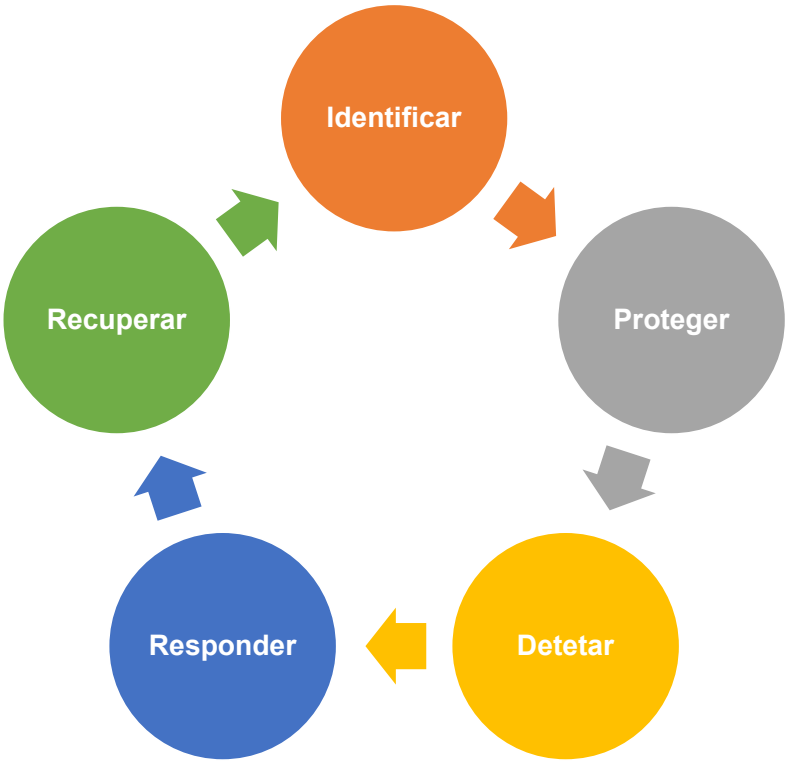
microcredencial
alv Aprendizagem ao Longo da Vida
PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia
NextGenerationEU



“A futura ciência do governo deveria ser chamada Cibernética”

[André-Marie Ampère - 1834]

ÍNDICE

ENQUADRAMENTO

O **Plano de Recuperação e Resiliência** (PRR) é um programa de aplicação nacional que visa implementar um conjunto de reformas e investimentos destinados a repor o crescimento económico sustentado, reforçando o objetivo de convergência com a Europa, ao longo da próxima década.

Um dos objetivos expressos no Programa de Recuperação e Resiliência (PRR) é o de assegurar que o país seja cada vez mais uma sociedade digitalizada. Para isso vêm sendo adotadas medidas de fomento da capacitação e inclusão digital das pessoas, através de ações de educação, de ensino e de formação profissional.

A transformação digital das empresas, além da transformação dos seus recursos humanos, deve integrar tecnologias digitais nas suas operações e, na medida em que o "digital" e o "físico" cada vez são mais integrados, mais importante é a cibersegurança em todas as suas atividades, não sendo exceção as atividades ligadas à segurança e proteção de bens, equipamentos, instalações e pessoas de que trata o presente curso, que agora se organiza e oferece.

A Sociedade da Informação está hoje presente nas nossas vidas como nunca esteve antes. 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. O próprio ensino está a passar por uma revolução através do ensino a distância permitindo chegar a pessoas e locais que não teriam esta oportunidade de desenvolvimento com o ensino tradicional presencial. Este curso é um exemplo disso, permitindo aos formandos estudar ao seu ritmo e realizar sua formação em qualquer lugar e a qualquer hora.

A segurança cibernética 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, e não menos importante, visa capacitar pessoas com comportamentos e atitudes que salvaguardem a segurança da informação.

O mundo digital trouxe inúmeras vantagens e progresso, mas também sabemos que existem fortes ameaças. É constante o aumento do número de dispositivos eletrónicos existentes e ligados em rede (Internet das coisas) e também dos seus utilizadores. Com o aumento dos negócios realizados pela Internet e das informações guardadas em rede, a segurança no Ciberespaço tornou-se hoje uma forte preocupação dos indivíduos, das empresas, dos governos e das nações. Para a evolução tecnológica ser aceite é necessário que haja confiança nos sistemas.

Este curso 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. Sendo certo que as principais ameaças provêm da exposição à Internet, esta não é a única fonte de ameaça digital e deste modo o curso abrange toda a ameaça digital de uma forma integrada e holística. De facto, esta abordagem não trata apenas a segurança da informação na Internet, mas da segurança da informação no seu todo, partindo do princípio que a Informação é o ativo mais valioso e crítico para o funcionamento e êxito de qualquer organização ou empresa.

Nesta perspetiva, a segurança cibernética ou cibersegurança deve ser considerada como parte integrante do modelo de negócio. Assim as empresas e organismos precisam de uma abordagem que integre a cibersegurança em todos os aspetos da organização, desde o departamento de tecnologias da informação até à formação de funcionários e colaboradores, dado que não é um assunto exclusivo de informáticos, é um trabalho de equipa. O desenvolvimento de um espaço digital seguro exige a participação e é responsabilidade de todos os indivíduos, empresas, instituições e governos.

Deste modo, investir na formação e capacitação das pessoas que inevitavelmente lidam com a Informação é dos investimentos mais acertados e que mais que mais retorno trará. Além deste ponto de vista organizacional, o curso é muito focado para o desenvolvimento de uma cultura pessoal de segurança da informação. Assim os formandos terão conhecimento dos riscos existentes da identidade digital e aprenderão a desenvolver uma presença consciente e informada que lhes será útil enquanto cidadão, ficando também apto a usar este conhecimento em benefício próprio e dos seus entes mais próximos. É sabido que as gerações mais novas são “nativos digitais”, isto é, já nasceram na era da Internet e cresceram a usar tablets e telefones inteligentes tratando o digital com perfeita naturalidade. Por outro lado, é um facto que estas gerações mais

novas não possuem os mecanismos de defesa que permitam a sua segurança no mundo digital que as gerações anteriores possuem. Caberá então às gerações de “emigrantes digitais” a sensibilização e educação das mais novas para criarem a sua própria defesa proporcionando uma presença digital segura e consciente.

