UNIVERSIDADE ABERTA

[GUIA DO CURSO]

CURSO DE ESPECIALIZAÇÃO EM

CIBER SEGURANÇA

Aprendizagem ao Longo da Vida

CURSO DE ESPECIALIZAÇÃO EM CIBERSEGURANÇA

|regime de e-learning|

**[Somente amadores atacam máquinas;
os profissionais atingem as pessoas.
Bruce Schneier, 1963]**

ÍNDICE

Universidade Pública de Ensino a Distância

A Universidade Aberta (UAb), universidade pública de ensino a distância estatutariamente tem como missão, no contexto universitário português e de acordo com a lei que o enquadra, a criação, transmissão e difusão da cultura, dos saberes, das artes, da ciência e da tecnologia, ao serviço da sociedade, através da articulação do estudo, do ensino, da aprendizagem, da investigação e da prestação de serviços.

A Universidade é uma pessoa coletiva de direito público (NPC 502 110 660) e goza de autonomia estatutária, pedagógica, científica, cultural, administrativa, financeira, patrimonial e disciplinar, podendo, na prossecução dos seus fins, por si só ou em cooperação com outras entidades, universitárias ou outras, tanto públicas como privadas, criar ou incorporar no seu âmbito pessoas coletivas de direito privado.

A Universidade tem a sua sede em Lisboa e dispõe de delegações nas cidades do Porto e de Coimbra, podendo criar outras delegações ou entidades de apoio, no território nacional ou fora dele, necessárias à realização dos seus objetivos.

Nos termos da lei, são atribuições da Universidade:

a) Realizar ciclos de estudos visando a atribuição de graus académicos, bem como de outros cursos pós -secundários, de cursos de formação pós -graduada e de outros, nos termos da lei, destinados a populações que procurem o ensino a distância;

b) Promover a aprendizagem ao longo da vida, nomeadamente através de ações de formação, qualificação e reconversão profissional, em domínios estratégicos para o desenvolvimento e a atualização de conhecimentos;

c) Garantir que, a todo o tempo, será considerada a especificidade dos estudantes de ensino a distância, através do apoio e enquadramento pedagógico, bem como da salvaguarda dos respetivos direitos;

d) Realizar investigação e apoiar a participação dos seus docentes e investigadores em instituições científicas;

e) Conceber, produzir e difundir recursos educacionais mediatizados e em rede, suscetíveis de utilização através das tecnologias de informação e comunicação, destinados ao ensino formal e não formal a qualquer nível, à defesa e promoção da língua e da cultura portuguesas, no País e no estrangeiro, com especial relevo para os países e comunidades de língua portuguesa;

f) Contribuir para a difusão e a promoção da sociedade do conhecimento, incentivando, pela sua metodologia própria, a inclusão digital, a apropriação e a autoconstrução de saberes e a transferência e a valorização económica do conhecimento científico e tecnológico;

g) Promover a cooperação e o intercâmbio cultural, científico e técnico com instituições congéneres, nacionais e estrangeiras;

h) Contribuir, no seu âmbito de atividade, para a cooperação internacional e para a aproximação entre os povos, com especial destaque para os países de língua oficial portuguesa e os países europeus;

Estas atribuições abrangem o território nacional, podendo ser extensivas a estruturas delegadas, para esse fim criadas no estrangeiro.

Fundada em 1988, a UAb é a única instituição de ensino superior público vocacionada para o ensino a distância. Desde o início, a UAb tem estado orientada para a educação de grandes massas populacionais geograficamente dispersas, tendo-se já proporcionado formação de nível superior a mais de 10 mil estudantes, em 33 países dos cinco continentes, licenciando-se mais de 9 mil estudantes, concedendo-se mais de um milhar de graus de mestre e cerca de uma centena de graus de doutor. Pioneira no ensino superior a distância em Portugal, a UAb tem promovido ações relacionadas com a formação superior e a formação contínua, contribuindo igualmente para a divulgação e a expansão da língua e da cultura portuguesas, com especial relevo nos países e comunidades lusófonos. Ao longo dos 20 anos de existência da UAb, os seus docentes e investigadores têm desenvolvido atividades de investigação científica através da utilização das tecnologias da informação e da comunicação, concebendo e produzindo materiais pedagógicos nas áreas da tecnologia do ensino e da formação a distância, e da comunicação educacional multimédia.
Com mais de 400 títulos editados, de 3500 horas de produções audiovisuais e de 6000 horas de emissões televisivas, produzidas nos seus estúdios, a UAb tem procurado sobretudo incentivar a apropriação e a autoconstrução de saberes, concebendo e lecionando cursos, formando técnicos e docentes, de acordo com uma filosofia de prestação de serviço público.

Estudantes-alvo

A UAb assume como missão fundamental formar estudantes que, por várias razões, não puderam, no seu tempo próprio, encetar ou prosseguir estudos universitários. Por outro lado, a UAb procura corresponder às expectativas de quantos, tendo eventualmente obtido formação superior, desejam reconvertê-la ou atualizá-la; o que significa que, por vocação, tenta ir ao encontro das expectativas de um público adulto, com experiência de vida e normalmente já empenhado no exercício de uma profissão.

Assim, é condição necessária para ingressar na UAb ter mais de 21 anos de idade e realizar provas de acesso a esta universidade, que não integra o concurso nacional de acesso ao ensino superior. As licenciaturas da UAb não têm *numerus clausus*. A UAb também efetua provas especialmente destinadas a Avaliar a Capacidade para a Frequência do Ensino Superior (ACFES) dos maiores de 23 anos.

Pioneira no E-learning em Portugal

Enquanto universidade pioneira no Ensino Superior a Distância em Portugal, e tendo em conta a sua responsabilidade como principal centro nacional de competência nesta área, a UAb desenvolveu um inestimável *know-how,* que lhe permitiu constituir a maior bolsa de oferta de cursos *online* do País.

No ano letivo 2008-2009, a UAb tornou-se na primeira e única universidade (pública) em Portugal a lecionar todas as licenciaturas e mestrados pela Internet, em regime de e-learning, através de um Modelo pedagógico virtual inédito no País e desenvolvido por esta instituição.

A UAb é também considerada um dos *mega-providers* de *e-learning* europeus, desempenhando um papel preponderante na lecionação de cursos de 1.º Ciclo (licenciaturas) e de 2.º Ciclo (mestrados), em domínios das Humanidades, das Ciências e Tecnologia, da Educação e Ensino a Distância, das Ciências Sociais e da Gestão. Todos os cursos de licenciatura e mestrado da UAb estão adequados ao Processo de Bolonha.

Modelo pedagógico virtual

O modelo pedagógico da UAb assenta no regime de *e-learning* e na utilização intensiva das novas ferramentas de comunicação *online*. Promovendo a interação entre estudantes e docentes, este modelo está fortemente *centrado no estudante* enquanto indivíduo ativo e construtor do seu conhecimento. Permite ainda uma maior *flexibilidade na aprendizagem*, onde a comunicação e a *interação* se processam de acordo com a disponibilidade do estudante, partilhando recursos, conhecimentos e atividades com os seus pares. A avaliação dos conhecimentos e competências,

baseada na avaliação contínua, assume soluções diversificadas. Nos cursos de graduação, o estudante possui um cartão de aprendizagem onde investe ao longo do seu percurso, realizando *e-fólios*, creditando *e-valores* e efetuando provas presenciais. Nos cursos de pós-graduação, a avaliação desenvolve-se de formas muito variadas, recorrendo, por exemplo, a *portfólios*, blogs, projetos, ensaios, resolução de problemas, participação em discussões, relatórios e testes.

Inclusão digital

A frequência da UAb é fator de inclusão social pela vertente da alfabetização digital: o ensino *online* exige competências específicas por parte do estudante, pelo que todos os programas de formação certificados pela UAb incluem um módulo prévio, de frequência gratuita. Deste modo, os novos estudantes podem adquirir as competências necessárias à frequência do curso ou do programa de formação em que se inscrevem.

