redencial
alv Aprendizagem ao Longo da Vida
POLÍCIA SEGURANÇA PÚBLICA
PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

[“Conhece o teu inimigo e conhece-te a ti próprio
e em cem batalhas nunca serás derrotado.

Se não conheces o teu inimigo e apenas te conheces a ti mesmo,
por cada vitória sofrerás uma derrota.

Se não conheces o teu inimigo nem te conheces a ti mesmo
serás derrotado em todas as batalhas.”

SunTzu, A Arte da Guerra, 400 a.c.]

ÍNDICE

MICROCREDENCIAIS

Segundo a Comissão Europeia, “microcredenciais” são qualificações que certificam resultados de aprendizagens resultantes de cursos curtos ou de módulos, tendo em vista a requalificação e atualização profissional de cada um. Estas qualificações podem ser obtidas pelos cidadãos com diversas modalidades de aprendizagem, presencial, a distância online ou mista.

Seja qual for o regime ou forma como são obtidas estas qualificações, a Comissão Europeia vê nas microcredenciais uma oportunidade de aprendizagem flexível e inclusiva, no contexto dos sistemas de ensino e formação europeus e uma nova forma de acreditação adequada a diferentes necessidades.

Estas qualificações, por norma de curta duração, serão essencialmente úteis para quem pretende complementar o seu conhecimento e competências ou para quem pretende requalificar-se, procurando novas oportunidades num mercado de trabalho em constante mudança.

Na sua essência as microcredenciais assentam e dão resposta ao conceito e à prática de uma “aprendizagem ao longo da vida”.

ENQUADRAMENTO

A Sociedade da Informação trouxe consigo novas ameaças e oportunidades no contexto da vida de pessoas, empresas, instituições, nações e regiões de todo o mundo. A segurança e a competitividade tornaram-se imperativos na realidade atual, tendo em conta que a presença digital é agora uma realidade incontornável para organizações, empresas e indivíduos.

A evolução tecnológica ofereceu inúmeras oportunidades de desenvolvimento e bem-estar, desburocratizando e acelerando processos, e permitindo alcançar públicos mais vastos para criar riqueza e desenvolvimento. Paralelamente, surgiu a necessidade de cibersegurança.

A cibersegurança engloba um conjunto de meios, de técnicas e de tecnologias, que visam proteger computadores, programas, redes e dados, de danos e intrusões. Por outro lado, visa capacitar pessoas com comportamentos e atitudes que salvaguardem a segurança da informação.

Deste modo, esta microcredencial procura identificar as ameaças do mundo digital e equipar os formandos com técnicas, comportamentos, atitudes e competências para neutralizar os efeitos dessas ameaças. O objetivo é proporcionar uma presença segura e consciente no mundo digital, evitando, mitigando ou anulando os riscos.

É neste contexto de ameaças e invasões, exacerbado pela recente pandemia, que a Universidade Aberta (UAb) organizou esta microcredencial em cibersegurança. Esta formação, a desenvolver em regime teórico-prático a distância (*e-learning*), é destinada especificamente à Polícia de Segurança Pública (PSP). Procura-se assim responder às necessidades específicas da PSP na Rede Nacional de Segurança Interna (RNSI), assegurando que os seus membros estejam bem equipados para aplicar as boas práticas informáticas e garantir a segurança digital dentro do seu domínio.

OBJETIVOS GERAIS

Os objetivos desta microcredencial são:

- Proporcionar conhecimentos e competências que permitam aos participantes caracterizar os ataques típicos bem como as defesas correspondentes, tecnológicas e procedimentais.
- Capacitar os participantes a identificar, reagir e proteger das principais ciberameaças.
- Proporcionar conhecimentos e competências fundamentais no uso de ferramentas e tecnologias para defesa às ciberameaças.
- Desenvolver competências para aplicar as boas práticas informáticas no domínio PSP da RNSI.
- Capacitar os participantes na gestão de passwords e na verificação da veracidade de emails recebidos.
- Proporcionar conhecimentos sobre a encriptação de dados e sobre as precauções a ter na utilização de recursos na cloud.

