UNIVERSIDADE ABERTA
www.uab.pt

ANALISTA DE CIBERSEGURANÇA

alv Aprendizagem ao Longo da Vida

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

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

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

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

ÍNDICE

1. A UNIVERSIDADE ABERTA

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 https://elearning.uab.pt/) que se vai desenvolver a ação de formação de aprendizagem ao longo da vida designada **Curso de Analista de 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 ou 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 de acreditação ou certificação setorial.

2. ENQUADRAMENTO DO CURSO

O ciberespaço é um ambiente complexo, materializado por redes e sistemas de informação que permitem a sociedade em rede e criam novas oportunidades, potenciando

as organizações e as suas atividades. A cibersegurança compreende as medidas e ações de prevenção e monitorização que visam cumprir os requisitos de autenticidade, confidencialidade, integridade, disponibilidade e não repúdio da informação contida no ciberespaço. A crescente dependência da sociedade nas tecnologias assentes no ciberespaço, cria vulnerabilidades e oportunidades de serem exploradas, por hackers em nome individual, pelo crime organizado, por extremistas ideológicos e políticos, e mesmo pelos Estados.

As vulnerabilidades dos sistemas ou software, são exploradas por atores maliciosos que procuram lucro ou vantagem estratégica ao nível político, militar ou organizacional. Verifica-se que a evolução tecnológica aumenta a complexidade do ciberespaço e não tem foco na segurança, fazendo as vulnerabilidades prevalecerem porque os protocolos, arquiteturas das redes de computadores, o software e hardware são inseguros. A severidade do impacto de uma vulnerabilidade explorada por um ator mal-intencionado (a ameaça), constitui assim um risco que é fundamental mitigar ou eliminar.

O sucesso da cibersegurança está assente na necessidade de uma monitorização contínua em vez de assentar numa postura reativa e passiva. Muitas vezes essa postura tradicional, pressupõe a implementação de uma solução de segurança na expectativa que seja a solução infalível para o problema. Contudo, esta abordagem não é suficiente para as ameaças atuais, sendo necessário adotar uma postura proativa, orientada à deteção de ameaças ou anomalias, partindo da premissa de que o sistema possa já ter sido comprometido. Até mesmo os mais recentes sistemas de deteção de intrusão e outros sistemas de segurança, são suscetíveis a falhas e a ataques avançados e direcionados. É essencial apostar na capacitação da componente humana para configurar adequadamente as redes, *endpoints* e dispositivos de segurança, e para monitorizar os sistemas de forma sistematizada, tendo em conta as novas ameaças e formas de atuação dos agentes maliciosos. A enorme quantidade de dados que é gerada nos sistemas de uma organização, pode e deve ser potenciada para detetar potenciais ameaças, num processo designado *Threat Hunting*.

Este curso é direcionado para quem pretender aprofundar as suas competências de cibersegurança e especificamente para analistas de segurança que poderão desempenhar funções num Centro de Operações de Segurança (SOC). O curso prepara os formandos para analisarem e interpretarem de forma eficiente, os dados recolhidos na rede de uma organização, permitindo a deteção de anomalias e possíveis comprometimentos

aos sistemas, bem como a consequente atualização e implementação de políticas de segurança segundo as boas práticas das normativas internacionais.

É neste enquadramento que a Universidade Aberta (UAb) organizou e pretende oferecer ao mercado de formação este curso. O presente curso desenvolve-se em regime de formação teórica e prática à 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.

O curso, de cariz eminentemente prático, inclui o enquadramento e conceitos de base, a modelação das ciberameaças, arquiteturas de rede seguras, operações de segurança, implementação e utilização eficiente de um SIEM, notas práticas de um SOC, monitorização de segurança contínua, análise de eventos de rede e de *endpoint*, configurações seguras, Threat Intelligence, *Threat Hunting*, inteligência artificial na deteção de intrusões, desafios futuros e muito mais.

3. OBJETIVOS DO CURSO

O objetivo do curso é proporcionar conhecimentos e competências que permitam aos formandos zelar pela autenticidade, integridade, confidencialidade, disponibilidade e não repúdio da informação numa organização. Assim, no final, os participantes saberão:

- Configurar e utilizar diversos dispositivos de segurança;
- Avaliar os pontos fortes e fracos dos dispositivos de segurança perante diversos cenários de ataque;
- Analisar e usar diferentes formas de deteção de ameaças e rastreamento de Indicadores de Comprometimento;
- Reconhecer e implementar controlos de segurança críticos;
- Explicar a estrutura e funcionamento de um Centro de Operações de Segurança (SOC) e discutir os desafios que se colocam.
- Explicar a importância da *Threat Intelligence* e praticar a sua utilização no processo de monitorização contínua;
- Adotar uma abordagem proativa de *Threat Hunting*;
- Avaliar o impacto da inteligência artificial na cibersegurança e reconhecer as novas técnicas de deteção de intrusões.

O regime de funcionamento online suportado por uma plataforma informática de gestão da formação/aprendizagem permitirá ainda alcançar outros objetivos e adquirir outras competências, secundárias em relação ao âmbito geral deste curso, mas de extrema e atual importância para a empregabilidade. Deste modo os formandos vão 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.

