine pseudorandom number generators
- Develop real-world cryptography application cases, such as Kerberos, PGP or smart cards
- Examine related associations and organizations, such as ISO, NIST or NCSC
- Determine the challenges in quantum computing cryptography
- Develop the concept of digital identity
- Evaluating physical access control to information
- Fundamentals of biometric authentication and MFA authentication
- Evaluate attacks related to information confidentiality
- Analyze identity federation
- Establish network access control
- Develop expertise in physical and logical security
- Demonstrate knowledge of communications and networks
- Identify major malicious attacks
- Establish a secure development framework
- Demonstrate knowledge of the main regulations for information security management systems
- Demonstrate the operation of a cybersecurity operations center
- Demonstrate the importance of having cybersecurity practices for organizational disasters
- Identify risks of a public *cloud* infrastructure deployment
- Define security requirements
- Developing a security plan for a *cloud* deployment
- Identify the *cloud* services to be deployed for the execution of a security plan
- Determine the operations necessary for the prevention mechanisms

- Establish guidelines for a *logging* and monitoring system
- Propose incident response actions
- Introduce the simplified IoT architecture
- Explain the differences between generalist connectivity technologies and connectivity technologies for the IoT
- Establish the concept of the iron triangle of IoT connectivity
- Analyze the security specifications of LoRaWAN technology, NB-IoT technology and WiSUN technology
- Justify the choice of the appropriate IoT technology for each project
- Present the key elements of each phase and Analyze the characteristics
- of the Business Continuity Plan (BCP)
- Justify the need for a Business Continuity Plan
- Determine the success and risk maps for each phase of the Business Continuity Plan
- Specify how to establish an Action Plan for implementation
- Evaluating the completeness of a Business Continuity Plan (BCP)
- Successfully develop the Implementation Plan for a Business Continuity Plan
- for our Business

“

One more step in your career ascybersecurity specialist thanks to this Grand Master, with which you will acquireeverything you need to adapt to the current complex situation of computing”

03
Skills

Throughout this Advanced Master's Degree, the professional will acquire a series of tools and skills that will enable them to work in the cybersecurity management of a large company. For that reason, this program does not only focus on IT aspects, but pays attention to the digitization process, emerging technologies, and how these elements have affected the common and daily activities of organizations. In this way, the graduate student will have been able to adapt to the current context, knowing the best security solutions for each company.

Improve your skills to become the top cybersecurity specialist in your environment"

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
- Apply the most appropriate security measures depending on the threats
- Determine the security policy and plan for a company's information system, completing the design and implementation of the Contingency Plan
- Establish an audit program that meets the organization's cybersecurity self-assessment needs
- Develop a vulnerability scanning and monitoring program and a cybersecurity incident response plan
- Maximize the opportunities presented and eliminate exposure to all
- potential risks from the design itself
- Compile key management systems
- Evaluate a company's information security
- Analyze information access systems
- Develop best practices in secure development
- Present the risks involved for companies in not having a secure IT environment

"This program will take you into the future of cybersecurity"

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) and current cybersecurity regulations
- Understand the importance of devising a multi-layered defense, also known as "Defense in Depth", covering all aspects of a corporate network where some of the concepts and systems we will see 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 defence techniques available
- Analyze the role of the Cybersecurity Management Analyst (Chief Information Security Officer)
- Know how social engineering works and its methods
- Develop an Information Security Management System (ISMS)
- Identify the key elements that make up an ISMS
- Apply the MAGERIT methodology to evolve the model and take it a step further
- Design new risk management methodologies based on the agile risk management
- Identify, analyze, evaluate and treat the risks faced by the professional from a new business perspective based on a risk-driven model that allows not only to survive in its own environment, but also to boost the contribution of its own value
- Examine the process of designing a security strategy when deploying corporate cloudservices
- Assess the differences in the concrete implementations of different public *cloud* vendors
- Evaluate IoT connectivity options to address a project, with special emphasis on LPWAN technologies
- Present the basic specifications of the main LPWAN technologies for the IoT

04

Course Management

TECH has put together the most up-to-date information in the field of information systems management so that computer scientists can find, in a single program, the necessary teaching support to improve their qualifications and become a successful chief information officer. Undoubtedly, an Advanced Master's Degree that will mark a before and after in their specialization and will give them the opportunity to increase their employability options.

A complete syllabus that will bring you closer to the latest concepts on business management and IT systems to become a successful Chief Information Officer"

International Guest Director

Dr. Frederic Lemieux is internationally recognized as an innovative expert and inspirational leader in the fields of **Intelligence, National Security, Homeland Security, Cybersecurity,** and **Disruptive Technologies.** And his consistent dedication and significant contributions to Research and Education position him as a key figure in promoting security and understanding emerging technologies today. Throughout his professional career, he has conceptualized and led cutting-edge academic programs in various renowned institutions, such as **the University of Montreal**, the **George Washington University,** and **Georgetown University**.

Over the course of his extensive career, he has authored multiple highly relevant books, all related to **criminal intelligence, law enforcement, cyber threats, and international security.** Likewise, he has made significant contributions to the field of Cybersecurity through the publication of numerous articles in academic journals, which examine crime control during major disasters, counterterrorism efforts, intelligence agencies, and police cooperation. Furthermore, he has served as a panelist and keynote speaker at various national and international conferences, establishing himself as a prominent figure in both academic and professional field.

Dr. Lemieux has held editorial and evaluative roles in various academic, private, and government organizations, reflecting his influence and commitment to excellence in his specialized field. In this manner, his esteemed academic career has led him to serve as a Practitioner Professor 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

- Researcher in Intelligence, Cybersecurity, and Disruptive Technologies at Georgetown University
- Director of the Master's in Information Technology Management at Georgetown University
- Director of the Master's in Technology Management at Georgetown University
- Director of the Master's in Cybersecurity Risk Management at Georgetown University
- Director of the Master's in Applied Intelligence at Georgetown University
- Practitioner Professor at Georgetown University
- Ph.D. in Criminology from the School of Criminology at the University of Montreal
- Graduate in Sociology with a Minor Degree in Psychology from Laval University
- Member of: New Program Roundtable Committee by Georgetown University

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

Management

Ms. Fernández Sapena, Sonia

- Trainer in Computer Security and Ethical Hacking at the National Reference Center for Information Technology and Telecommunications
- 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