COMPETÊNCIAS

No final desta microcredencial, os formandos ficarão habilitados com um conjunto de ferramentas tecnológicas e procedimentais que lhes permitirão:

- Tomar ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.
- Aplicar as boas práticas informáticas no domínio PSP da RNSI, incluindo a gestão segura de passwords e a verificação da veracidade de emails recebidos.
- Utilizar efetiva e autonomamente as ferramentas para encriptação de dados e tomar as precauções adequadas ao usar recursos na cloud.

PROGRAMA E CONTEÚDOS

Esta microcredencial tem a duração de 65 horas (2,5 ECTS da UAb) e está estruturada em 5 módulos com a duração de uma semana cada. Os módulos desenvolvem-se sequencialmente. Estes módulos são precedidos de um módulo de ambientação ao contexto online do curso e de integração dos participantes, designado módulo 0 ou pré--curso.

A microcredencial realiza-se em regime de e-learning. Na Internet a microcredencial é suportado pela PlataformAbERTA em utilização na UAb e adaptada ao seu Modelo Pedagógico Virtual.

MÓDULOS	DESCRIÇÃO
0. Ambientação ao contexto online	Módulo que pretende uma socialização dos participantes e a familiarização com a utilização do software de gestão do curso.
1. Fundamentos de Cibersegurança	Neste módulo pretende-se passar a navegar na Internet de forma segura e reconhecer e reagir adequadamente às ciberameaças.
2. Encriptação de dados	Pretende proporcionar a capacidade de encriptar dados em suporte físico e em correio eletrónico.
3. Anatomia de um ciberataque	Proporcionar a perceção de como um agente malicioso pensa e as ações que pode desenvolver, com enfoque na recolha de informação (OSINT).
4. Ciberhigiene	Pretende proporcionar capacidades para adotar medidas de defesa ativa que melhorem a cibersegurança.
5. A PSP na Rede Nacional de Segurança Interna (RNSI)	Este módulo destina-se a habilitar os formandos com as boas práticas informáticas no domínio PSP da RNSI.

MÓDULO 0: AMBIENTAÇÃO AO CONTEXTO ONLINE

[Duração: 13 horas | 1 semana]

1. A PlataformAbERTA, *layout*, recursos e atividades
2. Ferramentas/funcionalidades da PlataformAbERTA

Objetivos do módulo

Este módulo tem por objetivos a socialização dos participantes e a criação de "um grupo" de trabalho online e a familiarização com a utilização do software de gestão do curso, a PlataformAbERTA, que integra l LMS Moodle.

Competências a adquirir

No final deste módulo, pretende-se que os formandos sejam capazes de:

- Interagir e comunicar com os colegas, com os formadores e com o interface de aprendizagem no sentido de conseguir resolver problemas básicos de interação, de comunicação;
- Explorar autonomamente e com eficácia todas as ferramentas e possibilidades da PlataformAbERTA, com o estatuto de formando.

Conteúdos programáticos

Unidade Didática 1: A PlataformAbERTA

O que é o LMS Moodle;

Formas de organizar espaços/sites no Moodle;

Recursos e atividades da plataforma Moodle;

Estrutura do espaço Moodle; tópicos do curso; recursos disponíveis eferramentas a utilizar.

Unidade Didática 2: Treino na exploração das ferramentas e recursos da plataforma

Treino com as ferramentas/funcionalidades fóruns, trabalhos, questionários, wikis, referendos, equipas, etc.

MÓDULO 1: FUNDAMENTOS DE CIBERSEGURANÇA

[Duração: 13 horas teórico-práticas | 1 semana]

1. Introdução à cibersegurança
2. Identidade digital e Informações de Identificação Pessoal (PII)
3. Conhecer e saber combater as ciberameaças mais comuns
4. Prática em contexto de formação

Objetivos do módulo

Desenvolver competências e ficar apto utilizar a Internet de forma segura.

Competências a adquirir

- Navegar na Internet de forma segura;
- Reconhecer e reagir adequadamente às ciberameaças;
- Saber usar ferramentas para conferir proteção no ciberespaço.