4. COMPETÊNCIAS A ADQUIRIR

No final do curso os formandos ficarão habilitados com um conjunto de ferramentas tecnológicas e procedimentais que lhes permitirão tomar ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

Deste modo os participantes irão adquirir as seguintes competências:

- Reconhecer o contexto atual da cibersegurança ao nível organizacional e perceber os elementos estruturantes das tecnologias e sistemas de informação;
- Adotar uma postura proativa na monitorização de cibersegurança;
- Entender como os sistemas e dispositivos de segurança funcionam, quais as suas capacidades e os seus papéis na monitorização contínua;
- Perceber como e porquê usar determinadas ferramentas de monitorização (de rede e *endpoint*) de acordo com os diversos cenários de ataque;
- Analisar e gerir vulnerabilidades;
- Usar a auditoria de configuração de uma *baseline* e *patching* para tornar os *endpoints* mais resilientes;
- Implementar controlos de segurança;
- Saber a constituição e organização de um SOC e qual o papel do analista;
- Adotar uma abordagem correta na triagem de alarmes de um SIEM;

- Perceber o papel do analista no reporte de problemas e no processo de resposta a incidentes;
- Reconhecer a importância do SIEM e os princípios gerais para uma implementação de sucesso;
- Utilizar a *Threat Intelligence* como suporte à segurança organizacional;
- Saber tirar proveito da *Cyber Kill Chain*, *Mittre Att&ck framework* e o *Diamond Model*, no âmbito do processo de *Threat Hunting*;
- Compreender os conceitos de Inteligência Artificial e *Machine Learning* e fazer a associação com a cibersegurança e com os desafios futuros;

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 atividades.

5. PROGRAMA E CONTEÚDOS DO CURSO

Este curso de 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, designado módulo 0 ou pré-curso e incluído gratuitamente.

A componente escolar do curso tem a duração de 104 horas (volume de trabalho dos formandos) a que corresponde um crédito de 4 ECTS[1] da UAb e realiza-se em regime de formação a distância online (e-learning) ao longo das 9 semanas.

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

[1] 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 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.
- 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.

Conteúdos programáticos

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.

MÓDULO 1: FUNDAMENTOS E ENQUADRAMENTO

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

Objetivos do módulo

Enquadrar a cibersegurança no contexto organizacional.

Explicar os conceitos estruturantes das tecnologias e sistemas de informação. Demonstrar a utilização das máquinas virtuais e usar o Virtual Box em apoio ao ambiente virtual para o curso.

Praticar comandos em ambiente Linux.

Discutir os desafios relativos à monitorização da cibersegurança e motivar para os restantes módulos.

Competências a adquirir

- Identificar as principais ameaças no ciberespaço;
- Reconhecer o contexto atual da cibersegurança ao nível organizacional;
- Perceber os elementos estruturantes das tecnologias e sistemas de informação;
- Instalar e utilizar um sistema operativo numa máquina virtual;
- Utilizar os principais comandos em ambiente Linux;
- Adotar uma postura proativa na monitorização de cibersegurança.

Conteúdos programáticos

Unidade Didática 1: A Cibersegurança

As ameaças - como pensa o atacante;

Requisitos de segurança;

Legislação e normas de referência;

Risco no contexto organizacional (dimensão física, humana e tecnológica);

Controlos de segurança e papéis dos responsáveis na cibersegurança.

Unidade Didática 2: Conceitos fundamentais

Hardware/Software;

Aplicações, Sistemas Operativos, Drivers;

Bits, Bytes, Codificação;

Características e finalidades das redes de computadores;

Componentes de uma rede e topologias;

Modelos de referência (OSI e TCP-IP);

Os principais protocolos.

Unidade Didática 3: Máquinas virtuais

Virtualização e emulação;

Instalar e utilizar o Virtual Box;

Preparar o ambiente virtual para o curso.

Unidade Didática 4: Ambiente Linux

Generalidades;

Utilização do terminal;

Comandos de base;

Utilizadores e superuser.

Unidade Didática 5: Monitorização da cibersegurança (desafios e motivação)

Abordagem tradicional (reativa): cibersegurança abaixo das operações;

Nova abordagem (proativa): cibersegurança com as operações;

Monitorização contínua.

Prática em contexto de formação

Para além da componente teórica, este módulo visa também preparar os formandos numa perspetiva prática. Nesse sentido, os formandos irão fazer alguns exercícios nos seus próprios computadores, como exemplo, irão instalar um sistema operativo numa máquina virtual e preparar o ambiente virtual que será utilizado ao longo do curso. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 2: ARQUITETURAS DE SEGURANÇA EM REDE

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

Objetivos do módulo

Apresentar diferentes tipos de cenários de ataques modernos.

Identificar e descrever diferentes tipos de dispositivos de segurança.

Praticar a configuração e utilização dos dispositivos de segurança.

Avaliar os pontos fortes e fracos destes dispositivos de segurança perante os cenários anteriormente apresentados.

