Designação do Curso	Proteção Empresarial e Cibersegurança
Àrea de Formação:	481 – Ciências Informáticas
Modalidade de formação:	Formação Extra Curricular
Forma de organização:	Presencial
Nº Mínimo de Formandos	6
Nº Máximo de Formandos	18
Carga horária total:	60
Horas de formação teórica:	10
Horas de formação prática:	10
Equipa Pedagógica:	Coordenador e formadores
Coordenador Pedagógico:	A definir na altura de concretização da ação
Formadores	A definir na altura de concretização da ação
Data de início	A definir na altura de concretização da ação
Data de Fim	A definir na altura de concretização da ação
Horário de funcionamento	A definir na altura de concretização da ação
Local de realização	Laboratório de Cibersegurança.

OBJETIVOS DO PROGRAMA

Objetivos Gerais:	No Final do Curso os formandos devem estar aptos a: • Monitorar e proteger eficazmente uma rede informática empresarial e equipamentos a ela conectados. • Discutir e aplicar técnicas de segurança de informação aplicáveis em cada situação. • Configurar a sua rede empresarial de modo a se protegerem eficazmente de potenciais ciberataques. • Conhecer a legislação existente na área de cibersegurança, e atuar em conformidade com esta. • Ter um comportamento ciberseguro na gestão do dia-a-dia.
Objetivos especificos:	No final da formação espera-se que os formandos estejam aptos a: • Identificar e entender os principais protocolos de Internet. • Detetar e entender os ataques que podem ocorrer a estes protocolos, e as suas vulnerabilidades. • Entender como a encriptação de dados é feita na Internet e como poderá ser subvertida. • Instalar, configurar e parametrizar sistemas IDPS. • Reconhecer falhas de segurança e eventos num SIEM que utilize dados IDPS. • Analisar e avaliar o nível de segurança (ou falta dela) duma rede informática empresarial e detetar as suas vulnerabilidades. • Definir perfis específicos de utilizadores para atuar como vigilantes e protetores da rede empresarial. • Desenhar e projetar ferramentas para detetar intrusões e tomar as respetivas ações de defesa, utilizando para tal dados recolhidos em ferramentas de *Big Data monitoring* para analisar o tráfego na rede, detetar intrusões e desenvolver as necessárias ações de prevenção e resposta. • Analisar o nível de segurança de sistemas e redes informáticas e assim definir estratégias de melhoria. • Analisar ocorrências de malware e tomar as necessárias

	medidas corretivas. • Analisar e ler as informações duma Sandbox, e em consequência das conclusões, tomar as necessárias medidas de modo a aumentar as necessárias medidas de proteção da rede. • Definir e implementar a melhor arquitetura de rede de modo a poder garantir o melhor nível de cibersegurança na mesma. • Instalar e configurar um Firewall em ambiente corporate configurando corretamente para proteção dos computadores e equipamentos da empresa. • Configurar uma rede empresarial de modo a se protegerem eficazmente de potenciais ciberataques.

PRÉ-REQUISITOS E FORMA DE SELEÇÃO

Condições de Acesso:	Inscrição online e entrevista de seleção Ser um normal utilizador da Internet como pré-requisito mínimo.
Forma de seleção	Atender ao nível de utilização da internet e realização de entrevista de acolhimento. Identificação e consideração dos pré-requisitos e objetivos a atingir com o curso.

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 Temáticas/ Módulos		Objectivos No final da unidade os formandos deverão estar aptos a:	Temas/Conteúdos Programáticos	Metodologia Pedagógica	Recursos e atividades Didáticas	Carga horária
1	**Introdução à proteção de dados e à Cibersegurança**	Adquirir todos os conhecimentos necessários a entender o funcionamento duma rede e os seus protocolos envolvidos, e os tipos de ameaças associadas a cada um deles. Ter um comportamento ciberseguro na gestão do dia-a-dia. Saber concretizar as ações corretivas necessárias para fazer face às várias ameaças Conhecer toda a legislação e regulamentação de suporte à temática da Cibersegurança em Portugal e na EU.	1. Introdução à proteção de dados e cibersegurança. 1.1 – Conceitos básicos e elementos da rede a proteger 1.2 – Tipos de ataques e ameaças 1.3 – Estratégias de segurança 1.4 – Legislação portuguesa e europeia a aplicar 2 Proteção de dados 2.1- Princípios básicos de proteção de dados 2.2- Atitudes conducentes a uma correta proteção de dados na vida diária. 3. Implementação de regras básicas de Cibersegurança 3.1 – Identificação e autenticação 3.2 – Gestão de riscos 3.3 – Conceitos básicos e standards de gestão de Cibersegurança. 3.4 – Standards ISO 2700XX 4. Gestão da Cibersegurança na vida diária 4.1 – Correta gestão de passwords 4.2 – Backup de dados 4.3 – Regras de segurança de e-mail 4.4 – Proteção contra vírus e malware 4.5 – Comportamento seguro nas redes sociais. 5. Redes e Comunicações 5.1 – Tecnologia de Firewall 5.2 – Separação e segmentação de redes 5.3 – Cibersegurança em ambiente WLAN, redes móveis e Bluetooth 6. Cibersegurança no departamento de software e gestão de rede 6.1 – Proteção do ambiente de desenvolvimento 6.2 – Técnicas seguras para desenvolvimento de software.	Método expositivo com interação com os formandos.	Apoios pedagógicos multimédia disponibilizados online	15H