Com o surgimento da Indústria 4.0 e da Internet das Coisas (IoT), acrescidas das constantes evoluções dos dispositivos de tecnologias da Informação, a segurança cibernética torna-se fundamental para garantir a confidencialidade, a integridade e a disponibilidade dos dados e informações que transitam e que são armazenadas ou manipuladas no espaço cibernético, considerando este como a metáfora que descreve o espaço não físico criado por redes de computador e a internet, onde as pessoas podem comunicar de diferentes maneiras.

OBJETIVOS

Os objetivos deste curso são:

- Aprofundar conhecimentos técnico-jurídicos na área da segurança com particular incidência sobre a formação específica e habilitante para o exercício de funções de direção e gestão de segurança.
- Obter conhecimentos teóricos e práticos na área da segurança no que respeita à prevenção e atuação realizada através de meios humanos e de equipamentos e sistemas, interagindo com o objetivo principal de proteger pessoas e bens.
- Proporcionar conhecimentos e competências que permitam aos participantes caracterizar os ataques cibernéticos típicos e as defesas correspondentes.
- Proporcionar conhecimentos e competências que permitam aos participantes, tratar a informação de modo a garantir a sua autenticidade, integridade, confidencialidade, privacidade e não repúdio.

Assim, no final, os participantes saberão:

a) Usar mecanismos seguros de autenticação;

b) Encriptar dados em dispositivos de retenção e em mensagens de correio eletrónico;

c) Usar técnicas de análise forense digital para reconhecer e produzir prova digital de crime e conhecer as técnicas *anti-forense* que os criminosos usam;

d) Aprender as técnicas que os criminosos (*hackers*) utilizam e a morfologia de um ataque com vista a detetar as vulnerabilidades da sua organização e tomar as respetivas medidas (*Ethical Hacking*);

e) Aprender técnicas de proteção digital de modo a configurar redes e sistemas e para reduzir o risco de ataque.

COMPETÊNCIAS

Espera-se que no final do curso os participantes tenham adquirido as seguintes competências:

- Aplicar conhecimentos técnico-jurídicos na área da segurança, com particular incidência sobre a formação específica e habilitante para o exercício de funções de direção segurança privada.
- Aplicar a legislação da segurança privada, distinguindo-a da segurança pública e interligando-a com o Regulamento Geral de Proteção de Dados.
- Implementar o Regulamento Geral de Proteção de Dados numa organização/ empresa/instituição.
- Conceber diversos tipos de segurança física em função das ameaças identificadas.
- Conhecer e selecionar com critério tipos de barreiras físicas e sistemas de controlos de acesso, considerando o seu enquadramento legal e a sua eficácia prática.
- Obter conhecimento dos sistemas de controlo de acessos, o seu enquadramento legal, a sua aplicação e interação com outras aplicações, e resultados.
- Detetar e avaliar os ciberataques típicos a que as organizações estão sujeitas e planear atuações concretas que permitam eliminar ou minimizar as consequências desses ataques.
- Cifrar a informação existente em todo o suporte informático e nas comunicações por correio eletrónico.
- Usar mecanismos de autenticação forte.
- Conhecer e aplicar a legislação referente ao cibercrime.
- Conhecer e implementar na prática o Regulamento Geral de Proteção de Dados.
- Elaborar uma Política de Segurança da Informação para uma empresa ou instituição.

- Conhecer e implementar as normas internacionais (ISO) referentes a segurança da informação.
- Saber os princípios da análise forense digital e realizar algumas técnicas em sistemas Windows.
- Realizar técnicas *anti-forense* e de anonimização.
- Compreender a morfologia de um ataque e empreender a respetiva defesa.
- Caracterizar serviços de autenticação.
- Aplicar técnicas de navegação digital segura.
- Reagir a ataques e adotar procedimentos de resposta a incidentes.

DESTINATÁRIOS

Este curso destina-se a, entre outros:

- Todos os indivíduos que desejem aumentar os seus conhecimentos de segurança física, da segurança da informação e de ciberdefesa de modo a ter uma presença responsável e consciente no ciberespaço, e que cumpram os pré-requisitos expressos abaixo.
- Indivíduos que já possuam o curso de qualificação inicial de Diretor de Segurança Privada obtido na UAb ou de qualquer outro estabelecimento de ensino superior, e desejem (re)orientar a sua carreira profissional para a segurança cibernética.

Pré-requisitos dos participantes

Além de necessário interesse e motivação, os participantes devem ter disponibilidade de tempo, que se estima em 2 horas por dia, para estudarem os conteúdos, interagirem com colegas e professores nos fóruns de discussão, elaborarem todas as atividades sugeridas, as avaliações propostas e o exercício final.

Devem possuir ainda:

- Habilitações mínimas ao nível do 12.º ano ou legalmente equivalente, devendo apresentar o certificado.
- Conhecimentos e prática de informática como utilizadores avançados em ambiente Windows.
- Prática de utilização de browsers de navegação na Web.

- Uma conta de correio eletrónico ativa.

Ao formalizarem a sua candidatura a este curso, os interessados assumem, implicitamente, que cumprem todos os pré-requisitos acima descritos.