Competências a adquirir

- Diferenciar entre técnicas de ataques tradicionais e modernos;
- Demonstrar entendimento de como sistemas de firewall e de deteção/prevenção de intrusões funcionam, quais as suas capacidades e os seus papéis na monitorização contínua;
- Demonstrar e aplicar entendimento de como e porquê usar um conjunto de ferramentas de monitorização na rede para melhorar a capacidade de deteção de intrusões na rede;
- Demonstrar compreensão de como os proxies e SIEMs funcionam, quais são as suas capacidades e as funções que desempenham na monitorização contínua;
- Demonstrar capacidade de identificar pontos de acesso ao perímetro e dispositivos de rede que podem ser usados para proteger o perímetro.

Conteúdos programáticos

Unidade Didática 1: Cenários do adversário moderno

Ataque a Aplicações Web;

Ataque *Client-Side* e *Pivoting*.

Unidade didática 2: Dispositivos de segurança

Routers;

Firewalls State Inspection de perímetro;

WAFs;

Exercício com o ModSecurity;

Network Intrusion Detection Systems;

Network Intrusion Prevention Systems;

Next Generation Firewalls;

Exercício OpenAppId com o Snort;

Dispositivos de deteção de *malware* (Sandboxes);

Proxies;

Security Information and Event Management (SIEM);

Dispositivos de Captura de Pacotes;

Dispositivos de deceção do adversário (HoneyPots) ;

Switches.

Unidade didática 3: Análise dos dispositivos de segurança face aos diferentes cenários de ataque

Abordagem de Prevenção;

Abordagem de Deteção.

Prática em contexto de formação

Para além da componente teórica, este módulo visa prevê a realização de diversos exercícios práticos relacionados com o tema que está a ser discutido. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 3: MONITORIZAÇÃO DE SEGURANÇA EM REDE

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

Objetivos do módulo

Apresentar o conceito de Monitorização de Segurança Contínuo (MSC), distinguir MSC de Monitorização de Segurança de Rede (MSR) e apresentar um caso de estudo real. Descrever e aplicar um conjunto de ferramentas de MSR. Analisar e usar diferentes formas de deteção de ameaças e rastreamento de Indicadores de Comprometimento (IOC).

Competências a adquirir

- Demonstrar entendimento dos princípios de defesa tradicional e moderna;
- Demonstrar entendimento das ferramentas e técnicas usadas para levantamento de dispositivos de rede e *hosts* e de análise de vulnerabilidades;
- Aplicar métodos e princípios de análise de tráfego em rede para deteção de explorações e estar apto a rapidamente encontrar intrusões na rede;
- Aplicar os princípios de deteção de uma exploração para identificar intrusões cifradas na rede;
- Demonstrar entendimento de como e porquê usar um conjunto de ferramentas de monitorização na rede para melhorar a capacidade de deteção de intrusões na rede.

Conteúdos programáticos

Unidade Didática 1: Monitorização da segurança contínua

Conceito de Monitorização de Segurança Contínua;

Diferenças entre MSC e MSR;

Caso de estudo NotPetya.

Unidade Didática 2: Ferramentas de monitorização de segurança em rede

Security Onion;

NSM Frontends;

Squil;

Wireshark;

TShark;

NIDS;

Bro/Zeek.

Unidade Didática 3: Formas de deteção de ameaças e de rastreamento de indicadores de comprometimento

Deteção por assinatura;

Blacklisting é uma abordagem falhada;

Evasão de deteção por assinatura;

Deteção por comportamento de protocolo;

Deteção por anomalia;

Fontes de dados de MSR;

Rastreamento de executáveis;

Identificação de tráfego C&C;

Rastreamento de User-Agents;

C2 via HTTPS;

Rastreamento de Certificados.

Prática em contexto de formação

Para além da componente teórica, este módulo visa familiarizar os formandos com a distribuição Security Onion,com diversos *frontends* para MSR, assim como com as ferramentas Sguil, Elastic Stack, Wireshark, TShark e Zeek. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 4: ARQUITETURA DE SEGURANÇA NOS DISPOSITIVOS *ENDPOINT* E MONITORIZAÇÃO DE SEGURANÇA CONTÍNUA

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

Objetivos do módulo

Descrever e explicar os controlos de segurança críticos, nomeadamente *patching*, *whitelisting* de aplicações, configuração de *baseline* segura e monitorização de aplicações. Identificar e demonstrar o uso de ferramentas de proteção no *host*. Enunciar e empregar o uso de técnicas de monitorização de segurança contínua através da realização de diversos exemplos práticos maioritariamente em ambiente Windows.

Competências a adquirir

- Demonstrar habilidade para controlar os níveis de privilégios de contas e aplicações;
- Demonstrar entendimento das ferramentas e técnicas usadas para a monitorização de alteração de configurações;
- Demonstrar entendimento das ferramentas e técnicas usadas para levantamento de dispositivos de rede e *hosts* e de análise de vulnerabilidades;
- Compreender como usar a auditoria de configuração de uma *baseline* e *patching* para tornar os *endpoints* mais resilientes;
- Demonstrar compreensão das estruturas de arquitetura de segurança tradicionais e modernas e qual o papel dos SOCs;
- Demonstrar compreensão dos benefícios de manter inventários de software e listas de permissões.

