Designação do Curso	Crescer em Cibersegurança
Àrea de Formação:	481 - Informática
Modalidade de formação:	B-learning
Forma de organização:	
Nº Mínimo de Formandos	6
Nº Máximo de Formandos	10
Carga horária total:	50
Horas de formação teórica:	
Horas de formação prática:	
Equipa Pedagógica:	
Coordenador Pedagógico:	
Formadores	
Data de início	
Data de Fim	
Horário de funcionamento	
Local de realização	

OBJETIVOS DO PROGRAMA

Objetivos Gerais:	No Final do Curso os formandos devem estar aptos a: Projetar e garantir ambientes ciberseguros para sistemas informáticos Conhecer e aplicar a legislação referente a cibersegurança e proteção de dados
Objetivos especificos:	No final da formação espera-se que os formandos estejam aptos a: Projetar Redes com Arquitetura CiberSegura e sistemas de monitorização e deteção de intrusão e ataques cibernéticos Instalar e configurar todos os componentes ativos que garantem a cibersegurança dum sistema informático. Garantir a manutenção de firewalls, gateways e agentes de monitorização de cibersegurança Proteger as redes de vários tipos de ataques cibernéticos Realizar análise forense de ataques ocorridos Através de modlos matemáticos, prever e prevenir ciberataques a redes, servidores, ativos e clientes

PRÉ-REQUISITOS E FORMA DE SELEÇÃO

Condições de Acesso:	Conhecimentos de Informática na ótica do utilizador, Conhecimentos de Sistemas Operativos
Forma de seleção	Entrevista Individual

AVALIAÇÃO

A avaliação dos formandos será feita, de forma contínua, através de parâmetros **quantitativos**:

- Ficha de avaliação no Final de cada Unidade (Formativa)
- Ficha de Avaliação Final (Sumativa)
- Assiduidade (frequência mínima de 90% da carga total do curso, não podendo faltar a uma unidade por completo)

E com base em parâmetros **qualitativos**, por observação:

- Pontualidade, Participação, Motivação, Interesse, Maturidade, Relacionamento com os colegas e Relacionamento com os formadores

A Classificação Final = **Classificação da Ficha de avaliação final** (ponderada em relação aos parâmetros qualitativos)

Serão aprovados todos os formandos com uma **Classificação Final igual ou superior a 50%**, de acordo com a seguinte escala avaliativa:

0% - 49%	Insuficiente	Não Apto
50% - 69%	Suficiente	Apto
70% a 89%	Bom	
90% a 100%	Muito Bom	

A todos os formandos que obtiverem aproveitamento será entregue um Certificado de Formação Profissional emitido pela entidade formadora.

O não cumprimento das regras de assiduidade, a falta de aproveitamento, ou o não pagamento das prestações previstas determinam a não emissão do Certificado de Formação Profissional.

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9187	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas

Legislação segurança e privacidade
(25 Horas)
	• Identificar os conceitos fundamentais de direitos, liberdades e garantias, internacionais e nacionais.
	• Identificar legislação nacional e comunitária de proteção de dados (LPDP).
	• Interpretar a legislação nacional sobre manuseamento de informação classificada (SEGNAC).
	• Interpretar a legislação nacional sobre cibercriminalidade.
		• Princípios da Declaração Universal dos Direitos Humanos
		• Direito de imagem
		• Princípios da Carta dos Direitos Fundamentais da União Europeia aplicados à cibersegurança
		• Princípios constitucionais da Constituição da República Portuguesa (CRP) e os preceitos constitucionais respeitantes aos direitos, liberdades e garantias
		• Conceitos de privacidade, dados pessoais e dados sensíveis
		• Conceitos nacionais e comunitários em matéria de administração eletrónica e proteção de dados
		  ○ Direito de informação
		  ○ Direito de acesso
			Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

