



CYBER SECURITY AND DATA PROTECTION

Post-Graduation



CYBER SECURITY & DATA PROTECTION

Scientific Coordination

Virgínia Araújo

Partnership

Escola Universitária Atlântica
www.uatlantica.pt

Credits

25 ECTS (European Credit Transfer System)

Presentation

Nowadays, Information Security is a visible and increasing concern in organizations. Business competitiveness is highly dependent on access and generation of more and better information. The perimeter of organizations with the outside is more permissive. Business processes are executed in a context of continuous exchange of information with external elements in relationship with customers and suppliers. The employee's social habits within organizations have changed the access to the organization's networks using their own devices, not always properly protected taking into consideration their personal data, allowing the creation of backdoors to corporate data, even in behaviours and attitudes seemingly harmless.

Ensuring cybersecurity and compliance requires ongoing evaluation, implementation, and maintenance. Organizations that do not implement essential safety practices, are significantly reducing their legal defence in case of violation. The new European Regulation GDPR (General Data Protection Regulation) that establishes rules on citizen's privacy rights, becomes enforceable from 25 May 2018.

In this sense, this new edition of the postgraduate course, deepens current and relevance topics such as:

- Information Security Management and Governance
- Data Protection and Privacy
- Cyber Security and Resilience

On behalf of the partnership with the Atlantica, this post-graduation assigns credits ECTS (European Credit Transfer System).

http://ec.europa.eu/education/resources/european-credit-transfer-accumulation-system_en

Main Benefits

The Postgraduate in Cyber Security and Data Protection, is a program of studies totally aligned with the current needs of the market, giving the students the ability to:

- Understand the risks organizations face in their activity regarding information security
- Answer the challenges of data protection and privacy
- Implement information security management systems aligned with business goals
- Understand the causes of attacks and identify the threats to information security
- Help the development of an organizational culture towards information security
- Understand and answer the requirements of the new data protection law allowing organizations to achieve compliance with EU GDPR.

Professional Certification:

Students who successfully complete the Postgraduate Diploma are qualified to implement the ISO 27001 (Information Security Management System) and the ISO 22301 (Business Continuity Management System) standards, to support the external audit certification process in an organization and also achieve the ISO/IEC 27001 professional certification. These achievements, gives organizations the ability to manage and protect their valuable data and information assets, as well as increase their business resilience and strengthen the organization market positioning.

Target Groups

- Managers, technicians and consultants of information systems and technologies
- Executives interested in understanding how Cyber Security, Data Protection and Business Continuity, to increase resilience and bring value to the organizations
- New graduates wishing to acquire Information Security knowledge to expand their possibilities in the job market.

Entry Requirements

The application is open to individuals with an undergraduate degree or higher in the scientific areas and to professionals with or without an academic degree whose experience is considered adequate for the student to succeed in the course and the groups are homogeneous.

The selection will always be made through curricular analysis by the Scientific Coordination of the course, which can call the candidate to a face-to-face interview. In any case, the decision will always be substantiated and presented in writing to the candidate.

Methodology

The pedagogical methodology used involves the development of knowledge and competence simultaneously technical, professional and personal, through integrated expositive and interactive techniques, using case studies putting into practice the knowledge in an environment found in typical organizations.

It is intended students recognize themselves and be recognized as capable and differentiating elements, in professional environments in which they are integrated.

The Post-Graduation in Cyber Security and Data Protection is composed by 12 curricular units that are organized in 2 cycles of specializations:

1. Information Security Governance and Management
2. Information Security Operations and Support

Requirements for obtaining the Diploma

To award the postgraduate diploma in Cyber Security and Data Protection, students must complete the 12 curricular units that are part of the program.

Access to other courses

This postgraduate course offers credits for access a Master's Degree in Systems and Information Technology Management. For this purpose, the student must have an undergraduate degree or higher.

Evaluation Rules

The evaluation of each curricular unit is usually carried out by a final examination. The unit is successfully completed by obtaining a minimum score of 10 values.

