



CYBER SECURITY
& DATA PROTECTION

CIBERSEGURANÇA
& PROTEÇÃO DE DADOS

Pos-Graduação



CIBERSEGURANÇA & PROTEÇÃO DE DADOS

Coordenação Científica

Virgínia Araújo

Parceria

Escola Universitária
Atlântica

www.uatlantica.pt

Créditos

25 ECTS (European Credit Transfer System)

Apresentação

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 funcionários dentro das organizações mudaram o acesso às redes da organização usando os seus próprios dispositivos, nem sempre devidamente protegidos tendo em consideração seus dados pessoais, permitindo a criação de *backdoors* para dados corporativos, mesmo em comportamentos e atitudes aparentemente inofensivos.

Garantir a cibersegurança e a conformidade, requiere avaliação, implementação e manutenção contínuas. Organizações que não implementam práticas essenciais de segurança estão a reduzir significativamente a sua defesa legal em caso de violação. O novo Regulamento Europeu GDPR (Regulamento Geral de Proteção de Dados), que estabelece regras sobre os direitos de privacidade dos cidadãos, torna-se aplicável a partir de 25 de maio de 2018.

Neste sentido, esta nova 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
- Cibersegurança e Resiliência

Em nome da parceria com a Atlântica, esta pós-graduação atribui créditos ECTS (European Credit Transfer System)

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

Principais Benefícios

A Pós-Graduação em Cibersegurança e Proteção de Dados, 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 GDPR da UE.

Professional Certification:

Os alunos que concluírem com sucesso o 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.

Grupos alvo

- Gestores, técnicos e consultores de sistemas e tecnologias da informação

- Executivos interessados em perceber a Cibersegurança, 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.

Requisitos de Entrada

A candidatura à pós-graduação em Cibersegurança & Proteção de Dados está aberta a indivíduos com grau académico de licenciatura ou superior nas áreas científicas e a 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 colocando em prática o conhecimento num ambiente encontrado 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 Cibersegurança e Proteção de Dados é composta por 12 unidades curriculares que são organizadas em 2 ciclos de especializações:

1. Gestão e Governança da Segurança da Informação
2. Operação e Suporte à Segurança da Informação

Requisitos para obter o Diploma

Para conceder o diploma de pós-graduação em Cibersegurança e Proteção de Dados, os alunos devem completar as 12 unidades curriculares que fazem parte do programa.

Acesso a outros cursos

Este curso de pós-graduação oferece 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.

Regras de Avaliação

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.

Plano Curricular

ESPECIALIZAÇÃO	UNIDADE CURRICULAR	DOCENTE	Horas	ECTS
GESTÃO E GOVERNANÇA DA SEGURANÇA DE INFORMAÇÃO	• Conceitos de Segurança de Informação e Gestão de Risco	José Casinha	9	1
	• Gestão de Segurança de Informação	Virgínia Araújo	18	3
	• Proteção de Dados e Privacidade	Pedro Machado	18	3
	• Cibersegurança e Resiliência	Virgínia Araújo	15	2,5
	• Governança e Conformidade	Sérgio Nunes	9	1
	• Gestão de Continuidade de Negócio	José Casinha	12	2

ESPECIALIZAÇÃO	UNIDADE CURRICULAR	DOCENTE	Horas	ECTS
OPERAÇÃO E SUPORTE à SEGURANÇA DE INFORMAÇÃO	• Criptografia e Testes de Penetração	João Magalhães	18	3
	• Desenvolvimento de Aplicações Seguras	Alexandre Barão	18	3
	• Segurança de Sistemas e Redes	Sérgio Nunes	15	2,5
	• Segurança na Nuvem	José Casinha	9	1
	• Resposta a Incidentes de Segurança	Daniel Caçador	9	1
	• Auditoria de sistemas de informação e análise forense	Sérgio Nunes	12	2

Unidades Curriculares

GESTÃO E GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Conceitos de Segurança de Informação e Gestão de Risco

