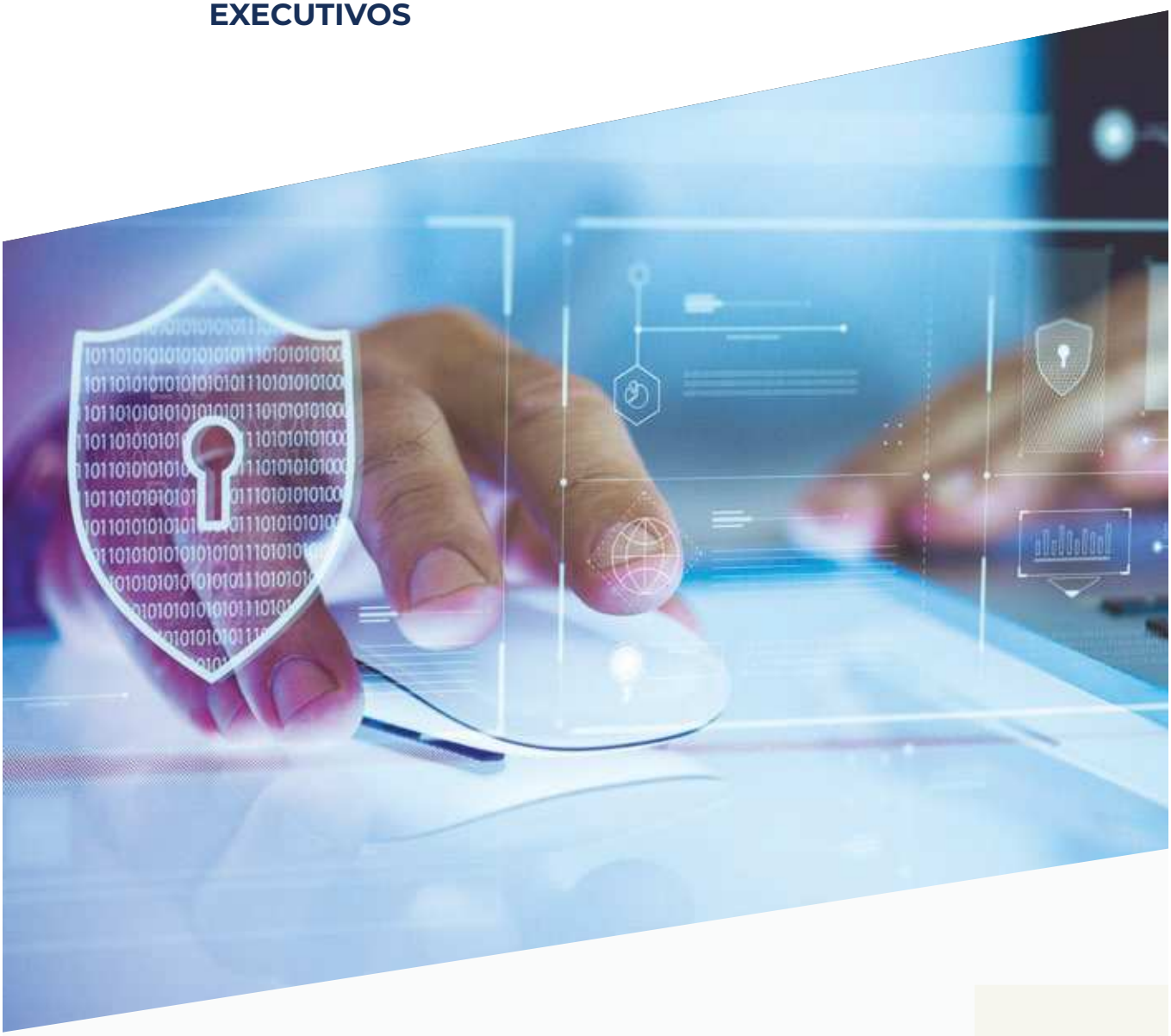
CATÓLICA LISBON
BUSINESS & ECONOMICS
EXECUTIVOS

TÉCNICO +
FORMAÇÃO AVANÇADA



CiberSegurança para Gestores

2 a 11 de dezembro de 2020

CiberSegurança para Gestores

O programa "CiberSegurança para Gestores" foi concebido conjuntamente entre a CATÓLICA-LISBON e o TÉCNICO+ com o objetivo de promover uma visão dos riscos atuais associados às Tecnologias de Informação e das práticas de Gestão destinadas a proteger as organizações, abordando componentes tecnológicas e humanas dos sistemas de informação, com especial atenção às suas vulnerabilidades. São também, identificados os riscos, assim como os recursos para os gerir, seguindo-se uma visão integrada da *governance* de todos esses recursos, com um foco particular nas pessoas. O programa termina com as atividades necessárias à criação de um plano de proteção dos sistemas informáticos no que diz respeito à CiberSegurança e também com um exercício da tomada de decisão sob pressão em caso de ataque.