		○ Direito de oposição ○ Direito de retificação e eliminação ○ Código de Procedimento Administrativo • Conceitos nacionais e comunitários em matéria informação classificada ○ Princípio da necessidade de conhecer ○ Manuseamento ○ Classificação da informação • Conceitos de cibercrime • Conceitos de competências de investigação criminal em cibercriminalidade • Conceitos de normas processuais na investigação de cibercrimes		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 5892	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Modelos de gestão de redes e de suporte a clientes (25 Horas)	• Identificar os modelos de gestão de redes. • Aplicar as técnicas de suporte a clientes.	• Modelo eTOM • Enquadramento • O Contexto das relações de negócio • O Modelo eTOM • ITIL • História e contexto de negócio do ITIL • Os processos nucleares ITIL • Abordagem ITIL à gestão de serviços • Relação entre eTOM e ITIL • Associação ITIL / eTOM • Estrutura em camadas	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

		• Harmonização da terminologia • Mapeamentos entre os dois quadros de referência • A incorporação do ITIL no eTOM (ITIL)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9189	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Tecnologias de análise de evidências (50 horas)	• Identificar as fontes de informação mais relevantes usadas na análise de evidências para os principais tipos de incidentes. • Reconhecer a alto nível expressões regulares e sua representação nas linguagens mais comuns de *scripting*. • Identificar a estrutura e propriedades dos elementos de informação relevantes a extrair dessas fontes de informação. • Identificar as representações textuais mais comuns de "*timestamps*". • Identificar os scripts simples de extração de informação de logs nas linguagens mais comuns de *scripting*. • Identificar as principais fontes de	• Composição e estrutura dos *Logs*: DHCP ○ *Microsoft Active Directory* (AD) ○ *Domain name server* (DNS) ○ RADIUS ○ *Squid Proxy Logs* ○ *Microsoft Exchange* ○ *WebServers*: IIS e *Apache* ○ *WebApplication Servers: JBoss* ○ *Windows EventLogs* ○ *Windows Registry* ○ *Unix/Linux SystemLogs* • Fontes públicas de informação sobre IPs e	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

	informação pública sobre vulnerabilidades, reputação e ameaças. • Reconhecer a alto nível o funcionamento de sistemas de extração, filtragem, transporte e registo de logs. • Reconhecer a alto nível o funcionamento de sistemas de indexação e correlação sobre logs. • Reconhecer a alto nível o funcionamento de sistemas de *Complex Event Processing* (CEP). • Reconhecer a alto nível o funcionamento de sistemas *Security Information and Event Managment* SIEM.	sua reputação • Fontes de informação sobre vulnerabilidades em formato CVE (*Common Vulnerabilities and Exposures*) • Arquitetura e funcionamento para análise de evidências ○ *SyslogNG* ○ *LogStash* ○ *Splunk* ○ ESPER ○ OSSIM • Deteção e análise de BOTNETs usados em ataques "*brute force*" (Cyber Ops Associate – CISCO)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo **UFCD 9190**	**Objectivos** **No final da unidade os formandos deverão estar aptos a:**	**Temas/Conteúdos Programáticos**	**Metodologia Pedagógica**	**Recursos e atividades** **Didáticas**

Introdução da programação aplicada à Cibersegurança (25 horas)	• Elaborar pequenos scripts sequenciais, utilizando linguagem moderna de *scripting*.
	• Aplicar técnicas de extração, filtragem e normalização de informação de logs aplicacionais ou de sistema.
	• Aplicar expressões regulares simples na extração de informação em linhas de *logs*.
		• Instalação do *Ruby*
		• Variáveis e seu escopo
		• Constantes e símbolos
		• Tipos de dados elementares do *Ruby*
		  ○ Booleanos
		  ○ Números e intervalos
		  ○ *Strings*
		• Tipos de dados não elementares
		  ○ *Arrays*
		  ○ *Hashes*
		  ○ Ficheiros
			Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

		○ Blocos de código ○ *Procs* • Estruturas de controlo -- operadores condicionais ○ *If / elsif / else / end* ○ *case / when / else / end* • Estruturas de controlo -- operadores de *loop* ○ *While* ○ *For* ○ *Until* ○ *Loop* • Blocos • Expressões regulares • Classes e métodos • Módulos		

		• Exceções (PCAP – Programming Essentials in Python)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9191	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas

Introdução às técnicas de análise de evidências
(50 Horas)
	• Elaborar *scripts*, utilizando uma linguagem moderna de *scripting*, de extração, filtragem e normalização de informação de logs aplicacionais e de sistema.
	• Normalizar timestamps em torno do referencial global UTC (*Universal Time Coordinated*).
	• Reconhecer e validar endereços de email com autenticação.
	• Reconhecer, resolver e normalizar URIs, domínios e IPs ou ranges de IPs (v4 e v6).
	• Utilizar bibliotecas de operações especializadas sobre timestamps, endereços de email, URIs, domínios e IPs ou *ranges* de IPs (v4 e v6).
		• Idiomas Ruby para extração, filtragem e normalização de *logs* em
		  ○ *Filesystem*
		  ○ Ambiente *Syslog*
		• Tipos mais comuns de codificação de strings em *logs*
		  ○ ASCII
		  ○ UTF-8
		• Expressões regulares para identificação e extração de
		  ○ *Timestamps*
		  ○ Endereços de email
		  ○ IPs ou *ranges* de IPs
			Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas, computadores, servidores e software de sistemas operativos

	• Utilizar bibliotecas de operações especializadas na geolocalização aproximada de IPs e suas distâncias. • Utilizar bibliotecas de algoritmos de medição da distância lexical entre *strings*. • Detetar e analisar BOTNETs.	○ Domínios (DNS) • Bibliotecas especializadas para manipular ○ URIs ○ Verificar a existência de endereços de email ○ Resolver domínios Internet (DNS) em IPs ○ IPs e *ranges* de IPs (v4 e v6) ○ Geolocalização aproximada de IPs (v4 e v6) ○ Operações sobre IPs e *ranges* de IPs • Introdução a outras bibliotecas relevantes e sua aplicação em cibersegurança ○ Distância *Levenshtein* entre *strings* ○ API Google Maps • BOTNETs e seus padrões de comportamento		

		(Introduction to Cybersecurity – CISCO) (Cybersecurity Essentials – CISCO)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9192	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas
Análise de Vulnerabilidades – Iniciação (50 H)	• Identificar o conjunto de vulnerabilidades *web* inventariadas pelo *Open Web Application Security Project* (OWASP). • Identificar as técnicas mais comuns na deteção de vulnerabilidades OWASP. • Ler *scripts* simples em *JavaScript* e PHP e analisar falhas de segurança. • Utilizar ferramentas de busca e análise de vulnerabilidades OWASP e interpretar os resultados obtidos.	• As top 10 vulnerabilidades *Web* inventariadas pelo *Open Web ApplicationSecurity Project* (OWASP) ○ *Injection* ○ *Broken Authentication and Session Management* ○ *Cross-Site Scripting* (XSS) ○ *Insecure Direct Object References* ○ *Security Misconfiguration* ○ *Sensitive Data Exposure* ○ *Missing Function Level Access Control* ○ *Cross-Site Request Forgery* (CSRF)	Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas e cibersegurança, computadores, servidores e software de sistemas operativos

		○ *Using Known Vulnerable Components* ○ *Insecure cryptographic storage* (ICS) • Introdução básica ao *JavaScript* e PHP • Análise de *scripts JavaScript* com vulnerabilidades • Análise de *scripts* PHP com vulnerabilidades • Introdução ao *ZedAttack Proxy* (ZAP) e sua aplicação no contexto OWASP • Introdução ao *OpenVASe* sua aplicação no contexto OWASP • Utilização do ZAP e *Open*VAS na descoberta e análise de vulnerabilidades em web sites ○ CVE ○ Segurança na sua configuração e gestão		

		○ Aplicação de scans NESSUS (CCNA Cybersecurity Operations CISCO)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9193	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas

Análise de Vulnerabilidades – Desenvolvimento (50 H)	• Identificar as boas práticas de segurança na configuração e gestão de sistemas de rede e de IT e seus protocolos operacionais.
	• Identificar vulnerabilidades em equipamentos de rede.
	• Identificar vulnerabilidades em servidores Linux/Unix e Windows.
	• Interpretar o dicionário público "CVE" (*Common Vulnerabilities and Exposures*) com informação de referência sobre vulnerabilidades conhecidas.
	• Aplicar as técnicas, baseadas em agentes, na deteção de vulnerabilidades de segurança em servidores Linux/Unix e Windows.
	• Aplicar as técnicas, baseadas em sondas de
		• Introdução às boas práticas gerais na configuração e gestão de plataformas de rede e IT
		• Ferramentas de deteção e gestão de vulnerabilidades
		  ○ Dicionário público "CVE" (*Common Vulnerabilities and Exposures*) com informação de referência sobre vulnerabilidades conhecidas
		  ○ CMDBs (*configuration management database*)
		  ○ Agentes OSSEC
		  ○ Motor de *scanning* NESSUS
		• Configuração e gestão de plataformas de rede
		  ○ Vulnerabilidades e tipos de ataque
			Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas e cibersegurança, computadores, servidores e software de sistemas operativos

	rede, na descoberta de vulnerabilidades de segurança em equipamentos de rede e servidores Linux/Unix e Windows. • Utilizar as ferramentas de busca e análise de vulnerabilidades em redes e servidores e interpretar os resultados obtidos.	mais comuns e sua codificação CVE ○ Segurança na sua configuração e gestão ○ Aplicação de scans NESSUS • Configuração e gestão de servidores Linux/Unix ○ Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE ○ Segurança na sua configuração e gestão ○ Aplicação de agentes OSSEC ○ Aplicação de scans NESSUS • Configuração e gestão de servidores Windows ○ Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE ○ Segurança na sua configuração e		

		gestão ○ Aplicação de agentes OSSEC ○ Aplicação de scans NESSUS • Configuração e gestão de servidores Web ○ Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE ○ Segurança na sua configuração e gestão ○ Aplicação de agentes OSSEC ○ Aplicação de scans NESSUS • Configuração e gestão de *desktops Windows* ○ Vulnerabilidades e tipos de ataque mais comuns e sua codificação CVE ○ Segurança na sua configuração e gestão ○ Aplicação de scans NESSUS		

		(CCNA Cybersecurity Operations CISCO)		

Conteúdos e Estratégia pedagógica

Unidades Temática/ Módulo UFCD 9194	Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas

Introdução à Cibersegurança e à Ciberdefesa
(50 H)
	• Identificar e caracterizar as componentes tangíveis e intangíveis do ciberespaço.
	• Identificar as potenciais ciberameaças e os riscos individuais.
	• Identificar as boas práticas associadas à cibersegurança e ciberdefesa.
	• Identificar a natureza transversal das ciberameaças e o seu impacto global.
	• Caracterizar os constrangimentos operacionais decorrentes do enquadramento legal aplicável à cibersegurança (direito nacional) e ciberdefesa (direito internacional).
	• Reconhecer a importância da ciberdefesa das organizacões tanto numa perspetiva
		• Introdução ao ciberespaço e terminologia
		• Tipos de ataque e de atacantes, métodos e técnicas de proteção correspondentes
		• Impacto e boas práticas individuais de cibersegurança
		  ○ Desktop e web
		• Regulação e enquadramento legal do ciberespaço
		  ○ Lei do cibercrime
		  ○ Leis internacionais
		  ○ Conflitos armados no ciberespaço
		• Impacto e boas práticas de segurança das redes sociais
			Sessões Teóricas expositivas e práticas em laboratóro	Laboratório de redes informáticas e cibersegurança, computadores, servidores e software de sistemas operativos

	nacional como internacional.
	• Identificar as políticas de cibersegurança e ciberdefesa.
	• Reconhecer as potenciais ameaças cibernéticas e riscos para as organizações.
	• Identificar as responsabilidades do indivíduo e o seu papel enquanto agente ativo da cibersegurança e ciberdefesa das organizações.
		• Estratégia Nacional de cibersegurança e de ciberdefesa
		• Cibersegurança em operações militares e ciberdefesa
		• Compreensão e avaliação do ambiente da ameaça cibernética
		• Tecnologias emergentes
		• Gestão dinâmica do risco
		• Política de cibersegurança das organizações
		  ○ Finalidade e nível de ambição
		  ○ Objetivos a atingir
		  ○ Linhas de ação e definição de prioridades
		  ○ Controlo de execução e alinhamento das ações a desenvolver
		
		(CCNA Cybersecurity Operations CISCO)		

Carga horária Total	**50 h**