Designação do Curso	Proteção Familiar e Cibersegurança
Àrea de Formação:	481 – Ciências Informáticas
Modalidade de formação:	Formação Extra Curricular
Forma de organização:	B-Learning
Nº Mínimo de Formandos	6
Nº Máximo de Formandos	18
Carga horária total:	20
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: • Conhecer os vários tipos de ataques e vulnerabilidades. • Aplicar as várias práticas de cibersegurança essenciais para a salvaguarda da informação dos seus computadores domésticos e promover a salvaguarda da sua família evitando exposições desnecessárias em redes sociais que podem comprometer a segurança de pessoas, nomeadamente crianças. • Configurar a sua rede doméstica de modo a se protegerem eficazmente de potenciais ciberataques.
Objetivos especificos:	No final da formação espera-se que os formandos estejam aptos a: • Instalar e configurar um Firewall doméstico configurando corretamente para proteção dos computadores domésticos de cada membro da família. • Aprender a restringir o acesso dos jovens e crianças a sites não convenientes e comprometedores da sua segurança. • Controlar a atividades das crianças e jovens da família na Internet e modo a não se exporem demasiado e fornecerem informações a estranhos, não divulgando as suas rotinas e locais nornais de permanência. • Configurar a sua rede doméstica 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 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
1	**Fundamentos sobre a Internet**	Conhecer fundamentos sobre a estrutura internet e seu funcionamento	Estrutura da Internet. Os serviços que a companhia de "Internet Service Provider" nos proporciona	Método expositivo online	Apoios pedagógicos multimédia disponibilizados online
2	**Ataques e Vulnerabilidades**	Conhecer os tipos de ataques e vulnerabilidades dos sistemas	- Tipos de ataques - Tipos de Hackers - Consequências e riscos dos ataques	Método expositivo online	Apoios pedagógicos multimédia disponibilizados online
3	**Utilização Segura da Internet**	Incutir uma utilização de internet de forma cibersegura. Selecionar os ficheiros e mails a abrir de forma consciente de modo a não comprometer a segurança do computador e da rede doméstica.	- Proteção de pessoas e dados - Tipos de Hackers - Utilização consciente da internet - Consequências e riscos dos ataques decorrentes duma utilização indevida e inconsciente da internet e redes sociais	Método expositivo online	Apoios pedagógicos multimédia disponibilizados online
4	**Configuração de Sistemas Domésticos**	Configurar os sistemas domésticos de acesso à internet em casa de modo a tornar a rede cibersegura	Gestão do Router doméstico e bloqueio de portas que podem comprometer a segurança da rede.	Sessão prática presencial em laboratório	Manuais de equipamentos, routers, switches, cabos, PCs para realizar a configuração.
Carga horária Total: 20 H					