Conteúdos programáticos

Unidade Didática 1: Introdução à cibersegurança

Gestão da identidade digital;

Os planos humano, tecnológico e físico e a necessidade de os enquadrar nos planos organizacionais – pessoas, processos e tecnologia;

Proteção para as ciberameaças;

Normas e leis de referência do Cibercrime.

Unidade Didática 2: Identidade digital e Informações de Identificação Pessoal (PII)

Construção de passwords fortes e fáceis de memorizar;

Teste de força de passwords;

Uso de Gestores de Passwords;

Boas práticas no uso de correio eletrónico;

Autenticação duas etapas ou dois fatores;

Ataques por correio eletrónico.

Unidade Didática 3: Combater as ciberameaças mais comuns

Conhecer e saber combater as 10 ciberameaças mais comuns;

Como formatar uma pen USB com partições;

Como fazer Backup da informação;

Como usar uma Rede privada virtual (VPN);

Tratamento e violação de dados pessoais;

Como criar uma rede guest.

Prática em contexto de formação

No decurso deste módulo, os alunos colocados perante situações práticas serão instados a efetuar exercícios práticos em ambiente Windows.

Os alunos realizarão um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 2: ENCRIPTAÇÃO DE DADOS

[Duração: 13 horas teórico-práticas | 1 semana]

1. Fundamentos de criptografia
2. Encriptação em suportes físicos
3. Encriptação de correio eletrónico
4. Prática de encriptação, em suporte físico e de mensagens de correio eletrónico

Objetivos do módulo

Desenvolver nos alunos a capacidade de cifrar a informação digital.

Competências a adquirir

- Encriptar dados em suporte físico e em mensagens de correio eletrónico.

Conteúdos programáticos

Unidade Didática 1: Fundamentos de criptografia

Criptografia Simétrica e Assimétrica;

Chave Pública e Chave privada;

Infraestrutura de Chave Pública;

PGP.

Unidade Didática 2: Encriptação em suportes físicos

A necessidade de encriptar a informação existente em suportes físicos;

Encriptação de informação em computadores;

Encriptação de informação em discos externos e pen-drives;

Encriptação noutros suportes (telemóveis, tablets);

Uso de ferramentas de encriptação em suportes físicos.

Unidade Didática 3: Encriptação de correio eletrónico

A necessidade de encriptar correio eletrónico;

Ferramentas de encriptação de correio eletrónico.

Prática em contexto de formação

Será solicitado ao aluno a encriptação de informação em suporte físico e de mensagens de correio eletrónico.

O trabalho final do módulo, de natureza essencialmente prática, consiste no envio de mensagens de correio eletrónico encriptadas que serão validadas pelo formador.

Os alunos realizarão ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 3: ANATOMIA DE UM CIBERATAQUE

[Duração: 13 horas teórico-práticas | 1 semana]

1. As fases de um ciberataque
2. Reconhecimento, OSINT e deteção de vulnerabilidades
3. Engenharia Social
4. Prática em contexto de formação

Objetivos do módulo

Compreender o modo de atuação de um agente malicioso e a anatomia de um ciberataque para melhor compreender como neutralizar ou mitigar os seus efeitos.

Competências a adquirir

- Capacidade para realizar algumas ações de OSINT (Open source intelligence);
- Capacidade para detetar e evitar ações de engenharia social;
- Deteção de vulnerabilidades.

Conteúdos programáticos

Unidade Didática 1: As fases de um ciberataque

Ameaças e tendências

As etapas da *Cyber Kill Chain* (Lockheed Martin)

Exemplos históricos de ciberataques.

Unidade Didática 2: Reconhecimento, OSINT e deteção de vulnerabilidades

Conceito de reconhecimento passivo *versus* ativo;

Principais fontes para recolher informações na web (e.g., *google dorks*, *Shodan*, *darkweb*, etc.);

Obter informações sobre pessoas ou organizações;

Vulnerabilidades, deteção e fontes de *threat intel*.