2	**Introdução a técnicas forenses de análise de redes**	Atuar na rede de modo a realizar o tracking de determinadas ações de ameaça ou intrusão. Identificar e entender os diferentes protocolos da internet. Detetar e entender os ataques que podem ocorrer a estes protocolos. Entender como a encriptação de dados é usada na Internet e como pode ser subvertida. Instalar, configurar e distribuir (em ambiente de rede) sistemas IDPS (Intrusion Detetion and Prevention System). Reconhecer e identificar falhas de segurança e eventos ameaçadores num SIEM (Security Information Event System) que utiliza dados IDPS.	1. Introdução a técnicas forenses de análise de redes 1.1. - Qual a necessidade de utilizar "network forensics". 1.2. - Objetivos da recolha de dados 1.3. - Recolha das provas e evidências forenses numa rede. 1.4. - Deteção de Intrusão. 1.5. - Deteção e mitigação de ataques DoS – Denial of Service. 2. Camadas de protocolos 2.1. - Hierarquia dos protocolos utilizados na internet. 2.2. - Leitura e interpretação de RFC's. 3. TCP vs UDP 3.1.- Protocolos UDP. 3.2 - Estabelecimento, perca e restabelecimento de comunicações. 3.3 - Proxy SOCKs 3.4. - Ataques contra protocolos TCP e UDP. 4. Protocolo da Internet. 4.1 – Endereços Ipv4 e Ipv6. 4.2. – Obtenção de endereços Ipv4 e Ipv6. 4.3. – Ips de Firewalls e NAT (Network Addresses Translations). 4.4. – Protocolo Proxy SOCKS e Attack Vector 5. Routeamento na camada link. 5.1. – ARP – Addressing Routing Protocol. 5.2. – Routeamento Dinâmico (RIP). 5.3. – Boarding Gateway Protocol. 5.4. – Sistemas autónomos de numeração de IPs na Internet. 5.5. – Ataques sobre sistemas de routeamento. 6. DNS – Domain Name System. 6.1. – DNS como uma base de dados distribuída. 6.2.- DNSSEC – Segurança de DNS.	Método expositivo com interação com os formandos. Sessões teórico-práticas com execução e observação de tráfego na rede e outros trabalhos	Apoios pedagógicos multimédia disponibilizados online	25H

			6.3. – SPF, DMARC e outros tipos de registos especiais. 7. Protocolos da camada de Aplicação 7.1. – HTTP 7.2. – HTTP/2 7.3 – SMTP 8. Encriptação da camada de transporte 8.1. – SSH – Secure Shell. 8.2. – IPSEC – Internet Protocol Security. 8.3. – Protocolo TLS – Criptografia end-to-end. 8.4. – Ataques “Man in the middle”. 8.5. – Certificados Digitais e entidades de certificação. 9. Sistemas de Intrusão e Prevenção (IDS). 9.1 – Tipos de eventos e “sensores” (software de monitorização). 9.2 – Monitorização de tráfego na rede. 9.3 – SIEMs – Security Events Management Systems. 9.4. – Tecnologias de prevenção de ataques. 10. Correlação e enriquecimento de fontes de dados 10.1. – Origem de dados DNS 10.1.1. – DNS’s passivos 10.1.2. – Repositórios de DNS 10.2. – Análise e bloqueio preventivo de IP’s 10.2.1. – AS Numbers 10.2.2. – IPBlocks 10.2.3. – GeoIP 10.2.4. – Whois data 10.3.- Transparência de certificados 10.4.- Métodos de Correlação			

3	**Conceitos de segurança técnica e operacional em sistemas de informação**	Analisar e avaliar o nível de segurança em redes informáticas e detetar vulnerabilidades Desenvolver perfis específicos para proteção da rede empresarial Desenhar e projetar ferramentas para detetar intrusões e tomar ações de defesa da estrutura de rede Utilizar mecanismos de análise de Big Data para analisar o tráfego na rede, detetar intrusões e desenvolver ações de resposta Avaliar o nível de segurança e redes informáticas e assim definir estratégias de melhoria Analisar malware e tomar as necessárias medidas corretivas Analisar e ler as informações de uma Sandbox, e em função dos resultados obtidos tomar as necessárias ações corretivas.	1.Avaliação e análise do tráfego em redes informáticas 1.1. – Ameaças e vulnerabilidades de camadas específicas. 1.2. – Fluxo de dados, interdependências e interrelações. 1.3 – Scan e deteção de vulnerabilidades. 1.4 – Técnicas e ferramentas de suporte. 2. Perfis de proteção. 2.1- Arquitetura e tecnologia de referência para redes seguras. 2.2 – Gestão de riscos. 2.3 - Requisitos de segurança e salvaguarda. 2.4 – Análise e avaliação de sistemas de soluções de segurança informática. 2.5 – Acreditação de redes e sistemas informáticos 3. Análise e deteção de Malware. 3.1.- Técnicas de análise e deteção de Malware. 3.2. – Classificação de Malware. 4. Sandbox 4.1 – Análise e recolha de informação duma “Sandbox”. 4.2. – Investigação “profunda” na Sandbox para deteção de ameaças.	Método expositivo com interação com os formandos. Sessões teórico-práticas com execução e observação de tráfego na rede e outros trabalhos	Apoios pedagógicos multimédia disponibilizados online	20H
					Carga horária Total	**60 H**