UNIVERSIDADE ABERTA
www.uab.pt

ANÁLISE FORENSE DIGITAL E A INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS

PRR Plano de Recuperação e Resiliência
REPÚBLICA PORTUGUESA
Financiado pela União Europeia NextGenerationEU

ÍNDICE

1. MICROCREDENCIAIS

Segundo com a Comissão Europeia, “microcredenciais” são qualificações que certificam resultados de aprendizagens resultantes de cursos curtos ou de módulos. Estas qualificações podem ser obtidas pelos cidadãos com diversas modalidades de aprendizagem, presencial, a distância online ou mista.

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

Estas qualificações, por norma de curta duração, serão essencialmente úteis para quem pretende complementar o seu conhecimento e competências ou para quem pretende requalificar-se, procurando novas oportunidades no mercado de trabalho.

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

2. ENQUADRAMENTO

A análise forense digital e a inteligência de ameaças cibernéticas são componentes essenciais da cibersegurança moderna, permitindo a investigação de incidentes, a recuperação de evidências digitais e a identificação de ameaças cibernéticas emergentes. A capacidade de examinar sistemas comprometidos, correlacionar dados e antecipar ameaças é um diferencial crítico para profissionais de segurança e investigadores digitais.

A análise forense digital envolve a recolha, preservação e exame de evidências digitais com o objetivo de identificar atividades maliciosas e reconstruir eventos relacionados a incidentes de segurança.

A compreensão de artefactos do sistema, logs de eventos e estruturas de dados permite a identificação da origem de um ataque e das técnicas utilizadas pelos atacantes. Além disso, a análise forense estende-se a múltiplos ambientes, incluindo sistemas Windows, Linux, dispositivos móveis e redes, tornando-se uma competência indispensável para profissionais da área.

A inteligência de ameaças cibernéticas (Cyber Threat Intelligence – CTI) complementa a análise forense ao fornecer uma visão contextualizada sobre atores maliciosos, as suas técnicas e motivações.

O uso de inteligência cibernética permite que organizações antecipem e mitiguem ataques, identificando indicadores de comprometimento (IoCs) e correlacionando eventos para uma resposta mais eficiente a incidentes de segurança.

O curso de Analista Forense Digital e CTI destina-se a profissionais e estudantes que desejam aprofundar os seus conhecimentos em análise forense digital e inteligência de ameaças cibernéticas, combinando uma abordagem teórica e prática. O curso aborda desde os conceitos fundamentais da análise forense até técnicas avançadas de investigação, utilizando ferramentas especializadas para análise de sistemas Windows, Linux, dispositivos móveis e redes.

Adicionalmente, os participantes aprenderão a aplicar inteligência de ameaças para melhorar a resposta a incidentes e fortalecer a segurança organizacional. Os módulos do curso incluem temas essenciais, como recolha e preservação de evidências digitais, análise de artefactos forenses em diferentes sistemas operativos, investigação de incidentes em redes, uso de ferramentas especializadas, e técnicas de inteligência de ameaças. A formação culmina num teste final, no qual os participantes aplicarão os conhecimentos adquiridos na resolução de questões relacionadas com a investigação digital e análise de ameaças.

A Universidade Aberta (UAb) oferece este curso em regime de ensino a distância (e-learning), combinando teoria e prática através de metodologias interativas e estudos de caso.

A avaliação final baseia-se na realização de uma prova final, submetida na plataforma da universidade, permitindo que os formandos demonstrem as suas competências na análise forense digital e inteligência de ameaças cibernéticas. Este curso prepara os participantes para atuar em ambientes corporativos, governamentais e forenses, fortalecendo as suas habilidades na deteção, análise e mitigação de incidentes de segurança.

3. OBJETIVOS

O objetivo deste curso é proporcionar conhecimentos e competências essenciais para a realização de investigações forenses digitais e análise de ameaças cibernéticas, permitindo aos formandos identificar, preservar, analisar e reportar evidências digitais de forma metódica e rigorosa. Assim, no final, os participantes saberão:

- Os aspetos legais e éticos associados à análise forense digital e à inteligência de ameaças cibernéticas;