PROGRAMA E CONTEÚDOS

Este curso está estruturado em 4 módulos que decorrem sequencialmente, e terminam com um Exercício Final. Estes módulos são precedidos de um período de ambientação ao contexto online do curso e de integração dos participantes, por vezes designado Módulo 0, Módulo de Ambientação ou Pré-curso. A duração do curso é de 156 horas (volume de trabalho dos formandos) a que correspondem **6 ECTS** da UAb* e realiza-se em regime de formação a distância online (e-learning) ao longo de 12 semanas.

Na Internet o curso é suportado pela plataforma informática PlataformAbERTA em utilização na UAb e adaptada ao seu Modelo Pedagógico Virtual.

MÓDULOS	DESCRIÇÃO
0. Ambientação ao contexto online do curso	Período para a socialização dos participantes, criação de "um grupo" de trabalho online e familiarização e treino com a utilização do software de gestão do curso.
1. Legislação sobre Segurança Privada e Regulamento Geral de Proteção de Dados (RGPD)	Módulo para dotar os formandos dos conhecimentos de legislação da segurança privada e da segurança pública, interligando-as com o RGPD.
2. Sistemas de Segurança Física (SSF): instalações, perímetros, equipamentos e pessoas	Módulo sobre principais meios e equipamentos disponíveis para a proteção de Infraestruturas críticas e outras, sua correta implementação e utilização.
3. Como prevenir ciberataques?	Módulo que pretende implementar atitudes e práticas de prevenção e interceção de ataques digitais e, ainda, de procedimentos de segurança digital.
4. Como reagir a ciberataques? Como recuperar de ciberataques?	Módulo que visa planear e implementar planos de resposta a incidentes, recuperação de sistemas e retoma das operações normais.
5. Exercício final	Este exercício tem como objetivo aplicar os conhecimentos adquiridos num cenário prático de criptografia.

* O ECTS (Sistema Europeu de Transferência de Créditos) foi desenvolvido pela Comissão Europeia. Os créditos ECTS representam o volume de trabalho que o estudante/formando deve produzir. Na UAb 1 ECTS equivale a 26 horas de trabalho do formando.

MÓDULO 0: AMBIENTAÇÃO AO CONTEXTO ONLINE DO CURSO

[Duração: 13 horas | 1 semana]

1. A plataforma informática de ensino/aprendizagem da UAb, PlataformAbERTA. Layout, recursos e atividades
2. Treino na exploração autónoma das ferramentas e recursos da plataforma

Objetivos do módulo

Neste módulo pretende-se que os formandos sejam capazes de:

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

Competências a adquirir

- Utilizar eficazmente e de forma autónoma as diversas ferramentas/funcionalidades da PlataformAbERTA a utilizar durante o curso.

Conteúdos programáticos

Unidade Didática 1: A PlataformAbERTA de ensino/aprendizagem da UAb

Esta unidade didática aborda fundamentalmente as formas possíveis de organizar os espaços para desenvolvimento de um curso online da UAb, e as diferentes atividades que se podem realizar nesse espaço.

- Formas de organizar espaços/sites na plataforma;
- Recursos e atividades da plataforma;
- Estrutura do site do curso; tópicos do curso; recursos disponíveis
- Ferramentas a utilizar.

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

Esta unidade didática consiste em realizar treinos práticos individualizados na utilização pelos alunos das ferramentas informáticas que integram a PlataformAbERTA e que serão utilizadas no curso.

- Treino com as ferramentas que podem integrar qualquer tópico do espaço onde decorre o curso, e que possibilitam diversas funcionalidades, designadamente:
  - fóruns, de diversos tipos;
  - trabalhos, online e offline;

– testes;
– questionários;
– wikis;
– referendos, etc.

MÓDULO 1: LEGISLAÇÃO SOBRE SEGURANÇA PRIVADA (SP) E REGULAMENTO GERAL DE PROTEÇÃO DE DADOS (RGPD)

[Duração: 26 horas teórico-práticas | 2 semanas]

1. Introdução à legislação de segurança privada
2. Leis e regulamentações em Portugal
3. Regulamento Geral de Proteção de Dados (RGPD)
4. Direitos dos titulares dos dados e obrigações dos responsáveis pelo tratamento
5. Implementação e conformidade com o RGPD nas empresas

Objetivos do módulo

O objetivo essencial do módulo é (1) dotar os formandos dos conhecimentos de legislação da segurança privada e da sua distinção da segurança pública, interligando-as com o RGPD e (2) fazer adquirir competências para a implementação do Regulamento Geral de Proteção de Dados nas organizações, evitando assim o pagamento de coimas pesadas que possam advir do seu incumprimento.

Competências a adquirir

- Conhecer e aplicar a legislação de segurança privada e pública, e fazer sua distinção;
- Identificar as Leis e entidades reguladoras do setor da SP.
- Aplicar os procedimentos do licenciamento da SP e os requisitos legais.
- Compreender o enquadramento normativo da proteção de dados.
- Distinguir os conceitos de dados pessoais e dados sensíveis.
- Conhecer e compreender as novas regras relativas à validade do consentimento;
- Identificar os direitos dos titulares dos dados pessoais.
- Perceber o impacto do RGPD a nível de segurança de dados, na forma como as organizações atuam e nas próprias relações laborais.
- Identificar o papel e as funções do Encarregado de Proteção de Dados.
- Identificar as consequências do incumprimento do Regulamento Geral de Proteção de Dados.

Conteúdos programáticos

Unidade Didática 1: Introdução à Legislação de Segurança Privada

Esta unidade servirá de introdução ao estudo da legislação atual da segurança privada. Abordará os conceitos e objetivos da segurança privada e distinguirá a segurança pública da privada, que são componentes cruciais no âmbito da legislação em Portugal.

- Conceito e objetivos da segurança privada.
- Distinção entre segurança pública e privada.

Unidade Didática 2: Leis e Regulamentações em Portugal

Esta unidade foca-se no estudo das leis e das entidades reguladoras da segurança privada em Portugal. Incluirá também os procedimentos de licenciamento e os requisitos legais na área da segurança privada.

