Curso: Pós-Graduação: Cyber Security & Data Protection (PGCS&DP)

Duração: 162h
Área formativa: PG's & MBA's

Sobre o curso

Atualmente, a **Segurança da Informação é uma preocupação visível e crescente nas Organizações**. A competitividade empresarial é altamente dependente do acesso e da geração de mais e melhores informações. O perímetro das Organizações com o exterior é mais permissivo. Os processos de negócios são executados num contexto de troca contínua de informações com elementos externos no relacionamento com clientes e fornecedores.

Os hábitos sociais dos colaboradores mudaram o acesso às redes da Organização, usando os seus próprios dispositivos, nem sempre devidamente protegidos, tendo em consideração os seus dados pessoais, permitindo a criação de backdoors para dados corporativos, mesmo em comportamentos e atitudes aparentemente inofensivos.

Garantir a segurança cibernética e a conformidade, requere avaliação, implementação e manutenção contínuas. Organizações que não implementem práticas essenciais de segurança estão a reduzir significativamente a sua defesa legal em caso de violação.

O novo Regulamento Geral de Proteção de Dados (RGPD), que estabelece regras sobre os direitos de privacidade dos cidadãos, torna-se aplicável a partir de 25 de maio de 2018. Neste sentido, esta edição do curso de pós-graduação, aprofunda temas atuais e de relevância, como:

- Gestão e Governança da Segurança da Informação
- Proteção de Dados e Privacidade
- Segurança e Resiliência Cibernética

Desenvolvida ao abrigo do protocolo com a **Universidade Atlântica**, esta **Pós-graduação em Cyber Security & Data Protection** que tem como objetivo preparar os alunos para compreenderem os riscos, causas de ataques e ameaças de segurança que poderão afetar as Organizações, bem como, proporcionar os conhecimentos necessários para implementar um sistema de gestão de segurança, alinhado com as normas e objetivos de negócio, por forma a garantir a segurança da informação e os dados de uma Organização.

Composição
O programa do ciclo de estudos de Pós-Graduação em Cyber Security & Data Protection (PGCS&DP) é composta por dois ciclos de especialização, Especialização Information Security Governance and Management e Especialização Information Security Operation and Support que no seu conjunto

permitem aos alunos ficarem com uma visão alargada e detalhada dos conceitos e metodologias subjacentes à área de Cyber Segurança.

Os alunos que concluírem com sucesso esta Pós-graduação estão qualificados para implementar os padrões internacionais ISO 27001 (Sistema de Gestão de Segurança da Informação) e ISO 22301 (Sistema de Gestão de Continuidade de Negócios), para apoiar o processo de certificação da organização no âmbito de auditoria externa e também alcançar a Certificação Profissional ISO/IEC 27001.

Essas conquistas proporcionam às organizações a capacidade de gerir e proteger seus valiosos ativos de dados e de informação, além de aumentar a resiliência dos seus negócios e fortalecer o seu posicionamento do mercado.

Diploma de Estudos
Para conceder o diploma de Pós-Graduação em Cyber Security & Data Protection, os alunos devem completar as 12 unidades curriculares que fazem parte do programa. A avaliação de cada unidade curricular é geralmente realizada por um teste e trabalho final. A unidade é concluída com sucesso obtendo uma pontuação mínima de 10 valores.

Atribuição de ECTS
No âmbito da parceria com a Universidade Atlântica, esta Pós-graduação atribui 25 créditos ECTS (European Credit Transfer System).

Esta Pós-graduação oferece, desta forma, créditos para acesso a um Mestrado em Sistemas e Gestão de Tecnologia da Informação. Para este propósito, o estudante deve ter um diploma de graduação ou superior.

Objetivos
A Pós-graduação em Cyber Security & Data Protection é um programa de estudos totalmente alinhado com as necessidades atuais do mercado, dando aos alunos a capacidade de:

- Compreender os riscos relativos à segurança da informação que as organizações enfrentam nas suas atividades
- Responder aos desafios da proteção de dados e privacidade
- Implementar sistemas de gestão de segurança da informação alinhados com as metas e objetivos de negócio
- Compreender as causas dos ataques e identificar as ameaças à segurança da informação
- Ajudar no desenvolvimento de uma cultura organizacional para a segurança da informação
- Compreender e responder aos requisitos da nova lei de proteção de dados, permitindo às organizações alcançar a conformidade com o regulamento RGPD da UE.