Unidade Didática 3: Engenharia Social

Fatores de motivação e persuasão;

Tipos de ataques de engenharia social;

Exemplos da vida real.

Prática em contexto de formação

No decurso deste módulo, os alunos vão efetuar exercícios práticos. O trabalho final do módulo, igualmente de natureza prática, consiste na realização de técnicas de reconhecimento passivo.

Os alunos realizarão ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 4: CIBERHIGIENE

[Duração: 13 horas teórico-práticas | 1 semana]

1. Segurança e *hardening* em sistemas Windows
2. Segurança na Internet
3. Virtualização e emulação de software
4. Prática em contexto de formação

Objetivos do módulo

Dotar os alunos com as capacidades para adotar medidas de defesa ativa que lhes permitam melhorar a sua cibersegurança.

Competências a adquirir

- Aplicar boas práticas para a utilização segura das aplicações e dos sistemas operativos.

Conteúdos programáticos

Unidade Didática 1: Segurança e *hardening* em sistemas Windows

Recomendações gerais e conduta;

Software, Serviços e Processos;

User account control;

Privilégios de contas;

Atualizações e *Patching*;

Firewall, Antivirus;

Cloud, partições, *backups*.

Unidade Didática 2: Segurança na Internet

Cuidados genéricos no correio eletrónico, redes sociais e *cloud*;

Cuidados a ter na utilização e configuração de redes *Wi-fi*;

Gestão segura de dispositivos IoT (*Internet das coisas*);

Identificar notícias falsas na Internet;

Procedimentos na resposta a incidentes.

Unidade Didática 3: Virtualização e emulação de software

Emulação de software;

Virtualização;

Máquinas virtuais.

Prática em contexto de formação

No decurso deste módulo, os alunos vão efetuar exercícios práticos e implementar as técnicas de proteção ministradas. O trabalho final do módulo, igualmente de natureza prática, consiste na prática com software de virtualização ou em alternativa com software de emulação.

Os alunos realizarão ainda um teste na plataforma Moodle para validação de conhecimentos.

MÓDULO 5: A PSP NA REDE NACIONAL DE SEGURANÇA INTERNA (RNSI)

[Duração: 13 horas teórico-práticas | 1 semana]

1. Apresentação da RNSI
2. A PSP na RNSI
3. Recomendações de boas práticas informáticas no dia-a-dia dos elementos da PSP
4. Prática em contexto de formação

Objetivos do módulo

Desenvolver competências e ficar apto a aplicar as boas práticas informáticas no domínio PSP da RNSI.

Competências a adquirir

- Gerir passwords;
- Gerir e utilizar com precauções os recursos na cloud;
- Saber encriptar dados;
- Verificar a veracidade de emails recebidos.

Conteúdos programáticos

Unidade Didática 1: Apresentação da RNSI

Normativa;

Data Center;

Recursos;

Aplicações;

Domínios;

Comunicações;

Forças e serviços de segurança presentes na RNSI;

Centro de Operações de Segurança Informática (COSI).

Unidade Didática 2: A PSP na RNSI

Domínio;

Correio eletrónico;

Aplicações;

Gestão utilizadores;

Servidores;

Acesso à informação.

Unidade Didática 3: Recomendações de boas práticas informáticas quotidianas aos elementos da PSP

Passwords seguras;

Encriptação de dados no contexto da RNSI;

Utilização de sites https;

Logout online e no computador;

Evitar phishing;

Evitar erros comuns na prática cibernética da PSP.

Prática em contexto de formação

No decurso deste módulo, os alunos, colocados perante situações práticas, serão instados a efetuar exercícios em ambiente formativo. Os alunos realizarão um teste na plataforma Moodle para validação de conhecimentos.