Mr. Olalla Bonal, Martín

- Senior Blockchain Practice Manager at EY
- Blockchain Client Technical Specialist for IBM
- Director of Architecture for Blocknitive
- Non-Relational Distributed Databases from Team Coordinator for WedoIT, an IBM Subsidiary
- Infrastructure Architect at Bankia
- Head of Layout Department at T-Systems
- Department Coordinator for Bing Data España SL

Professors

Ms. Marcos Sbarbaro, Victoria Alicia

- Native Android Mobile Applications Developer at B60. UK
- Analyst Programmer for the Management, Coordination and Documentation of a virtualized security alarm environment
- Analyst Programmer of Java Applications for ATMs
- *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 Systems Informatics from the University Oberta de Cataluña
- Master's Degree in Computer Security and Ethical Hacking by EC-Council and CompTIA from the Professional School of New Technologies CICE

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 in Professional Office: Óscar Padura
- Grade in Law by the Public University of the Basque Country
- Master's Degree in Data Protection Officer at EIS Innovative School
- Master's Degree in Advocacy at the Public University of the Basque Country
- Master's Degree in Civil Litigation Practice from the International University Isabel I of Castilla
- Professor in Master's Degree in Personal Data Protection, Cybersecurity and ICT Law

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
- Telecommunications Equipment and Services Installer at Lican Comunicaciones SL, Castilla y León
- Certificate in Computer Security by CFTIC Getafe, Madrid
- Higher Technician in Telecommunications and Computer Systems from IES Trinidad Arroyo, Palencia
- Higher Technician in MV and LV Electrotechnical Installations from IES Trinidad Arroyo, Palencia
- Formation in Reverse Engineering, Steganography, and Encryption from the Hacker Academy Incibe

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

Mr. Nogales Ávila, Javier

- Enterprise Cloud and Sourcing Senior Consultant at Quint
- Cloud and Technology Consultant at Indra
- Associate Technology Consultant at Accenture
- Graduate in Industrial Organization Engineering from the University of Jaén
- MBA in Business Administration and Management by ThePower Business School

Mr. Gómez Rodríguez, Antonio

- Principal Cloud Solutions Engineer for Oracle
- Co-organizer of Málaga Developer Meetup
- Specialist Consultant for Sopra Group and Everis
- Team Leader at System Dynamics
- Software Developer at SGO Software
- Master's Degree in E-Business from La Salle Business School
- Postgraduate degree in Information Technologies and Systems from the Catalan Institute of Technology
- Graduate in Telecommunications Engineering from the Polytechnic University of Catalonia

Mr. Catalá Barba, José Francisco

- Electronic Technician Cybersecurity Expert
- Mobile Application Development for Mobile Devices
- Electronics Technician in Intermediate Command in the Spanish Ministry of Defense
- Electronic technician at Ford's Factory located in Valencia

Mr. Gonzalo Alonso, Félix

- CEO and Founder from Smart REM Solutions
- Head of Risk Engineering and Innovation at Dynargy
- Manager and founding partner of the technological expert firm Risknova
- Master's Degree in Insurance Management from the Institute for Collaboration between Insurance Entities
- Grade in Industrial Technical Engineering, specializing in Industrial Electronics by Pontificia de Comillas University

Mr. Entrenas, Alejandro

- Cybersecurity Project Manager
- Cybersecurity Project Manager. Entelgy Innotec Security
- Cybersecurity Consultant Entelgy
- Information Security Analyst. Innovery Spain
- Information Security Analyst. Atos
- Degree in Technical Engineering in Computer Systems from the University of Cordoba
- Master's Degree in Information Security Management from the Polytechnic University of Madrid
- ITIL v4 Foundation Certificate in IT Service Management. ITIL Certified
- IBM Security QRadar SIEM 7.1 Advanced. Avnet
- IBM Security QRadar SIEM 7.1 Foundations. Avnet

Mr. Del Valle Arias, Jorge

- Telecommunications Engineer specialized in Business Development
- Smart City Solutions & Software Business Development Manager Spain. Itron, Inc IoT Consultant
- Interim Director of IoT Business. TCOMET
- Head of IoT, Industry 4.0 Business Unit. Diode Spain
- IoT and Telecommunications Sales Area Manager Aicox Soluciones
- Chief Technical Officer (CTO) and Business Development Manager. TELYC Consulting
- Founder and CEO of Sensor Intelligence
- Operations and Projects Manager. Codio
- Operations Director at Codium Networks
- Chief Hardware and Firmware Design Engineer. AITEMIN
- Regional Head of RF Planning and Optimization - LMDS 3.5 GHz Network. Clearwire
- Telecommunications Engineer from Universidad Politécnica de Madrid
- Executive MBA from the International Graduate School of La Salle of Madrid
- Master's Degree in Renewable Energies. CEPYME

Mr. Gozalo Fernández, Juan Luis

- Blockchain-based Product Manager for Open Canarias
- Director Blockchain DevOps Director at Alastria
- Director of Service Level Technology at Santander Spain
- Tinkerlink Mobile Application Development Manager at Cronos Telecom
- IT Service Management Technology Director at Barclays Bank Spain
- Bachelor's Degree in Computer Engineering from UNED
- Deep Learning Specialization in DeepLearning.ai

Ms. Jurado Jabonero, Lorena

- Chief Information Security Officer (CISO) at Grupo Pascual
- Cybersecurity Manager at KPMG. Spain
- IT Process and Infrastructure Project Control and Management Consultant at Bankia
- Operating Tools Engineer at Dalkia
- Developer at Grupo Banco Popular
- Applications Developer from Universidad Politécnica de Madrid
- Graduate in Computer Engineering from University Alfonso X El Sabio
- Technical Engineer in Computer Management from the Polytechnic University of Madrid
- Certified Data Privacy Solutions Engineer (CDPSE) by ISACA

Mr. Ortega Esteban, Octavio

- Marketing and Web Development Specialist
- Freelance Applications Programmer and Web Developer
- Chief Operating Officer at Smallsquid SL
- E-commerce Administrator at Ortega y Serrano
- Teacher for Professional Certificates in IT and Communications
- Teacher for Cybersecurity Courses
- Graduate in Psychology from the University Oberta de Catalunya
- Higher University Technician in Software Analysis, Design, and Solutions
- Higher University Technician in Advanced Programming

Mr. Embid Ruiz, Mario

- Lawyer Expert in ICT and Data Protection at Martínez-Echevarría Abogados
- Legal Liability officer at Branddocs SL
- Risk Analyst in the SME Segment at BBVA
- Teacher in postgraduate university studies related to Law
- Graduate in Law from Rey Juan Carlos University
- Graduate in Business Administration and Management from Rey Juan Carlos University
- Master's in Law of New Technologies, Internet, and Audiovisual from the Centro de Estudios Universitarios Villanueva