José Casinha

- Esta UC apresenta as seguintes competências:
Saber contextualizar a temática da segurança da informação nas organizações e identificar as áreas de atuação do profissional de segurança de informação. Perceber os conceitos básicos de gestão de risco relacionados com a segurança de informação. Identificar os objetivos dos referenciais, ISO 27001, ISO 27005 e ISO 31000. Desenhar um sistema de gestão de risco de acordo com o apetite de risco da organização.
- Programa
Conceitos de Segurança de Informação
O que é Informação?
Tipos e classificação da informação.
Confidencialidade, Integridade and 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

Virgínia Araújo

- Esta UC apresenta as seguintes competências:
Saber definir e manter um sistema de gestão da segurança da informação recorrendo às melhores práticas e normas internacionais, saber diagnosticar os riscos decorrentes de uma quebra de segurança de informação e a melhor forma de a gerir no contexto de uma organização, saber como alcançar e manter uma certificação internacional ISO/IEC 27001 na organização.
- Programa
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

Pedro Machado

- Esta UC apresenta as seguintes competências:
Saber definir e manter um programa de proteção de dados, recorrendo às melhores práticas e normas internacionais. Saber diagnosticar os riscos decorrentes de uma violação de dados pessoais e a melhor forma de a gerir no contexto de uma organização. Saber assumir o papel de DPO independentemente do contexto/dimensão/organização.
- Programa
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

Cibersegurança e Resiliência

Virginia Araújo

- **Esta UC apresenta as seguintes competências:**
Perceber o propósito, os benefícios e conceitos Cibersegurança, Segurança da Informação, Ciber Resiliência no contexto da sociedade atual, saber identificar ataques e ameaças e diagnosticar os riscos decorrentes de uma quebra de segurança de informação e cibersegurança, conhecer as atividades principais para a implementação e manutenção de um sistema de gestão da Ciber Resiliência na organização.
- **Programa**
Introdução e Conceitos Chave
Cibersegurança, Segurança da Informação, Ciber Resiliência
Ciber Ataques e Ameaças
Gestão de riscos
Gestão da Ciber Resiliência
Estratégia de Ciber Resiliência
Desenho de Ciber Resiliência
Transição de Ciber Resiliência
Operação de Ciber Resiliência
Melhoria Contínua da Ciber Resiliência

Governance and Compliance

Sérgio Nunes

- Esta UC apresenta as seguintes competências:
Saber planear a segurança de informação, definir uma estratégia de segurança da informação, governar a estrutura de segurança da informação, avaliar a arquitetura empresarial de SI e avaliar a conformidade com standards de SI.
- Programa
Planeamento de Segurança
Estratégia de Segurança
Governança de estruturas de segurança
Arquitetura Empresarial de Segurança
SDLC
Conformidade com padrões de segurança

Business Continuity Management

José Casinha

- Esta UC apresenta as seguintes competências:

Desenhar uma estratégia que permita avaliar a análise de impacto no negócio das atividades de uma organização. Identificar os vários planos necessários para elaborar uma estratégia de recuperação de negócio em caso de interrupção. Conhecer as várias opções para recuperação das infraestruturas de IT de acordo com o RTO e RPO definidos para as várias atividades da organização.

- Programa

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

Secure Applications Development

Alexandre Barão

- Esta UC apresenta as seguintes competências:
Conhecer conceitos-chave de segurança e tipos de ameaças mais frequentes, identificar técnicas de defesa e mitigação de riscos em contexto de desenvolvimento de software. Compreender o ciclo de vida de desenvolvimento de software e neste contexto, identificar problemas na criação de aplicativos seguros.
- Programa
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)
Cyber Frauds
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 network security

Sérgio Nunes

- Esta UC apresenta as seguintes competências:
Definir e avaliar a segurança de um sistema operativo, definir e avaliar a segurança de uma rede de computadores.
- Programa
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

José Casinha

- Esta UC apresenta as seguintes competências:
Conhecer as várias opções de serviços cloud. Identificar os serviços que melhor se adequam às necessidades do negócio. Desenvolver capacidades de desenho de serviços seguros de cloud.
- Programa
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 Lifecycle
Cloud threads
OWASP
DevSecOps