A importância da CiberSegurança nas Organizações

A CiberSegurança é mais importante do que nunca, tendo em conta a recente mudança de paradigma social e laboral. As organizações e indivíduos estão ainda mais dependentes de dispositivos digitais, sendo a internet o principal canal para trabalhar, para o contacto e partilha de informações entre equipas, amigos e famílias. Esta situação leva, inevitavelmente, a um aumento da exposição a ciberataques. Alguns exemplos: em abril de 2020, a OMS informou que, desde o início da pandemia da COVID-19, houve um grande aumento no número de ciberataques direcionados aos seus colaboradores e em e-mails fraudulentos destinados ao público em geral; a Honda e a Life Healthcare foram também atingidas por ciberataques em junho de 2020. Estes ataques causam sérios danos, que vão desde a perda de receitas a pedidos de resgate por parte dos hackers, podendo ascender a milhões de euros.

Objetivos

- Compreender os sistemas de informação atuais e suas principais vulnerabilidades;
- Compreender a importância do fator humano na defesa da infraestrutura informática;
- Tomar contacto com a cultura de ataque aos sistemas de informação;
- Compreender a arquitetura da infraestrutura de sistema de informação a proteger;
- Tomar contacto com as principais técnicas, abordagens e tecnologias usadas na proteção dos sistemas;
- Saber como gerir o risco e o acesso às fontes de informação e organizações disponíveis para participar na defesa conjunta da infraestrutura tecnológica;
- Estar preparado para reagir a ataques aos sistemas de informação, nomeadamente na tomada de decisão em ambiente de crise;
- Conhecer as soluções de *governance* mais apropriadas e as funções necessárias à gestão da CiberSegurança;
- Saber desenhar e gerir um plano de CiberSegurança.

Destinatários

Este programa destina-se aos gestores de todos os setores que enfrentam o risco de exposição a ataques informáticos e que necessitem de ter o respetivo conhecimento do tema para participarem efetivamente na discussão dos problemas, análise de soluções e tomada de decisão.

- Alta direção
- Gestores da estratégia do negócio;
- Consultores;
- Chefes de projeto de transformação digital.

Destina-se também a outros interessados no tema.

Programa

O QUE É PRECISO SABER DE TECNOLOGIA PARA ABORDAR A CIBERSEGURANÇA

- Infraestruturas de TI;
- Internet e redes;
- Bases de dados.

Formadores: Pedro Adão
Duração: 3,5h
Atividade de ensino: Exposição

Este módulo destina-se a apresentar as principais Tecnologias da Informação e comunicação atuais, de modo a permitir compreender os problemas e as soluções de CiberSegurança: vulnerabilidades, proteções tecnológicas e processos. Serão destacados os potenciais alvos de ataques (tanto sistemas como dados).

O QUE É PRECISO SABER SOBRE CIBERSEGURANÇA

- Definição e âmbito;
- Vulnerabilidades técnicas;
- Fator humano;
- Ameaças típicas e o atual panorama de ameaças;
- Quadro legal.

Formadores: Miguel P. Correia
Duração: 3,5h
Atividade de ensino: Exposição

Este módulo define o que é a CiberSegurança e conceitos fundamentais como os de propriedades de segurança, vulnerabilidade, ataque e ameaça. Apresenta tanto vulnerabilidades técnicas como humanas, bem como os principais tipos de ameaças atuais.

COMO GERIR CIBERSEGURANÇA DE FORMA PROACTIVA

- Análise e gestão de risco;
- Análise prática de vulnerabilidades;
- Compreender os riscos e fazer uso da informação disponível.

Formadores: Rui Shantilal
Duração: 3,5h
Atividade de ensino: Exposição e exercícios

Este módulo fornece as bases das medidas a tomar por parte da organização para mitigar o risco de ataque e preparar potenciais respostas aos ataques.

OS MECANISMOS PRÁTICOS DE CIBERSEGURANÇA PARA MANAGERS

- Criptografia, certificados digitais e assinatura digital;
- Gestão de identidades, autenticação e controlo de acessos;
- Segurança de instalações e de centros de dados;
- Avaliação e gestão técnicas de Cibersegurança;
- Investigação forense.

Formador: Nelson Escravana
Duração: 3,5h
Atividade de ensino: Exposição e exercícios

O módulo apresenta os mecanismos tecnológicos de proteção contra ciberataques. O objetivo é compreender um conjunto de mecanismos que, embora não sejam implementados diretamente pelos gestores, são componentes fundamentais de uma solução de segurança.

GOVERNANCE DE CIBERSEGURANÇA

- Papel da gestão da segurança da informação;
- *Frameworks/standards* de melhores práticas de gestão de segurança da informação;
- Integrar a Cibersegurança na gestão organizacional: um problema de gestão;
- Organização para a Cibersegurança;
- Desenvolver uma cultura de Cibersegurança;
- Conceito de *security by design*;
- Métricas para a gestão de segurança da informação;
- Resposta a Incidentes: "Fui alvo de ataque e agora?" Simulação de caso concreto.