Destinatários

Gestores, técnicos e consultores de sistemas e tecnologias da informação. Executivos interessados

em perceber a Segurança Cibernética, Proteção de Dados e Continuidade de Negócios, para aumentar a resiliência e trazer valor para as organizações. Recém-licenciados que desejam adquirir conhecimentos em Segurança da Informação para expandir suas possibilidades no mercado de trabalho

---

Pré-requisitos

As candidaturas à Pós-graduação em Cyber Security & Data Protection estão abertas a:

- Todos os que tenham um grau académico de licenciatura ou superior nas áreas científicas;
- Todos os profissionais com ou sem grau académico, cuja experiência seja considerada adequada para que o aluno tenha sucesso no curso e as turmas resultem homogéneas.

A seleção será sempre feita mediante análise curricular pela Coordenação Científica do curso, que pode chamar o candidato a uma entrevista presencial. Em qualquer dos casos, a decisão será sempre fundamentada e apresentada por escrito ao candidato.

Metodologia

A metodologia pedagógica utilizada envolve o desenvolvimento de conhecimentos e competências simultaneamente técnicos, profissionais e pessoais, através de técnicas expositivas e interativas integradas, utilizando estudos de casos e colocando em prática o conhecimento num ambiente que também encontramos em organizações típicas.

Pretende-se que os alunos se reconheçam e sejam reconhecidos como elementos capazes e diferenciadores, em ambientes profissionais nos quais estão integrados.

A Pós-Graduação em Cyber Security & Data Protection é composta por 12 unidades curriculares que são organizadas em 2 ciclos de especializações:

- Information Security Governance and Management
- Information Security Operation and Support

Programa

Ciclo de especialização Information Security Governance and Management

- Information Security Concepts and Risk Management (9 horas / 1 ECTS)
  - por: José Casinha, Chief Information Security Officer @ Outsystems
- Information Security Management (18 horas / 3 ECTS)
  - por: Virgínia Araújo, University Professor @ Atlântica
- Data Protection and Privacy (18 horas / 3 ECTS)
  - por: Pedro Machado, DPO @ Grupo Ageas Portugal
- Cyber Security and Cyber Resilience (15 horas / 2,5 ECTS)
  - por: Virgínia Araújo, University Professor @ Atlântica

- Governance and Compliance (9 horas / 1 ECTS)
  - por: Sérgio Nunes, University Professor @ Atlântica
- Business Continuity Management (12 horas / 2 ECTS)
  - por: José Casinha, Chief Information Security Officer @ Outsystems

Ciclo de especialização Information Security Operation and Support

- Secure Applications Development (18 horas / 3 ECTS)
  - por: Alexandre Barão, University Professor @ Atlântica
- Systems and Networks Security (15 horas / 2,5 ECTS)
  - por: Sérgio Nunes, University Professor @ Atlântica
- Cloud Security (9 horas / 1 ECTS)
  - por: José Casinha, Chief Information Security Officer @ Outsystems
- Security Incident Response (9 horas / 1 ECTS)
  - por: Daniel Caçador, IT Security Manager @ Caixa Económica Montepio Geral
- Cryptography and Penetration Testing (18 horas / 3 ECTS)
  - por: João Magalhães, CTO @ Globinnova Cyber Intelligence
- Auditing Information Systems and Forensics (12 horas / 2 ECTS)
  - por: Sérgio Nunes, University Professor @ Atlântica

Ciclo de especialização Information Security Governance and Management
Information Security Concepts and Risk Management

- Conceitos de Segurança de Informação
  - O que é Informação?
  - Tipos e classificação da informação.
  - Confidencialidade, Integridade e Disponibilidade
  - Princípios de segurança de informação
  - Fundamentos de Arquitetura de Segurança
  - O conceito de defesa em profundidade
- Gestão de Risco
  - Metodologias de gestão de Risco
  - Riscos e Ameaças
  - O processo de gestão de risco
  - Os standards ISO 27005 e ISO 31000

Information Security Management

- Introdução, Antecedentes e Definições
- Standards e Frameworks
- Família ISO/IEC 27000 e Publicações-chave
- Usar o ITIL para gerir a Segurança da Informação
- Usar o COBIT para gerir a segurança da informação
- Estabelecer e Planear a implementação de um SGSI
- Suportar e operar um Sistema de Gestão de Segurança da Informação
- Gerir e reportar Incidentes de Segurança
- Controlar, gerenciar e relatar segurança da informação
- Certificar a Organização e as Pessoas

Data Protection and Privacy

- Conceitos e definição de proteção e privacidade de dados
- Terminologia do Regulamento Geral de Proteção Geral de Dados