- Identificar, recolher e preservar evidências digitais, garantindo a sua integridade e cadeia de custódia;
- Analisar artefactos digitais em diferentes sistemas operativos, incluindo Windows, Linux e dispositivos móveis;
- Investigar logs, metadados e outros vestígios digitais para compreender a origem e o impacto de incidentes de segurança;
- Utilizar ferramentas especializadas para análise forense, incluindo Autopsy, Sleuth Kit, Wireshark, Volatility e outras;
- Realizar análise forense de rede, identificando tráfego suspeito e correlacionando dados com outras descobertas forenses;
- Compreender e aplicar conceitos fundamentais de inteligência de ameaças cibernéticas (CTI) para fortalecer investigações;
- Correlacionar indicadores de comprometimento (IoCs) com os eventos forenses para suportar a resposta a incidentes;
- Estruturar e redigir relatórios forenses detalhados para públicos técnicos e não técnicos;
- Aplicar metodologias de investigação digital para auxiliar processos judiciais e corporativos.

O regime de funcionamento online, suportado por uma plataforma informática de gestão da formação/aprendizagem, permitirá ainda alcançar outros objetivos e adquirir competências transversais fundamentais para a empregabilidade. Deste modo, os formandos irão desenvolver e aprimorar competências nos domínios da comunicação e das Tecnologias de Informação e Comunicação (TIC), essenciais para a pesquisa eficiente de informações técnicas, colaboração com especialistas nacionais e internacionais e participação em futuras formações na modalidade de e-learning.

4. COMPETÊNCIAS

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

Competências Técnicas

- Aplicar os conceitos fundamentais da análise forense digital na investigação de incidentes de cibersegurança.
- Identificar e preservar evidências digitais de forma adequada, garantindo a integridade dos dados.

- Analisar estruturas de sistemas de ficheiros e utilizar técnicas de recuperação de dados.
- Redigir relatórios forenses claros e estruturados, adequados para públicos técnicos e não técnicos.
- Identificar e interpretar artefactos do sistema Windows para análise de atividades e rastreio de utilizadores.
- Utilizar ferramentas forenses para análise de logs, registos e eventos do Windows.
- Realizar a recolha e análise de dados forenses em dispositivos móveis, incluindo extração de mensagens, chamadas e dados de localização.
- Aplicar técnicas de análise forense em sistemas Linux, incluindo a interpretação de logs e rastreamento de atividades suspeitas.
- Capturar e analisar pacotes de rede para deteção de atividades suspeitas e correlação com outras evidências forenses.
- Aplicar metodologias de inteligência de ameaças para complementar a análise forense e melhorar a resposta a incidentes.
- Usar plataformas de inteligência de ameaças (Threat Intelligence) para análise e correlação de indicadores de comprometimento (IoCs).

Competências Transversais

- Desenvolver um pensamento analítico e crítico para a investigação de incidentes e correlação de evidências.
- Aprender continuamente e adaptar-se às novas ameaças e desafios da cibersegurança.
- Trabalhar em equipa em investigações forenses e partilhar descobertas com diferentes stakeholders.
- Gerir eficazmente o tempo e organizar investigações forenses de forma metódica.
- Comunicar descobertas forenses de forma clara e objetiva, tanto para equipas técnicas como para gestores e decisores.

5. PROGRAMA E CONTEÚDOS

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. O curso tem

a duração de 104 horas 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 PlataformAbERTA em utilização na UAb e adaptada ao seu Modelo Pedagógico Virtual.

MÓDULOS	DESCRIÇÃO
Módulo 0 Ambientação ao contexto online	Pretende socializar os participantes, criar de "um grupo" de trabalho online e familiarizar com a utilização do software de gestão do curso (o Learning Management System PlataformAbERTA) para uma exploração eficaz de todas as suas funcionalidades.
Módulo 1 Introdução à análise forense digital	Conceitos e importância da análise forense digital, recolha de evidências digitais e análise de sistemas de ficheiros. Desenvolvimento de relatórios forenses detalhados.
Módulo 2 Forense em sistemas Windows	Identificação e análise de artefactos em sistemas Windows, utilização de ferramentas forenses específicas e correlação de logs com atividades dos utilizadores.
Módulo 3 Forense em dispositivos móveis	Análise forense em dispositivos móveis, recolha e análise de dados de aplicações e sistemas móveis. Técnicas de aquisição e recuperação de dados em dispositivos móveis.
Módulo 4 Forense em sistemas Linux	Identificação de artefactos críticos em sistemas Linux, utilização de ferramentas forenses e análise de logs e atividades no sistema Linux.
Módulo 5 Forense em redes	Análise de pacotes de rede e identificação de atividades suspeitas usando ferramentas como Wireshark. Compreensão dos principais protocolos de rede na forense digital.
Módulo 6 Inteligência de ameaças cibernéticas – Fundamentos	Compreensão do ciclo de inteligência de ameaças cibernéticas, utilização de dados de inteligência para melhorar a resposta forense.
Módulo 7 Inteligência de ameaças cibernéticas – Análise e aplicação	Aplicação de técnicas de análise de ameaças para fortalecer investigações forenses e correlacionar descobertas com dados de investigação forense.
Módulo 8 Exercício final	Revisão dos conceitos abordados durante o curso e preparação para a avaliação final.