- Leis e entidades reguladoras
- Licenciamento e requisitos legais.

Unidade Didática 3: Regulamento Geral de Proteção de Dados (RGPD)

Esta unidade foca-se no estudo das leis e das entidades reguladoras da segurança privada em Portugal. Incluirá também os procedimentos de licenciamento e os requisitos legais na área da segurança privada.

- Princípios e objetivos
- Âmbito de aplicação.

Unidade Didática 4: Direitos dos Titulares dos Dados e Obrigações dos Responsáveis pelo Tratamento

A quarta unidade abordará a questão do consentimento, a transparência, a portabilidade e a retificação dos dados pessoais, segundo as regras do RGPD. Explorará os direitos dos titulares dos dados e as obrigações dos responsáveis pelo seu tratamento.

- Consentimento e transparência
- Portabilidade e retificação dos dados.

Unidade Didática 5: Implementação e Conformidade com o RGPD nas Empresas

Na última unidade, o foco estará na aplicação prática do RGPD nas empresas, incluindo a avaliação de impacto e a figura do Encarregado de Proteção de Dados. Nela, serão abordadas as consequências do incumprimento do RGPD, de modo a evitar coimas pesadas.

- Avaliação de impacto
- Encarregado de Proteção de Dados (DPO).

MÓDULO 2: SISTEMAS DE SEGURANÇA FÍSICA (SSF): INSTALAÇÕES, PERÍMETROS, EQUIPAMENTOS E PESSOAS

[Duração: 26 horas teórico-práticas | 2 semanas]

1. Conceitos básicos de segurança física
2. Avaliação de riscos e vulnerabilidades
3. Proteção de instalações e perímetros
4. Equipamentos de segurança e tecnologias de deteção
5. Gestão de pessoal de segurança e treino específico

Objetivos do módulo

Dotar os formandos de conhecimentos teóricos sobre os principais meios e equipamentos disponíveis para a proteção de Infraestruturas críticas, sua correta implementação e utilização, normas e procedimentos para a proteção de infraestruturas desta natureza e realização de avaliações de riscos e vulnerabilidades.

Competências a adquirir

- Aplicar quando necessário a interligação e convergência entre segurança física e segurança lógica;
- Definir Infraestruturas críticas e reconhecer a sua importância;
- Capacidade de identificar, avaliar e responder aos diversos tipos de ameaças numa perspetiva holística de integração entre as valências físicas e digitais;
- Capacidade de delinear planos e procedimentos de execução permanente, avaliar a sua eficácia e aplicar medidas corretivas;
- Capacidade para conceber planos de contingência, realizar simulações e analisar os resultados;
- Aplicar os conhecimentos adquiridos sobre os diversos sistemas de segurança, enumerar a sua aplicação e reconhecer os seus resultados;
- Aplicar conhecimento sobre os diversos tipos de barreiras físicas e sistemas eletrónicos, e reconhecer os seus resultados;
- Enumerar e aplicar os sistemas de controlo de acessos, considerando a sua interação com outras aplicações e reconhecer os resultados;
- Capacidade de interligar todos os meios de segurança existentes, obtendo o conceito de segurança integrada;
- Capacidade de selecionar e avaliar o pessoal de Segurança Privada tendo em conta as especificidades e exigência do desempenho de funções em Infraestruturas

Críticas;

- Enumerar os riscos laborais e psicossociais específicos inerentes ao desempenho de funções em cibersegurança e infraestruturas críticas.

Conteúdos programáticos

Unidade Didática 1: Conceitos Básicos de Segurança Física

Esta unidade servirá de introdução ao estudo das medidas físicas de segurança e seus conceitos básicos, como garante da integridade do hardware em complemento da Segurança Cibernética.

- Prevenção, deteção e resposta
- Integração com a segurança digital.

Unidade Didática 2: Avaliação de Riscos e Vulnerabilidades

Esta unidade aborda a forma como os riscos e ameaças poderão ser identificados e, com base em modelos de cenarização, como poderá ser calculada a sua possibilidade de concretização bem como o nível de gravidade dessa concretização.

- Identificação e análise de ameaças
- Avaliação da probabilidade e impacto.

Unidade Didática 3: Proteção de Instalações e Perímetros

Esta unidade foca-se no estudo das medidas físicas de segurança, tais como áreas de segurança, barreiras e controlo de acessos, e sua aplicação tendo em conta as especificidades inerentes às infraestruturas críticas.

- Barreiras físicas e controle de acessos
- Sistemas de iluminação e vigilância.

Unidade Didática 4: Equipamentos de Segurança e Tecnologias de Deteção

Esta unidade didática dotará os formandos de conhecimento sobre as tecnologias de deteção e monitorização existentes, sua aplicação e utilização.

- Câmaras e sistemas de alarme
- Deteção de intrusão e movimento.

Unidade Didática 5: Gestão de Pessoal de Segurança e Treino Específico

A última unidade aborda as questões da seleção e treino de elementos para postos de grande complexidade e exigência, a formação específica e os procedimentos a adotar num ambiente de proteção de infraestruturas críticas.

- Seleção e formação de pessoal
- Procedimentos operacionais e coordenação.

MÓDULO 3: COMO PREVENIR CIBERATAQUES?

