

# Pós-Graduação em Cybersecurity

Instituto Politécnico de Santarém | Claranet

Esta formação tem como objetivo a capacitação de ativos do mercado de trabalho. Os destinatários da formação procuram o reforço das suas competências em conhecimentos vulgarmente associados à cibersegurança, como sejam a determinação do risco e a deteção de vulnerabilidades, a resposta a incidentes e o contexto regulamentar vigente, entre outros de alcance idêntico. Por seu turno, de um ponto de vista mais determinado tecnicamente, procura-se ainda fixar fundamentalmente sobre um contexto organizacional, as noções relativas a arquiteturas seguras e ao papel dos algoritmos criptográficos e das demais técnicas estabelecidas na concepção e na exploração de sistemas e tecnologias de informação entre outras aprendizagens relevantes.

Desenvolvida em parceria com a Claranet, o curso de Pós-graduação em **Cybersecurity** visa desenvolver um elevado nível de conhecimentos e de competências relevantes para aqueles que desempenham funções em áreas técnicas, associadas aos currículos e certificações de indústria com maior implantação permitem melhorar a visibilidade da oferta formativa e elevar o perfil técnico de saída dos estudantes.

## Principais características da pós-graduação

- Duração de **175 horas | 25 ECTS**
- Formação com componente prática com experimentação de natureza laboratorial;
- Acesso a certificações da indústria:
  - **CompTIA A+**
  - **CompTIA Security +**
  - **ISO 27001**
  - **CEH - Certified Ethical Hacker (EC-Council)**

|                                 |                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ► <b>CURSO</b>                  | <b>Pós-graduação em Cybersecurity</b>                                                                                                                                                                                                                                                                                                                                  |
| ► <b>FORMATO</b>                | <b>Híbrido (Presencial + a Distância)</b>                                                                                                                                                                                                                                                                                                                              |
| ► <b>CARGA HORÁRIA TOTAL</b>    | <b>175h   25 ECTS</b>                                                                                                                                                                                                                                                                                                                                                  |
| ► <b>CERTIFICAÇÕES OFICIAIS</b> | CompTIA A+<br>CompTIA Security +<br>ISO 27001<br>CEH - Certified Ethical Hacker (EC-Council)                                                                                                                                                                                                                                                                           |
| ► <b>DESTINATÁRIOS</b>          | Profissionais inseridos no mercado de trabalho (em todos os setores de actividade) em conteúdos relacionados com o (re)conhecimento de equipamentos, serviços de rede e outras soluções de gestão de infraestrutura, considerando a exploração de sistemas em operação e o processo de identificação e mitigação de vulnerabilidades de segurança em redes e sistemas. |
| ► <b>PRÉ-REQUISITOS</b>         | <ul style="list-style-type: none"><li>• Formação superior na área de informática ou áreas afins;</li><li>• Conhecimentos de língua inglesa;</li><li>• Conhecimentos de Informática (Sistemas e Redes; Algoritmos Criptográficos).</li></ul>                                                                                                                            |
| ► <b>OBJETIVOS GERAIS</b>       | <ul style="list-style-type: none"><li>• Determinar os objetivos e as capacidades das tecnologias de segurança informática, aplicada em contextos e ambientes de rede e respetivos serviços, num cenário promiscuo, heterogéneo e complexo.</li><li>• Identificar as técnicas, as ferramentas e os sistemas que contribuem para a redução de riscos.</li></ul>          |

- Conhecer e implementar os padrões e boas práticas, aplicando metodologias de gestão do risco e os recursos empregues em cenários de ataque, considerando a existência de sistemas críticos num plano organizacional.
- Implementação de sistemas e ferramentas e usar conceitos para minimizar os riscos associados ao uso de tecnologias e de redes numa organização, para a gestão das funções de segurança em contexto da ameaça cibernética.
- Desenvolver as políticas e os procedimentos necessários para mitigar os efeitos de potenciais ou efetivos ataques cibernéticos, com a preservação das funções críticas e o desencadear dos procedimentos de continuidade sobre os recursos e as infraestruturas de comunicações.