Mr. Rodrigo Estébanez, Juan Manuel

- Co-founder of Ismet Tech
- Information Security Manager at Ecix Group
- Operational Security Officer at Atos IT Solutions and Services A/S
- Teacher in Cybersecurity Management in university studies
- Graduate in Engineering from the University of Valladolid
- Master's in Integrated Management Systems from the Universidad CEU San Pablo

05

Structure and Content

This Advanced Master's Degree in Senior Cybersecurity Management is composed of 20 modules, and has been carefully designed to bring the professional closer to the latest developments in this field. Thus, you will learn about the latest advances in issues such as security in smartphones, security in the Internet of Things, secure development, cryptography or security in cloud computing. environments. With this syllabus, therefore, the computer scientist will have access to the most up-to-date and complete knowledge, quickly preparing them to become a highly prestigious cybersecurity specialist.

You won't find more comprehensive content than this to bring you up to date in the field of cybersecurity"

Module 1. All concepts of Cyber Intelligence and Cybersecurity implemented in a structured way in a study approach focused on efficiency

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. All concepts of Cyber Intelligence and Cybersecurity implemented in a structured way in a study approach focused on efficiency."
 1.1.2. Intelligence Analyst
  1.1.2.1. The Role of the Intelligence Analyst
  1.1.2.2. Biases of the Intelligence Analyst in Evaluative Activity
1.2. Cybersecurity
 1.2.1. Security Layers
 1.2.2. Identification of Cyberthreats
  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. Intelligences Techniques and Tools
 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. Audits in Computer Security
 1.5.2. Documentation and Permissions for Audits
 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 on the Web
 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
1.10.2. OEA
1.10.3. 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 Phising Detection
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/Host, Container and *Serverless* Communication and Discovery
3.2. Firewall
3.2.1. Types of Firewall
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 Firewall
3.4.2. Main Capabilities
3.4.3. Commercial Solutions
3.4.4. Firewalls for Cloud Services
3.4.4.1. Architecture Cloud VPC
3.4.4.2. ACLs Cloud
3.4.4.3. Security Group
3.5. Proxy
3.5.1. Types of Proxy
3.5.2. Use of Proxy Advantages and Disadvantages
3.6. Antivirus Motors
3.6.1. General Context of Malware and IOCs
3.6.2. Antivirus Engine Problems
3.7. Mail 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. Others 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 Project
4.2.1.1. Top 10 Vulnerabilities
4.2.2. Communications, Networks and Connection Modes
4.3. The Mobile Device in the Enterprise Environment
4.3.1. Risk
4.3.2. Security Policies
4.3.3. Device Monitoring
4.3.4. Mobile Device Management (MDM)
4.4. User Privacy and Data Security
4.4.1. Information States
4.4.2. Data Protection and Confidentiality
4.4.2.1. Licences
4.4.2.2. Encryption

4.4.3. Secure Data Storage
4.4.3.1. Secure Storage in 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 Non-Existent 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. Installation of Malware 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. Data Science
4.10. Protections and Security
4.10.1. Security Configuration
4.10.1.1. On IoS Devices
4.10.1.2. On Androind Devices
4.10.2. Security Measures
4.10.3. Protection Tools

Module 5. IoT Security

5.1. Devices
5.1.1. Types of Devices
5.1.2. Standardized Architecture
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
- 5.5.3. Security/Safety

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 Manager
- 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. Firewall and 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 Analysis 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. Wireless Network Attacks
  6.7.1. Wireless Network Hacking Methodology
    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 Network Security
6.8. Hacking of Web Servers
  6.8.1. *Cross Site Scripting*
  6.8.2. CSRF
  6.8.3. Session Hijacking
  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 Scheduled 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 Compiler Analysis
  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. Assembler Data Structures
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
7.4.3. Functions
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 Architecture Hardware
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. Communication
7.8.1.2. 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. Android *Sandbox*
7.10. Malware Analysis
7.10.1. Methods of Malware Analysis
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. Secure Coding Best 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 BBDD
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 Anti-Forensic Techniques
 9.2.1. Objectives of Anti-Forensic 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. Forensic Analysis of the Operating System
9.3.1. Windows Forensic Analysis
9.3.2. Linux Forensic Analysis
9.3.3. Mac Forensic Analysis
9.4. Network Forensic Analysis
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 Analysis of Databases
9.6.1. MSSQL Forensic Analysis
9.6.2. MySQL Forensic Analysis
9.6.3. PostgreSQL Forensic Analysis
9.6.4. MongoDB Forensic Analysis
9.7. Cloud Forensic Analysis
9.7.1. Types of Crimes in the Cloud
9.7.1.1. Cloud as a Subject
9.7.1.2. Cloud as an Object
9.7.1.3. Cloud as a Tool
9.7.2. Cloud Forensic Analysis Challenges
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. Email Forensic Tools
9.9. Mobile Forensic Analysis
9.9.1. Mobile 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. Writing and Presentation of Forensic Reports
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 IT Security Challenges

10.1. Technology Blockchain
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. Protection 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 in "*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 of 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. Security in System Design and Development

11.1. Information Systems
- 11.1.1. Information System Domains
- 11.1.2. Components of an Information System
- 11.1.3. Activities of an Information System
- 11.1.4. Life Cycle of an Information System
- 11.1.5. Information System Resources

11.2. IT systems. Typology
- 11.2.1. Types of Information Systems
  - 11.2.1.1. Enterprise
  - 11.2.1.2. Strategic
  - 11.2.1.3. According to the Scope of Application
  - 11.2.1.4. Specific
- 11.2.2. Information Systems Real Examples
- 11.2.3. Evolution of Information Systems: Stages
- 11.2.4. Information Systems Methodologies

11.3. Security of Information Systems. Legal implications
- 11.3.1. Access to Data
- 11.3.2. Security Threats Vulnerabilities
- 11.3.3. Legal Implications Crimes
- 11.3.4. Information System Maintenance Procedures

11.4. Security of an Information System. Security Protocols
- 11.4.1. Security of an Information System
  - 11.4.1.1. Integrity
  - 11.4.1.2. Confidentiality
  - 11.4.1.3. Availability
  - 11.4.1.4. Authentication
- 11.4.2. Security Services
- 11.4.3. Information Security Protocols. Typology
- 11.4.4. Sensitivity of an Information System

