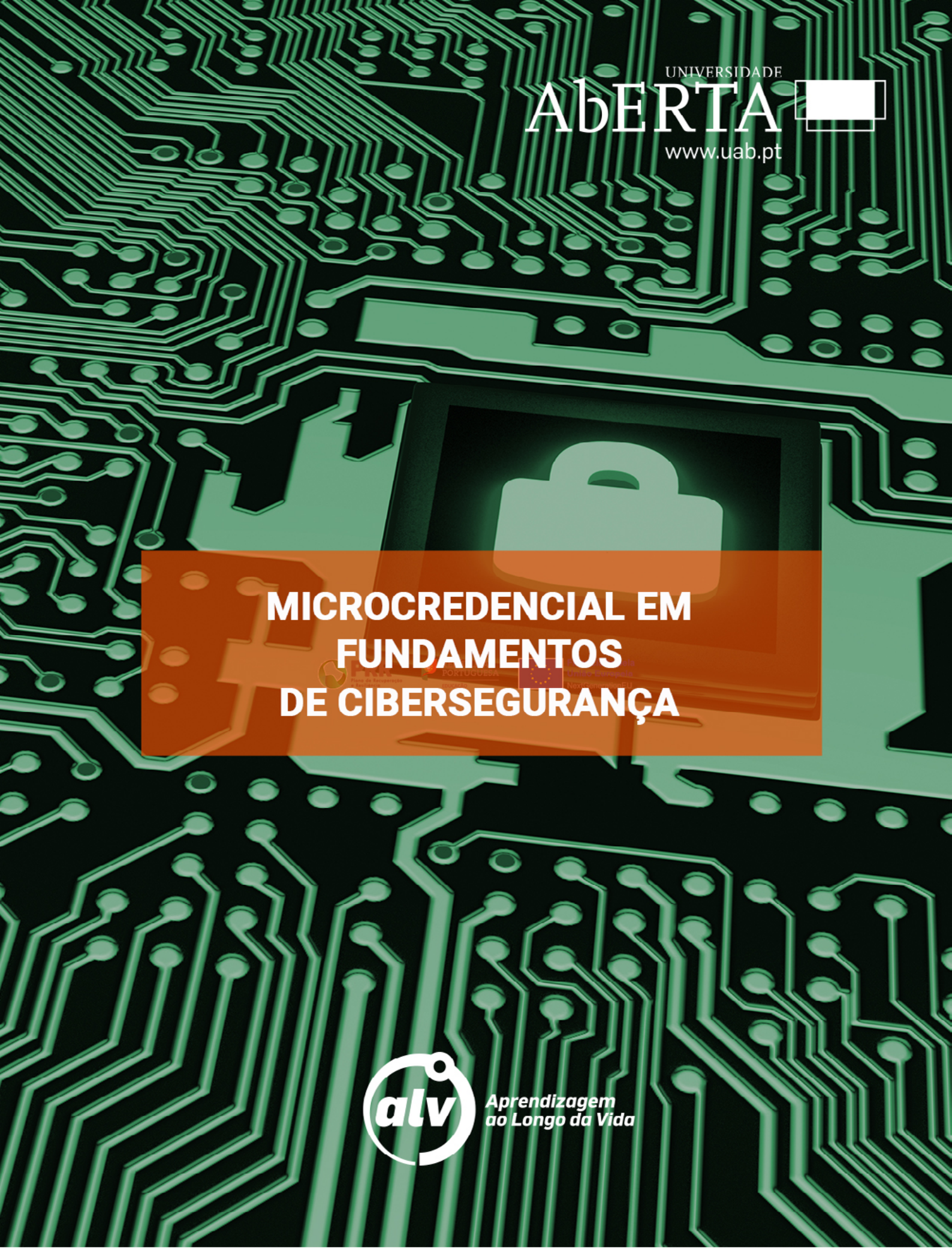
UNIVERSIDADE ABERTA
www.uab.pt



MICROCREDENCIAL EM FUNDAMENTOS DE CIBERSEGURANÇA

alv Aprendizagem ao Longo da Vida

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 gerou novas ameaças e oportunidades no contexto da vida das pessoas, empresas, instituições, nações e regiões de todo o mundo, onde a segurança e a competitividade são desígnios da realidade atual. A presença das organizações e empresas e do próprio indivíduo no mundo digital é uma realidade. A evolução tecnológica trouxe consigo inúmeras oportunidades de desenvolvimento e bem-estar geral pela desburocratização e consequente aceleração nos processos e por permitir alcançar um público mais vasto criando riqueza e desenvolvimento, outrora não possível.

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

Esta microcredencial faz o levantamento das ameaças do mundo digital para habilitar

os formandos com técnicas, comportamentos, atitudes e saber-fazer para anular os efeitos destas ameaças e poder ter uma presença segura e consciente no mundo digital, evitando, mitigando ou anulando os riscos.

É neste enquadramento e ambiente geral de amaças e de invasões, agravado com a atual pandemia, que a Universidade Aberta (UAb) organizou e pretende oferecer ao mercado de formação esta microcredencial base de cibersegurança a desenvolver em regime de formação teórica e prática a distância online (*e-learning*).

OBJETIVOS

Os objetivos desta microcredencial são:

- Proporcionar conhecimentos e competências fundamentais em redes de computadores e sistemas operativos, os principais alvos de ataques.