## ► MÓDULO 1

### CompTIA A+

28 horas | 4 ECTS

#### Additional information:

CompTIA A+ is the preferred qualifying credential for technical support and IT operational roles. CompTIA A+ certified professionals are proven problem solvers.

They support today's core technologies from security to cloud to data management and more.

CompTIA A+ is the industry standard for launching IT careers in today's digital world.

To receive the CompTIA A+ certification, learners must pass two exams:

- Core 1 (220-1101)
- Core 2 (220-1102)

## Tópicos

- Supporting Operating Systems
- Installing and Configuring PC Components
- Installing, Configuring, and Troubleshooting Display and Multimedia Devices
- Installing, Configuring, and Troubleshooting Storage Devices
- Installing, Configuring, and Troubleshooting Internal System Components
- Installing, Configuring, and Maintaining Operating Systems Maintaining and Troubleshooting Microsoft Windows
- Network Infrastructure Concepts
- Configuring and Troubleshooting Networks
- Managing Users, Workstations, and Shared Resources
- Implementing Client Virtualization and Cloud Computing
- Security Concepts
- Securing Workstations and Data
- Troubleshooting Workstation Security Issues
- Supporting and Troubleshooting Laptops Supporting and Troubleshooting Mobile Devices
- Installing, Configuring, and Troubleshooting Print Device
- Implementing Operational Procedures

## ► MÓDULO 2

### CompTIA Security+

42 horas | 6 ECTS

#### Additional information:

The Official CompTIA Security+ Instructor and Student Guides (SY0-601) have been developed by CompTIA for the CompTIA certification candidate.

Rigorously evaluated to validate coverage the CompTIA Security+ (SY0-601) exam objectives,

The Official CompTIA Security+ Instructor and Student Guides teach students the knowledge and skills required to:

- Assess the security posture on an enterprise environment and recommend and implement appropriate security solutions.
- Monitor and secure hybrid environments, including cloud, mobile and IoT.
- Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance.

## Tópicos

- Comparing and Contrasting Attacks
- Comparing and Contrasting Security Controls
- Using Security Assessment Tools
- Comparing and Contrasting Basic Concepts of Cryptography
- Implementing Public Key Infrastructure
- Implementing Identity and Access Management Controls
- Managing Access Services and Accounts
- Implementing Secure Network Architecture Concepts
- Installing and Configuring Security Appliances
- Installing and Configuring Wireless and Physical Access Security Deploying Secure Hosts Embedded, and Mobile Systems
- Implementing Secure Network Access Protocols
- Implementing Secure Network Applications
- Explaining Risk Management and Disaster Recovery Concepts
- Summarizing Secure Application Development Concepts
- Explaining Organizational Security Concepts