11.5. Security in an Information System. Access Control Measures and Systems
- 11.5.1. Safety Measures
- 11.5.2. Type of Security Measures
  - 11.5.2.1. Prevention
  - 11.5.2.2. Detection
  - 11.5.2.3. Correction
- 11.5.3. Access Control Systems. Typology
- 11.5.4. Cryptography

11.6. Network and Internet Security
- 11.6.1. Firewalls
- 11.6.2. Digital Identification
- 11.6.3. Viruses and Worms
- 11.6.4. Hacking
- 11.6.5. Examples and Real Cases

11.7. Computer Crimes
- 11.7.1. Computer Crime
- 11.7.2. Computer Crimes. Typology
- 11.7.3. Computer Crimes Attacks. Typology
- 11.7.4. The Case for Virtual Reality
- 11.7.5. Profiles of Offenders and Victims. Typification of the Crime
- 11.7.6. Computer Crimes. Examples and Real Cases

11.8. Security Plan in an Information System
- 11.8.1. Security Plan. Objectives
- 11.8.2. Security Plan. Education
- 11.8.3. Risk Plan. Analysis
- 11.8.4. Security Policy. Implementation in the Organization
- 11.8.5. Security Plan. Implementation in the Organization
- 11.8.6. Security Procedures. Types
- 11.8.7. Security plans. Examples:

11.9. Contingency Plan
- 11.9.1. Contingency Plan. Functions
- 11.9.2. Emergency Plan Elements and Objectives
- 11.9.3. Contingency Plan in the Organization. Implementation
- 11.9.4. Contingency Plans. Examples:

11.10. Information Systems Security Governance
- 11.10.1. Legal Regulations
- 11.10.2. Standards
- 11.10.3. Certifications
- 11.10.4. Technologies

Module 12. Information Security Architectures and Models

12.1. Information Security Architecture
- 12.1.1. ISMSI / PDS
- 12.1.2. Strategic Alignment
- 12.1.3. Risk Management
- 12.1.4. Performance Measurement

12.2. Information Security Models
- 12.2.1. Based on Security Policies
- 12.2.2. Based on Protection Tools
- 12.2.3. Based on Work Teams

12.3. Safety Model. Key Components
- 12.3.1. Identification of Risks
- 12.3.2. Definition of Controls
- 12.3.3. Continuous Assessment of Risk Levels
- 12.3.4. Awareness-Raising Plan for Employees, Suppliers, Partners, Etc

12.4. Risk Management Process
- 12.4.1. Asset Identification
- 12.4.2. Threat Identification
- 12.4.3. Risk Assessment

12.4.4. Prioritization of Controls
12.4.5. Re-Evaluation and Residual Risk
12.5. Business Processes and Information Security
12.5.1. Business Processes
12.5.2. Risk Assessment Based on Business Parameters
12.5.3. Business Impact Analysis
12.5.4. Business Operations and Information Security
12.6. Continuous Improvement Process
12.6.1. The Deming Cycle
12.6.1.1. Planning
12.6.1.2. Do
12.6.1.3. Verify
12.6.1.4. Act
12.7. Security Architectures
12.7.1. Selection and Homogenization of Technologies
12.7.2. Identity Management. Authentication
12.7.3. Access Management. Authorization
12.7.4. Network Infrastructure Security
12.7.5. Encryption Technologies and Solutions
12.7.6. Terminal Equipment Security (EDR)
12.8. Regulatory Framework
12.8.1. Sectoral Regulations
12.8.2. Certifications
12.8.3. Legislation
12.9. The ISO 27001 Standard
12.9.1. Implementation
12.9.2. Certification
12.9.3. Audits and Penetration Tests
12.9.4. Continuous Risk Management
12.9.5. Classification of Information
12.10. Privacy Legislation. GDPR
12.10.1. Scope of General Data Protection Regulation (GDPR)
12.10.2. Personal Data
12.10.3. Roles in the Processing of Personal Data
12.10.4. ARCO Rights
12.10.5. El DPO. Functions

Module 13. IT Security Management

13.1. Safety Management
13.1.1. Security Operations
13.1.2. Legal and Regulatory Aspects
13.1.3. Business Qualification
13.1.4. Risk Management
13.1.5. Identity and Access Management
13.2. Structure of the Security Area. The CISO's Office
13.2.1. Organisational Structure. Position of the CISO in the Structure
13.2.2. Lines of Defense
13.2.3. Organizational Chart of the CISO's Office
13.2.4. Budget Management
13.3. Security Governance
13.3.1. Safety Committee
13.3.2. Risk Monitoring Committee
13.3.3. Audit Committee
13.3.4. Crisis Committee
13.4. Security Governance. Functions
13.4.1. Policies and Standards
13.4.2. Security Master Plan
13.4.3. Control Panels
13.4.4. Awareness and Education
13.4.5. Supply Chain Security
13.5. Security Operations
13.5.1. Identity and Access Management
13.5.2. Configuration of Network Security Rules. Firewalls
13.5.3. IDS/IPS Platform Management
13.5.4. Vulnerability Analysis
13.6. Cybersecurity Framework NIST CSF
13.6.1. NIST Methodology
13.6.1.1. Identify

13.6.1.2. Protect
13.6.1.3. Detect
13.6.1.4. Respond
13.6.1.5. Retrieve
13.7. Security Operations Center (SOC). Functions
13.7.1. Protection Red Team, Pentesting, Threat Intelligence
13.7.2. Detection. SIEM, User Behavior Analytics, Fraud Prevention
13.7.3. Response
13.8. Security Audits
13.8.1. Intrusion Test
13.8.2. Red Team Exercises
13.8.3. Source Code Audits. Secure Development
13.8.4. Component Safety (Software Supply Chain))
13.8.5. Forensic Analysis
13.9. Incident Response
13.9.1. Preparation
13.9.2. Detection, Analysis and Notification
13.9.3. Containment, Eradication and Recovery
13.9.4. Post-Incident Activity
13.9.4.1. Evidence Retention
13.9.4.2. Forensic Analysis
13.9.4.3. Gap Management
13.9.5. Official Cyber-Incident Management Guidelines
13.10. Vulnerability Management
13.10.1. Vulnerability Analysis
13.10.2. Vulnerability Assessment
13.10.3. System Basing
13.10.4. Zero-Day Vulnerabilitie. Zero-Day