DESTINATÁRIOS

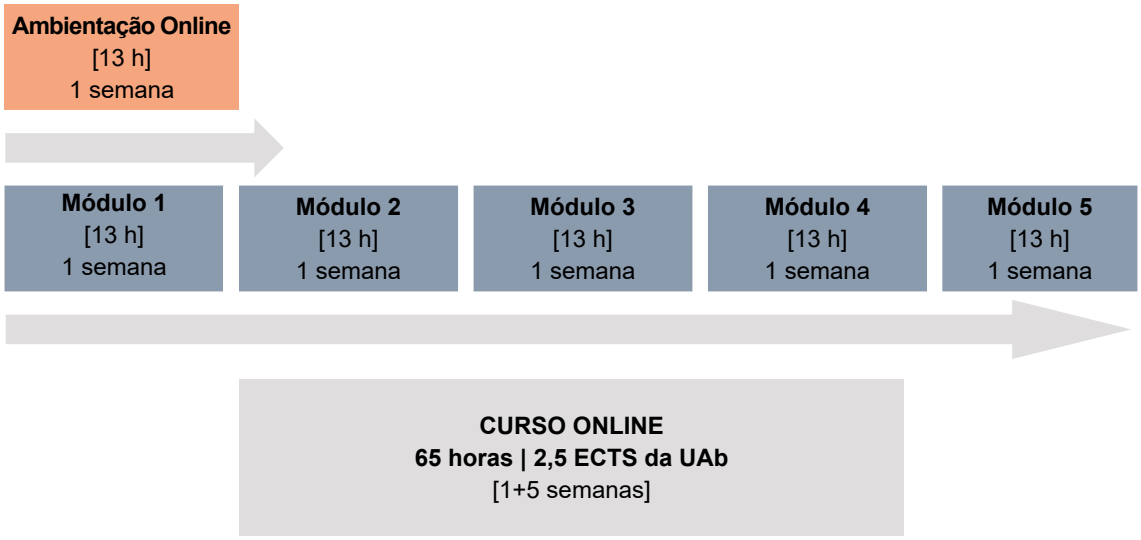
Dada a natureza específica desta ação de formação, o público-alvo são todos os utilizadores dos sistemas de informação da Polícia de Segurança Pública e da RNSI pertencentes à PSP.

Considera-se como fator de sucesso nesta microcredencial a motivação dos formandos e a sua disponibilidade total para interagirem com os formadores e com os outros formandos na colocação de questões ou dúvidas sobre a matéria e, ainda, disponibilidade de tempo para estudarem os conteúdos, elaborarem todas as atividades sugeridas e as avaliações propostas.

Cumulativamente, os formandos devem possuir habilitações mínimas ao nível do 12.º ano ou legalmente equivalente, e conhecimentos/prática de informática como utilizadores, em ambiente Windows.

ESTRUTURA

A duração total da microcredencial é de 65 horas (volume de trabalho dos formandos) sendo estruturada em 5 módulos de realização sequencial, precedidos de um módulo ou período de Ambientação ao Contexto Online do curso, de socialização online e de treino com a plataforma informática que suporta o curso.



METODOLOGIA

A metodologia seguida neste curso é a estabelecida no Modelo Pedagógico Virtual da UAb para ações de aprendizagem ao longo da vida a desenvolver em regime de e-learning, e adota o modelo de ensino/aprendizagem de 5 níveis de Gilly Salmon (2000).

Nesta ação de formação os formandos terão, sequencialmente, acesso aos conteúdos dos diversos módulos, para o seu estudo e para a execução das atividades solicitadas, em situações on e offline. O acesso offline possibilita a leitura/estudo dos conteúdos dos módulos por parte dos formandos sem necessidade de ligação à Internet.

A tutoria a prestar pelos formadores será ativa e permanente e far-se-á preferencialmente através dos fora de discussão abertos nos diversos tópicos (correspondentes aos módulos da estrutura do curso) na plataforma.

Podem realizar-se sessões síncronas de discussão online (chats), em datas, horários e locais (Tópicos do site do curso) a comunicar antecipadamente pelos formadores aos alunos.