A atual expansão da *Internet* e da *Word Wide Web (WWW)* e o desenvolvimento ainda mais recente dos programas informáticos de gestão do ensino/aprendizagem, vieram modificar o panorama do ensino a distância, permitindo a criação de espaços virtuais de ensino com designações diversas, *centro de ensino virtual, escola virtual, etc.,* onde a palavra virtual apenas significa que esses espaços não têm implantação e realidade físicas palpáveis.

É, pois, no espaço virtual de formação/aprendizagem da UAb (em http://www.moodle.univ-ab.pt/moodle/) que se vai desenvolver a ação de formação de aprendizagem ao longo da vida designada ***Curso de Especialização em Cibersegurança.***

A Universidade Aberta, instituição de direito público, tutelada pelo Ministério da Ciência, Tecnologia e Ensino Superior, encontra-se abrangida pelo Art.º 2.º da Portaria n.º 782/97 de 29 de agosto e, por força dos seus estatutos, não carece de acreditação/certificação como entidade formadora por parte Direção de Serviços de Qualidade e Acreditação da **Direção-Geral do Emprego e das Relações de Trabalho (DGERT)** ou de qualquer outra entidade certificadora**.**

"O *hardware* é fácil de proteger: de trancar numa sala, prender com cadeados a uma mesa ou comprar um suplente. A informação é que representa o problema. Pode existir em mais de um lugar; ser transportada pelo planeta em segundos; e ser roubada sem o seu conhecimento."[1]

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 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.

Sendo certo que o mundo digital trouxe inúmeras vantagens e progresso, também é verdade que existem fortes ameaças neste mundo. 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

[1] Bruce Schneier - criptólogo

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 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.

É neste enquadramento que a **Universidade Aberta** (UAb) organizou e pretende oferecer ao mercado de formação este curso de especialização.

O presente curso desenvolve-se em regime de formação teórica e prática a distância online (também dito *e-learning*), com uma componente de avaliação final baseada na elaboração de um projeto prático, a depositar na plataforma informática para análise, correção e classificação pelos professores até à data-hora estabelecida.

OBJETIVOS DO CURSO

Os objetivos do curso são:

- Proporcionar conhecimentos e competências que permitam aos participantes caracterizar os ataques típicos bem como as defesas correspondentes, bem como o enquadramento legal do cibercrime, o Regulamento Geral de Proteção de Dados e as normas internacionais (ISO) sobre segurança da informação;
- 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;

f) Realizar na prática e em ambiente simulado ataques a redes e sistemas (testes de penetração – "*pen tests*") que poderão replicar em ambiente real de modo a testar a sua própria organização;

g) Realizar na prática e em ambiente simulado a defesa a ataques a redes e sistemas e os respetivos procedimentos na resposta a incidentes.

O regime de funcionamento *online* suportado por uma plataforma informática de gestão da formação/aprendizagem permitirá ainda alcançar outros objetivos e adquirir outras competências, secundários em relação ao âmbito geral deste curso, mas de extrema e atual importância para a empregabilidade. Deste modo os formandos irão adquirir e treinar competências nos domínios da comunicação e das Tecnologias de Informação e Comunicação (TIC) que lhes permitam no futuro uma mais fácil pesquisa de informações técnicas de que necessitem para o seu trabalho, mais rápido e fácil contacto com os seus pares nacionais e internacionais e ainda competências para a frequência de outras ações de formação a distância na modalidade de *e-learning*.

COMPETÊNCIAS A ADQUIRIR

No final do curso espera-se que os participantes tenham adquirido as seguintes competências:

- 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;
- Realizar testes de penetração em redes e sistemas (*Pen-Tests*);
- Aplicar técnicas de navegação digital segura;
- Reagir a ataques e adotar procedimentos de resposta a incidentes;
- Pesquisar e organizar informação, de forma orientada, com recurso à Web;

Este curso permitirá ainda aos formandos adquirir diferentes competências ditas para a empregabilidade, designadamente competências:

- Para aprender continuamente e em regime de autoaprendizagem;
- De orientação para resultados;
- De intercomunicação *online* e de *networking;*
- De trabalho em equipa;
- Na utilização de tecnologias informáticas;
- Na autogestão do tempo e das actividades.

O curso de Especialização em Cibersegurança está estruturado em 8 módulos, com a duração de uma semana cada, que se desenvolvem sequencialmente. Estes módulos são precedidos de um módulo de ambientação ao contexto *online* do curso e de integração dos participantes, por vezes designado módulo 0 ou pré-curso.

A componente escolar do curso tem a duração de 104 horas (volume de trabalho dos formandos) a que corresponde um crédito de 4 ECTS[2] da UAb e realiza-se em regime de formação a distância online (*e-learning*) ao longo de 9 semanas.

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

Módulo 0: Ambientação ao contexto o*nline* do curso
Duração: 13 horas práticas/1 semana

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* por forma a adquirirem as competências necessárias à exploração eficaz de todas as suas funcionalidades de intercomunicação, em especial as assíncronas, necessárias à frequência do curso.

Durante o Módulo 0 será ainda explicada e treinada a forma como pesquisar "depressa e bem" informação na Web e será pedido aos participantes a procura (na Web) de informação relevante sobre temas que constituam matérias do curso

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.

[2] 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.

- Pesquisar, selecionar e organizar informação a partir da Web para a transformar em conhecimento mobilizável.
- Pesquisar, organizar, tratar e produzir informação em função das necessidades, problemas a resolver e das situações.

Unidade Didática 1: A plataforma informática de ensino/aprendizagem da UAb

O que é o Moodle;

Formas de organizar espaços/sites no Moodle;

Recursos e atividades da plataforma Moodle

Estrutura do espaço Moodle do CEDS; tópicos do curso; recursos disponíveis e ferramentas a utilizar.

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

Treino com fóruns, trabalhos, questionários, wikis, referendos, equipas, etc.

Unidade Didática 3: Prática de pesquisa de informação na Web

Como procurar informação usando: palavras-chave, operadores booleanos, sinais, especificação de formatos, aspas e asteriscos;

Motores de busca e meta-motores;

Credibilidade da informação na Web. Critérios de avaliação.

Módulo 1: Requisitos de segurança
Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo

Enquadrar a segurança de informação no contexto geral da segurança da empresa/organização.

Compreender objetivos e os requisitos de Segurança da Informação.

Aplicar na prática os requisitos de Segurança da Informação

Competências a adquirir

- Capacidade para distinguir os requisitos de segurança da informação;
- Capacidade para usar o cartão do cidadão para autenticação;
- Capacidade para usar o cartão do cidadão na assinatura digital de documentos com força legal;

Unidade Didática 1: Objetivos da segurança da informação

Criação de uma base de proteção e confiança sobre a qual é desenvolvida o negócio da empresa/organização

Proteção e preservação de ativos - processos, produtos, informação

Relação Custo/Benefício, Concentração, Proteção em Profundidade, Consistência, Redundância.

Unidade Didática 2: Princípios e Requisitos da Segurança da Informação

Vertentes e Princípios da Segurança da Informação

Requisitos da Segurança da Informação

Autenticidade, Integridade, Confidencialidade, Privacidade, Responsabilidade (Não Repúdio), Disponibilidade, Autorização

Unidade Didática 3: Aplicação dos princípios da Segurança da Informação

Autenticação com Cartão do Cidadão.

Assinatura de documentos digitais com força legal com o Cartão do Cidadão aplicando os requisitos de Segurança da Informação.

Prática em contexto de formação

No decurso deste módulo, os alunos colocados perante situações práticas serão instados a:

- Efetuar a autenticação com o cartão do cidadão num organismo do estado português.
- Assinar eletronicamente um documento digital, com força legal.

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

Módulo 2: Encriptação de dados e infraestrutura de chave pública
Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo:

Desenvolver nos alunos a capacidade de cifrar a informação digital.