Curricular Plan

SPECIALIZATION	CURRICULAR UNIT	TUTOR	Hours	ECTS
INFORMATION SECURITY GOVERNANCE AND MANAGEMENT	• Information Security Concepts and Risk Management	José Casinha	9	1
	• Information Security Management	Virgínia Araújo	18	3
	• Data Protection and Privacy	Pedro Machado	18	3
	• Cyber Security and Cyber Resilience	Virgínia Araújo	15	2,5
	• Governance and compliance	Sérgio Nunes	9	1
	• Business Continuity Management	José Casinha	12	2

SPECIALIZATION	CURRICULAR UNIT	TUTOR	Hours	ECTS
INFORMATION SECURITY OPERATIONS AND SUPPORT	•Cryptography and Penetration Testing	João Magalhães	18	3
	•Secure Applications Development	Alexandre Barão	18	3
	•Systems and Networks Security	Sérgio Nunes	15	2,5
	•Cloud Security	José Casinha	9	1
	•Security Incident Response	Daniel Caçador	9	1
	•Auditing Information Systems and Forensics	Sérgio Nunes	12	2

Curricular Units

INFORMATION SECURITY GOVERNANCE AND MANAGEMENT

Information Security Concepts and Risk Management

José Casinha

- This CU provides the following competencies:
Know how to contextualize the information security issues in organizations and identify areas of activity for the information security professional.
Understand the basic concepts of risk management related to information security. Identify the objectives of the benchmarks, ISO 27001, ISO 27005 and ISO 31000. Design a risk management system according to the organization's risk appetite.
- Contents
Information Security Concepts
What is information?
Types and classification of information.
Confidentiality, Integrity and Availability
Principles of information security
Security Architectures Fundamentals
The concept of depth defense
Risk Management
Methodologies of Risk management
Risks and Threats
The risk management process
ISO 27005 and ISO 31000 standards

Information Security Management

Virgínia Araújo

- This CU provides the following competencies:
Know how to define and maintain an information security management system using recognized best practices and international standards, how to diagnose the risks arising from an information security breach and how to manage it in the context of an organization, how to achieve and maintain an international ISO / IEC 27001 certification in the organization.
- Contents
Introduction, Background and Definitions
Standards and Frameworks
ISO/IEC 27000 Family and Key Publications
Using ITIL to manage Information Security
Using COBIT to manage Information Security
Establishing and Planning an ISMS
Support and Operating an ISMS
Managing Security Incidents
Controlling, managing and reporting Information Security
Achieving Certification for the Organization and Individuals

Data Protection and Privacy

Pedro Machado

- This CU provides the following competencies:
Know how to define and maintain a data protection program, using best practices and international standards. Know how to diagnose the risks arising from a violation of personal data and how best manage it in the organization's context. Know how to assume the role of DPO regardless of context / dimension / organization.
- Contents
Data Protection and Privacy concepts and definition
Terminology of the General Regulation of General Data Protection
Principles of data protection
Categories of personal data
The rights of people
Drivers & Processors
Design for data protection
Protection of personal data
Related Data Violation Procedures
How to conduct a Data Protection Impact Assessment (DPIA)
The role of the Data Protection Supervisor (DPO)
Transfer personal data outside the European Union
The powers of the supervisory authorities

Cyber Security and Cyber Resilience

Virginia Araújo

- This CU provides the following competencies:
Understand the purpose, benefits and concepts of Cyber Security, Information Security, Cyber Resilience in current society context, how to identify security attacks and threats, and diagnose the risks of cyber security and information security breaches. How to implement and maintain a cybersecurity resilience management system in the organization.
- Contents
Introduction, Background and Key Concepts
Cyber Security, Information Security, Cyber Resilience
Cyber Attacks and Threats
Risk Management
Managing Cyber Resilience
Cyber Resilience Strategy
Cyber Resilience Design
Cyber Resilience Transition
Cyber Resilience Operation
Cyber Resilience Continual Improvement

Governance and Compliance

Sérgio Nunes

- This CU provides the following competencies:
Know how to plan information security, define an information security strategy, govern the information security structure, evaluate the business architecture of IS and evaluate compliance with IS standards.
- Contents
 - Security Planning
 - Security Strategy
 - Governance of security structures
 - Security Enterprise Architectures
 - SSDLC
 - Compliance with security standards

Business Continuity Management

José Casinha

- This CU provides the following competencies:
Design a strategy that allows to evaluate the impact analysis in the business activities of an organization. Identify the various plans needed to define a business recovery strategy in case of disruption. Know the various options to recover IT infrastructures according to the RTO and RPO defined for the various activities of the organization.
- Contents
Business Impact Analysis
Identification of continuity requirements business
Definition of RTO and OF
Business Impact Analysis (BIA)
Business Continuity Plan
Continuity Plan in Business
Recovery strategy and ancillary plans
IT Disaster Recovery Plan
Disaster Recovery Strategies for IT Infrastructures
IT Architectures High Availability
Designing IT DRP