Module 14. Risk Analysis and IT Security Environment

14.1. Analysis of the environment
14.1.1. Analysis of the Economic Situation
14.1.1.1. VUCA Environments
14.1.1.1.1. Volatile
14.1.1.1.2. Uncertain
14.1.1.1.3. Complex
14.1.1.1.4. Ambiguous
14.1.1.2. BANI Environments
14.1.1.2.1. Brittle
14.1.1.2.2. Anxious
14.1.1.2.3. Nonlinear
14.1.1.2.4. Incomprehensible
14.1.2. Analysis of the General Environment. PESTEL
14.1.2.1. Politics
14.1.2.2. Economics
14.1.2.3. Social
14.1.2.4. Technological
14.1.2.5. Ecological/Environmental
14.1.2.6. Legal
14.1.3. Analysis of the Internal Situation SWOT Analysis
14.1.3.1. Objectives
14.1.3.2. Threats
14.1.3.3. Opportunities
14.1.3.4. Strengths
14.2. Risk and Uncertainty
14.2.1. Risk
14.2.2. Risk Management
14.2.3. Risk Management Standards
14.3. ISO 31.000:2018 Risk Management Guidelines
14.3.1. Object
14.3.2. Principles
14.3.3. Frame of Reference
14.3.4. Process
14.4. Information Systems Risk Analysis and Management Methodology (MAGERIT)
14.4.1. MAGERIT Methodology

14.4.1.1. Objectives
14.4.1.2. Method
14.4.1.3. Components
14.4.1.4. Techniques
14.4.1.5. Available Tools (PILAR)

14.5. Cyber Risk Transfer
- 14.5.1. Ristk Transfer
- 14.5.2. Cyber Risks. Typology
- 14.5.3. Cyber Risk Insurance

14.6. Agile Methodologies for Risk Management
- 14.6.1. Agile Methodologies
- 14.6.2. Scrum for Risk Management
- 14.6.3. *Agile Risk Management*

14.7. Technologies for Risk Management
- 14.7.1. Artificial Intelligence Applied to Risk Management
- 14.7.2. *Blockchain* and Cryptography. Value Preservation Methods
- 14.7.3. Quantum Computing Opportunity or Threat

14.8. IT Risk Mapping Based on Agile Methodologies
- 14.8.1. Representation of Probability and Impact in Agile Environments
- 14.8.2. Risk as a Threat to Value
- 14.8.3. Re-Evolution in Project Management and Agile Processes based on KRIs

14.9. *Risk-Driven* in Risk Management
- 14.9.1. *Risk Driven*
- 14.9.2. *Risk-Driven* in Risk Management
- 14.9.3. Development of a Risk-Driven Business Management Model

14.10. Innovation and Digital Transformation in IT Risk Management
- 14.10.1. Agile Risk Management as a Source of Business Innovation
- 14.10.2. Transforming Data into Useful Information for Decision Making
- 14.10.3. Holistic View of the Enterprise through Risk

Module 15. Cryptography in IT

15.1. Cryptography
- 15.1.1. Cryptography
- 15.1.2. Fundamentals of Mathematics

15.2. Cryptology
- 15.2.1. Cryptology
- 15.2.2. Cryptanalysis
- 15.2.3. Steganography and Stegoanalysis

15.3. Cryptographic Protocols
- 15.3.1. Basic Blocks
- 15.3.2. Basic Protocols
- 15.3.3. Intermediate Protocols
- 15.3.4. Advanced Protocol
- 15.3.5. Exoteric Protocols

15.4. Cryptographic Techniques
- 15.4.1. Key Length
- 15.4.2. Key Management
- 15.4.3. Types of Algorithms
- 15.4.4. Key Management *Hash*
- 15.4.5. Pseudo-Random Number Generators
- 15.4.6. Use of Algorithms

15.5. Symmetric Cryptography
- 15.5.1. Block Ciphers
- 15.5.2. DES (*Data Encryption Standard*)
- 15.5.3. RC4 Algorithm
- 15.5.4. AES (*Advanced Encryption Standard*)
- 15.5.5. Combination of Block Ciphers
- 15.5.6. Key Derivation

15.6. Asymmetric Cryptography
- 15.6.1. Diffie-Hellman
- 15.6.2. DSA (*Digital Signature Algorithm*)
- 15.6.3. RSA (*Rivest, Shamir and Adleman*)
- 15.6.4. Elliptic Curve
- 15.6.5. Asymmetric Cryptography. Typology

15.7. Digital Certificates

15.7.1. Digital Signature
15.7.2. X509 Certificates
15.7.3. Public Key Infrastructure (PKI)

15.8. Implementations
15.8.1. Kerberos
15.8.2. IBM CCA
15.8.3. *Pretty Good Privacy* (PGP)
15.8.4. ISO *Authentication Framework*
15.8.5. SSL and TLS
15.8.6. Smart Cards in Means of Payment (EMV)
15.8.7. Mobile Telephony Protocols
15.8.8. *Blockchain*

15.9. Steganography
15.9.1. Steganography
15.9.2. Stegoanalysis
15.9.3. Applications and Uses

15.10. Quantum Cryptography
15.10.1. Quantum Algorithms
15.10.2. Protection of Algorithms from Quantum Computing
15.10.3. Quantum Key Distribution

Module 16. Identity and Access Management in IT security

16.1. Identity and Access Management (IAM)
16.1.1. Digital Identity
16.1.2. Identity Management
16.1.3. Identity Federation

16.2. Physical Access Control
16.2.1. Protection Systems
16.2.2. Area Security
16.2.3. Recovery Facilities

16.3. Logical Access Control
16.3.1. Authentication Typology
16.3.2. Authentication Protocols
16.3.3. Authentication Attacks

16.4. Logical Access Control. MFA Authentication
16.4.1. Logical Access Control. MFA Authentication
16.4.2. Passwords. Importance
16.4.3. Authentication Attacks

16.5. Logical Access Control. Biometric Authentication
16.5.1. Logical Access Control Biometric Authentication
16.5.1.1. Biometric Authentication. Requirements
16.5.2. Operation
16.5.3. Models and Techniques

16.6. Authentication Management Systems
16.6.1. *Single Sign On*
16.6.2. Kerberos
16.6.3. AAA Systems

16.7. Authentication Management Systems: AAA Systems
16.7.1. TACACS
16.7.2. RADIUS
16.7.3. DIAMETER

16.8. Access Control Services
16.8.1. FW - Firewall
16.8.2. VPN - Virtual Private Networks
16.8.3. IDS - Intrusion Detection System