- Proporcionar conhecimentos e competências que permitam aos participantes caracterizar os ataques típicos bem como as defesas correspondentes.
- Capacitar os participantes a identificar, reagir e proteger das principais ciberameaças.

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.

PROGRAMA E CONTEÚDOS

Esta microcredencial tem a duração de 52 horas (2 ECTS da UAb) e está estruturada em 4 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. Redes de computadores e sistemas operativos	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.
3. Anatomia de um ciberataque	Proporcionar capacidade para realizar algumas ações de OSINT (Open source intelligence) e de deteção de vulnerabilidades.
4. Ciberhigiene	Módulo que pretende proporcionar as capacidades para adotar medidas de defesa ativa que melhorem a cibersegurança.

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, a familiarização com a utilização do software de gestão do curso (o *Learning Management System 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 com eficácia todas as ferramentas e possibilidades da plataforma Moodle, com o estatuto de formando.

MÓDULO 1: FUNDAMENTOS DE CIBERSEGURANÇA, REDES DE COMPUTADORES E SISTEMAS OPERATIVOS

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

1. Introdução à cibersegurança
2. Redes de computadores
3. Sistemas operativos
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.

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.

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.

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

DESTINATÁRIOS

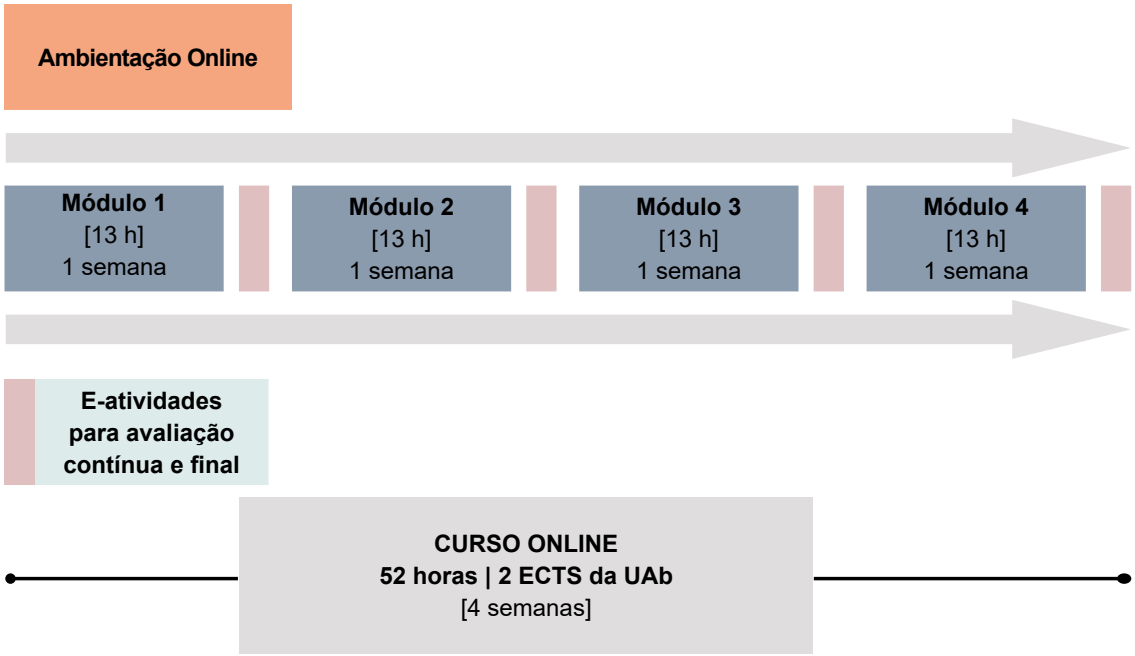
O público-alvo desta microcredencial inclui:

- Todos os profissionais e responsáveis de empresas/organizações;
- Responsáveis por crianças, jovens e idosos;
- Indivíduos que desejem aumentar os seus conhecimentos de segurança da informação e de ciberdefesa de modo a ter uma presença responsável e consciente no ciberespaço.

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 52 horas (volume de trabalho dos formandos) sendo estruturada em 4 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 que nos fala 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 Moodle.

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

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

Todos os módulos 1 a 4 do curso são sujeitos a avaliação que integra:

- Uma componente contínua ao longo do módulo (participação nos fóruns de discussão e eventual realização de e-atividades intermédias);
- Uma componente final do módulo baseada na realização de uma e-atividade final que pode revestir qualquer forma (trabalho, teste, projeto, etc.)

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 2 ou 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. **Excepcionalmente**, 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:

$$\mathrm{CFC} = \frac{\mathrm{AFM1} + \mathrm{AFM2} + \mathrm{AFM3} + \mathrm{AFM4}}{4}$$

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, não tendo tido, em qualquer dos módulos, classificação inferior a 8 valores.

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. Fundamentos de *ethical hacking* 4. Ciberhigiene

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 Informática na Academia Militar.

Foi Professor Regente do Departamento de Ciências Exatas e Tecnologias da Engenharia da Academia Militar das cadeiras de Programação, Informática, Redes e Instalações Elétricas, Sistemas Computacionais e de Comunicação, Algoritmos e Estruturas de Dados, Redes de Computadores, Investigação Operacional, Gestão e Teoria da Decisão

e de Tática de Transmissões. Assumiu os cargos de Diretor de Curso do Mestrado Militar de Transmissões e de Diretor do Mestrado em Guerra da Informação/Competitive Intelligence.

Foi Chefe do Centro de Informática da Academia Militar e Webmaster tendo sido responsável pela implementação do Portal, da Rede Académica em Moodle e pelo webmail (@academiamilitar.pt). Como área de investigação dedica-se à aplicação dos Sistemas de Informação e Comunicação ao Ensino a Distância, colaborando em experiências com docentes do Centro de Matemática da Universidade do Minho e do Departamento de Matemática da Universidade Lusófona.

É Professor Auxiliar Convidado de Investigação Operacional, de Planeamento e Gestão de Projetos, de Aplicações Informáticas, de Sistemas de Informação Aplicados, de Métodos Quantitativos, de Matemática e de Qualidade na Universidade Lusófona, e atualmente no IPLuso, desde o ano letivo de 1998/99.

Foi Chefe da Repartição de Projetos do Centro de Informática do Exército tendo sido responsável pela implementação de vários projetos de Sistemas de Informação no Ministério da Defesa.

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.

UNIVERSIDADE
ABERTA
www.uab.pt