INFORMATION SECURITY OPERATIONS AND SUPPORT

Secure Applications Development

Alexandre Barão

- This CU provides the following competencies:
Know key security concepts and types of threats most frequently, identify defense techniques and risk mitigation in the context of software development. Understand the software development lifecycle and in this context, identify problems creating secure applications.
- Contents
 - Security and Internet Key Concepts
 - Threats Overview
 - Malware
 - Security Breaches
 - Denial of Service
 - Web Attacks
 - Session Hijacking
 - DNS Poisoning
 - Cyber Frauds
 - Analysing SQL Injection and other hacking techniques
 - Tools Overview
 - The Software Development Life Cycle
 - Apply security through the SDLC
 - Secure Applications Building Issues
 - Security Policies and Best Practices
 - Analysing Network Vulnerabilities

Systems and network security

Sérgio Nunes

- This CU provides the following competencies:
Define and evaluate the security of an operating system, define and evaluate the security of a computer network.
- Contents
 - Operating systems security
 - Secure Authentication
 - Secure communications
 - Network Security Architectures
 - Firewalls
 - IDS
 - Distributed systems security
 - IOT Security
 - Mobile Security

Cloud Security

José Casinha

- **This CU provides the following competencies:**
Get to know the various cloud service options. Identify the services that best fit the needs of the business. Develop design capabilities for secure cloud services.
- **Contents**
 - Architectural concepts and design requirements
 - NIST SP800-145
 - IaaS
 - PaaS
 - SaaS
 - Public, Private na Hybrid Cloud
 - Cloud data security
 - Data Life Cycle in the Cloud
 - Information Rights Management
 - Prevention of information leakage
 - Data encryption
 - Cloud Platforms
 - Hypervisors
 - Virtualization Security
 - Perimeter Security
 - Application Security in the Cloud
 - Secure Lifecycle Software
 - Cloud threads
 - OWASP
 - DevSecOps

Security Incident Response

Daniel Caçador

- This CU provides the following competencies:
Get to know the most current models, methodologies and practices in the area of the curricular unit and its application. Construction and management of contingency response plans for security, emergency, contingency, disaster recovery, and the respective framework for the business continuity. Creation and preparation of teams and development of processes to respond to security incidents of different types. Organizational Resilience and Crisis Management.
- Contents
 - Security incident management
 - Event and Incident detection
 - Security Vulnerabilities
 - Computer Security Incident Response Teams

Cryptography and Penetration Testing

João Paulo Magalhães

- This CU provides the following competencies:

Understand key concepts related to computer security, the importance of cryptography and enunciate cryptographic systems, state and understand different systems of authentication and access control, understand the importance of security entities, identify the most common vulnerabilities in a computer network, design, install and use vulnerability protection mechanisms, identify the most common causes of intrusions on a computer network, design, install and use intrusion detection mechanisms and solutions.

- Contents

Cryptography

- Symmetric ciphers

- Frequency analysis

- Asymmetric ciphers (Public Key Cryptography)

- Hash Functions, Digital Signatures and Message Authentication

- Codes

- Authentication and Access Control

- Certification and Public Key Infrastructure

Penetration Testing

- Phases of an attack

- Reconnaissance

 - Footprinting

 - Scanning

 - Enumeration

- System hacking

- Penetration testing

Process of Auditing Information System and Forensics

Sérgio Nunes

- This CU provides the following competencies:
Understand how to audit an information system, figure out how to perform a forensic analysis.
- Contents
 - Principles of Auditing Information Systems
 - Auditor Behaviour & Profile
 - Auditing methodologies
 - Managing the auditing team
 - Information gathering
 - Writing and presenting an audit report
 - Evidence chain of custody
 - Evidence lifecycle
 - Forensic tools

TUTORS



Virginia Araújo

PhD in Software Engineering, Degree in Mathematics and Computer Science and several professional certifications, such as ITIL EXPERT, ISO/IEC 20000 PRACTITIONER, ISO/IEC 27001 PRACTITIONER, PMP, PRINCE2 PRACTITIONER, LEAN IT, COBIT, BIG DATA and DEVOPS. More than 20 years of professional experience in Technologies and Information Systems, Senior consultant and trainer accredited by different international Examination Institutes, such as APMG, PEOPLECERT, EXIN. Specialized in Information Security Management, Service Management and Governance, and Project Management in Europe, Africa and Asia. Professor at Atlantica University Higher Institution, member of a research group on Knowledge Management and Software Engineering, Scientific Committee member of Iberian Conference on Information Systems and Technologies, Scientific Committee member of Ibero-American Congress of Qualitative Research. Invited Professor and lecturer at different universities, lecturer at international congresses and author of articles published in specialized magazines. Distinguished by AXELOS Inc. in 2017, as leading woman in ITSM (IT Service Management).