Conteúdos programáticos

Unidade Didática 1: Controlos de segurança críticos

Endpoints Windows;

Patching;

Configuração de *baseline* segura;

Monitorização aplicacional e Sysmon;

Whitelisting de Aplicações;

Contas Administrativas: Monitorização e Redução de privilégios;

Autenticação.

Unidade Didática 2: Ferramentas de proteção no *host*

Anti-malware;

Dispositivos de proteção no *Host*: *Endpoint Firewalls* e HIDS/HIPS;

Exercício com o AppLocker.

Unidade Didática 3: Monitorização de segurança contínua

Boas práticas da Indústria;

Descoberta ativa e passiva de serviços e *hosts*;

Análise de vulnerabilidades;

Monitorização de *patching*;

Monitorização de serviços de logs;

Monitorização de mudanças de estado de dispositivos e aplicações;

Análise dos dados de *proxies* e *firewalls*;

Monitorização de eventos críticos do Windows;

Deteção pós intrusão.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos com diversas técnicas de monitorização de segurança contínua no *endpoint* através da monitorização através da utilização da ferramenta Sysmon, AppLocker, descoberta de ativa e passiva de serviços e *hosts* e monitorização de serviços de *logs* e eventos do sistema operativo Windows. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 5: NOTAS PRÁTICAS DE UM CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

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

Objetivos do módulo

Explicar a estrutura e funcionamento de um SOC, focando os aspetos mais pertinentes para um analista.

Discutir os desafios que se colocam ao analista no âmbito das suas funções.

Debater o papel do SIEM num SOC e explicar os passos fundamentais para a sua implementação com sucesso.

Diferenciar as principais atividades na resposta a incidentes e o contributo do analista de segurança.

Competências a adquirir

- Saber a constituição e organização de um SOC e qual o papel do analista;
- Ser capaz de adotar uma abordagem correta na triagem de alarmes;
- Perceber o papel do analista no reporte de problemas e no processo de resposta a incidentes;
- Reconhecer a importância do SIEM e os princípios gerais para uma implementação de sucesso.

Conteúdos programáticos

Unidade Didática 1: O SOC

Definição de SOC;

Os serviços de um SOC;

Interno, outsourcing ou híbrido;

Métricas;

Operações de Segurança e Dados de Segurança;

Treino, competências, pessoal e responsabilidades.

Unidade Didática 2: Um dia do analista de segurança SOC

Triagem de alarmes;

Dashboards;

Estado da segurança;

Identificar e reportar problemas.

Unidade Didática 3: O SIEM e gestão de eventos

Princípios gerais para um SIEM de sucesso;

Critérios de severidade, prioridade, urgência, confiança;

Checklist para um SIEM bem implementado;

Normalização;

Agentes;

Coleção de dados - métodos e considerações;

Gestão de eventos.

Unidade Didática 4: Contributos para a resposta a incidentes

As fases da resposta a incidentes;

A comunicação;

Coordenação;

Treino e testes.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos para o desempenho das funções de analista numa perspetiva prática e orientada para a postura do analista na organização. Adicionalmente, o módulo foca a importância do SIEM e as melhores práticas. No conjunto dos tópicos abordados, serão realizados alguns exercícios práticos para apreciação (avaliação sumativa).

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 6: *THREAT INTELLIGENCE* E *THREAT HUNTING*

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

Objetivos do módulo

Explicar a importância da *Threat Intelligence*, o conhecimento das ameaças e a análise dos dados sobre as mesmas. Demonstrar e exemplificar a importância de uma abordagem proativa de *Threat Hunting*.

Competências a adquirir

- Utilizar a *Threat Intelligence* como suporte à segurança organizacional;
- Identificar as fontes de informação que são relevantes para o processo de *Threat Intelligence* vocacionado para a organização;
- Compreender como é realizada a partilha de *Threat Intelligence*;
- Saber tirar proveito da *Cyber Kill Chain*, *Mittre Att&ck Framework* e o *Diamond Model*, no âmbito do processo de *Threat Hunting*;
- Conseguir exemplificar a utilização de *Threat Hunting*, identificando indicadores de comprometimento típicos nos cenários de ataque mais populares.

Conteúdos programáticos

Unidade Didática 1: *Threat Intelligence*

Classificação de ameaças;

O ciclo de *Intelligence*;

As fontes de *Intelligence*;

Partilha de *Intelligence*;

OSINT (e.g., Shodan);

Google Hacking.

Unidade Didática 2: *Threat Hunting*

Melhores práticas para o SOC;

Gerar hipóteses;

Potenciar a Framework MITRE ATT&CK;

Potenciar o conhecimento da *Cyber Kill Chain*.

Unidade Didática 3: Exemplos de *Threat Hunting*

Indicadores de Comprometimento;

Movimento lateral;

C2;

Volume HTTP;

Múltiplos IPs de login.

Prática em contexto de formação

Para além da componente teórica, este módulo visa preparar os formandos para o mundo real, focando as técnicas de *Threat Intelligence* e de *Threat Hunting*, com diversos exemplos práticos e um conjunto de exercícios para apreciação (avaliação sumativa).