RECURSOS DE APRENDIZAGEM

Os materiais técnico-pedagógicos a fornecer aos formandos para utilização no curso são:

- Textos base sobre os temas a abordar, colocados online no curso criado na plataforma Moodle e/ou na Web em servidor a indicar aos participantes para procederem o seu download;
- Apresentações multimédia diversas concebidas pelos formadores para situações de aprendizagem específicas;
- Tutorial sobre a forma de utilizar a PlataformAbERTA na situação de e-formando;
- Tutorial "Como Fazer para…", documento orientador dos procedimentos para aceder ao curso alojado na plataforma Moodle da UAb;
- Guia da Microcredencial;
- Guia do Formando Online.

Recursos técnicos

Plataforma informática Moodle (V 2.4), em https://elearning.uab.pt/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

AVALIAÇÃO E CLASSIFICAÇÃO

A avaliação em formação online tem uma importância acrescida em relação à avaliação em regime presencial em virtude da natureza particular do contexto de ensino-aprendizagem. Os instrumentos de avaliação devem, por isso, ser variados por forma a anular ou reduzir a um mínimo aceitável, a possibilidade de fraude intelectual quanto à autoria dos trabalhos. Por isso, todos os aspetos da avaliação devem ser muito claros e explícitos e a avaliação deve ser definida e planeada a par com o percurso formativo, que se deseja e estar intimamente relacionada com os objetivos a atingir..

Avaliação nos Módulos

Os módulos 1 a 5 do curso são sujeitos a avaliação, que integra 3 componentes por módulo:

- Avaliação contínua ao longo do módulo (participação nos fóruns de discussão abertos no espaço do curso);
- Realização de uma e-atividade a submeter na plataforma;
- Um teste final do módulo a realizar na plataforma.

Os instrumentos de avaliação de um módulo têm o mesmo peso e, por isso, a avaliação final do módulo é dada pela média simples das 3 provas realizadas, numa escala de 0 a 20 valores.

A média final da avaliação dos módulos traduz a classificação final.

Na avaliação da participação dos alunos num fórum de discussão têm-se em atenção os seguintes fatores:

- A qualidade e a quantidade de mensagens com conteúdo significativo para o(s) assunto(s) em discussão;
- A relevância das mensagens para os temas em discussão;
- A clareza e objetividade das mensagens;
- A redação das mensagens (pontuação, erros de ortografia, etc.);
- A oportunidade do envio das mensagens, privilegiando-se a distribuição destas ao longo de todo o período de discussão em fórum.

Todas as mensagens enviadas para os fóruns de módulos já terminados **não são consideradas** para efeitos de avaliação.

As e-atividades a realizar em cada um dos módulos (tanto as intermédias como a final) podem revestir qualquer tipo – teste tradicional, trabalho offline, trabalho online, síntese, pesquisa, relatório, etc. - ficando a sua escolha ao critério do formador do respetivo módulo.

É obrigatória a realização de todas as e-atividades de avaliação dos módulos que contam para a classificação final do curso. A não realização de uma e-atividade é contabilizada com 0 valores para efeitos de obtenção da média. A não participação num fórum de discussão traduz-se numa classificação de 0 valores nesse fórum.

Todas as e-atividades de avaliação final dos diversos módulos realizam-se numa só data e num período de 24 a 48 horas. **Excecionalmente**, e apenas por razões de doença ou de inoperacionalidade da plataforma, ambas devidamente comprovadas, se admite a realização das e-atividades para avaliação numa data de **segunda oportunidade**.

Classificação Final no curso

A classificação final no curso (CFC) é obtida pela aplicação da fórmula:

$$CFC = \frac{AFM1 + AFM2 + AFM3 + AFM4 + AFM5}{5}$$

onde AFMx representa a Avaliação Final do Módulo x.

Consideram-se com aproveitamento no curso os formandos que obtiverem classificação Final no Curso **igual ou superior 10 valores**, numa escala de 0 a 20 e, cumulativamente, tenham uma avaliação final em todos os módulos 1 a 7 igual ou superior a 8 valores.

Para efeitos de aproveitamento e de inscrição no Certificado as classificações finais com décimas de 0,5 a 0,9 são arredondadas para o valor inteiro superior e as de 0,1 a 0,4 para o valor inteiro inferior.