16.9. Network Access Control Systems
16.9.1. NAC
16.9.2. Architecture and Elements
16.9.3. Operation and Standardization

16.10. Access to Wireless Networks
16.10.1. Types of Wireless Networks
16.10.2. Security in Wireless Networks
16.10.3. Attacks on Wireless Networks

Module 17. Security in communications and software operation

17.1. Computer Security in Communications and Software Operation
 17.1.1. IT Security
 17.1.2. Cybersecurity
 17.1.3. Cloud Security
17.2. IT Security in Communications and Software Operation Typology
 17.2.1. Physical Security
 17.2.2. Logical Security
17.3. Communications Security
 17.3.1. Main Elements
 17.3.2. Network Security
 17.3.3. Best Practices
17.4. Cyberintelligence
 17.4.1. Social Engineering
 17.4.2. *Deep Web*
 17.4.3. *Phishing*
 17.4.4. *Malware*
17.5. Secure Development in Communications and Software Operation
 17.5.1. Secure Development. HTTP Protocol
 17.5.2. Secure Development. Life Cycle
 17.5.3. Secure Development. PHP Security
 17.5.4. Secure Development. NET Security
 17.5.5. Secure Development. Best Practices
17.6. Information Security Management Systems in Communications and software Operations
 17.6.1. GDPR
 17.6.2. ISO 27021
 17.6.3. ISO 27017/18
17.7. SIEM Technologies
 17.7.1. SIEM Technologies
 17.7.2. SOC Operation
 17.7.3. SIEM *Vendors*
17.8. The Role of Security in Organizations
 17.8.1. Roles in Organizations
 17.8.2. Role of IoT Specialists in Companies
 17.8.3. Recognized Certifications in the Market
17.9. Forensic Analysis
 17.9.1. Forensic Analysis
 17.9.2. Forensic Analysis. Methodology
 17.9.3. Forensic Analysis. Tools and Implementation
17.10. Cybersecurity Today
 17.10.1. Major Cyber-Attacks
 17.10.2. Employability Forecasts
 17.10.3. Challenges

Module 18. Security in Cloud Environments

18.1. Security in Cloud Computing Environments
 18.1.1. Security in Cloud Computing Environments
 18.1.2. Security in Cloud Computing Environments Threats and Security Risks
 18.1.3. Security in Cloud Computing Environments Key Security Aspects
18.2. Types of Cloud Infrastructure
 18.2.1. Public
 18.2.2. Private
 18.2.3. Hybrid
18.3. Shared Management Model
 18.3.1. Security Elements Managed by Vendor
 18.3.2. Elements Managed by Customer
 18.3.3. Definition of the Security Strategy
18.4. Prevention Mechanisms
 18.4.1. Authentication Management Systems
 18.4.2. Authorization Management Systems: Access Policies
 18.4.3. Key Management Systems
18.5. System Securization
 18.5.1. Securitization of Storage Systems
 18.5.2. Protection of Database Systems
 18.5.3. Securing Data in Transit

18.6. Infrastructure Protection
 18.6.1. Secure Network Design and Implementation
 18.6.2. Security in Computing Resources
 18.6.3. Tools and Resources for Infrastructure Protection
18.7. Detection of Threats and Attacks
 18.7.1. Auditing, *Logging* and Monitoring Systems
 18.7.2. Event and Alarm Systems
 18.7.3. SIEM Systems
18.8. Incident Response
 18.8.1. Incident Response Plan
 18.8.2. Business Continuity
 18.8.3. Forensic Analysis and Remediation of Incidents of the Same Nature
18.9. Security in Public *Clouds*
 18.9.1. AWS (Amazon Web Services)
 18.9.2. Microsoft Azure
 18.9.3. Google GCP
 18.9.4. Oracle Cloud
18.10. Regulations and Compliance
 18.10.1. Security Compliance
 18.10.2. Risk Management
 18.10.3. People and Process in Organizations

Module 19. Security in IoT Device Communications

19.1. From Telemetry to IoT
 19.1.1. Telemetry
 19.1.2. M2M Connectivity
 19.1.3. Democratization of Telemetry
19.2. IoT Reference Models
 19.2.1. IoT Reference Model
 19.2.2. Simplified IoT Architecture
19.3. IoT Security Vulnerabilities
 19.3.1. IoT Devices
 19.3.2. IoT Devices. Usage Case Studies
 19.3.3. IoT Devices. Vulnerabilities
19.4. IoT Connectivity
 19.4.1. PAN, LAN, WAN Networks
 19.4.2. Non IoT Wireless Technologies
 19.4.3. LPWAN Wireless Technologies
19.5. LPWAN Technologies
 19.5.1. The Iron Triangle of LPWAN Networks
 19.5.2. Free Frequency Bands vs. Licensed Bands
 19.5.3. LPWAN Technology Options
19.6. LoRaWAN Technology
 19.6.1. LoRaWAN Technology
 19.6.2. LoRaWAN Use Cases. Ecosystem
 19.6.3. Security in LoRaWAN
19.7. Sigfox Technology
 19.7.1. Sigfox Technology
 19.7.2. Sigfox Use Cases. Ecosystem
 19.7.3. Sigfox Security
19.8. IoT Cellular Technology
 19.8.1. IoT Cellular Technology (NB-IoT and LTE-M)
 19.8.2. Cellular IoT Use Cases Ecosystem
 19.8.3. IoT Cellular Security
19.9. WiSUN Technology
 19.9.1. WiSUN Technology
 19.9.2. WiSUN Use Cases Ecosystem
 19.9.3. Security in WiSUN
19.10. Other IoT Technologies
 19.10.1. Other IoT Technologies
 19.10.2. Use Cases and Ecosystem of Other IoT Technologies
 19.10.3. Security in Other IoT Technologie

Module 20. Business Continuity Plan Associated with Security

20.1. Business Continuity Plans
- 20.1.1. Business Continuity Plans (BCP)
- 20.1.2. Business Continuity Plans (BCP) Key Aspects
- 20.1.3. Business Continuity Plan (BCP) for Business Valuation

20.2. Metrics in a Business Continuity Plan (BCP)
- 20.2.1. *Recovery Time Objective* (RTO) and *Recovery Point Objective* (RPO)
- 20.2.2. Maximum Tolerable Time (MTD)
- 20.2.3. Minimum Recovery Levels (ROL)
- 20.2.4. Recovery point objective (RPO)

20.3. Continuity Projects. Typology
- 20.3.1. Business Continuity Plan (BCP)
- 20.3.2. ICT Continuity Plan (ICTCP)
- 20.3.3. Disaster Recovery Plan (DRP)