- Identify, analyze and respond to security events and incidents.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>► <b>MÓDULO 3</b><br/> <b>ISO/IEC 27001 Foundation</b><br/> 21 horas   3 ECTS</p> <p><b>Additional information:</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p><b>Tópicos</b></p> <ul style="list-style-type: none"> <li>• The scope and purpose of ISO/IEC 27001 and how it can be used,</li> <li>• The key terms and definitions used in the ISO/IEC 27000 series</li> <li>• The fundamental requirements for an ISMS in ISO/IEC 27001 and the need for continual improvement.</li> <li>• The processes, their objectives, and high-level requirements.</li> <li>• Applicability and scope definition requirements.</li> <li>• Use of controls to mitigate IS risks.</li> <li>• The purpose of internal audits and external certification audits, their operation, and the associated terminology.</li> <li>• The relationship with best practices and with other related International Standards: ISO 9001 and ISO/IEC 20000.</li> </ul>                      |
| <p>► <b>MÓDULO 4</b><br/> <b>GDPR - General Data Protection Regulation</b><br/> 7 horas   1 ECTS</p> <p><b>Additional information:</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p><b>Tópicos</b></p> <ul style="list-style-type: none"> <li>• Introducing to Personal Data Concept.</li> <li>• Legitimacy and purpose limitations.</li> <li>• Responsibilities in data processing.</li> <li>• Requirements for personal data processing.</li> <li>• The Sensitive Data concept</li> <li>• Privacy by Design &amp; Privacy by Default</li> <li>• Data Protection on Companies.</li> <li>• IAPP professional certifications.</li> <li>• Right to be forgotten (RTBF), access to information, portability, correction and elimination.</li> <li>• "Data breach" and notifications to controller entity and citizens.</li> <li>• Personal data transfer to third countries.</li> <li>• The regulatory bodies.</li> <li>• The Information Technologies in supporting of GDPR.</li> </ul> |
| <p>► <b>MÓDULO 5</b><br/> <b>CyberSec First Responder</b><br/> 21 horas   3 ECTS</p> <p><b>Additional information:</b><br/> It is ideal for candidates who have been tasked with the responsibility of monitoring and detecting security incidents in information systems and networks, and for executing standardized responses to such incidents.</p> <p>The course introduces tools, tactics, and procedures to manage cybersecurity risks, defend cybersecurity assets, identify various types of common threats, evaluate the organization's security, collect and analyze cybersecurity intelligence, and remediate and report incidents as they occur.</p> <p>This course provides a comprehensive methodology for individuals responsible for defending the cybersecurity of their organization</p> | <p><b>Tópicos</b></p> <p>Network defense and incident response methods, tactics, and procedures industry frameworks:</p> <ul style="list-style-type: none"> <li>• NIST 800-61r2 (Computer Security Incident Handling Guide);</li> <li>• US-CERT's National Cyber Incident Response Plan (NCIRP);</li> <li>• Presidential Policy Directive (PPD)-41 on Cyber Incident Coordination;</li> <li>• NIST 800.171r2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations);</li> </ul>                                                                                                                                                                                                                                                                                    |
| <p>► <b>MÓDULO 6</b><br/> <b>Basic Web Hacking</b><br/> 14 horas   2 ECTS</p> <p><b>Additional information:</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p><b>Tópicos</b></p> <ul style="list-style-type: none"> <li>• Understanding the HTTP Protocol</li> <li>• Information Gathering</li> <li>• Username Enumeration &amp; Faulty Password Reset</li> <li>• Issues with SSL/TLS</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>This is an entry-level web application security testing course.</p> <p>This foundation course of “Web Hacking” familiarizes the attendees with the basics of web application and web application security concerns.</p> <p>Several tools and techniques, backed up by a systematic approach on the various phases of hacking will be discussed.</p>                                                                                                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• Authorization Bypass</li> <li>• Cross Site Scripting (XSS)</li> <li>• Cross Site Request Forgery (CSRF)</li> <li>• SQL Injection</li> <li>• External Entity (XXE) Attacks</li> <li>• Insecure File Uploads</li> <li>• Deserialization Vulnerabilities</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>► <b>MÓDULO 7</b><br/> <b>CEH - Certified Ethical Hacker</b><br/> 42 horas   6 ECTS</p> <p><b>Additional information:</b><br/> The Certified Ethical Hacker (CEH) provides an in depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures.</p> <p>It will teach you how hackers think and act so you will be better positioned to set up your security infrastructure and defend against attacks.</p> <p>By providing an understanding of system weaknesses and vulnerabilities, the CEH course helps students learn to protect their organizations and strengthen their security controls to minimize the risk of a malicious attack.</p> | <p><b>Tópicos</b></p> <ul style="list-style-type: none"> <li>• Introduction to Ethical Hacking</li> <li>• Foot-printing and Reconnaissance</li> <li>• Scanning Networks • Enumeration</li> <li>• Vulnerability Analysis</li> <li>• System Hacking</li> <li>• Malware Threats</li> <li>• Sniffing</li> <li>• Social Engineering</li> <li>• Denial-of-Service</li> <li>• Session Hijacking</li> <li>• Evading IDS, Firewalls, and Honeypots</li> <li>• Hacking Web Servers</li> <li>• Hacking Web Applications</li> <li>• SQL Injection</li> <li>• Hacking Wireless Networks</li> <li>• Hacking Mobile Platforms</li> <li>• IoT and OT Hacking</li> <li>• Cloud Computing</li> <li>• Cryptography</li> </ul> |