Alexandre Barão

PhD in Information Systems and Computer Engineering (Instituto Superior Técnico) and MSc in Computer and Electrotechnical Engineering (Instituto Superior Técnico).

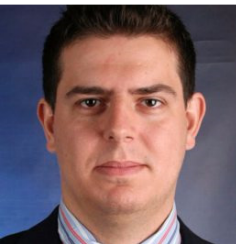
More than 30 years of professional experience in software development. More than 20 years as programming consultant and trainer. Main research interests and competencies: software engineering with object oriented programming languages, knowledge management, network analysis.

Author of a data science book and author/co-author of several technical book chapters and international scientific communications.



João Paulo Magalhães

Professor and researcher at ESTG - Porto Polytechnic, a researcher at CISUC- University of Coimbra, and the director of the Licenciatura in Computer and Networks Security at ESTG. He holds a PhD in dependable systems from University of Coimbra and is author of several scientific publications in dependability and cybersecurity. He keeps a close relationship with the industry, being the CTO at Globinnova Cyber Intelligence (Malware Analysis, Digital Vigilance, Big Data Security). Previously, João worked as team coordinator and sysadmin (UNIX) at SONAE.



Sérgio Nunes

Pursuing the PhD in Information Systems Management from ISEG (thesis delivered and waiting discussion). Bachelors in Computer Engineering, a Masters in Information Security (FCUL), and a Masters in Information Security from Carnegie Mellon University, USA. Assistant Professor at the Atlantica University Higher Institution and University of Lisbon. More than ten years' experience as a consultant in the fields of information systems management, IT audits and information security. Several professional certificates from organizations such as: CISSP, CISA, CISM, CEH, CPTS, APOGEP/IPMA-D, COBIT, ITIL.



José Casinha

Professional with more than 20 years of experience in the areas of Information Security Management and Service Management, in telecommunication service providers, computer technologies and software manufacturers. Collaborated with the Ministry of Education, FCCN with Oni Telecom and is currently Chief Information Security Officer of Outsystems. ISO27001 Lead Auditor, CISA (Certified Information Systems Auditor), ISO22301 Lead Implementer, ISO 20000 Lead Auditor, ITIL V3 Certificate and PMP (Project Management Professional).

Member of CT-163 Information Security on ISO / IEC JTC1 SC27. Deeply knowledgeable of leadership processes of ISMS and BCMS implementations in the financial and telecommunications industries. Degree in Computer Science and an MBA in Management, associating technology and business alignment skills with his technological profile.



Pedro Machado

Data Protection Officer of a lead European financial group, responsible for data protection in 7 leading insurance companies. Previously he worked for Vodafone Portugal in risk management, corporate security and privacy management. Professor at Universidade Europeia, and he was lecturer at Universidade Fernando Pessoa and EdEA. He is trainer of international certifications at Grupo Rumos. Master in Management and International Business Administration and post-graduate in Foreign Trade and International Marketing from the Universidad Politécnica de Madrid (UPM). He holds an MBA and a degree in Computer Science and another degree in Multimedia Engineering. Certified in Project Management by IPMA and PRINCE2, ITIL, ISO/IEC 27002, C|PTE (Certified Penetration Testing Engineer), CIW Security Analyst, and others. Author of several articles and key-speaker in national and international security events. Board Member and Head of Cyber Committee Board of AFCEA Portugal. In the past 20 years he worked for some of the world's largest technology manufacturers, participating in complex projects in both the public and private sector.



Daniel Caçador

With an experience around 30 years in the world of information technologies, began his career as the responsible for the development of IT solutions at NCR Portugal. Later, moved to Caixa Económica Montepio Geral where he participated in the development of projects and solutions as systems and communications architect and project manager. Later, was responsible for the Distributed Systems and Communications Office, managing and coordinating communications, systems and information security areas. Currently is responsible for the Information Security area of a financial institution, having as main functions the coordination and management of the Global Security Plan, IT risk management, development of Information Security policies and processes, coordination and management of Information Security Incidents. Certificate in ITIL 2011 and COBIT 5. Member of CT-163 Information Security in ISO / IEC JTC1 SC27. Speaker at various national and international events. Was a professor at several universities teaching subjects in the area of Informatics engineering and cybersecurity. Graduated in Electrotechnical Engineering - Systems and Communications, holds a postgraduate degree in Computer Engineering from the Faculty of Sciences and Technology of the New University of Lisbon, Postgraduate in Information Systems Security, Postgraduate in Audit in Information Systems and Masters in Information Systems Security.