Competências a adquirir:

- Encriptar dados em suporte físico.
- Implementar um sistema de correio eletrónico cifrado para a sua empresa/organização

Unidade didática 1: Fundamentos de criptografia

Criptografia Simétrica e Assimétrica;
Chave Pública;
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).

Unidade didática 3: **Encriptação de correio eletrónico**

A necessidade de encriptar correio eletrónico.
Ferramentas e encriptação de correio eletrónico.

Prática de encriptação 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: Normas e legislação aplicável
Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo

Conhecer a legislação nacional relativa ao cibercrime e proteção de dados.

Conhecer as principais normas internacionais (ISO) referentes à segurança da informação.

Elaborar uma Política de Segurança da Informação.

Competências a adquirir

- Identificar os principais diplomas relativos ao cibercrime;
- Identificar as principais normas internacionais relativas à segurança da informação;
- Saber elaborar uma Política de Segurança da Informação para uma empresa/organização.

Conteúdos programáticos

Unidade didática 1: Legislação e regulamentação nacionais

Lei do Cibercrime.

Regulamento Geral de Proteção de Dados

Unidade didática 2: Normas Internacionais

Norma ISO 27001 - Requisitos para Sistema de Gestão de Segurança da Informação.

Norma ISO 27002 - Código de Boas Práticas para Gestão da Segurança da Informação.

Norma ISO 27005 - Técnicas de segurança - gestão de risco de SI.

Unidade didática 3: Documentos fundamentais ao negócio

Plano de continuidade de negócio (ISO 22301)

Plano de recuperação de desastres (ISO 27031).

Política de Segurança da Informação (ISO 27001).

O trabalho final deste módulo consiste na elaboração de uma Política de Segurança da Informação para a empresa/organização do formando ou empresa/organização fictícia. Os alunos realizarão ainda um teste na plataforma Moodle para validação de conhecimentos.

Módulo 4: Análise forense digital
Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo:

Conhecer o enquadramento legal da Análise Forense Digital.

Conhecer algumas técnicas de análise forense digital que permitam a obtenção de prova digital.

Conhecer as técnicas anti-forense e de anonimização mais comuns.

Competências a adquirir

- Identificar o enquadramento legal do cibercrime.
- Obtenção de provas focando a integridade.
- Diagnosticar – "Quem, O quê, Onde e Quando"
- Documentar ataques e ações maliciosas

Conteúdos programáticos

Unidade didática 1: Introdução à Análise Forense Digital

Enquadramento Legal da obtenção de provas.

Construção do laboratório forense com recurso a máquinas virtuais

Exemplos de casos reais de aplicação da análise forense digital.

Unidade didática 2: Conceitos técnicos chave

Bits, Bytes, Codificação. Tipos de ficheiros e assinaturas.

Dispositivos de armazenamento voláteis e não voláteis. Sistemas de ficheiros, espaço alocado e não alocado.

Unidade didática 3: Identificação, isolamento, colheita e preservação da prova digital

Obtenção de provas, focando os requisitos de integridade e admissibilidade.

Aquisição de prova digital e documentação (cadeia de custódio da prova digital).

Clonagem e verificação de integridade. Aquisição Live ou offline.

Prática em contexto de formação adequada à unidade didática.

Unidade didática 4: Aquisição em sistemas Windows

Técnicas mais comuns para obtenção de provas em sistemas Windows:
ficheiros apagados, ficheiros de hibernação ou sleep, registo do windows, atividade do utilizador, pontos de restauro, recentemente usados, spooler de impressão, metadados, prefetch, ficheiros .lnk, dispositivos USB.

Unidade didática 5: Anti-forense digital e desafios futuros

Ocultação, ofuscação e encriptação de dados. Falsificação, exclusão e destruição de dados. Obstrução à colheita de prova digital.
Técnicas anti-forense: anonimização, deep web, dark web, bitcoins e criptocurrency. Ferramentas e exemplos práticos - Thor.Desafios atuais e futuros: Análise Forense em redes, plataforma móveis e cloud.

Prática em contexto de formação

Para além da componente teórica, o módulo de Análise forense digital visa também preparar os formandos numa perspetiva prática. Por esse motivo, no decorrer do mesmo, os formandos serão colocados perante situações práticas e incentivados a:

- Elaborarem prova de um ataque e
- Debaterem no respetivo fórum os vários temas que constituem o objeto do módulo (objeto de apreciação e avaliação formativa).

O trabalho final deste módulo consiste na resolução de um caso prático em ambiente de laboratório forense, em que os formandos deverão ser capazes de distinguir evidências de um ataque.
Este trabalho é objeto de apreciação e de avaliação sumativa.
Os alunos realizarão ainda um teste na plataforma Moodle para validação de conhecimentos.

Módulo 5: Segurança de sistemas informáticos
Duração: 13 horas teórico-práticas/1 semanas

Objetivos do módulo

Identificar e caracterizar os ataques típicos de modo a estabelecer as respetivas defesas.
Ter conhecimento das principais tipologias de ataques que a sua empresa ou organização poderá ser alvo e ele próprio como cidadão.
Conhecer os principais serviços de autenticação e canais seguros, de modo a mitigar

o risco de intrusão de utilizadores não credenciados.

Competência a adquirir

- Capacidade para avaliar ataques;
- Capacidade para adotar e fazer adotar medidas preventivas;
- Capacidade para autenticar e usar canais seguros de comunicação.

Conteúdos programáticos

Unidade Didática 1: Ataques típicos

Caracterização dos ataques típicos.

Defesas para os ataques típicos;

Ameaças e vulnerabilidades;

Sistemas defensivos / meios de proteção;

Unidade Didática 2: Autenticação e serviços de autenticação

Caracterização dos protocolos de autenticação, elementos de prova e medidas defensivas contra-ataques de dicionário;

Autenticação baseada no conhecimento;

Autenticação baseada na propriedade;

Autenticação baseada na característica;

Senhas, chaves secretas partilhadas, chaves privadas e senhas descartáveis;

Unidade Didática 3: Utilização de canais seguros

Saber verificar e adoptar utilização de canais seguros na internet (VPN, TLS – SSL).

Prática em contexto de formação:

No decurso deste módulo, os alunos são incentivados e orientados para:

- Usar técnicas de autenticação forte;
- Usar canais seguros.

O trabalho final do módulo consiste na resolução de um caso prático que será objeto de apreciação e de avaliação sumativa.

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

Módulo 6: *Ethical Hacking*

Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo:

Compreender o modo de atuação de um hacker e a morfologia de um ataque para poder neutralizar ou mitigar os efeitos de suas ações.

Competências a adquirir:

- Capacidade para realizar ações de OSINT (Open source intelligence);
- Deteção de vulnerabilidades;
- Exploração da vulnerabilidade com código malicioso - Payload - fornecendo acesso privilegiado e permissões;
- Execução de ações no alvo após ter obtido o acesso;
- Adquirir conceitos base para execução de testes de penetração;

Conteúdos programáticos:

Unidade didática 1: Morfologia de um Ciber ataque

1. Reconhecimento (recolher informação)
2. Aquisição da ferramenta para chegar ao alvo (gerar o *malware*)
3. Fazer entrar o *malware* na empresa (entregar e instalar o *malware,* por exemplo com Engenharia Social)
4. Ações no objetivo e apagar vestígios.

Unidade didática 2: OSINT (Open source intelligence)

Conceito de reconhecimento passivo *versus* ativo.

Principais fontes para a recolher informações na web (WHOIS, google dorks, Shodan, Netcraft, Sensys, Maltego, etc.).

Obter informações sobre empresas e sobre pessoas.

Desenhar o grafo que permite identificar pontos vulneráveis.

Unidade didática 3: Testes de penetração

Introdução aos conceitos de PenTest (black-box, whitebox, grey-box).

Frameworks para Pentests (OWASP, OSSTMM, ISSAF).

Instalar o Kali Linux: utilizar o metasploit, veil e empire. Criar backdoors para sistemas Windows e Linux. Enviar o payload para a vítima contornando os sistemas de

segurança (antivírus, etc.). Realizar ações no objetivo (como exemplo obter passwords guardadas nos browsers).