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 7: INTELIGÊNCIA ARTIFICIAL E DETEÇÃO DE INTRUSÕES

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

Objetivos do módulo

Explicar os conceitos fundamentais relacionados com a Inteligência Artificial. Demonstrar a utilização de algoritmos de *Machine Learning* na deteção de intrusões. Debater, em análise prospetiva, os desafios futuros relacionados com o impacto da Inteligência Artificial na cibersegurança.

Competências a adquirir

- Compreender os conceitos de Inteligência Artificial e *Machine Learning*;
- Perceber os conceitos fundamentais relacionados com *Machine Learning*;
- Reconhecer as limitações dos sistemas de deteção de intrusões tradicionais;
- Conseguir fazer a aplicação prática de algoritmos baseados em métodos não supervisionados, na deteção de intrusões;

- Discutir os desafios futuros e o impacto da inteligência artificial na cibersegurança.

Conteúdos programáticos

Unidade Didática 1: Conceitos fundamentais e *machine learning*

Inteligência Artificial vs *Machine Learning*;

Tecnologias e *frameworks* para processamento (Big Data);

Engenharia e seleção de *features*;

Métodos supervisionados e não supervisionados.

Unidade Didática 2: Deteção de intrusões com *machine learning*

Limitações dos sistemas de deteção tradicionais (anomalias e assinaturas);

Exemplos de aplicação práticos (classificação de *malware*, websites, spam, etc);

Exemplo prático com *unsupervised learning* (anomalias em netflow);

Geração de *features* dinâmicas baseadas em portos mais usados, menos usados, e usados por poucas máquinas.

Unidade Didática 3: Ética e deontologia profissional na segurança privada

O SIEM de próxima geração;

Novas tecnologias de cibersegurança baseadas em IA;

A IA como uma ferramenta ofensiva;

O Hacker, o estatístico e o especialista de segurança.

Prática em contexto de formação

Para além da componente teórica, este módulo visa também preparar os formandos numa perspetiva prática, fomentando a execução de exercícios práticos e a utilização de ferramentas previamente desenvolvidas para aplicar algoritmos de *Machine Learning*. O módulo tem um trabalho prático para apreciação (avaliação sumativa) que materializa alguns conhecimentos adquiridos no módulo.

A utilização do fórum para debater os vários temas que constituem o objeto do módulo são também objeto de apreciação e avaliação formativa.

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

MÓDULO 8: EXERCÍCIO FINAL

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

O exercício final consiste na realização de um conjunto de pequenos exercícios sobre as diversas temáticas abordadas no decorrer do curso, e numa análise de um cenário que representa um sistema de rede que apresenta indícios de comprometimento, através

de logs e ficheiros de captura de pacotes de rede. Os formandos deverão responder às questões previamente elencadas pelos formadores, sob a forma de um relatório a ser submetido *online*, para poder ser visualizado, analisado, avaliado e classificado pelos formadores. 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.

6. PÚBLICO-ALVO DO CURSO

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

- Todos os profissionais que trabalham na área de IT ou cibersegurança das empresas/organizações e desejem aprofundar os conhecimentos na área da análise de eventos de segurança, gestão de vulnerabilidades e ameaças;
- Todos os profissionais que pretendam iniciar-se na resposta a incidentes de cibersegurança;
- Indivíduos que desejem especializar-se em operações de cibersegurança e análise de eventos de segurança para poderem desempenhar a função de analistas de cibersegurança nas organizações/empresas;
- 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.

7. 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.

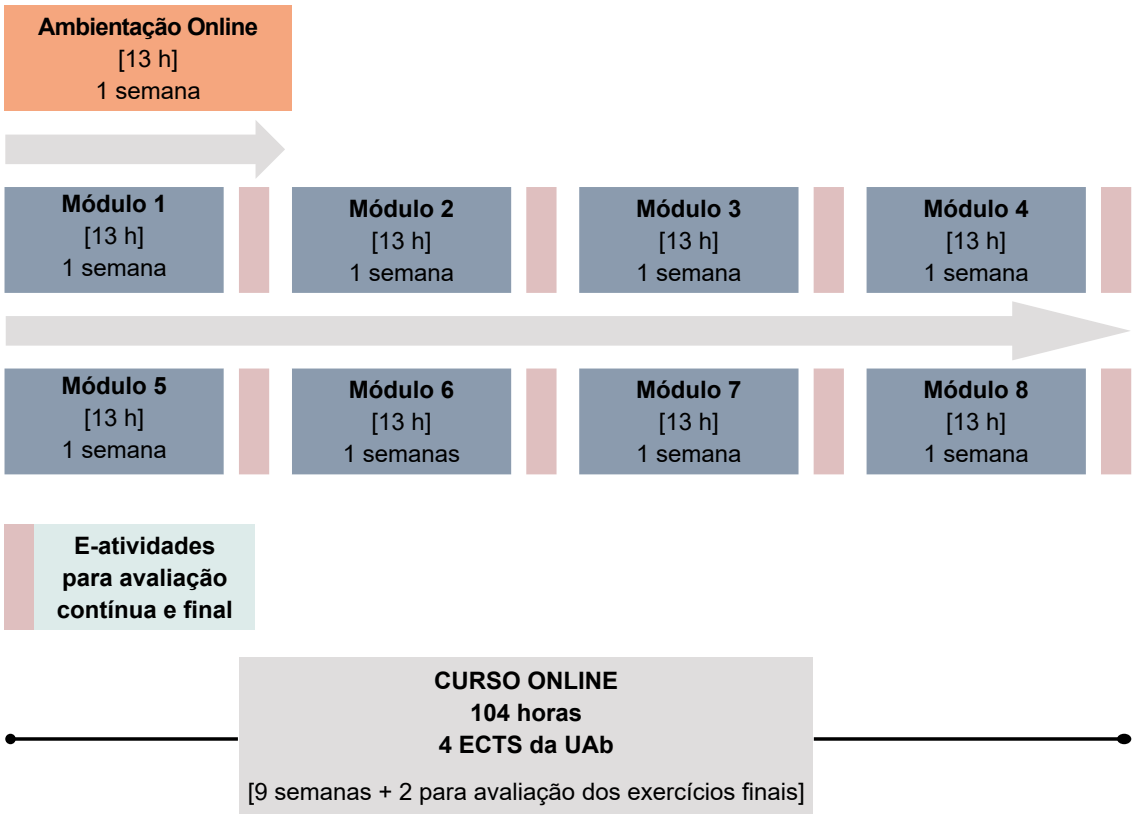
Cumulativamente, os formandos devem possuir:

- Habilitações mínimas ao nível do 12.º ano ou equivalente;
- Computador com pelo menos 8GB de memória RAM e 50 GB de espaço em disco disponível;
- Conhecimentos e prática de informática como utilizadores;
- Prática de utilização de browsers de navegação na Web;
- Uma conta de correio eletrónico ativa e prática na sua utilização;
- Disponibilidade de tempo mínima de 13 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.

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

8. 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.



9. CALENDARIZAÇÃO DO CURSO

MÓDULOS	DATAS
Módulo 0 Ambientação ao contexto online do curso e ao Moodle	A calendarizar
Módulo 1: Fundamentos e enquadramento	Imediatamente a seguir ao módulo anterior
Módulo 2: Arquiteturas de segurança em rede	idem
Módulo 3: Monitorização de segurança em rede	idem
Módulo 4: Arquitetura de segurança nos dispositivos *Endpoint* e monitorização de Segurança Contínua	idem
Módulo 5: Notas práticas de um SOC	idem
Módulo 6: *Threat Intelligence* e *Threat Hunting*	idem
Módulo 7: Inteligência artificial e deteção de intrusões	idem
Módulo 8: Exercício Final	idem

10. ATIVIDADES DOS FORMANDOS

MÓDULOS	DESCRIÇÃO
Sessão presencial caso se realize	Abertura do curso Apresentação do plano do curso e dos coordenadores e dos formadores dos diferentes módulos Acesso ao curso na PlataformAbERTA|Moodle da UAb Apresentação da estrutura do curso criado na plataforma e da forma como participar Treino com a PlataformAbERTA|Moodle
Módulo 0 ou **Módulo de Ambientação *Online*** Familiarização com a plataforma Moodle e socialização no ambiente *online*	Aceder à PlataformAbERTA|Moodle 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 PlataformAbERTA|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 Estruturação e redação do texto 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.**

11. 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 PlataformAbERTA|Moodle.

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

12. RECURSOS DE APRENDIZAGEM

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

- Textos base sobre os temas a abordar, colocados *online* no curso criado na plataforma Moodle e/ou na Web em servidor a indicar aos participantes para procederem o seu *download*;
- Apresentações multimédia diversas concebidas pelos formadores para situações de aprendizagem específicas;

- Tutorial sobre a forma de utilizar a 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 https://elearning.uab.pt/, apoiada por 4 servidores e utilizando uma ligação com 200 MB de largura de banda.

13. SISTEMA DE AVALIAÇÃO E CLASSIFICAÇÃO

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

Avaliação nos Módulos

Todos os módulos 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, projeto, etc.)

Os instrumentos de avaliação de um módulo têm o mesmo peso e, por isso, a avaliação final do módulo é dada pela média simples das 2 ou 3 provas realizadas, numa escala de 0 a 20 valores.

A média final da avaliação dos módulos 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**.

Classificação Final no curso

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

$$CFC = \left(\frac{AFM1 + AFM2 + AFM3 + AFM4 + AFM5 + AFM6 + AFM7}{7}\right) \times 0{,}6 + AFM8 \times 0{,}4$$

$AFMx$ representa a Avaliação Final do Módulo x.

Consideram-se com aproveitamento no curso os formandos que obtiverem classificação Final no Curso **igual ou superior 9,5 valores**, 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**.