[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: AMBIENTAÇÃO AO CONTEXTO ONLINE DO CURSO

Duração: 13 horas práticas/1 semana

Objetivos

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 PlataformAbERTA) por forma a adquirirem as competências necessárias à exploração eficaz de todas as suas funcionalidades de intercomunicação, em especial as assíncronas por força do Modelo Pedagógico Virtual da UAb.

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 a interface de aprendizagem no sentido de conseguir resolver problemas básicos de interação e de comunicação;
- Explorar com eficácia todas as ferramentas e possibilidades da PlataformAbERTA, 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 a PlataformAbERTA; Formas de organizar espaços/sites;

Recursos e atividades da PlataformAbERTA;

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

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

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

MÓDULO 1: INTRODUÇÃO À ANÁLISE FORENSE DIGITAL

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Entender os conceitos e a importância da análise forense digital.

- Identificar evidências digitais e métodos de preservação.
- Analisar a estrutura de sistemas de ficheiros e a importância dos metadados.
- Redigir relatórios forenses detalhados e claros.

Competências a adquirir

- Domínio de conceitos fundamentais da forense digital.
- Capacidade de recolher e preservar evidências digitais.
- Análise e recuperação de dados de sistemas de ficheiros.
- Estruturar e redigir relatórios forenses.

Conteúdos programáticos

- Conceitos e importância da forense digital.
- Recolha e preservação de evidências.
- Sistemas de ficheiros e técnicas de recuperação de dados.
- Estruturação e redação de relatórios forenses.
- Prática em contexto de formação.

Prática em contexto de formação

- Estudo de caso sobre cadeia de custódia e prática com ferramentas de bloqueio de escrita.
- Teste de avaliação.

MÓDULO 2: FORENSE EM SISTEMAS WINDOWS

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Identificar e interpretar artefactos do sistema Windows.
- Utilizar ferramentas forenses específicas para análise em Windows. Correlacionar dados de registo e logs com atividades dos utilizadores.

Competências a adquirir

- Extração e análise de artefactos forenses no Windows.
- Identificação de eventos críticos em logs.
- Capacidade de documentar e reportar descobertas.

Conteúdos programáticos

- Artefactos do Windows (registos, logs de eventos, etc.).
- Ferramentas e técnicas de análise forense em Windows.
- Análise de logs de eventos e rastreamento de atividades dos utilizadores.

Prática em contexto de formação

- Análise de registos e logs de eventos.

- Teste de avaliação.

MÓDULO 3: FORENSE EM DISPOSITIVOS MÓVEIS

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Compreender a análise forense em dispositivos móveis.
- Realizar a recolha e análise de dados em sistemas móveis.
- Extrair dados de aplicações móveis, como mensagens e localização.

Competências a adquirir

- Artefactos do Windows (registos, logs de eventos, etc.).
- Ferramentas e técnicas de análise forense em Windows.
- Análise de logs de eventos e rastreamento de atividades dos utilizadores.

Conteúdos programáticos

- Introdução à forense em dispositivos móveis.
- Recolha e análise de dados em dispositivos móveis.
- Desafios e limitações na análise forense móvel.

Prática em contexto de formação

- Aquisição e análise de dados de dispositivos móveis.
- Teste de avaliação.

MÓDULO 4: FORENSE EM SISTEMAS LINUX

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Identificar artefactos críticos em sistemas Linux.
- Utilizar ferramentas forenses específicas para analisar sistemas Linux. Interpretar logs e rastrear atividades no sistema.
- Competências a adquirir.
- Artefactos do Windows (registos, logs de eventos, etc.). Ferramentas e técnicas de análise forense em Windows.
- Análise de logs de eventos e rastreamento de atividades dos utilizadores.