Security Incident Response

Daniel Caçador

- Esta UC apresenta as seguintes competências:
Conhecer modelos, metodologias e práticas mais atuais na área da disciplina e sua aplicação. Construção e gestão de planos de resposta a incidentes de segurança, emergência, contingência, recuperação de desastre (Disaster Recovery) e o respetivo enquadramento na continuidade de negócio das organizações. Criação e preparação de equipas e desenvolvimento de processos para a resposta a incidentes de segurança de diversas naturezas. Resiliência organizacional e Gestão de crises.
- Programa
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

João Paulo Magalhães

- Esta UC apresenta as seguintes competências:

Compreender os principais conceitos relacionados com a segurança informática, a importância da criptografia e enunciar sistemas criptográficos, enunciar e entender diferentes sistemas de autenticação e controlo de acesso, compreender a importância das entidades de segurança, identificar as vulnerabilidades mais comuns numa rede informática, projetar, instalar e utilizar mecanismos de proteção contra vulnerabilidades, identificar as causas mais comuns de intrusões numa rede informática, projetar, instalar e utilizar mecanismos/soluções de deteção de intrusões.

- Programa

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

Process of Auditing Information System and Forensics

Sérgio Nunes

- Esta UC apresenta as seguintes competências:
Perceber como auditar um sistema de informação, perceber como executar uma análise forense.
- Programa
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

DOCENTES



Virgínia Araújo

Doutoramento em Engenharia de Software, Licenciatura em Matemática e Informática e diversas certificações profissionais, nomeadamente ITIL EXPERT, ISO/IEC 20000 PRACTITIONER, ISO/IEC 27001 PRACTITIONER, PMP, PRINCE2 PRACTITIONER, LEAN IT, COBIT, BIG DATA e DEVOPS. Mais de 20 anos de experiência profissional em tecnologias e sistemas de informação, consultora sénior e formadora acreditada por diferentes Institutos de Exame internacionais, nomeadamente APMG, PEOPLECERT, EXIN. Especializada em Gestão de Segurança de Informação, Gestão e Governança de Serviços e Gestão de Projetos na Europa, África e Ásia. Professora da Escola Universitária Atlântica, membro do grupo de investigação em Gestão do Conhecimento e Engenharia de Software, membro do Comité Científico da Conferência Ibérica de Sistemas e Tecnologias de Informação, membro do Comité Científico do Congresso Ibero-americano de Investigação Qualitativa. Professora convidada em diferentes universidades, oradora em congressos internacionais e autora de artigos publicados em revistas especializadas. Distinguida em 2017 pela AXELOS Inc. mulher líder em ITSM (IT Service Management).



Alexandre Barão

Doutoramento em Sistemas de Informação e Engenharia Informática (Instituto Superior Técnico) e MsC em Engenharia Informática e Eletrotécnica (Instituto Superior Técnico).

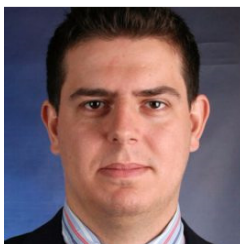
Mais de 30 anos de experiência profissional em desenvolvimento de software. Mais de 20 anos como consultor e instrutor de programação. Principais interesses e competências de pesquisa: engenharia de software com linguagens de programação orientada a objetos, gestão do conhecimento, análise de redes.

Autor de um livro de ciência de dados e autor/coautor de vários capítulos de livros técnicos e comunicações científicas internacionais.



João Paulo Magalhães

Doutoramento em sistemas confiáveis da Universidade de Coimbra e autor de várias publicações científicas sobre segurança e cibersegurança. Professor e investigador na ESTG - Politécnico do Porto, investigador do CISUC Universidade de Coimbra, e diretor da Licenciatura em Segurança de Redes e Computadores na ESTG. Mantém um relacionamento próximo com a indústria, sendo o CTO da Globinnova Cyber Intelligence (Análise de Malware, Vigilância Digital, Big Data Security). Anteriormente, trabalhou como coordenador de equipa e administrador de sistemas (UNIX) na SONAE.