14. 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 Fernando Caetano 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
Luís Dias André Calvinho	1. Fundamentos e enquadramento
André Calvinho	2. Arquiteturas de segurança em rede
André Calvinho	3. Monitorização de segurança em rede
André Calvinho	4. Arquitetura de segurança nos dispositivos *Endpoint* e Monitorização de Segurança Contínua
Luís Dias	5. Notas práticas de um SOC
Luís Dias	6. *Threat intelligence* e *Threat Hunting*
Luís Dias	7. Inteligência artificial e deteção de intrusões
Luís Dias André Calvinho	8. Exercício Final – Ambiente Virtual
Luís Dias André Calvinho	Análise, avaliação e classificação dos trabalhos finais

Sínteses dos *curricula vitae* dos formadores

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. Está habilitado com o Curso de Estado Maior – Conjunto das Forças Armadas, 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 é docente de "Segurança Informação, Sistemas de Informação e Ciberdefesa" na Academia Militar. Desempenhou funções na componente operacional de ciberdefesa do Exército, entre 2010 e 2015. Participou como jogador em diversas edições de exercícios de ciberdefesa Nacionais e Internacionais (Ciber Perseu, Cyber Coalition da NATO). Em 2018 e 2019 foi organizador dos Exercícios Nacionais de Ciberdefesa (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

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.

É formador de cursos de Aprendizagem ao Longo da Vida da Universidade Aberta desde 2019.

ANDRÉ VICENTE CALVINHO é Capitão Engenheiro da Arma de Transmissões do Exército Português, especializado na área da ciberdefesa e Segurança da Informação. Possui 7 anos de experiência na área da cibersegurança. É engenheiro de cibersegurança, investigador na área da segurança e penetration tester. É mestre em Engenharia Eletrotécnica e de Computadores na Academia Militar e Instituto Superior Técnico.

Possui diversas certificações da indústria, tais como: Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) e GIAC Certified Intrusion Analyst (GCIA). Possui ainda a certificação em GIAC Continuous Monitoring Certification (GMON), é membro do GIAC

Advisory Board e detentor de inúmeros cursos na área dos sistemas de informação entre os quais o CCNA-Exploration da Cisco e IBM Security QRadar.

Possui ainda experiência nas áreas de Information Assurance, Vulnerability Assessment, Penetration Testing, Forensics, Configurations Analysis, Security Analysis, Hardening e Incident Response. Desenvolveu vários projetos na área, entre os quais a criação da ferramenta EmailAnalyzer, disponível na plataforma GitHub. Destaque ainda para a sua participação nos seguintes exercícios internacionais: NATO Cyber Coalition (2014, 2015, 2016 e 2019), NATO Locked Shields (2018, 2019 e 2021), CrossedSwords (2020), BRAZIL – CyberSecurity Brazilian Army Course e Ibero-Armerican Exercise of Cyber Defense (2018).

15. 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 *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-limite estabelecida no Calendário.

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

Sábado (xx/yy)	**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 20 minutos vezes o n.º 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 curso, na plataforma.

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 da 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 o qualidade 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 PLATAFORMAbERTA

Este curso desenvolve-se na PlataformAbERTA da UAb que integra o LMS Moodle. Martin Dougiamas lançou em 1999 a primeira versão do LMS 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 te 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”.

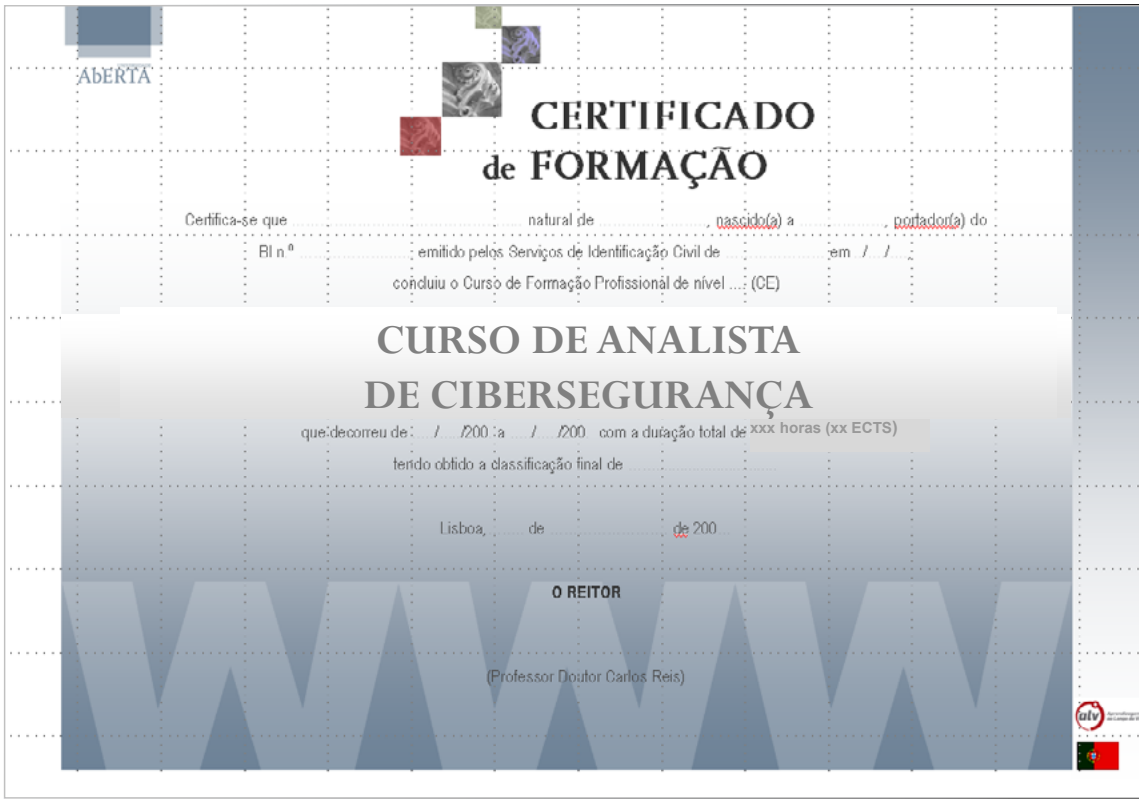
Teste – o formador pode construir uma base de dados de perguntas e respostas. Os testes podem ter diferentes formatos de resposta (verdadeiro ou falso, escolha múltipla, resposta curta ou numérica, correspondência, etc.) e é possível escolher perguntas aleatoriamente, corrigir respostas automaticamente 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 6: MODELO DO CERTIFICADO DE FORMAÇÃO