20.4. Risk Management Associated with the BCP
- 20.4.1. Business Impact Analysis
- 20.4.2. Benefits of Implementing a BCP
- 20.4.3. Risk-Based Mentality

20.5. Life Cycle of a Business Continuity Plan
- 20.5.1. Phase 1: Analysis of the Organization
- 20.5.2. Phase 2: Determination of the Continuity Strategy
- 20.5.3. Phase 3: Contingency Response
- 20.5.4. Phase 4: Testing, Maintenance and Review

20.6. Organizational Analysis Phase of a BCP
- 20.6.1. Identification of Processes in the Scope of the BCP
- 20.6.2. Identification of Critical Business Areas
- 20.6.3. Identification of Dependencies Between Areas and Processes
- 20.6.4. Determination of Appropriate BAT
- 20.6.5. Deliverables. Creation of a Plan

20.7. Determination Phase of the Continuity Strategy in a BCP
- 20.7.1. Roles in the Strategy Determination Phase
- 20.7.2. Tasks in the Strategy Determination Phase
- 20.7.3. Deliverables

20.8. Contingency Response Phase of a BCP
- 20.8.1. Roles in the Response Phase
- 20.8.2. Tasks in This Phase
- 20.8.3. Deliverables

20.9. Testing, Maintenance and Revision Phase of a BCP
- 20.9.1. Roles in the Testing, Maintenance and Review Phase
- 20.9.2. Tasks in the Testing, Maintenance and Review Phase
- 20.9.3. Deliverables

20.10. ISO Standards Associated with Business Continuity Plans (BCP)
- 20.10.1. ISO 22301:2019
- 20.10.2. ISO 22313:2020
- 20.10.3. Other Related ISO and International Standards

> *"You will be able to delve into issues such as business continuity planning associated with security or identity and access management in IT security"*

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

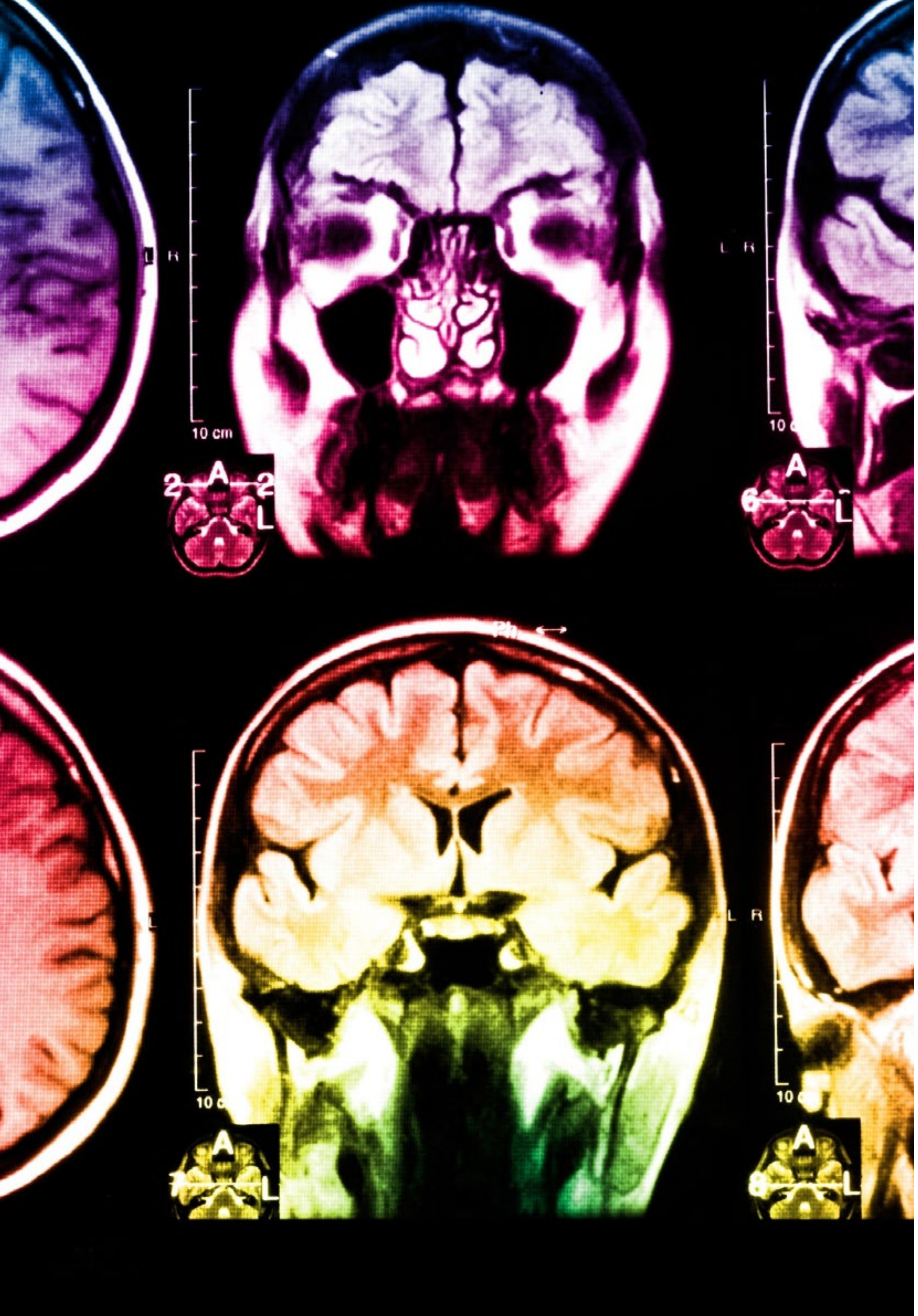
TECH effectively combines the Case Study methodology with a 100% online learning system based on repetition, which combines different teaching elements in each lesson.

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.



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.