Prática em contexto de formação

Recolha de informação com recurso a "fontes abertas".

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

Módulo 7: Técnicas de proteção digital
Duração: 13 horas teórico-práticas/1 semana

Objetivos do módulo

Identificar e explicar boas práticas para utilização segura dos sistemas operativos, aplicações, redes *wi fi cloud* e dispositivos IoT (*internet das coisas*).

Identificar e caracterizar canais seguros para comunicar na Internet

Aprender os requisitos de prevenção, de recuperação e de mitigação de ciberataques e adoção de medidas de defesa ativa.

Prevenir os ataques de engenharia social.

Configurar o sistema operativo de forma segura.

Recomendações para limitar acesso a informações sensíveis e/ou pessoais, na internet.

Competências a adquirir

- Capacidade de reconhecer e avaliar as ameaças mais comuns no ciberespaço;
- Caracterização das principais ameaças de Engenharia Social;
- Usar ferramentas de proteção digital;
- Configurar o sistema operativo de forma segura

Conteúdos programáticos

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

Instalação de software

User account control

Priviliégios de contas

Atualização de software

Firewall

Criar partições para dados

Antivírus

Emulação e simulação de aplicações

Recomendações gerais e conduta

Prática em contexto de formação

Unidade didática 2: Segurança na Internet (*browsing*, e-mail, redes sociais, *cloud*)

Cuidados genéricos;

Cuidados no correio eletrónico;

Cuidados nas redes sociais

Cuidados na *cloud*

Recomendações para autenticação com passwords

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

Cuidados a ter na configuração inicial e gestão de dispositivos IoT (*Internet das coisas*)

Utilização de canais seguros (VPN, TLS).

Cuidados a ter na utilização de VPN

Procedimentos na resposta a incidentes

Unidade didática 3: Virtualização e emulação de software

Emulação de software.

Virtualização

Máquinas virtuais

Preparação do Ambiente do Exercício Final

Prática em contexto de formação

Durante o percurso do módulo os formandos são colocados perante diversos exercícios práticos onde deverão demonstrar atuação correta nos diversos pedidos.

Prática com software de emulação.

Prática com software de virtualização.

Módulo 8: Exercício final
Duração: 13 horas teórico-práticas/1 semana

O exercício final consiste em duas fases:

1. Planeamento e execução de um teste de penetração em ambiente virtual.
2. Defesa e recuperação de um ataque em ambiente virtual e procedimentos na resposta a incidentes.

Os formandos deverão produzir um relatório destas duas fases que colocarão *online* de modo a ser visualizado, analisado, avaliado e classificado pelo formador. Este trabalho tem por objetivo a aplicação dos conhecimentos e competências adquiridas ao longo de todo o curso.

O trabalho final é de realização obrigatória. A sua não realização implica a não aprovação no curso.

O trabalho final escrito é objeto de classificação quantitativa e, para aprovação no curso, a classificação deste trabalho deve ser igual ou superior a 9,5 valores, numa escala de 0 a 20.

PÚBLICO-ALVO DO CURSO

Potencialmente o curso tem um vasto público-alvo que inclui, designadamente:

- Todos os profissionais e responsáveis de empresas/organizações;
- Individuos que desejem aumentar os seus conhecimentos de segurança da informação e de ciberdefesa de modo a ter uma presença responsável e consciente no ciberespaço.

Trata-se, portanto, de um público adulto, por norma trabalhador no ativo, e este facto deve ser considerado na forma como se deve fazer aprender, como motivar para essa aprendizagem e como avaliar os conhecimentos e competências adquiridos.

PRÉ-REQUISITOS DOS FORMANDOS

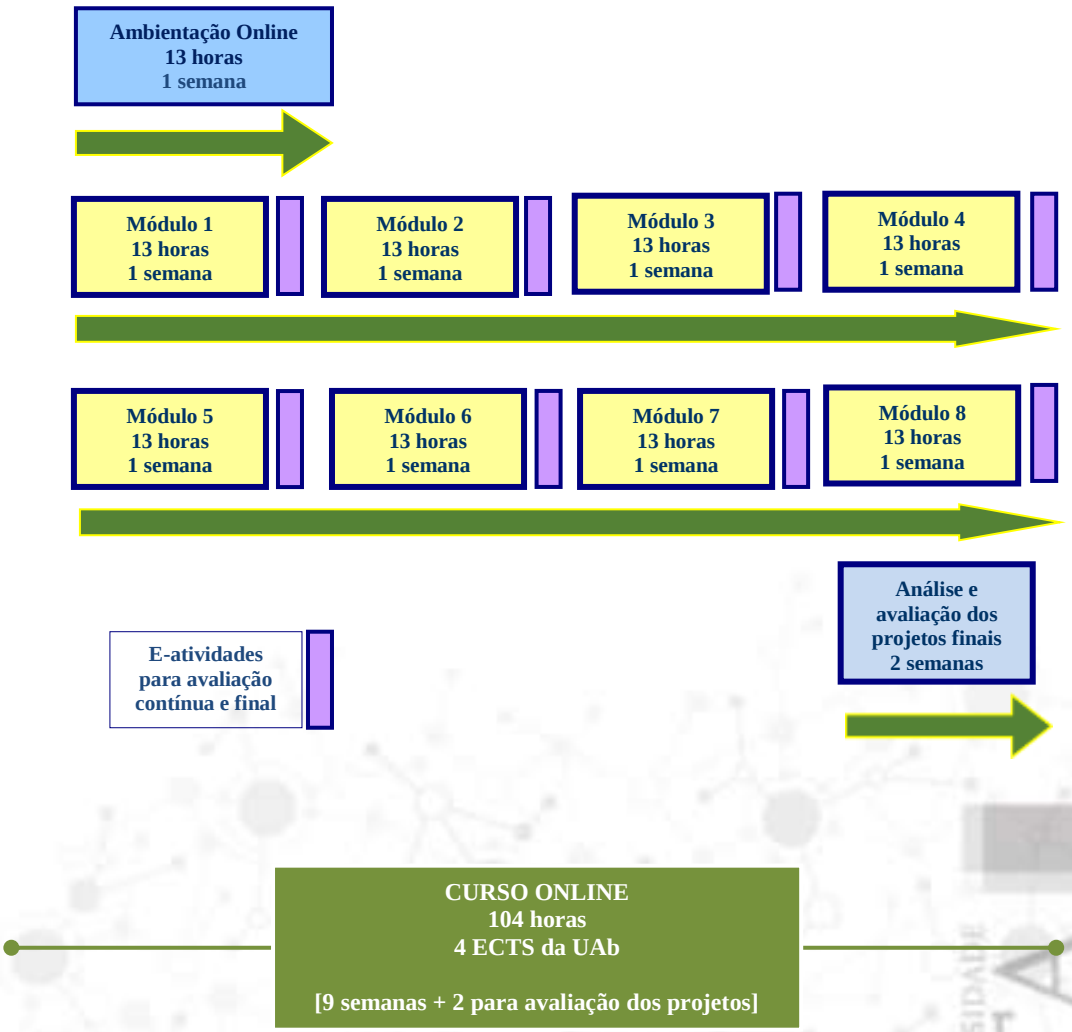
Considera-se como fator do seu sucesso neste curso a motivação dos formandos e a sua disponibilidade total para interagirem com os formadores e com os outros formandos na colocação de questões ou dúvidas sobre a matéria e disponibilidade de tempo para estudarem os conteúdos, elaborarem todas as atividades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

Cumulativamente, os formandos devem possuir:

- Habilitações mínimas ao nível do 12º ano ou equivalente;
- Conhecimentos e prática de informática como utilizadores, em ambiente Windows;
- Prática de utilização de *browsers* de navegação na Web;
- Uma conta de correio eletrónico ativa e prática na sua utilização;
- Disponibilidade de tempo mínima de13 horas por semana para:
  - Participação nos fóruns de discussão e nos *chats;*
  - Realização do autoestudo dos conteúdos disponibilizados online;
  - Pesquisa de informação com interesse para o âmbito dos diversos módulos;
  - Realização de todas as e-atividades propostas (testes, trabalhos, etc.);
  - Elaboração do trabalho final de projeto.