ABERTA

CERTIFICADO
de FORMAÇÃO

Certifica-se que natural de , nascido(a) a , portador(a) do
BI n.º emitido pelos Serviços de Identificação Civil de em / /
concluiu o Curso de Formação Profissional de nível ... (CE)

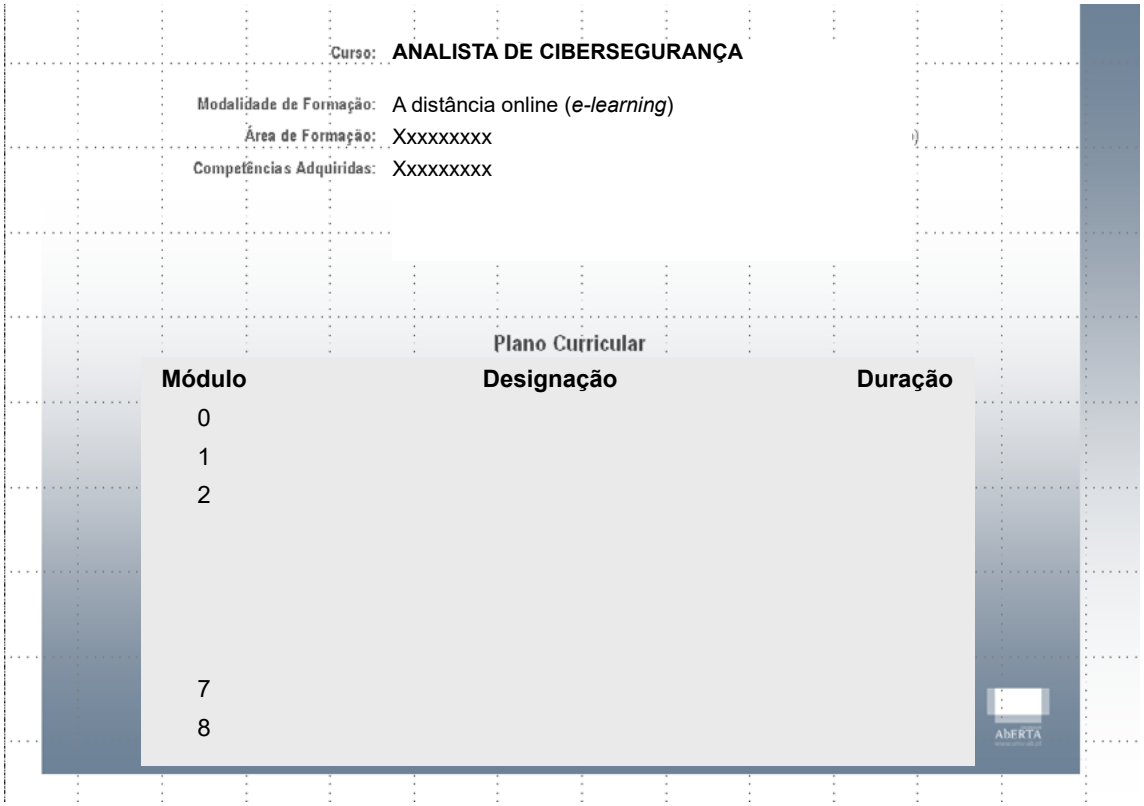
CURSO DE ANALISTA
DE CIBERSEGURANÇA

que decorreu de / /200 a / /200 com a duração total de xxx horas (xx ECTS)
tendo obtido a classificação final de

Lisboa, de de 200

O REITOR

(Professor Doutor Carlos Reis)



Curso: **ANALISTA DE CIBERSEGURANÇA**

Modalidade de Formação: A distância online (*e-learning*)
Área de Formação: Xxxxxxxxx
Competências Adquiridas: Xxxxxxxxx

Plano Curricular

Módulo	Designação	Duração
0		
1		
2		
7		
8		

ABERTA


UNIVERSIDADE
ABERTA
www.uab.pt