Conteúdos programáticos

- Arquitetura do sistema Linux e estruturas de dados.
- Ferramentas e técnicas de análise forense em Linux.
- Análise de logs e recuperação de ficheiros excluídos.

Prática em contexto de formação

- Extração e análise de logs de sistemas Linux.

- Teste de avaliação.

MÓDULO 5: FORENSE EM REDES

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Compreender os principais protocolos de rede e a sua relevância na forense digital.
- Capturar e analisar pacotes de rede para identificar atividades suspeitas.

Competências a adquirir

- Artefactos do Windows (registos, logs de eventos, etc.).
- Ferramentas e técnicas de análise forense em Windows.
- Análise de logs de eventos e rastreamento de atividades dos utilizadores.

Conteúdos programáticos

- Fundamentos de protocolos de rede e análise de pacotes.
- Integração de dados de rede com evidências digitais.

Prática em contexto de formação

- Análise de pacotes de rede e simulação de incidentes.
- Teste de avaliação.

MÓDULO 6: INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS – FUNDAMENTOS

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Compreender o ciclo de inteligência de ameaças cibernéticas.
- Identificar diferentes tipos de inteligência de ameaças e aplicar essas informações na análise forense.

Competências a adquirir

- Capacidade de utilizar dados de inteligência de ameaças para melhorar a resposta forense.

Conteúdos programáticos

- Ciclo de inteligência de ameaças e sua aplicação.
- Fontes de inteligência (OSINT, feeds de ameaças).

Prática em contexto de formação

- Criação de um perfil de ameaça básico usando dados de OSINT.
- Teste de avaliação

MÓDULO 7: INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS – ANÁLISE E APLICAÇÃO

Duração: 13 horas teórico-práticas/1 semana

Objetivos

- Aplicar técnicas de análise de ameaças para fortalecer investigações forenses.
- Correlacionar descobertas de inteligência de ameaças com dados de investigação forense.

Competências a adquirir

- Utilização de plataformas de Threat Intelligence para análise de incidentes e indicadores de comprometimento.

Conteúdos programáticos

- Correlação de eventos com partilha estruturada de inteligência de ameaças.

Prática em contexto de formação

- Uso de plataformas de Threat Intelligence para investigação forense.
- Teste de avaliação.

MÓDULO 8: EXERCÍCIO FINAL

Duração: 13 horas teórico-práticas/1 semana

- Revisão dos conceitos abordados durante o curso.
- Preparação para uma avaliação final.

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

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

6. DESTINATÁRIOS E PRÉ-REQUISITOS

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 vulnerabilidades e testes de penetração para melhor protegerem as redes e sistemas;
- Todos os profissionais que pretendam iniciar-se numa carreira de Analista Forense Digital;
- Indivíduos que desejem iniciar uma especialização em análise forense digital para poderem desempenhar a função de analista forense digital e integrar equipas de

resposta a incidentes de organizações/empresas;

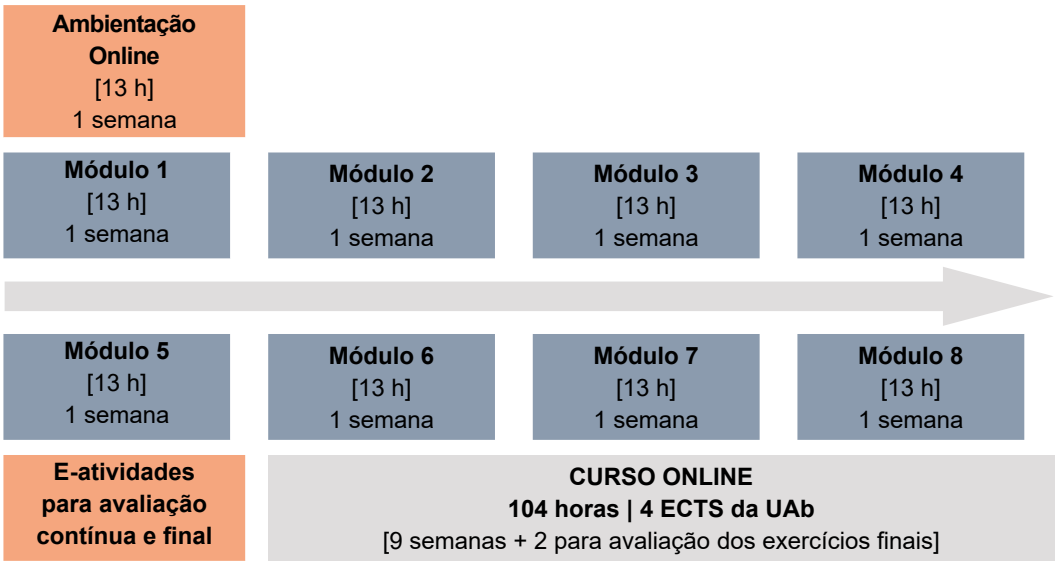
Trata-se, portanto, de um público adulto, por norma trabalhador no ativo, e este facto deve ser considerado na forma como se deve fazer aprender, como motivar para essa aprendizagem e como avaliar os conhecimentos e competências adquiridos.