[Duração: 39 horas teórico-práticas | 3 semanas]

1. Normas internacionais de segurança digital
2. Consciencialização e treino de colaboradores
3. Implementação de políticas e procedimentos de segurança digital
4. Gestão de acessos e autenticação
5. Monitorização e procura de ameaças digitais
6. Prevenção e interceção de ataques digitais

Objetivos do módulo

- Compreender as normas internacionais de segurança digital como a ISO 27001 e o NIST, bem como o processo de certificação para essas normas.
- Desenvolver uma consciencialização sobre a importância da segurança digital entre os colaboradores e fornecer-lhes treino adequado para a identificação e prevenção de possíveis ameaças.
- Implementar políticas e procedimentos robustos de segurança digital na organização, incluindo a definição de responsabilidades e a revisão regular das políticas.
- Estabelecer uma gestão de acessos e autenticação eficaz, que inclui o controle de acessos, a atribuição de privilégios e a utilização de autenticação multifatorial.
- Desenvolver uma estratégia para a monitorização constante e a procura ativa de ameaças digitais, utilizando ferramentas e técnicas adequadas.
- Preparar a organização para prevenir e intercetar ataques digitais, através do uso de firewalls, sistemas de prevenção de intrusões, proteção contra *malware* e medidas contra ataques de *phishing*.

Competências a adquirir

- Aplicação das normas internacionais de segurança digital (ISO 27001, NIST) e do processo para a obtenção da respetiva certificação.
- Capacidades para consciencializar e treinar colaboradores no âmbito da segurança digital, incluindo a implementação de programas de educação e sensibilização e a condução de simulações e exercícios práticos.
- Competência para implementar políticas e procedimentos de segurança digital na organização, definindo responsabilidades claras e assegurando um controlo eficaz e a revisão regular das políticas.

- Capacidades para gerir acessos e autenticação na organização, incluindo o controlo de acessos, a atribuição de privilégios e a implementação de autenticação multifatorial.
- Capacidades para monitorizar e procurar ativamente ameaças digitais, utilizando para isso as ferramentas e técnicas mais adequadas.
- Competência para prevenir e intercetar ataques digitais, através do uso de firewalls, sistemas de prevenção de intrusões, e medidas de proteção contra *malware* e ataques de *phishing*.

Conteúdos programáticos

Unidade Didática 1: Normas internacionais de segurança digital

Esta unidade foca-se no estudo das normas internacionais de segurança digital, como a ISO 27001 e a NIST. Os participantes vão aprender sobre a estrutura e os objetivos destas normas, bem como sobre o processo de certificação.

- Estrutura e objetivos
- Processo de certificação.

Unidade Didática 2: Consciencialização e treino de colaboradores

Esta unidade aborda a importância da consciencialização e do treino dos colaboradores no âmbito da segurança digital. Os tópicos incluem a criação de programas de educação e sensibilização, e a realização de simulações e exercícios práticos.

- Programas de educação e sensibilização
- Simulações e exercícios práticos.

Unidade Didática 3: Implementação de políticas e procedimentos de segurança digital

Nesta unidade os participantes aprenderão como implementar políticas e procedimentos de segurança digital numa organização. Isso inclui a definição de responsabilidades e o controlo e revisão das políticas.

- Definição de responsabilidades
- Controle e revisão das políticas.

Unidade Didática 4: Gestão de acessos e autenticação

Esta unidade didática foca-se na gestão de acessos e autenticação. Os participantes vão aprender sobre o controlo de acessos e privilégios, bem como sobre a implementação de autenticação multifatorial.

- Controle de acessos e privilégios

- Autenticação multifatorial.

Unidade Didática 5: Monitorização e procura de ameaças digitais

A quinta unidade aborda a monitorização e a procura de ameaças digitais. Aqui, serão discutidas as ferramentas e técnicas de monitorização, bem como a análise de eventos e incidentes.

- Ferramentas e técnicas de monitorização
- Análise de eventos e incidentes.

Unidade Didática 6: Prevenção e interceção de ataques digitais

A última unidade didática foca-se na prevenção e interceção de ataques digitais. Os tópicos incluem o uso de *firewalls* e sistemas de prevenção de intrusões, bem como medidas de proteção contra *malware* e ataques de *phishing*.

- Firewalls e sistemas de prevenção de intrusões
- Proteção contra *malware* e ataques de *phishing*.

MÓDULO 4: COMO REAGIR A CIBERATAQUES? COMO RECUPERAR DE CIBERATAQUES?

[Duração: 39 horas teórico-práticas | 3 semanas]

1. Planear e implementar planos de resposta a incidentes
2. Normas internacionais para a resposta a incidentes (ISO 27035)
3. Coordenação e comunicação durante uma crise
4. Análise forense digital e recolha de provas
5. Recuperação de sistemas e retoma das operações
6. Revisão e melhoria contínua do plano de resposta a incidentes

Objetivos do módulo

- Compreender e ser capaz de planear e implementar planos de resposta a incidentes, conhecendo o processo e as etapas da resposta, assim como a necessidade de comunicação e coordenação interna e externa.
- Adquirir conhecimento sobre as normas internacionais para a resposta a incidentes, como a ISO 27035, compreendendo a sua estrutura, objetivos, e as boas práticas e procedimentos recomendados.
- Desenvolver capacidades para coordenação e comunicação eficazes durante uma crise, incluindo a definição dos papéis e responsabilidades da equipa de resposta e a comunicação com partes interessadas e autoridades.

- Ganhar competências na análise forense digital e recolha de provas, familiarizando-se com as metodologias e ferramentas de análise forense e compreendendo a importância da cadeia de custódia e preservação de evidências.
- Adquirir conhecimento sobre a recuperação de sistemas e retoma das operações após um ataque digital, aprendendo sobre as estratégias de recuperação e continuidade dos negócios, e como testar e validar planos de recuperação.
- Compreender a importância da revisão e melhoria contínua do plano de resposta a incidentes, incluindo a análise pós-incidente e a atualização de planos e políticas de segurança.

