Claranet | **Claranet University**

POLITÉCNICO DE SANTARÉM | ignít

Pós-graduação em Cibersegurança

A Claranet University, em parceria com a Ignít e a Escola Superior de Gestão e Tecnologia de Santarém do Instituto Politécnico de Santarém (ESGTS-IPS), promove a Pós-graduação em Cibersegurança, com o objetivo de preparar os profissionais com um elevado nível de conhecimento e competências para lidar com as ameaças cada vez mais complexas de cibersegurança.

Numa altura em que a procura por profissionais altamente especializados continua a aumentar, a Claranet University e a Ignít uniram a sua elevada experiência na implementação de soluções de cibersegurança à oferta formativa da ESGTS-IPS nesta área.

A Pós-graduação em Cibersegurança propõe uma abordagem transversal aos riscos de cibersegurança e às formas mais inovadoras de os combater, incluindo técnicas, regulamentos e boas práticas que os profissionais poderão aplicar nos mais diversos contextos.

Principais características do curso:

- Duração de 175 horas;
- Atribuição de 25 ECTS;
- Formação com forte componente prática;
- Percurso formativo com quatro certificações oficiais integradas.

Se o contexto de aumento dos riscos de cibersegurança a nível global exige recursos humanos cada vez com melhor preparação, esta formação pretende dotar os profissionais com as melhores competências para construírem – ou consolidarem – uma carreira de sucesso na área da Segurança de Informação.

NOME DA FORMAÇÃO	**Pós-graduação em Cibersegurança**
FORMATO	**Virtual**
CARGA HORÁRIA TOTAL	**175 horas**
CERTIFICAÇÕES OFICIAIS	• CompTIA A+ • CompTIA Security • ISO 27001 • CEH – Certified Ethical Hacker
PRÉ-REQUISITOS	• Os participantes devem ter conhecimentos técnicos de informática e redes. • Os participantes devem igualmente ter bons conhecimentos de língua inglesa, atendendo ao facto de os manuais entregues durante a formação estarem neste idioma e os exames serem realizados em inglês.

claranet | Make modern happen®

POLITÉCNICO DE SANTARÉM | ignít | DGES | PRR | REPÚBLICA PORTUGUESA | Financiado pela União Europeia NextGenerationEU

OBJETIVOS GERAIS

- Dotar os profissionais com as competências necessárias para identificar ameaças e vulnerabilidades de segurança;
- Ministrar uma formação abrangente, que inclui componentes técnicas, regulamentos e boas práticas;
- Permitir aos alunos implementarem e gerirem, de forma autónoma, a segurança da informação numa organização.

PROGRAMA

Módulo 1 Comptia A+
(28 Horas)

Neste módulo serão adquiridas as competências e informação essenciais para instalar, atualizar, reparar, configurar, otimizar e manter preventivamente o hardware e software de computadores pessoais.

Este curso vai ajudar na preparação para os exames de certificação CompTIA A+ Core 1 e Core 2.

- Identificar os componentes de computadores pessoais;
- Identificar os componentes e funções fundamentais dos sistemas operativos dos computadores pessoais;
- Identificar as melhores práticas seguidas pelos técnicos profissionais;
- Instalar e configurar componentes dos computadores e dos sistemas;
- Manter e diagnosticar componentes periféricos;
- Diagnosticar componentes de sistemas;
- Instalar e configurar sistemas operativos;
- Manter e diagnosticar instalações do Microsoft Windows;
- Identificar tecnologias de rede;
- Instalar e gerir ligações de rede;
- Dar assistência a dispositivos de computação móvel;
- Dar assistência a impressoras e digitalizadores;
- Identificar conceitos de segurança no âmbito da computação pessoal;
- Dar assistência à segurança de computadores pessoais.

Módulo 2 CompTIA Security
(42 Horas)

Este módulo apresenta o tema da segurança das redes e a sua relação com outras áreas das TI.
Será uma introdução à componente de Segurança, ou um estágio inicial para estudos mais especializados em segurança.
Ao longo do curso, será possível distinguir as áreas funcionais associadas às funções de Segurança da Informação.

Nos primeiros módulos, os alunos terão oportunidade de realizar atividades práticas com ferramentas e software de segurança cibernética, antes de prosseguirem com os conceitos de gestão de identidade e acesso à infraestrutura, e design do sistema de segurança. O curso termina com conceitos de gestão de risco, desenvolvimento seguro de software e políticas organizacionais de segurança.

Este módulo vai ajudar na preparação para o exame de certificação CompTIA Security SY0-601.

- Identificar conceitos fundamentais de segurança informática;
- Identificar ameaças e vulnerabilidades de segurança em:
  - redes;
  - aplicações, dados e máquinas;
  - controlo de acessos, autenticação e gestão de contas;
  - gestão de certificados;
- Lidar com questões de cumprimento de regras e normas de operação;
- Identificar problemas de gestão do risco;
- Gerir incidentes de segurança;
- Contribuir para o planeamento da continuação do negócio e da recuperação de desastres.

Módulo 3 ISO/IEC27001 Foundation
(21 Horas)

O módulo ISO/IEC 27001 Foundation tem como tema principal a norma ISO 27001 – Segurança da Informação.