- Princípios da proteção de dados
- Categorias de dados pessoais
- Os direitos das pessoas
- Drivers e Processadores
- Design para proteção de dados
- Proteção de dados pessoais
- Procedimentos de Violação de Dados Relacionados
- Como conduzir uma Avaliação de Impacto de Proteção de Dados (DPIA)
- O papel do supervisor de proteção de dados (DPO)
- Transferir dados pessoais para fora da União Europeia
- Os poderes das autoridades de supervisão

Cyber Security and Cyber Resilience

- Introdução e Conceitos Chave
- Segurança Cibernética, Segurança da Informação, Resiliência Cibernética
- Ataques e ameaças cibernéticas
- Gestão de riscos
- Gestão da Resiliência Cibernética
- Estratégia de resiliência cibernética
- Desenho de resiliência cibernética
- Transição de Resiliência Cibernética
- Operação de resiliência cibernética
- Melhoria Contínua da Resiliência Cibernética

Governance and Compliance

- Planeamento de Segurança
- Estratégia de Segurança
- Governança de estruturas de segurança
- Arquitetura Empresarial de Segurança
- SDLC
- Conformidade com padrões de segurança

Business Continuity Management

- Business Impact Analysis
  - Identificação dos requisitos de continuidade de negócio
  - Definição de RTO e de POR
  - Elaboração de BIA (Business Impact Analysis)
- Business Continuity Plan
  - Plano de Continuidade de negócio
  - Os planos acessórios que compõem a estratégia de recuperação
  - IT Disaster Recovery Plan
- Estratégias de Disaster Recovery para infraestruturas de IT
- Arquiteturas IT de Alta Disponibilidade
- Cuidados no desenho de IT DRP

Ciclo de especialização Information Security Operation and Support
Secure Applications Development

- Conceitos chaves de Segurança e Internet

- Visão geral de Ameaças
  - Malware
  - Quebras de segurança
  - Negação de serviço
  - Ataques da Web
  - Sequestro de Sessão (Session Hijacking)
  - Envenenamento de DNS (DNS Poisoning)
  - Fraudes cibernéticas
- Analisando SQL Injection e outras técnicas de hacking
- Visão geral das ferramentas
- O ciclo de vida de desenvolvimento de software
- Aplicação de segurança através do SDLC
- Problemas na criação de aplicativos seguros
- Políticas de segurança e melhores práticas
- Análise de vulnerabilidades de rede

Systems and Networks Security

- Segurança dos sistemas operativos
- Autenticação segura
- Comunicações seguras
- Arquiteturas de segurança de rede
- Firewalls
- IDS
- Segurança de sistemas distribuídos
- Segurança IOT
- Segurança móvel

Cloud Security

- Conceitos de arquitetura e requisitos de desenho
  - NIST SP800-145
  - IaaS, PaaS, SaaS
  - Public Cloud, Private Cloud, Hybrid Cloud
- Segurança de dados da cloud
  - Ciclo de vida dos dados na Cloud
  - Gestão de direitos de informação
  - Prevenção de fugas de informação
  - Encriptação de dados
- Plataformas de Cloud
  - Hypervisors
  - Segurança da virtualização
  - Segurança de Perímetro
- Segurança de Aplicações na Cloud
  - Secure Software Lifecyle
  - Cloud threads
  - OWASP
- DevSecOps

Security Incident Response

- Gestão de incidentes de segurança

- Deteção de eventos e incidentes
- Vulnerabilidades de segurança
- Equipas de Resposta a Incidentes de Segurança de Computadores

Cryptography and Penetration Testing

- Criptografia
  - Cifras simétricas
  - Análise de frequências
  - Cifras assimétricas (Public Key Cryptography)
  - Funções de hash, assinatura digital e Message Authentication Codes
  - Autenticação e controlo de acessos
  - Certificados e infraestruturas de chave pública
- Testes de Penetração
  - Fases dos ataques
  - Reconhecimento
    - Footprinting
    - Exploração
    - Enumeração
  - Hacking de sistemas
  - Testes de penetração

Auditing Information Systems and Forensics

- Princípios de Sistemas de Informação de Auditoria
- Comportamento e Perfil do Auditor
- Metodologias de Auditoria
- Gestão da equipe de auditoria
- Recolha de informações
- Escrever e apresentar um relatório de auditoria
- Evidência CoC (Chain of Custody)
- Ciclo de vida de evidências
- Ferramentas forenses