Competências a adquirir

- Planeamento e implementação eficaz de planos de resposta a incidentes, incluindo a gestão de comunicação e coordenação interna e externa em caso de incidentes.
- Compreensão e aplicação das normas internacionais para resposta a incidentes, como a ISO 27035, e as boas práticas e procedimentos recomendados.
- Coordenação eficaz e comunicação durante uma crise, incluindo a capacidade para definir papéis e responsabilidades da equipa de resposta, bem como comunicar adequadamente com partes interessadas e autoridades.
- Domínio de metodologias e ferramentas de análise forense digital e recolha de provas, preservando a cadeia de custódia e as evidências.
- Recuperação de sistemas e retoma das operações após um ataque digital, incluindo estratégias de recuperação e testes e validação dos planos de recuperação.
- Capacidade para realizar uma revisão e melhoria contínua do plano de resposta a incidentes, incluindo a análise de lições aprendidas pós-incidente e atualizações e ajustes nos planos e políticas de segurança.

Conteúdos programáticos

Unidade Didática 1: Planos de Resposta a Incidentes

Esta unidade didática foca-se no planeamento e implementação de planos de resposta a incidentes, abordando o processo e as etapas da resposta, bem como a importância da comunicação e coordenação interna e externa em caso de incidentes.

- Processo e etapas da resposta
- Comunicação e coordenação interna e externa.

Unidade Didática 2: Normas Internacionais e Resposta a Incidentes

Dedicada ao estudo das normas internacionais para a resposta a incidentes, como a ISO 27035. Serão explorados a estrutura, os objetivos e os procedimentos recomendados desta norma.

- Estrutura e objetivos
- Boas práticas e procedimentos recomendados.

Unidade Didática 3: Gestão da Crise: coordenação e comunicação

Aborda a coordenação e a comunicação durante uma crise, discutindo os papéis e as responsabilidades da equipa de resposta e a comunicação eficaz com as partes interessadas e autoridades.

- Papéis e responsabilidades da equipe de resposta
- Comunicação com partes interessadas e autoridades.

Unidade Didática 4: Análise Forense Digital e Recolha de Provas

Nesta unidade serão discutidas as metodologias e as ferramentas de análise forense, além de temas como a cadeia de custódia e a preservação de evidências.

- Metodologias e ferramentas de análise forense
- Cadeia de custódia e preservação de evidências.

Unidade Didática 5: Recuperação e Continuidade dos Negócios

Aborda estratégias de recuperação e continuidade dos negócios após ataques digitais. Os participantes aprenderão sobre testes e validação dos planos de recuperação.

- Estratégias de recuperação e continuidade dos negócios
- Testes e validação dos planos de recuperação.

Unidade Didática 6: Revisão e Melhoria Contínua dos Planos de Resposta

Esta unidade foca-se na revisão e melhoria contínua do plano de resposta a incidentes. São abordadas as lições aprendidas, a análise pós-incidente, bem como as atualizações e ajustes nos planos e políticas de segurança.

- Lições aprendidas e análise pós-incidente
- Atualizações e ajustes nos planos e políticas de segurança.

MÓDULO 5: EXERCÍCIO FINAL

[Duração: 26 horas práticas | 2 semanas]

1. Criptografia simétrica e assimétrica
2. Chaves de encriptação (pública/privada)
3. Criptografar e-mails (criptografia assimétrica)
4. Criptografar dados em suporte físico (criptografia simétrica)

Objetivos do módulo

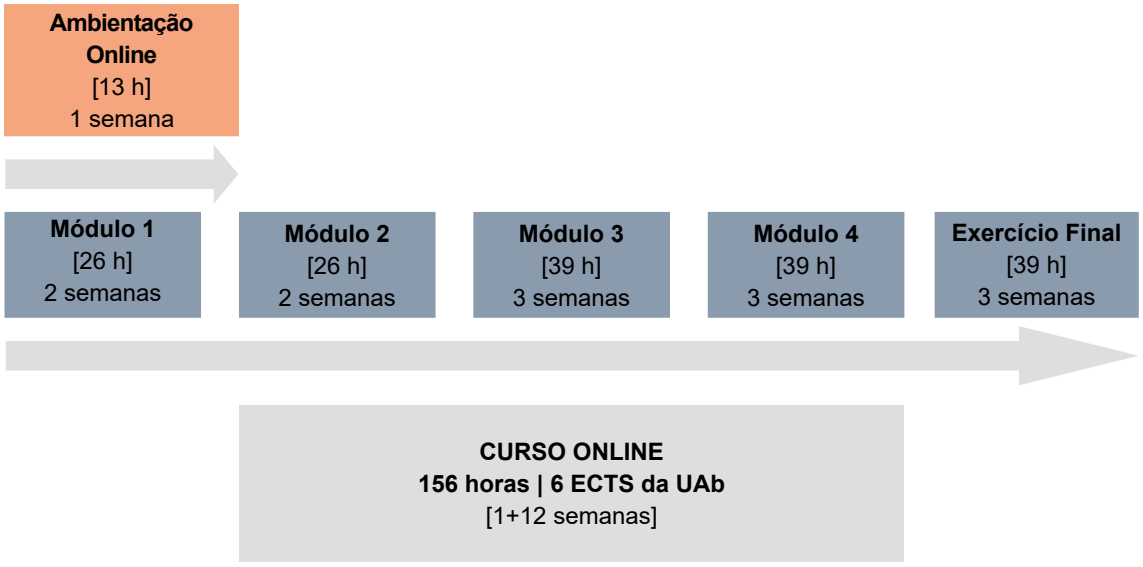
- Aplicar os princípios da segurança da informação, fundamentais para proteger dados e sistemas informáticos:
  - **Confidencialidade**: Garantia de que a informação é acessível apenas a pessoas autorizadas. É conseguida com criptografia.
  - **Integridade**: Garante que a informação só pode ser alterada por pessoas autorizadas e de que é maneira autorizada. É conseguida com funções de resumo criptográficas (hashes) e assinaturas digitais.
  - **Disponibilidade**: Assegura que a informação está disponível quando necessária. As cópias de segurança asseguram a disponibilidade.
  - **Autenticidade**: Assegura que as partes envolvidas numa comunicação são quem dizem ser. Os certificados digitais são uma forma de garantir a autenticidade.
  - **Não repúdio**: Assegura que uma parte envolvida numa transação não pode negar ter participado. As assinaturas digitais garantem o não repúdio.
  - **Legalidade**: Refere-se à necessidade de cumprir com as leis e regulamentações aplicáveis na recolha, utilização e gestão de dados.
- Compreender e aplicar criptografia simétrica e assimétrica.
- Configurar e utilizar corretamente software de código aberto para gerar um par de chaves pública/privada.
- Utilizar um servidor de chaves públicas para publicar a chave pública do remetente.
- Utilizar um servidor de chaves públicas para procurar a chave pública do destinatário para estabelecer com esse destinatário uma comunicação encriptada.
- Demonstrar compreensão dos princípios e práticas de criptografia (assimétrica) de correio eletrónico ao enviar e receber um e-mail encriptado e assinado digitalmente através do uso de software de código aberto.