A Segurança da Informação está relacionada com a proteção de todos os ativos de informação e infraestruturas de suporte (tecnológicos, humanos e financeiros), no sentido de preservar e rentabilizar o valor que possuem para a organização.

Durante este módulo serão apresentados os diferentes tópicos relativos a um Sistema de Gestão de Segurança da Informação (SGSI), incluindo política de SGSI, procedimentos, medições de desempenho, compromisso de gestão, auditoria interna, revisão de gestão e melhoria contínua.

Este módulo vai ajudar na preparação para o exame de certificação ISO/IEC 27001.

- Compreender a implementação de um Sistema de Gestão de Segurança da Informação de acordo com a norma ISO 27001;
- Compreender a relação entre um Sistema de Gestão de Segurança da Informação (SGSI), a gestão de riscos, o controlo e a conformidade com os requisitos de diferentes partes interessadas da organização;
- Conhecer os conceitos, abordagens, normas, métodos e técnicas que permitem gerir de forma eficaz um SGSI;
- Adquirir o conhecimento necessário para contribuir para a implementação de um SGSI, conforme especificado na ISO 27001.

Módulo 4 RGPD – Regulamento Geral de Proteção de Dados
(7 Horas)

O Regulamento Geral de Proteção de Dados (RGPD) traz consigo vários desafios, tanto aos cidadãos como às organizações públicas e privadas.

A proteção das pessoas singulares relativamente ao tratamento de Dados Pessoais constitui um direito fundamental.

A rápida evolução tecnológica e a globalização trouxeram novos desafios em matéria de Proteção de Dados, exigindo um quadro mais sólido e homogéneo na União Europeia.

- Introdução ao conceito de dados pessoais;
- Legitimidade e limitações de propósito;
- Responsabilidades no tratamento de dados;
- Requisitos para o tratamento de dados pessoais;
- O conceito de dados sensíveis;
- Privacy by Design e Privacy by Default;
- A proteção de dados nas empresas;
- As certificações profissionais IAPP;
- Direito ao esquecimento, acesso à informação, portabilidade, correção e eliminação;
- "Data breach" e notificações à entidade de controlo e aos sujeitos;
- Transferência de dados pessoais para países terceiros;
- As entidades reguladoras;
- As Tecnologias da Informação como suporte ao Regulamento.

Módulo 5 CyberSec First Responder
(35 Horas)

Para todos os responsáveis pela monitorização e deteção de incidentes ao nível da cibersegurança, o módulo CyberSafe é fundamental para adquirir as competências fundamentais à resposta mais acertada para a sua resolução.

Este módulo abrange as funções dos responsáveis pela monitorização e deteção de incidentes de segurança em sistemas e redes de informação, bem como pela execução de uma resposta adequada a esses incidentes. Dependendo da dimensão da organização, o profissional poderá atuar sozinho ou integrar uma equipa de resposta a incidentes de segurança cibernética.
Serão apresentadas ferramentas e táticas para gerir riscos de segurança, identificar vários tipos de ameaças comuns, avaliar a segurança da organização, reunir e analisar inteligência de segurança e lidar com incidentes, à medida que ocorrem.
Por fim, o módulo promove uma abordagem abrangente de segurança, voltada para aqueles que estão na linha da frente de defesa.

- Avaliar o risco em ambientes informáticos e de rede;
- Analisar o cenário de ameaças à segurança cibernética;
- Analisar ameaças de reconhecimento para ambientes informáticos e de rede;
- Analisar ataques em ambientes informáticos e de rede;
- Analisar técnicas pós-ataque em ambientes informáticos e de rede;
- Implementar um programa de gestão de vulnerabilidades;
- Avaliar a segurança da organização por meio de testes de penetração;
- Recolha de Cybersecurity Intelligence;
- Análise de dados de registo;
- Realizar análise ativa de bens e redes;
- Responder a incidentes de cibersegurança;
- Investigar incidentes de segurança cibernética.

Módulo 6 CEH – Certified Ethical Hacker
(42 Horas)

A Certified Ethical Hacker (CEH) é a certificação de ethical hacking mais prestigiada e recomendada pelos empregadores a nível mundial.
É a certificação em cibersegurança mais desejada e representa uma das credenciais valorizadas e também exigidas para profissionais que administrem infraestruturas críticas.

Este módulo vai ajudar na preparação para o exame de certificação CEH – Certified Ethical Hacker v12, reconhecido como um padrão dentro da comunidade de segurança da informação.

- Introdução ao Ethical Hacking;
- Foot Printing e reconhecimento;
- Redes de digitalização;
- Enumeração;
- Análise de vulnerabilidade;
- Hacking de sistema;
- Ameaças de malware;
- Sniffing;
- Engenharia social;
- Denial-of-Service;
- Session hijacking;
- Evasão de IDS, Firewalls e Honeypots;
- Hackear Servidores Web;
- Hackear aplicações Web;
- SQL injection;
- Hackear redes wireless;
- Hackear plataformas móveis;
- IoT hacking;
- Cloud Computing;
- Criptografia.

Parceiros de Formação:

POLITÉCNICO DE SANTARÉM
ESCOLA SUPERIOR DE GESTÃO E TECNOLOGIA

ignít