DURAÇÃO E ESTRUTURA DO CURSO

A duração total do curso é de 104 horas (volume de trabalho dos formandos) sendo o estruturado em 8 módulos de realização sequencial, precedidos de um módulo de Ambientação ao Contexto Online do curso (13 horas), de socialização online e de treino com a plataforma informática que suporta o curso.



CALENDARIZAÇÃO DO CURSO

Módulos	Datas
Ambientação ao contexto *online* do curso e ao Moodle	**06 a 12 de janeiro de 2020**
Módulo 1: **Requisitos da segurança da informação**	Imediatamente a seguir ao Módulo anterior
Módulo 2: **Encriptação de dados**	idem
Módulo 3: **Normas e legislação aplicável de segurança da informação**	idem
Módulo 4: **Análise forense digital**	idem
Módulo 5: **Segurança de Sistemas Informáticos**	idem
Módulo 6: ***Ethical Hacking***	idem
Módulo 7: **Técnicas de Proteção Digital**	idem
Módulo 8: **Exercício Final:** **1. Planeamento e execução de um teste de penetração em ambiente virtual.** **2. Defesa e recuperação de um ataque em ambiente virtual e procedimentos na resposta a incidentes**	idem
Análise crítica e avaliação dos trabalhos finais e sua discussão em fórum próprio	idem
Certificação dos formandos	idem

ATIVIDADES DOS FORMANDOS

MÓDULOS	DESCRIÇÃO
Sessão presencial caso se realize	Abertura do curso Apresentação do plano do curso, do coordenador e dos formadores dos diferentes módulos Acesso ao curso na plataforma Moodle da UAb Apresentação da estrutura do curso criado na plataforma e da forma como participar Treino com a plataforma Moodle
Módulo 0 ou Módulo de Ambientação Online Familiarização com a plataforma *Moodle* e socialização no ambiente *online*	Aceder à Plataforma *MoodleUAb* e ao curso Editar o seu perfil e colocar uma fotografia na plataforma Efetuar a apresentação individual no espaço Moodle do curso Consultar o Guia do Curso Consultar o Guia do Formando *Online* Consultar o tutorial sobre a Plataforma *Moodle* Executar as pesquisas de informação pedidas e colocar os resultados no Fórum de Discussão Treinar com as diversas ferramentas da plataforma e de acordo com instruções do formador Participar nos *fora* de discussão abertos e no chat.
Módulos 1 a 7	Ao longo dos diversos módulos os e-formandos são chamados a desenvolver uma série de atividades formativas que se podem sintetizar em: ▪ Leitura e estudo das matérias dos Módulos colocadas *online* e de outros documentos disponibilizados pelos e-formadores ▪ Interação com os formadores e com os outros formandos nos *fora* de discussão criados. **Esta interação (quantidade de mensagens, sua relevância para os temas em discussão e sua oportunidade) é considerada na avaliação contínua** ▪ Fazer as e-atividades correspondentes ao módulo. **Estas e-atividades são objeto de avaliação contínua**
Módulo 8 **Trabalho Final** **(e-atividade final)**	Recolha das informações necessárias Planeamento e execução de um ciberataque. Defesa e recuperação de um ciberataque e resposta ao incidente Estruturação e redação do relatório Alojamento do trabalho, no local próprio criado no espaço do curso na plataforma Moodle, dentro da data-hora limite imposta. Discussão dos trabalhos em fórum **Esta e-atividade é objeto de avaliação final e vale 40% da classificação final no curso.**

METODOLOGIA E SISTEMA DE TUTORIA

O curso segue um modelo no qual é a instituição formadora que define os objetivos, conteúdos, percursos de aprendizagem e meios e métodos de avaliação. Este modelo pressupõe a existência de canais de comunicação fáceis e disponíveis em permanência, entre a instituição e os formandos e entre estes e os formadores(es), canais esses integrados na plataforma Moodle a utilizar.

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).

A forma de trabalho utilizada neste curso compreende (1) a leitura e reflexão individuais dos conteúdos disponibilizados ou de outros sobre os mesmos temas obtidos pelos formandos, (2) a partilha da reflexão e do estudo com os colegas, assim como também (3) o esclarecimento de dúvidas nos fóruns moderados pelo formador e a (4) realização das e-atividades propostas.

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 *Moodle*.

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

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 plataforma *Moodle* 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

Plataforma informática Moodle (V 2.4), em http://www.moodle.univ-ab.pt/moodle/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

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 do curso são sujeitos a avaliação.

A avaliação nos módulos 1 a 7 integra:

- Uma componente contínua ao longo do módulo (participação no fórum 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, projecto, etc.)

Os instrumentos de avaliação de um módulo tem 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 tem um peso de 60% na 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

Exercício Final do Curso

Imediatamente após a realização do módulo 7, os alunos realizam um exercício final em ambiente virtual. Este trabalho final sobre um tema do curso vale 40% da nota final e é obrigatório. A classificação mínima admitida neste trabalho é de 9,5 valores; uma classificação inferior implica a não aprovação no curso, mesmo que a Classificação Final no Curso obtida pela aplicação da fórmula abaixo seja igual ou superior a 9,5 valores. A não entrega do trabalho final corresponde a uma nota de 0 valores e, igualmente, à não aprovação no curso

Classificação Final no Curso

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

$$\mathbf{CFC} = \frac{AFM1 + AFM2 + AFM3 + AFM4 + AFM5 + AFM6 + AFM7}{7} \mathbf{x\ 0,6 +\ NEF\ x\ 0,4}$$

AFMx representa a Avaliação Final do Módulo x e

NEF representa a Nota do Exercício Final

Consideram-se com aproveitamento no curso os formandos que obtiverem, **cumulativamente**:

- **Classificação Final no Curso igual ou superior 9,5 valores**, numa escala de 0 a 20;
- **Classificação no Trabalho Final do curso igual ou superior a 9,5 valores**, igualmente numa escala de 0 a 20.

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**.

DIRETOR, COORDENADOR E FORMADORES

O Curso de Especialização em Cibersegurança é dirigido pelo Diretor da Unidade de Aprendizagem ao Longo da Vida (UALV) Professor Doutor José Sales e coordenado por um técnico superior da UALV para os cursos de natureza profissional.
Os formadores do curso têm origens, formações e experiências académicas e profissionais diversas e são os que a seguir se indicam.

Formadores	Módulos
UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
João Mateus	1. Requisitos de segurança
João Mateus	2. Encriptação de dados e infra estrutura de chave pública
João Mateus	3. Normas e legislação aplicável de segurança da informação
Luís Dias	4. Análise forense digital
Luís Dias	5. Segurança de Sistemas Informáticos
Luís Dias	6. *Ethical Hacking*
Luís Dias	7. Técnicas de Proteção Digital
João Mateus e Luís Dias	8. Exercício Final – Ambiente Virtual
João Mateus e Luís Dias	Análise, avaliação e classificação dos trabalhos finais

Sínteses dos *curricula vitae* dos formadores

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. Tem o diploma de estudos avançados em Segurança de Informação no Instituto Superior Técnico e Mestrado em Engenharia Eletrotécnica Militar – Especialidade de Transmissões pela Academia Militar. Detém várias certificações da Indústria (SANS GCFE, EC-Council ECSA e ENSA, etc.) e é membro do GIAC *advisory board*.