- Demonstrar compreensão dos princípios e práticas de criptografia (simétrica) em suporte físico através do uso de software de código aberto.
- Importar a chave pública dos remetentes para os gestores de chaves dos softwares de código aberto utilizados para estabelecer com esses remetentes uma comunicação encriptada.
- Exportar as chaves públicas e privadas para um ficheiro de modo a poderem ser usadas noutro software de encriptação.
- Importar a chave privada para outros softwares de encriptação.
- Verificar a autenticidade de dados através de funções resumo (*hashes*).
- Demonstrar a capacidade de assinar um documento com o Cartão de Cidadão e com Chave Móvel Digital provando a sua autenticidade e não repúdio.
- Demonstrar a capacidade de autenticação com o Cartão de Cidadão e com a Chave Móvel Digital.

DURAÇÃO E ESTRUTURA

A duração do curso é de **156 horas**, que correspondem a **6 ECTS da UAb** (volume de trabalho dos formandos) e está estruturado em 4 módulos de realização sequencial, seguidos de um módulo correspondente a um Exercício Final, e precedidos de um módulo inicial de Ambientação ao Contexto Online.

O curso decorre durante 12 semanas, podendo, no entanto, esta duração alterar-se devido a circunstâncias anómalas e excecionais.



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).

A forma de trabalho utilizada neste curso compreende:

- a leitura e reflexão individuais dos conteúdos disponibilizados ou de outros sobre os mesmos temas obtidos pelos formandos;
- a partilha da reflexão e do estudo com os colegas;
- o esclarecimento de dúvidas nos fóruns moderados pelo formador;
- a realização das e-atividades propostas (testes, trabalhos, sínteses, etc.).

A leitura e a reflexão individuais devem acontecer ao longo de todo o processo de aprendizagem e sem elas o formando fica muito limitado na sua participação nos fóruns previstos, assim como também dificilmente poderá realizar com sucesso as atividades programadas.

A aprendizagem está estruturada por Tópicos que correspondem a módulos do curso. Em cada Tópico será criado um fórum moderado pelo formador para esclarecimento das dúvidas e ultrapassagem das dificuldades sentidas e apresentadas pelos formandos, proporcionando assim uma possibilidade de interação permanente dos formandos entre si e com o formador.

Todos os fóruns decorridos permanecerão abertos ao longo de todo o curso, possibilitando assim a consulta a todo o tempo das mensagens trocadas. No entanto, quaisquer mensagens enviadas depois de terminado o módulo em que o fórum de discussão decorreu não serão consideradas pelos professores para efeitos de classificação da participação nesse fórum.

No módulo 0 e de acordo com o modelo de ensino/aprendizagem de Salmon cumprem-se os níveis 1 e 2, respetivamente “acesso e motivação” e a “socialização online”; dependendo do grupo concreto de formandos iniciar-se-á, ou não, o nível 3 de “processamento de conteúdos” onde a tutoria se consubstancia no apoio na utilização de materiais pedagógicos e nas tarefas, nesta fase apenas em relação ao modo como fazer pesquisa orientada em WWW.

Nos módulos seguintes cumprem-se todos os restantes níveis do modelo de Gilly Salmon, “processamento de conteúdos” centrado na interação com os materiais de aprendizagem e com os restantes participantes do curso (colegas e formadores), “construção do conhecimento” onde é natural que o papel do formador se dilua e “exploração”, nível onde o suporte técnico disponibiliza novas fontes de informação e a tutoria dá apoio e resposta a questões.

Em dados momentos do curso os formadores enviam aos formandos as e-atividades que devem realizar no prazo previsto, e enviar ao formador para avaliação até a data e hora limite indicadas.

Dada a natureza do tipo de trabalho a realizar pelos participantes, o acompanhamento dos mesmos exige grande disponibilidade por parte dos formadores, pelo que cada turma virtual não deve ter um número muito elevado de e-formandos.

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 PlataformAbERTA.

Embora o curso seja essencialmente assíncrono, podem realizar-se sessões síncronas de discussão online ou de webconferência, em datas, horários e locais (Tópicos da Moodle) a comunicar antecipadamente pelos formadores.

RECURSOS DE APRENDIZAGEM

Recursos pedagógicos

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

- Textos base sobre os temas a abordar, colocados online no espaço do curso criado na PlataformAbERTA 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 do Curso;
- Guia do Formando Online.