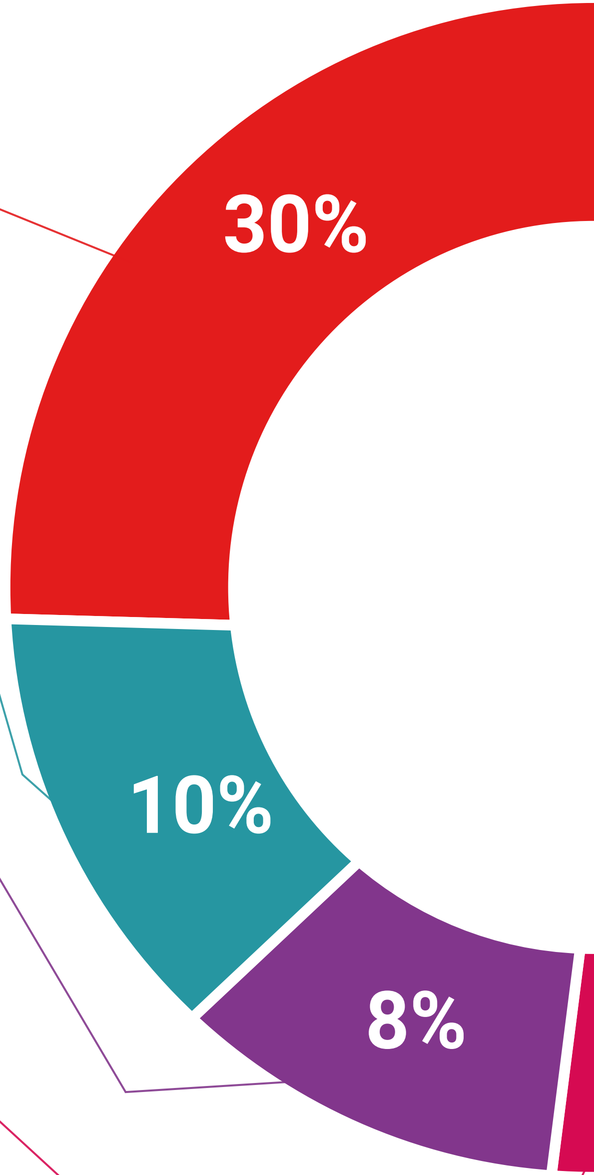
Learning from an Expert strengthens knowledge and memory, and generates confidence in future difficult decisions.

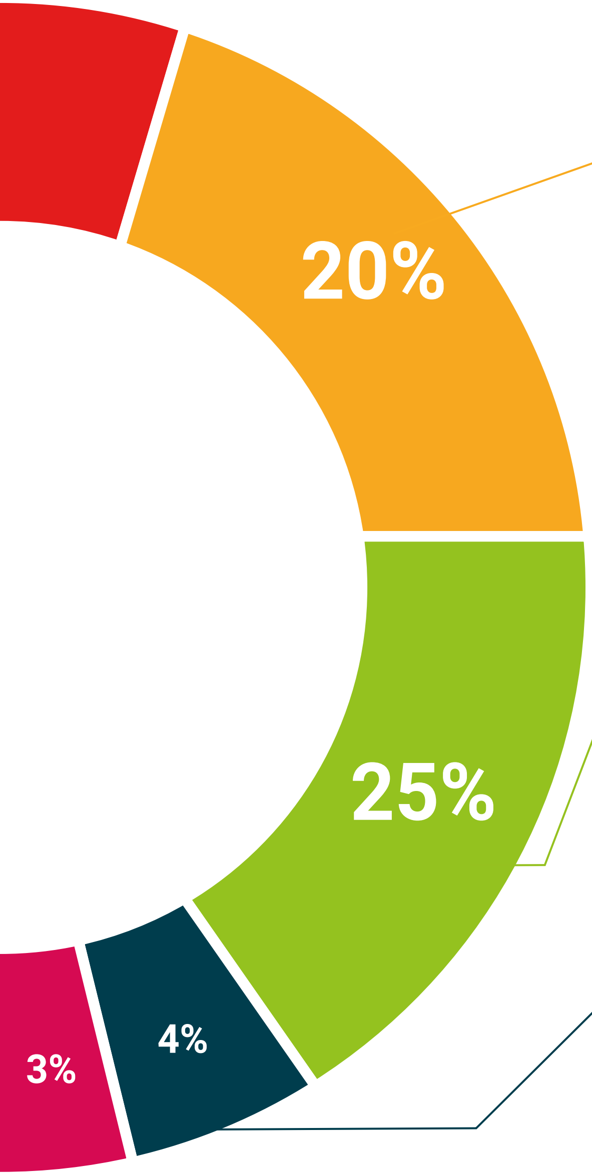
Practising Skills and Abilities

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 Professional Master's Degree in Advanced Master’s Degree in Senior Cybersecurity Management guarantees students, in addition to the most rigorous and up-to-date education, access to a Professional Master's Degree diploma issued by TECH Technological University.

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

This **Advanced Master’s Degree in Senior Cybersecurity in Management** contains the most complete and up-to-date program on the market.

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

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

Title: **Advanced Masters Degree in Senior Cybersecurity Management**

Official Nº of Hours: **3000 h.**

tech technological university

Awards the following

CERTIFICATE

to

Mr./Ms. _________________, with identification number ____________.

For having successfully passed and accredited the following program

ADVANCED MASTER’S DEGREE

in

Senior Cybersecurity Management

This is a qualification awarded by this University, equivalent to 3,000 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

Advanced Master’s Degree in Senior Cybersecurity Management

General Structure of the Syllabus

Year	Subject	Hours	Type
1º	All concepts of Cyber Intelligence and Cybersecurity implemented in a structured way in a study approach focused on efficiency	150	CO
1º	Host Security	150	CO
1º	Network Security (Perimeter)	150	CO
1º	Smartphone Security	150	CO
1º	IoT Security	150	CO
1º	Ethical Hacking	150	CO
1º	Inverse Engineering	150	CO
1º	Secure Development	150	CO
1º	Forensic Analysis	150	CO
1º	Current and Future IT Security Challenges	150	CO

Year	Subject	Hours	Type
2º	Security in System Design and Development	150	CO
2º	Information Security Architectures and Models	150	CO
2º	IT Security Management	150	CO
2º	Risk Analysis and IT Security Environment	150	CO
2º	Cryptography in IT	150	CO
2º	Identity and Access Management in IT security	150	CO
2º	Security in communications and software operation	150	CO
2º	Security in Cloud Environments	150	CO
2º	Security in IoT Device Communications	150	CO
2º	Business Continuity Plan Associated with Security	150	CO

Tere Guevara Navarro
Dean

tech technological university

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

tech technological university

Advanced Master's Degree
Senior Cybersecurity Management

» Modality: **online**
» Duration: **2 years**
» Certificate: **TECH Technological University**
» Dedication: **16h/week**
» Schedule: **at your own pace**
» Exams: **online**

Advanced Master's Degree
Senior Cybersecurity Management

tech technological university