Formadores: Paulo Cardoso do Amaral
Duração: 3,5h
Atividade de ensino: Exposição e exercícios

Neste módulo irão ser abordados os aspetos fundamentais relativos à gestão de segurança da informação, contemplando as melhores práticas enquadradas numa *framework* holística de gestão da CiberSegurança que irá culminar com um exercício demonstrativo de um incidente e a sua Gestão.

COMO CONSTRUIR O SEU PLANO DE CIBERSEGURANÇA

- As melhores práticas de desenvolvimento de um plano de mitigação e gestão de riscos de cibersegurança;
- Pistas para desenvolver o seu plano de cibersegurança;
- Gap analysis e plano de mitigação;
- Exemplos práticos de planos de cibersegurança;
- A economia dos resgates (simulação de caso real de pedido de resgate).

Formadores: João Ribeiro da Costa
Duração: 3,5h
Atividade de ensino: Exposição e exercícios

O último módulo do Programa procura dar os elementos necessários aos participantes para poderem começar a estruturar o seu Plano de CiberSegurança.

Direção de Programa

Paulo Cardoso do Amaral

Professor da CATÓLICA-LISBON em Gestão da Informação, Gestão do Conhecimento, Competitive Intelligence, Estratégia Empresarial, Consultoria Empresarial e Transformação Digital. É ainda diretor e docente nos cursos Fintech Disruption Program e BlockChain & SmartContracts na Formação de Executivos. Licenciado em Eletrotecnia de Telecomunicações, Sistemas e Computadores pelo IST, doutorado em Sistemas de informação pela Universidade de Paris e MBA em Gestão internacional pela UCP. O seu doutoramento em sistemas distribuídos confere-lhe as bases práticas por detrás da Blockchain e outras DLTs. Tem lecionado disciplinas de MBA na China, França, Bélgica, Tunísia e Marrocos. É atualmente empreendedor na área da hotelaria e turismo, e administrador do Grupo ExpoMundo.
Foi administrador do Grupo Sinfic com o pelouro da Internacionalização, e diretor informático no Grupo CGD e na Portugal Telecom. É autor do livro "Top Secret" em inteligência Competitiva e co-autor do livro "Capital Conhecimento".

Miguel Pupo Correia

Professor Associado do Instituto Superior Técnico da Universidade de Lisboa e investigador sénior do INESC-ID. Esteve envolvido em vários projetos de investigação no âmbito da cibersegurança e privacidade, entre os quais se destacam os projetos europeus MAFTIA, CRUTIAL, ReSIST, TCLOUDS, PCAS e SafeCloud. Os seus principais interesses são: blockchain e consenso bizantino; segurança e confiabilidade da cloud; trusted computing; segurança de software; segurança e confiabilidade móvel; deteção de intrusões e big data analytics; e segurança de comunicações.

Docentes

Pedro Adão

Professor Auxiliar no Departamento de Engenharia Informática do Técnico, é Doutorado em Matemática pela Universidade Técnica de Lisboa em Métodos Formais para Análise de Protocolos de Segurança. Durante o doutoramento foi exchange-student na Universidade da Pennsylvania, EUA, e research-intern na Microsoft Research em Cambridge, Inglaterra. É Membro do Security and Quantum Information Group do Instituto de Telecomunicações e coordena a equipa de segurança STT (Security Team@Técnico), formada por alunos do Técnico, que participa em competições internacionais de segurança e que, atualmente, está classificada no top-50 mundial.

Nelson Escravana

Diretor da Área de Comunicações e Cibersegurança do INOV INESC Inovação, possui mais de 20 anos de experiência profissional em telecomunicações e segurança da informação, sendo consultor regular de diversas entidades nacionais e internacionais. É responsável pela realização de auditorias de segurança no âmbito da prevenção e resposta a incidentes, análise e conceção de soluções. Realiza, regularmente, ações de formação e seminários em cibersegurança tendo participado em mais de uma dezena de projetos europeus de I&D.

Rui Shantilal

Fundador e Managing Partner da Integrity, uma empresa da área da Segurança da Informação. Foi Director da prática de Segurança da OniTelecom e é Mestre em Segurança da Informação pela Universidade de Londres. Tem várias certificações: CISSP, CISA, ISO 27001 LA, entre outras.

João Ribeiro da Costa

Doutorado em Análise de Sistemas pela Universidade de Lancaster do Reino Unido. Admnistrador da Claranet Portugal. Co-fundador e Administrador da Guestcentric.
Foi sócio fundador da e-Chiron. Criou a Truewind-Chiron, empresa de que foi Presidente do Conselhode Administração. Foi investigador do LNEC. Foi Professor na Faculdade de Ciências da Universidade Nova de Lisboa, lecionou na Universidade Católica Portuguesa, na University of London (Wye College) e na Universidade de Parma.

Horário:
O programa decorre três vezes por semana, das 17h30 às 21h

Duração: 21 horas

Preço: 1900€

Local: CATÓLICA-LISBON

MAIS INFORMAÇÕES E CANDIDATURAS

Ana Marisa Santos

Email: ana.marisa.santos@ucp.pt

Tel: 214 269 846

www.clsbe.lisboa.ucp.pt/executivos/ciberseguranca