Recursos técnicos

PlataformAbERTA que integra o LMS Moodle, em https://elearning.uab.pt/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

BIBLIOGRAFIA (Indicativa)

- Martins, José (2021). Gestão de Segurança da Informação e Cibersegurança nas Organizações - Sistema e Método, Sílabas & Desafios.
- Cunha, Luís et al (2022). Segurança e Defesa do Ciberespaço. Instituto de Defesa Nacional, Lisboa.
- Centro Criptológico Nacional, Ministério de Defensa, (2023). Guia de Seguridad da las TIC.
- National Institute of Standards and Technology (2019). Estrutura de Segurança Cibernética.
- Universidade Aberta (2022), Lisboa. Políticas Específicas de Segurança da Informação.
- Organização dos Estados Americanos. Manual de Suporte Sobre Risco Cibernético para o Conselho de Administração.
- U.S Chamber of Commerce (2014). Guia de Aperfeiçoamento da Segurança Cibernética para Infraestruturas Críticas.
- Center for Internet Security, V8.1. (pdf online) CIS (2018). 20 Controlos de Cibersegurança.
- CNCS (2019). Quadro Nacional de Referência para a Cibersegurança (QNRCS).

AVALIAÇÃO E CLASSIFICAÇÃO

Avaliação nos Módulos

Os módulos 1 a 4 do curso são sujeitos a avaliação. Cada módulo integra 3 instrumentos de avaliação:

- Avaliação contínua na participação individual nos fóruns de discussão abertos no espaço do módulo;
- Realização de uma e-atividade intercalar a submeter na plataforma da UAb;
- Um teste ou trabalho final do módulo, a realizar na plataforma de suporte ao curso.

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

A média final da avaliação dos módulos tem um peso de 60% na classificação final.

- Na avaliação da participação individual dos alunos num fora 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 intercalares 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:

$$CFC = \left(\frac{CM1 + CM2 + 1{,}5 \times CM3 + 1{,}5 \times CM4}{5}\right) \times 0{,}6 + (EF \times 0{,}4\ )$$

onde CMx representa a Avaliação Final do Módulo x e EF a classificação do Exercício final.

Consideram-se com aproveitamento no curso os formandos que obtiverem, **cumulativamente**, e sempre uma escala de 0 a 20 valores:

- Classificação mínima de 8 valores em cada módulo;
- Realização do Exercício Final com classificação mínima de 9,5 valores;
- **Classificação Final no Curso igual ou superior 9,5 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 candidatura ao curso.

A todos os formandos que tenham realizado integralmente o curso e o terminaram sem aproveitamento, **a seu pedido expresso**, será entregue uma **Declaração de Frequência**.

EQUIPA DOCENTE

FORMADORES	MÓDULOS
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas/funcionalidades da PlataformAbERTA
Luís Tavares de Jesus	1. Legislação sobre Segurança Privada (SP) e Regulamento Geral de Proteção de Dados (RGPD)
David Arroio Carreira	2. Sistemas de Segurança Física (SSF): instalações, perímetros, equipamentos e pessoas
João Magalhães Mateus	3. Como prevenir ciberataques? 4. Como reagir a ciberataques? Como recuperar de ciberataques? 5. Exercício Final

SÍNTESE DOS *CURRICULA VITAE* DOS FORMADORES

Luís Manuel Tavares de Jesus é licenciado em Direito pela Universidade Autónoma de Lisboa e possui diversos cursos de formação designadamente os de Formação Pedagógica de Formadores, de Técnico Superior de Segurança e Higiene do trabalho, de Legislação Laboral, de Formação de Formadores de Assistentes de Recintos Desportivos e de Formação de Formadores em Igualdade de Oportunidades.
Possui experiência profissional como gestor de logística e de ativos humanos e como formador de temas relacionados com a segurança privada e com segurança e higiene do trabalho. É titular de CAP de formador. Possui o CAP de Técnico Superior de Segurança e Higiene do Trabalho. Possui o igualmente o CAP de formador de Assistentes de Recinto Desportivo (autorização legislativa da Portaria n.º 1522-B/2002 de 20Dez.). É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2010. É formador do Curso de Especialização em Direção de Segurança (CEDS) da UAb.

David Elias Arroio Mendes Carreira é licenciado em Ciência Política pelo Instituto Superior de Ciências Sociais e Políticas (ISCSP) da Universidade Técnica de Lisboa e Mestre em Relações Internacionais pelo mesmo instituto. Possui a Pós-graduação em Informações e Segurança do ISCSP e os cursos de Vigilante de Segurança Privada (módulos 3 e 4). Desempenhou funções diversas no Departamento de Polícia e Fiscalização da Câmara Municipal de Cascais e numa empresa de Segurança Privada. É consultor de Segurança Privada nos domínios da segurança no trabalho (safety) e da segurança de pessoas, bens e equipamentos (security). É formador do Curso de Especialização em Direção de Segurança (CEDS) da UAb.

João Guilherme Conde Magalhães Mateus é licenciado em Engenharia Eletrotécnica e de Computadores e em Engenharia Informática, e mestre em Investigação Operacional e Engenharia de Sistemas, graus obtidos no Instituto Superior Técnico. É formador do Curso de Especialização em Direção de Segurança (CEDS) da UAb. É Professor de Cibersegurança na Universidade Aberta, na Universidade Europeia, na Universidade Atlântica e na Academia Militar. É formador da UALV/UAb desde 2010.

COORDENAÇÃO DO CURSO

O curso é coordenado pelo Diretor da UALV da UAb, Professor Doutor Fernando Caetano.

A coordenação do curso é responsável, nomeadamente, por:

a) superintender aos processos de seleção de candidatas/os;

b) coordenar a organização e atualização de um dossier técnico-pedagógico de curso, contendo os dados das/os estudantes inscritos, os contratos de aprendizagem/formação, das avaliações e classificações e demais documentos inerentes ao seu funcionamento;

c) organizar e dinamizar um módulo de ambientação online para as/os estudantes admitidas/os e que não tenham uma frequência anterior na Universidade;

d) organizar e dinamizar um espaço de socialização online aberto a toda/os as/os estudantes e docentes do curso;

e) decidir em eventuais conflitos decorrentes do funcionamento do curso e em casos não previstos no respetivo guia de curso.