

Ferramentas de avaliação

Licenciado por Creative Commons Attribution 4.0 International. Para ver uma cópia desta licença, visite <https://creativecommons.org/licenses/by/4.0/>



ÍNDICE

INTRODUÇÃO.....	4
UNIDADE 1. MELHORAR A LITERACIA NAS REDES SOCIAIS E O PENSAMENTO CRÍTICO	5
1.1 DESAFIO DE VERIFICAÇÃO DE FACTOS - DETETAR A DESINFORMAÇÃO"	6
LISTA DE CONTROLO DE AUTOAVALIAÇÃO	6
FEEDBACK DO DEBATE EM GRUPO.....	7
TESTE DE ESCOLHA MÚLTIPLA SOBRE INDICADORES DE DESINFORMAÇÃO.....	8
1.2 ANÁLISE DO CONTEÚDO DAS REDES SOCIAIS - CONTEÚDO DIGITAL SEGURO VERSUS PREJUDICIAL ..	10
AVALIAÇÃO POR LISTA DE VERIFICAÇÃO – ANÁLISE DA ADEQUAÇÃO DO CONTEÚDO	10
DEBATE BASEADO EM CENÁRIOS – ANÁLISE DE CASOS REAIS.....	11
REFLEXÃO ESCRITA – PRINCIPAIS LIÇÕES SOBRE LITERACIA DIGITAL NAS REDES SOCIAIS	12
UNIDADE 2. FUNDAMENTOS DA CIBERSEGURANÇA E MEDIDAS DE SEGURANÇA NA INTERNET	13
2.1 WORKSHOP SOBRE OS PRINCÍPIOS BÁSICOS DA CIBERSEGURANÇA PARA EDUCADORES DE ADULTOS	14
TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA	14
FICHA DE REFLEXÃO SOBRE CIBERSEGURANÇA	15
INQUÉRITO SOBRE O FEEDBACK E A CONFIANÇA NO WORKSHOP.....	16
TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA	17
2.2 WORKSHOP SOBRE CIBERSEGURANÇA	18
TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA	18
TESTE DE APLICAÇÃO DA CIBERSEGURANÇA	19
QUESTIONÁRIO SOBRE CIBERAMEAÇAS	20
2.3 WORKSHOP DE IDENTIFICAÇÃO E PREVENÇÃO DE CIBERAMEAÇAS.....	21
FICHA DE TRABALHO SOBRE CIBERAMEAÇAS.....	21
INQUÉRITO DE FEEDBACK DO WORKSHOP	22
UNIDADE 3. COMPREENDER OS AMBIENTES ONLINE DE MENORES	23
3.1 NAVEGAR NO MUNDO DIGITAL – COMO AS REDES SOCIAIS MOLDAM AS NOSSAS VIDAS	24
QUESTIONÁRIO PÓS-ATIVIDADE	24
3.2 MANTER-SE RESILIENTE ONLINE: LIDAR COM O CYBERBULLYING E O ASSÉDIO	26
QUESTIONÁRIO PÓS-ATIVIDADE	26

3.3 SEGURANÇA ONLINE PARA MENORES: UTILIZAÇÃO INTELIGENTE E SEGURA DA INTERNET	28
QUESTIONÁRIO PÓS-ATIVIDADE	28
UNIDADE 4. NAVEGAR NAS DEFINIÇÕES DE PRIVACIDADE E SEGURANÇA	30
4.1 WORKSHOP DE SENSIBILIZAÇÃO PARA A PRIVACIDADE DESTINADO ÀS FAMÍLIAS	31
TESTE DE SENSIBILIZAÇÃO PARA A PRIVACIDADE	31
INQUÉRITO SOBRE O <i>FEEDBACK</i> E A CONFIANÇA DO <i>WORKSHOP</i>	32
4.2 ANÁLISE DA PEGADA DIGITAL	34
PERGUNTAS DE REFLEXÃO	34
FICHA DE AUTOAVALIAÇÃO	35
4.3 <i>ROLE-PLAY</i> SOBRE DEFINIÇÕES DE PRIVACIDADE	36
FICHA DE ANÁLISE DE CENÁRIOS	36
FORMULÁRIO DE <i>FEEDBACK</i> DA DRAMATIZAÇÃO	37
UNIDADE 5. NETIQUETA: PROMOVER A PARTICIPAÇÃO NA SOCIEDADE E A CAPACITAÇÃO	38
5.1 ANALISAR AS INTERAÇÕES ONLINE	39
ANÁLISE DE CENÁRIOS	39
5.2 CRIAR UM GUIA DE NETIQUETA PARA AS FAMÍLIAS	41
QUESTIONÁRIO DE AUTORREFLEXÃO	41
UNIDADE 6. MEDIAÇÃO PARENTAL PARA UMA ABORDAGEM REFLEXIVA	43

INTRODUÇÃO

O *IPAD Currículo de formação*, complementa a **Plataforma de aprendizagem e recursos formativos**, disponibilizando um conjunto abrangente de recursos de avaliação alinhados com cada uma das atividades de formação das seis unidades do curso IPAD *b-Learning*. Desenvolvidas no âmbito do Projeto Erasmus+ IPAD (*Innovative Digital Awareness Resources for Parents on Social Media Literacy and Internet Safety*), estas ferramentas foram especificamente concebidas para **educadores de adultos que trabalham com famílias**, com o objetivo de apoiar e melhorar os processos de aprendizagem em torno da literacia digital, da utilização crítica das redes sociais e da segurança na Internet.