Atualmente, na Academia Militar, é Professor Regente de "Algoritmos e Estruturas de Dados" e de "Tática de Transmissões do Exército". É também Professor de "Segurança Informação, Sistemas de Informação e Ciberdefesa". Paralelamente assume os cargos de Diretor dos Cursos de Transmissões e de Diretor do Mestrado em Guerra da Informação. É membro das comissões de gestão de acompanhamento dos Projetos de Defesa Nacional "Themis - Distributed holistic emergency management intelligent system" e projeto "BMS - Battlefield Management System". É membro da comissão executiva das Jornadas das Engenharias da Academia Militar 2019 (foi também na edição 2018). Participou como jogador em diversas edições de exercícios de Ciber Defesa Nacionais e Internacionais (Ciber Perseu, *Cyber Coallition* da NATO).

Desde 2018, é organizador dos Exercícios Nacionais de Ciber Defesa do Exército (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

Membro do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento (INESC-ID) e do Centro de Investigação da Academia Militar (CINAMIL), desenvolve a sua investigação de doutoramento no âmbito da aprendizagem automática de ameaças no ciberespaço através da análise de dados de segurança, com recurso a algoritmos de aprendizagem não supervisionada.

ACOMPANHAMENTO DO CURSO

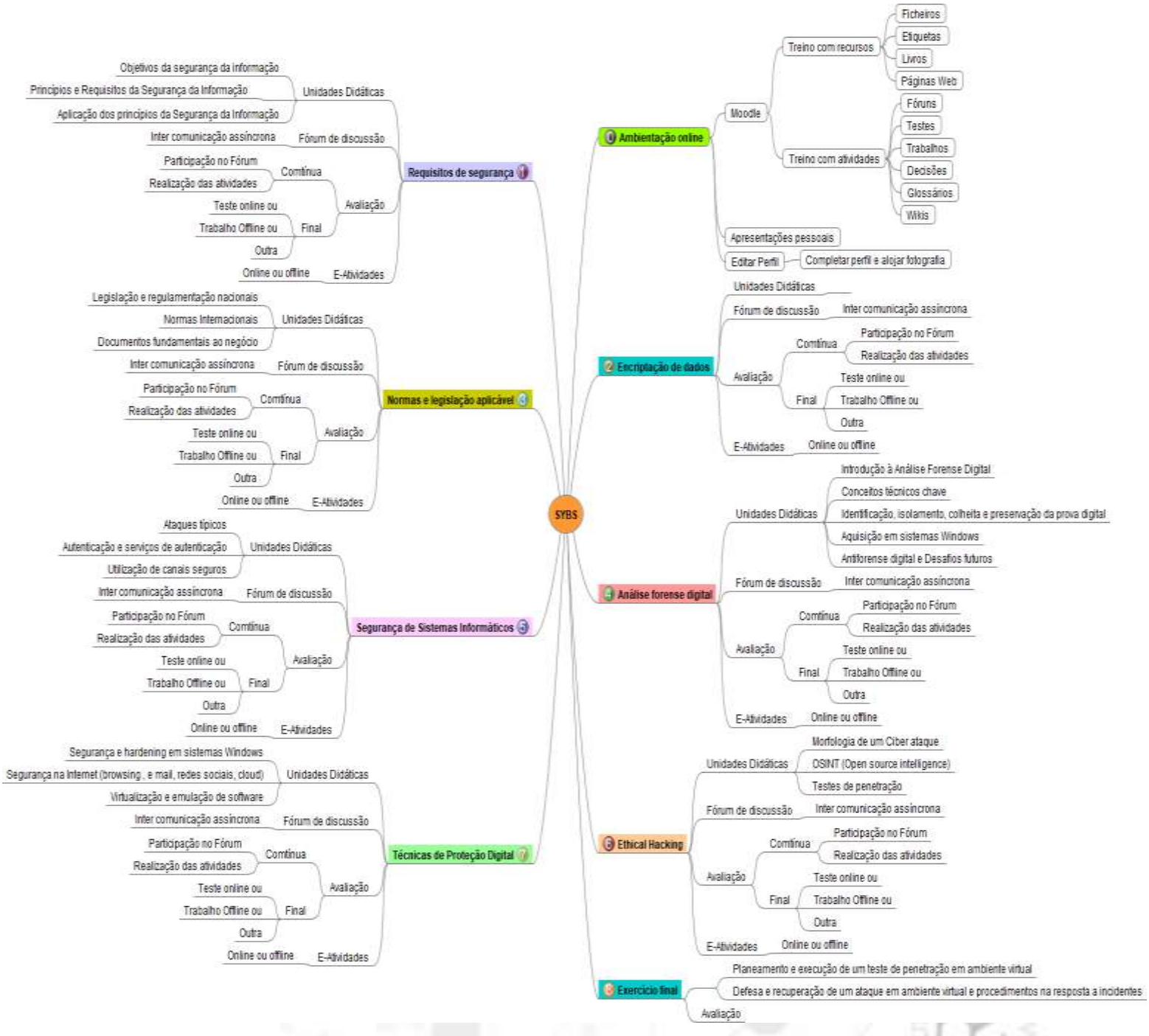
Para um acompanhamento permanente e coordenação do curso o Coordenador está inscrito como formador no espaço de aprendizagem criado na plataforma Moodle da UAb. Desta forma garante-se que tudo o que se passe *online* será do seu conhecimento imediato e sem necessidades de ser objeto de qualquer relatório, permitindo uma intervenção mais atempada sempre que as situações a justifiquem.

A plataforma Moodle a utilizar como suporte deste curso permite de uma forma automática:

- Controlar e registar as entradas, saídas e percursos dos formandos no espaço onde decorre o curso, indicando as respetivas horas e dias;
- Editar estatísticas da participação diária, de participação por períodos de tempo e de participação total de cada formando;
- Editar resultados da participação de cada participante nos fóruns de discussão;
- Registar a data/hora de entrega de trabalhos;
- Contabilizar as mensagens enviadas para os diversos fóruns por cada participante;

ANEXOS

ANEXO 1: MAPA CONCEPTUAL DO CURSO



ANEXO 2: O QUE SÃO E-ATIVIDADES?

Ao longo deste guia por diversas vezes se fala em e-atividades, pelo que se justifica esclarecer o seu significado.

Designam-se *e-atividades* as atividades a realizar pelos estudantes de cursos desenvolvidos em regime de *e-learning*. Este termo provém da analogia com o termo inglês de *e-tivities* enunciado por Gilly Salmon. Segundo Salmon, as *e-atividades* devem incluir o seguinte conjunto de características:

1. Possuir um título "apelativo" e motivador. Salmon defende que os títulos que os formadores *online* dão às *e-atividades* são muito importantes; os títulos devem dar informação, mobilizar os formandos e distinguir entre si as várias atividades.
2. Ter um elemento (faísca) que espolete a atividade e motive o envolvimento dos participantes. Esta "faísca" pode ser um estímulo, um desafio, uma informação.
3. Ter um conjunto de objetivos (e de competências) que os participantes podem esperar adquirir ou desenvolver com a atividade. Os objetivos e competências são desenvolvidos de modo diferente pelo tipo de atividade que foi concebida. O desenho e conceção da e-atividade pelo formador deve considerar esse aspeto.
4. Instruções que descrevam como o formando deve participar: por exemplo, explicitar que se espera que o estudante participe com, pelo menos, uma contribuição para a discussão e responda, pelo menos, a uma contribuição feita por um colega.
5. A lista de leituras bibliográficas ou de outros recursos relevantes para a sua resolução.
6. Instruções sobre o que os participantes devem fazer. De acordo com a autora, é difícil criar instruções claras e concisas, e esta competência desenvolve-se apenas com a prática e com o *feedback* de outros. Normalmente, as instruções criadas são ambíguas e incompletas, podendo gerar grandes dificuldades aos formandos (pois não incluem todas as ações necessárias para a sua realização).

De acordo com o Modelo Pedagógico Virtual da UAb as *e-atividades* podem adquirir variadas formas, designadamente: testes de tipos diversos (escolha múltipla, resposta verdadeira/falsa, de correspondência, etc.), pesquisas orientadas, projetos, sínteses, relatórios, trabalhos, etc. As e-atividades podem ser realizadas quer em situação *offline*, quer em situação *online*.