Além da motivação e ou interesse os formandos devem teros seguintes pré-requisitos:

- Habilitações mínimas ao nível do 12.º ano ou legalmente equivalente;
- Computador com pelo menos 8 GB 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 para o curso de 13 horas por semana.

7. DURAÇÃO E ESTRUTURA

A duração total da microcredencial é de 104 horas, estruturadas em 8 módulos de realização sequencial, precedidos de um módulo de Ambientação ao contexto online.



8. METODOLOGIA

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 PlataformAbERTA 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 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 fóruns de discussão abertos nos diversos tópicos (correspondentes aos módulos da estrutura do curso) na PlataformAbERTA.

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

9. RECURSOS DE APRENDIZAGEM

Recursos pedagógicos

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 PlataformAbERTA e/ou na Web em servidor a indicar aos participantes para procederem o seu download;
- Apresentações multimédia diversas concebidas pelos formadores para situações de aprendizagem específicas;
- Tutorial sobre a forma de utilizar a PlataformAbERTA na situação de e- formando;
- Tutorial “Como Fazer para…”, documento orientador dos procedimentos para aceder ao curso alojado na PlataformAbERTA;
- Guia da Microcredencial;
- Guia do Formando Online.

Recursos técnicos

Plataforma informática PlataformAbERTA, em http://elearning.uab.pt, apoiada por 4 servidores e utilizando uma ligação com 200 MB/s de largura de banda.

10. 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.

Avaliação nos Módulos

Os módulos 1 a 7 do curso são sujeitos a avaliação. A avaliação nos módulos 1 a 7 integra:

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

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

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

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

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

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

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

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

discussão traduz-se numa classificação de 0 valores nesse fórum.

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

Classificação Final no Curso

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

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

$AFMx$ representa a Avaliação Final do Módulo x.

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 e a seu pedido expresso, será entregue um Certificado de Frequência.

11. EQUIPA DOCENTE

FORMADORES	MÓDULOS
A cargo da UALV	0. Ambientação ao contexto do e-learning, socialização online e treino com ferramentas do Moodle
Luís Dias André Calvinho	1. Introdução à Análise Forense Digital
Luís Dias André Calvinho	2. Forense em Sistemas Windows
André Calvinho	3. Forense em Dispositivos Móveis
André Calvinho	4. Forense em Sistemas Linux
André Calvinho	5. Forense em Redes
Luís Dias	6. Inteligência de Ameaças Cibernéticas – Fundamentos
Luís Dias	7. Inteligência de Ameaças Cibernéticas – Análise e Aplicação
Luís Dias André Calvinho	8. Exercício Final

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

Atualmente e desde 2023, é formador em ciberdefesa numa organização internacional. Foi docente de "Segurança Informação, Sistemas de Informação e Ciberdefesa" (entre outras Unidades Curriculares) na Academia Militar, docente na Universidade Atlântica, docente de cibersegurança e Coordenador de Inovação Científica na área de cibersegurança na Universidade Europeia. Desempenhou funções na componente operacional de ciberdefesa do Exército, entre 2010 e 2015. Participou como "jogador" em diversas edições de exercícios de ciberdefesa Nacionais e Internacionais (Ciber Perseu, Cyber Coalition da NATO). Em 2018 e 2019 foi organizador dos Exercícios Nacionais de Ciberdefesa (Ciber Perseu) na área relativa à resposta técnica a incidentes informáticos.

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

ANDRÉ VICENTE CALVINHO, antigo Capitão Engenheiro da Arma de Transmissões do Exército Português, é especializado na área da ciberdefesa e Segurança da Informação. Possui 10 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).