Cada **ferramenta de avaliação** corresponde a uma atividade prática específica incluída no *IPAD Currículo de formação*. Estas ferramentas destinam-se a ajudar os educadores a **avaliar os progressos de aprendizagem dos participantes** e a **adaptar o processo de formação** de acordo com as necessidades dos formandos. Estão estruturadas para avaliar uma vasta gama de competências e de resultados de conhecimentos definidos em cada Unidade de Aprendizagem, tais como o pensamento crítico, a sensibilização para a cibersegurança, a gestão de riscos online para menores, a privacidade e a identidade digital, a comunicação online respeitadora e a mediação parental eficaz.

As ferramentas encontram-se classificadas em **dois tipos principais de estratégias de avaliação**:

- **ferramentas de avaliação quantitativa**: incluem questionários de escolha múltipla, afirmações de verdadeiro/falso, exercícios de correspondência e listas de verificação, concebidos para medir a compreensão factual e a aquisição de competências digitais;
- **ferramentas de avaliação qualitativa**: envolvem questões de reflexão, guias de observação, debates em grupo, demonstrações práticas e trabalhos escritos, que permitem aos educadores explorar uma compreensão mais profunda, mudanças de comportamento e desenvolvimento de atitudes.

Como utilizar este documento

Os educadores podem utilizar as ferramentas de avaliação **antes, durante ou depois de cada atividade** como instrumentos de diagnóstico, formativos ou sumativos. Podem ser utilizadas em **contextos de aprendizagem formais ou informais** e são adaptáveis tanto a **modelos online como presenciais**. Estas ferramentas não só ajudam a acompanhar o progresso dos formandos, como também permitem aos educadores personalizar o ensino, identificar lacunas de aprendizagem e reforçar os principais resultados de aprendizagem. Cada ferramenta foi concebida para ser **prática, fácil de implementar e flexível** e pode ser utilizada:

- tal como é apresentada, visando acompanhar a respetiva atividade
- de forma independente, possibilitando apoiar outras intervenções de formação
- como parte de uma estratégia de avaliação mais alargada no âmbito de uma sessão ou curso de formação completo.

Utilizado em combinação com o **IPAD Atividades Práticas**, este recurso permite que os educadores de adultos disponibilizem uma formação mais eficaz e baseada em evidências. Apoia a promoção de **um comportamento digital seguro, crítico e responsável entre as famílias**, especialmente pais e encarregados de educação, assegurando que a aprendizagem é mensurável, adaptável e alinhada com os desafios digitais.



UNIDADE 1.

MELHORAR A LITERACIA NAS REDES SOCIAIS
E O PENSAMENTO CRÍTICO



1.1 Desafio de verificação de factos - detetar a desinformação

LISTA DE CONTROLO DE AUTOAVALIAÇÃO

📌 **Instruções:** Os participantes avaliam a sua capacidade de identificar notícias falsas, marcando cada afirmação com √ (Sim), X (Não) ou ? (Talvez), de acordo com o seu nível de confiança.

Afirmativas	Sim	X	?
Consigo identificar fontes fiáveis de notícias e informação	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verifico as credenciais e a experiência do autor antes de confiar num artigo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Consigo identificar títulos sensacionalistas ou enganadores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Verifico notícias utilizando websites de verificação de factos (por exemplo, Snopes, FactCheck.org)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reconheço <i>clickbait</i> e teorias da conspiração em conteúdos online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Questiono a autenticidade de imagens e vídeos antes de os partilhar	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Comparo notícias em várias fontes antes de acreditar nelas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sei utilizar a Pesquisa Reversa de Imagens do Google para verificar fotografias	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Reconheço falácias lógicas e viés em artigos online	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Sinto-me confiante para ensinar outras pessoas a detetar desinformação	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

▪ Questões para reflexão:

1. Em que áreas se sente mais confiante?
2. Quais as competências que necessita de melhorar na avaliação de conteúdos online?
3. Que passos irá tomar para reforçar as suas competências de verificação de factos?

1.1 Desafio de verificação de factos - detetar a desinformação

FEEDBACK DO DEBATE EM GRUPO

📌 **Instruções:** Durante a sessão de reflexão, os facilitadores e colegas fornecem *feedback* sobre a capacidade de raciocínio e argumentação do participante na avaliação de notícias falsas.