ANEXO 3: EXEMPLO DE UMA E-ATIVIDADE

E-Atividade DO CURSO ……..

Trabalho organizado é meio caminho andado…

Em qualquer atividade os fatores que influenciam positiva ou negativamente as condições de trabalho podem ser materiais, ambientais, psicossociais ou associados à organização do trabalho. Os fatores referentes à organização do próprio trabalho……

……
……

Esta atividade integra o percurso formativo do curso……e será apresentada aos formandos no final da xª semana, devendo ser devolvida ao professor até às 23h55 da 2ª-feira da yª semana, o que significa que o aluno terá x dias úteis para a sua realização.

Objetivos e competências a adquirir

- Consolidar conhecimentos sobre organização e gestão do trabalho;
- Aplicar os conhecimentos adquiridos na análise de situações concretas de trabalho;
- Identificar os fatores de risco para a trabalhadora da situação de trabalho apresentada;
- Propor medidas preventivas para minimizar/eliminar os fatores de risco identificados.

Participantes

Esta atividade deve ser realizada, individualmente, por todos os formandos do curso ……
Durante esta atividade cada formando deve:

- Fazer uma nova leitura dos conteúdos ……..
- Elaborar a sua resposta, que passa a constituir o seu *e-fólio*;
- Enviar o e-fólio ao formador até à data-hora limite estabelecida pelo mesmo.

Estrutura da atividade

Esta atividade é realizada em apenas uma fase e deve dar origem apenas a 1 ficheiro.

Calendário da atividade

Sábado (xx/yy)	Domingo (…../…..)	2ª-Feira (…../…..)	3ª-Feira (…../…..)	4ª-Feira (…../…..)	5ª-Feira (…../…..)	6ª-Feira (…../…..)
	Apresentação da e-Atividade (e-Fólio) no Tópico x no Moodle	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Análise da situação laboral	Revisão dos conteúdos Redação da atividade	Redação da atividade
Sádado (…../…..)	**Domingo (…../…..)**	**2ª-feira (…../…..)**				
		Redação da atividade Envio ao formador				

Instruções e sugestões aos formandos

Até ao dia …./….vai realizar esta e-atividade na qual deve demonstrar que adquiriu conhecimentos e competências que lhe permitiram analisar a situação proposta e indicar medidas que possibilitem prevenir os fatores de risco que identificou.

Na sua análise os formandos, à medida que leem o caso prático, devem ir anotando aquilo que lhes parece ser um potencial fator de risco e ir esboçando as medidas preventivas que julga mais adequadas. Por exemplo, logo no início do texto da situação laboral diz-se que Filomena trabalha à tarefa. Será este facto um fator de risco ou não? Como poderá ser combatido?

O relatório correspondente à situação de trabalho analisada deve:

- ter no máximo 2 folhas A4, com margens de 2 cm, escritas a Arial 10 ou equivalente e um espaçamento de 1,5 linhas.
- Ser enviado ao professor em formatos doc. ou pdf.

Nos seus relatórios os formandos devem demonstrar que adquiriram as seguintes competências:

- Capacidade para identificar os fatores de risco riscos que podem afetar a organização do trabalho e o trabalhador;
- Capacidade para indicar medidas preventivas concretas para anular ou minimizar os riscos detetados e atribuir-lhes prioridades, se for o caso.

Os relatórios devem ainda ser redigidos em linguagem simples e terem uma estrutura que facilite a sua consulta. Devem ser identificados todos os riscos, sejam físicos, químicos, biológicos, psicossociais ou com implicações ergonómicas.

Recursos para a atividade

- Conteúdos sobre ……..……..
- Guia Orientador da Avaliação de Riscos nos Locais de Trabalho
- Recursos eventualmente obtidos pelo estudante

Ações e tempo do formador

- Tornar visível na Moodle esta e-atividade, no Tópico “E-Atividade”
- Avaliar e classificar (até x valores) os relatórios individuais dos estudantes (e-fólio) durante a semana seguintes ao final da atividade.

A carga total de trabalho do professor é de 3 horas para a conceção da atividade, acrescida de 30 minutos vezes o nº de relatórios recebidos para leitura/correção/avaliação e inserção da classificação na plataforma.

Ações e tempo do formando

Espera-se que cada formando:

- releia os conteúdos ……. e ……
- elabore um pequeno relatório individual de 2 páginas, sobre a avaliação de riscos que efetuou;
- coloque o seu relatório (o seu e-fólio) no site Moodle do curso, na plataforma de apoio;

Esta atividade exige a cada estudante uma carga de trabalho estimada de 2 a 3 horas.

Avaliação da atividade

Esta é uma atividade de avaliação sumativa que vale um máximo de x valores. Na avaliação do relatório considera-se:

- a correção na identificação dos fatores de risco (até x valores)
- a correção das medidas de prevenção apresentadas (até x valores)

Situação de trabalho para análise

Filomena é uma jovem trabalhadora de uma microempresa que repara circuitos de microeletrónica, onde oqualidade da iluminação do posto de trabalho é fundamental para o seu bom desempenho.

,……..

……

ANEXO 4: AVALIAÇÃO DAS MENSAGENS

Pelo seu interesse, e como complemento do constante no capítulo sobre a forma como será avaliada a participação nos fóruns de discussão, transcrevemos do Guia do Formando Online documento a que todos os alunos têm acesso no espaço *online* do curso:

Qualidade da participação em fóruns de discussão

Não escreva só por escrever, nem para apenas dizer que concorda com determinada opinião expressa; diga que concorda ou não, mas avance sempre um pouco mais, por exemplo, explicando as razões da concordância ou discordância e, se possível, contribuindo com novos argumentos, novas ideias, novos pontos de vista, novas interrogações, relatos de experiências pessoais ou conhecidas, etc. Em suma, faça a discussão avançar.

Lembre-se de que um dos critérios de avaliação é o da "qualidade das mensagens" de acordo com uma tabela antecipadamente apresentada aos formandos, por exemplo a que é apresentada abaixo (Philips, 2000)."

Categorias de Qualidade das Mensagens nos Fóruns de Discussão Online	
Categoria	**Descrição**
E	Irrelevante; inútil
D	Demonstra acompanhamento das discussões
C	Tentativa de envolvimento na discussão; demonstra pouca compreensão dos assuntos; não faz progredir o debate
B	Bom contributo; demonstra compreensão; faz progredir o debate
A	Excelente contributo; demonstra compreensão profunda; leva o debate para novas áreas

ANEXO 5: A PLATAFORMA MOODLE

Martin Dougiamas, graduado em informática e mais tarde também em educação, após vários anos ligado à gestão informática do CMS comercial WebCT, na Universidade de Perth (Austrália), iniciou o desenvolvimento de *software* mais prático e eficaz para utilização em ambiente educativo e colaborativo *online*.

Em 1999, lançou a primeira versão do Moodle (*modular object-oriented dynamic learning environment*) cuja base pedagógica é a abordagem social-construccionista da educação. Outras premissas do desenvolvimento deste *software* são o desenho modular, permitindo a evolução rápida das funcionalidades, e ainda uma filosofia *open source* na distribuição e desenvolvimento. O conceito fundamental consiste numa página, onde professores disponibilizam recursos e desenvolvem atividades com e para os alunos. Uma eventual metáfora para a página *Moodle* poderia ser a sala de aula ubíqua. A cada utilizador registado está associado um perfil e uma fotografia podendo comunicar com qualquer outro, reforçando a componente social desta plataforma. Atualmente, na versão 9, com milhares de utilizadores e *developers*, e traduzido para mais de 73 línguas, o *Moodle* tem-se revelado um importante Learning Managemt System devido à flexibilidade, valor educativo e facilidade de utilização graças à interface simples e amigável, mesmo para os utilizadores menos experientes.