A todos os formandos com aproveitamento é entregue um **Certificado de Formação** que será enviado para a morada que consta no formulário de inscrição no curso.

A todos os formandos que realizaram integralmente o curso e o terminaram sem aproveitamento, de acordo com o Regulamento do Curso e a seu pedido expresso, será entregue um **Certificado de Frequência**.

EQUIPA DOCENTE

FORMADORES	MÓDULOS
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
João Mateus	1. Fundamentos de cibersegurança 2. Encriptação de dados
Luís Dias	3. Anatomia de um ciberataque 4. Ciberhigiene
Tiago Moniz	5. A PSP na Rede Nacional de Segurança Interna (RNSI)

JOÃO GUILHERME CONDE MAGALHÃES MATEUS é Tenente-Coronel Engenheiro, da Arma de Transmissões do Exército português. Licenciado em engenharia eletrotécnica e de computadores, ramo de telecomunicações e eletrónica e em engenharia informática, ramo de programação e sistemas de informação, e mestre em investigação operacional e engenharia de sistemas, graus obtidos no Instituto Superior Técnico. É também Mestre em Engenharia Eletrotécnica Militar – Especialidade de Transmissões, pela Academia Militar. Atualmente é Professor de Cibersegurança na Academia Militar, na Universidade Aberta, na Universidade Europeia e na Universidade Atlântica

Foi galardoado com o Prémio Fernandes Costa do Instituto de Informática do Ministério das Finanças – Unidade de Missão, Inovação e Conhecimento – pelo seu projeto de Modelação e Reengenharia dos Processos de Negócio do Comando de Pessoal do Exército Português aplicado na prática na reestruturação dos Sistemas de Informação do Ministério da Defesa.

É membro da Ordem dos Engenheiros.

É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2010.

LUÍS FILIPE XAVIER CAVACO DE MENDONÇA DIAS é Major Engenheiro da Arma de Transmissões do Exército Português, especializado em Segurança da Informação e Docente na Academia Militar. É Doutorado em Segurança de Informação pelo Instituto Superior Técnico, Mestre em Engenharia Eletrotécnica Militar (Especialidade de Transmissões) pela Academia Militar, e está ainda habilitado com o Curso de Estado-Maior Conjunto das Forças Armadas. Detém várias certificações da Indústria (SANS GCFE, EC-Council ECSA e ENSA, etc.) e é membro do GIAC advisory board.

Atualmente e desde 2016, é docente de "Segurança Informação, Sistemas de Informação e Ciberdefesa" (entre outras Unidades Curriculares) na Academia Militar.

Desempenhou funções na componente operacional de ciberdefesa do Exército, entre 2010 e 2015. Participou como "jogador" em diversas edições de exercícios de ciberdefesa Nacionais e Internacionais (Ciber Perseu, Cyber Coalition da NATO). Em 2018 e 2019 foi organizador dos Exercícios Nacionais de Ciberdefesa (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

É membro investigador do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento (INESC-ID) e do Centro de Investigação da Academia Militar (CINAMIL). Desenvolve investigação no âmbito da aprendizagem automática de ameaças no ciberespaço através da análise de dados de segurança, com recurso a algoritmos de aprendizagem não supervisionada. É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2019.

TIAGO NUNO GOULART BETTENCOUR MONIZ é responsável pelo Núcleo de Sistemas de Informação e Comunicações do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI) . Desempenhou funções de gestão dos sistemas de informação da Polícia de Segurança Publica na área de recursos humanos, segurança privada, formação e recrutamento. Habilitado com o título de Mestre em Segurança

Interna pelo ISCSPI, pós-graduado em Administração Pública – área de especialização em Governance da Segurança pelo Instituto Superior de Ciências Sociais e Políticas e em Transição e Transformação Digital das Organizações pela Universidade Aberta. Possui ainda formação em Auditoria de Sistemas de Informação pelo Instituto Nacional de Administração e Docência Digital em Rede, E-atividades no desenho de cursos e Projeto de unidade curricular em Ambiente Digital pela Universidade Aberta.


AI