Sérgio Nunes

A concluir o doutoramento em Gestão de Sistemas de Informação pelo ISEG (tese entregue e discussão em espera). Licenciatura em Engenharia de Computação, Mestre em Segurança da Informação (FCUL) e Mestre em Segurança da Informação pela Carnegie Mellon University, EUA. Professor Auxiliar na Universidade Atlântica e na Universidade de Lisboa. Mais de dez anos de experiência como consultor nos campos de gestão de sistemas de informação, auditorias de TI e segurança da informação. Vários certificados profissionais de organizações tais como: CISSP, CISA, CISM, CEH, CPTS, APOGEP / IPMA-D, COBIT, ITIL.



José Casinha

Profissional com mais de 20 anos de experiência nas áreas de Gestão de Segurança da Informação e Gestão de Serviços, em prestadores de serviços de telecomunicações, tecnologias de computação e fabricantes de software. Colaborou com o Ministério da Educação, a FCCN na Oni Telecom e atualmente é Chief Information Security Officer da Outsystems. ISO27001 Lead Auditor, CISA (Certified Information Systems Auditor), ISO22301 Lead Implementer, ISO 20000 Lead Auditor, ITIL V3 Certificate and PMP (Project Management Professional). Membro do CT-163 Information Security na ISO/IEC JTC1 SC27. Conhecedor profundo de processos de liderança de implementações de SGSI e BCMS nos setores financeiro e de telecomunicações. Formado em Ciências da Computação e possui MBA em Gestão, associando habilidades de alinhamento de tecnologia e negócios com seu perfil tecnológico.



Pedro Machado

Responsável pela proteção de dados de um grupo financeiro europeu líder, responsável pela proteção de dados em 7 empresas líderes de seguros. Anteriormente, trabalhou para a Vodafone Portugal em gestão de risco, segurança corporativa e gestão de privacidade. Professor da Universidade Europeia, foi professor na Universidade Fernando Pessoa e EdEA. Formador de certificações internacionais no Grupo Rumos. Mestre em Administração e Administração de Negócios Internacionais e pós-graduado em Comércio Exterior e Marketing Internacional pela Universidade Politécnica de Madrid (UPM). MBA, licenciado em Informática e em Engenharia Multimedia. Certificado em Gestão de Projetos pelo IPMA e PRINCE2, ITIL, ISO/IEC 27002, Certified Penetration Testing Engineered (CPTE), CIW Security Analyst e outros. Autor de diversos artigos e orador em eventos nacionais e internacionais de segurança. Board member e head of do Comité de Cibersegurança da AFCEA Portugal. Nos últimos 20 anos, trabalhou para alguns dos maiores fabricantes de tecnologia do mundo, participando em projetos complexos nos setores público e privado.



Daniel Caçador

Com uma experiência de cerca de 30 anos no mundo das tecnologias de informação, iniciou a carreira como responsável pelo desenvolvimento de soluções de TI na NCR Portugal, tendo posteriormente transitado para a Caixa Económica Montepio Geral onde participou no desenvolvimento de projetos e soluções como arquiteto de sistemas e comunicações e gestor de projetos. Mais tarde assumiu funções de responsável pelo Gabinete de Sistemas Distribuídos e Comunicações, com a gestão e coordenação das áreas de comunicações, sistemas e segurança da informação. Atualmente responsável da área de Segurança da Informação de uma instituição financeira, tendo como principais funções a coordenação e gestão do Plano Global de Segurança, a gestão de riscos de TI, o desenvolvimento de políticas e processos de Segurança de Informação, na coordenação de gestão de Incidentes de Segurança de Informação. Certificado em ITIL 2011 e COBIT 5. Membro do CT-163 Information Security na ISO/IEC JTC1 SC27. Orador em diversos eventos nacionais e internacionais. Foi professor em diversas universidades lecionando disciplinas na área da eng. Informática e cibersegurança. Formado em Engenharia Eletrotécnica - Sistemas e Comunicações, possui Pós-graduação em Eng. Informática pela Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa, Pós-graduação em Segurança em Sistemas de Informação, Pós-graduação em Auditoria em Sistemas de Informação e Mestrado em Segurança de Sistemas de Informação.