O *Moodle* como sistema de gestão de ensino e aprendizagem apresenta funcionalidades com forte componente de participação, comunicação e colaboração entre formandos, formadores e pares. Enquanto *software* educativo, a componente de avaliação (*assessment and inquiry*) não poderia ser esquecida. São oferecidas ferramentas de avaliação específicas de diversas atividades, como a possibilidade de classificar (pelos formadores ou pares), através de escala elaborada para o efeito, discussões de fórum, trabalhos enviados ou realizados *online*, lições com questões, entradas de glossário, etc.

As principais funcionalidades do LMS Moodle são:

Fórum – é uma ferramenta de discussão por natureza, mas pode ter outro tipo de uso, como por exemplo uma *mailing list*, um blogue, um *wiki* ou mesmo um espaço de reflexão

sobre um determinado conteúdo. Os fóruns do Moodle podem ser estruturados de diversas maneiras (discussão geral, uma única discussão, sem respostas, etc.) e podem permitir classificação de cada mensagem, (inclusivamente pelos alunos). As mensagens podem incluir anexos (imagem, pdf, doc, vídeo, áudio, zip).

Trabalho - os trabalhos permitem ao professor classificar e comentar na página Moodle materiais submetidos pelos alunos, ou atividades *offline* como por exemplo apresentações (texto, *powerpoint*, gráficos/desenhos, etc.). As notas são do conhecimento do próprio aluno e o professor pode exportar os resultados para uma folha em Excel.

Chat - facilita a comunicação síncrona, através de pequenas mensagens, entre formadores e formandos. Pode ser útil como espaço de esclarecimento de dúvidas, mas pode ter outros usos. A sessão de chat pode ser agendada, com repetição.

Referendo - pode ser usado de diversas formas, como recolha de opinião ou inscrição numa determinada atividade, sendo dado aos formandos a escolher de uma lista de opções definida pelo formador.

Diálogo – permite a comunicação privada entre dois participantes da disciplina. O formador pode abrir um diálogo com um formando, o formando pode abrir um diálogo com o formador, e podem existir diálogos entre dois formandos.

Glossário - possibilita aos participantes da disciplina criar dicionários de termos relacionados com a disciplina, bases de dados documentais ou de ficheiros, galerias de imagens ou mesmo *links* que podem ser facilmente pesquisados. Cada entrada permite comentários e avaliação.

Lição - associa a uma lógica de *delivery* uma componente interativa e de avaliação. Consiste num número de páginas ou diapositivos, que podem ter questões intercaladas com classificação e em que o prosseguimento do aluno está dependente das suas respostas. Um conceito baseado na “aprendizagem programada de Skinner”.

Teste - o formador pode construir uma base de dados de perguntas e respostas. Os testes podem ter diferentes formatos de resposta (verdadeiro ou falso, escolha múltipla, resposta curta ou numérica, correspondência, etc.) e é possível escolher perguntas aleatoriamente, corrigir respostas automaticamente e exportar os dados para Excel.

Questionário - permite construir inquéritos quer a participantes de uma página, quer a participantes do *Moodle*. É possível manter o anonimato dos inquiridos, e os resultados podem ser exportados para Excel.

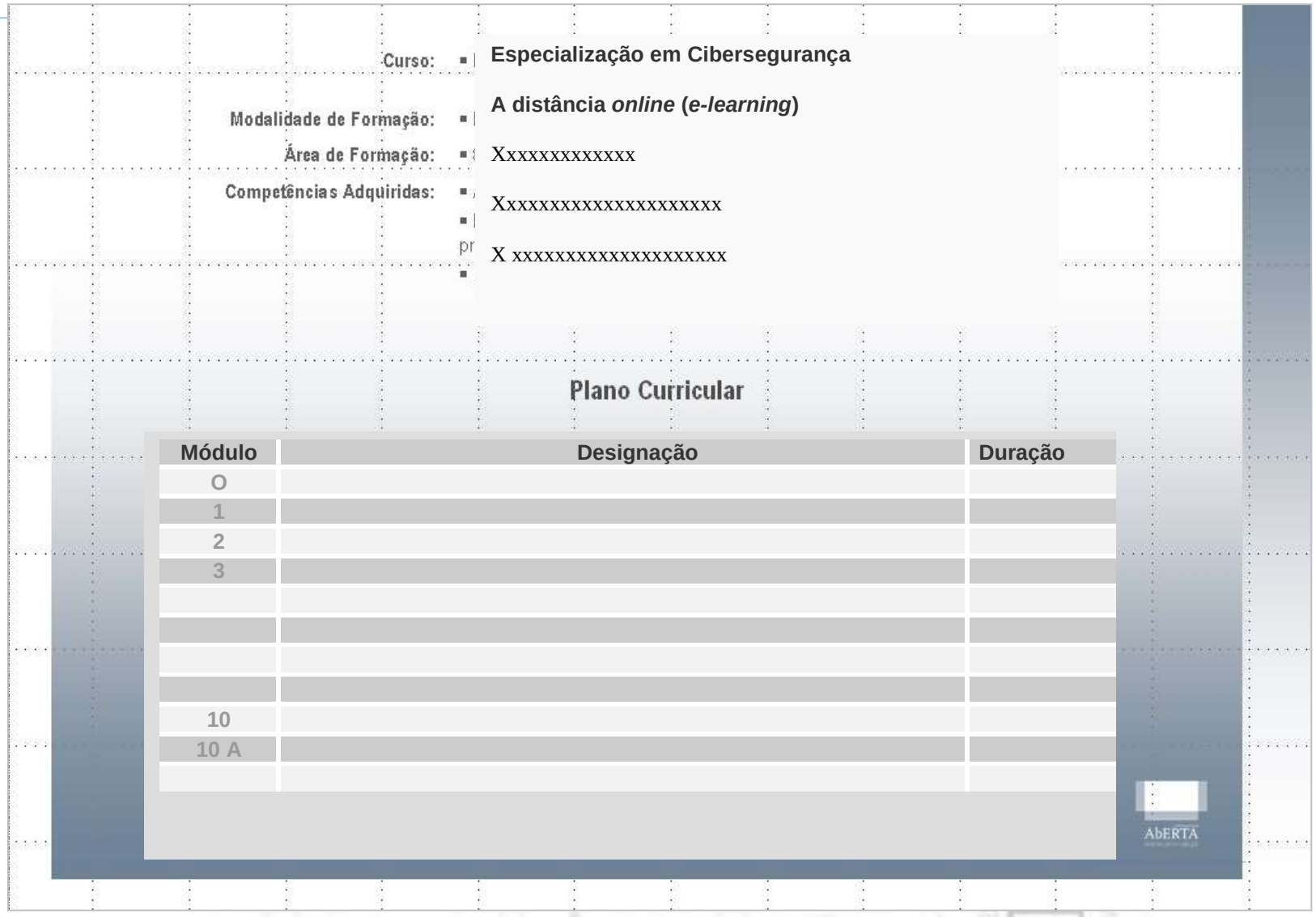
Wiki - torna possível a construção de um texto (com elementos multimédia) por vários participantes, onde cada um dá o seu contributo e/ou revê o texto. É possível aceder às várias versões do documento e verificar diferenças entre versões. Quem não conhece a Wikipedia® (http://pt.wikipedia.org/)?

(de ***O Moodle e as comunidades virtuais de aprendizagem***,
por Paulo Legoinha, João Pais & João Fernandes)

ANEXO 5: POSSÍVEL MODELO DO CERTIFICADO DE FORMAÇÃO

As informações, pessoais e sobre o curso, constantes neste possível modelo de Certificado de Formação obedecem aos estipulado na Lei sobe certificados de formação profissional.

Certificado ALV/UAb nº ……./20--


Curso:
Especialização em Cibersegurança
Modalidade de Formação:
A distância *online* (*e-learning*)
Área de Formação:
Xxxxxxxxxxxxx
Competências Adquiridas:
Xxxxxxxxxxxxxxxxxxxxx
X xxxxxxxxxxxxxxxxxxxx
Plano Curricular
Módulo
Designação
Duração
O
1
2
3
10
10 A
AbERTA