Critérios	Excelente (5)	Bom (4)	Mediano (3)	Precisa de melhorias (2)	Fraco (1)
Uso de Evidências: Utilizou evidências sólidas para fundamentar afirmações e verificações de factos	<input type="checkbox"/>				
Verificação de Fontes: Verificou eficazmente múltiplas fontes e utilizou ferramentas de verificação de factos	<input type="checkbox"/>				
Raciocínio Lógico: Apresentou argumentos lógicos na análise das notícias	<input type="checkbox"/>				
Deteção de Viés: Identificou possíveis vieses ou elementos enganadores no artigo	<input type="checkbox"/>				
Colaboração em Equipa: Trabalhou de forma eficaz com o grupo na avaliação da credibilidade das notícias	<input type="checkbox"/>				
Competências de Apresentação: Explicou claramente as conclusões e os resultados aos outros	<input type="checkbox"/>				

▣ Tópicos para Debate

1. Quais foram os maiores desafios na verificação de factos nos artigos de notícias?
2. Como é que diferentes grupos chegaram a conclusões distintas sobre as mesmas histórias?
3. Que estratégias utilizará no futuro para evitar a disseminação de desinformação?

1.1 Desafio de verificação de factos - detetar a desinformação

TESTE DE ESCOLHA MÚLTIPLA SOBRE INDICADORES DE DESINFORMAÇÃO

📌 **Instruções:** Selecione a melhor resposta para cada pergunta.

1. Qual é um dos principais sinais de que um artigo de notícias pode ser falso?

- A) É publicado num website governamental
- B) Utiliza linguagem exagerada ou emocional
- C) Tem várias citações de fontes fiáveis
- D) Foi escrito por um jornalista premiado

Resposta: B) Utiliza linguagem exagerada ou emocional

2. Qual é a melhor forma de verificar se uma imagem num artigo é real?

- A) Assumir que é real se parecer profissional
- B) Verificar a fonte, mas não confirmar mais nada
- C) Utilizar a Pesquisa Inversa de Imagens do Google para encontrar a sua origem
- D) Analisar o número de partilhas nas redes sociais

Resposta: C) Utilizar a Pesquisa Inversa de Imagens do Google para encontrar a sua origem

3. Qual dos seguintes é um sinal de alerta para notícias falsas

- A) O artigo é publicado por um meio de comunicação social conhecido e reputado
- B) A história cita fontes anónimas sem apresentar provas
- C) O relatório inclui várias opiniões de especialistas e pesquisas
- D) O website tem uma política editorial claramente definida

Resposta: B) A história cita fontes anónimas sem apresentar provas

4. Por que motivo é importante verificar a informação em várias fontes?

- A) Para garantir que o artigo tem mais alcance nas redes sociais
- B) Para confirmar que a notícia não é enganadora ou tendenciosa
- C) Porque todos os websites de notícias publicam exatamente as mesmas histórias
- D) Para poder partilhá-la rapidamente antes de a verificar

Resposta: B) Para confirmar que a notícia não é enganadora ou tendenciosa

5. Qual das seguintes fontes tem maior probabilidade de ser credível?

- A) Um website com um autor desconhecido e sem data de publicação
- B) Um website de verificação de factos conhecido, como o Snopes ou o FactCheck.org
- C) Uma publicação viral nas redes sociais sem fonte verificável
- D) Um blogue pessoal que faz afirmações chocantes sem referências

Resposta: B) Um website de verificação de factos conhecido, como o Snopes ou o FactCheck.org

➡ Pontuação:

- 5/5 corretas → 🏆 Especialista em Desinformação (Pode ensinar os outros!)
- 3-4 corretas → ✅ Profissional em Verificação de Factos (Boas competências, mas deve continuar a praticar!)
- 1-2 corretas → ⚠️ Necessita de Melhorar (Deve trabalhar na identificação de notícias falsas.)
- 0 corretas → ✗ Alerta! Risco de Desinformação! (Precisa de praticar mais a verificação de factos.)

1.2 Análise do conteúdo das redes sociais - conteúdo digital seguro *versus* prejudicial

AVALIAÇÃO POR LISTA DE VERIFICAÇÃO – ANÁLISE DA ADEQUAÇÃO DO CONTEÚDO

💡 **Instruções:** Os participantes analisam conteúdos digitais e avaliam a sua adequação etária, fiabilidade e impacte emocional utilizando a lista de verificação abaixo.

Título do conteúdo: _____

Fonte (Plataforma, Website ou Criador) _____

Critérios de Avaliação	Sim	Não	Notas/Justificação
Adequação Etária			
O conteúdo é adequado para crianças e não contém linguagem ou imagens inapropriadas	<input type="checkbox"/>	<input type="checkbox"/>	
A informação está alinhada com padrões educativos e apropriados para crianças	<input type="checkbox"/>	<input type="checkbox"/>	
Não há estereótipos prejudiciais, violência ou temas explícitos	<input type="checkbox"/>	<input type="checkbox"/>	
Fiabilidade das Fontes			
O conteúdo provém de uma fonte credível e baseada em factos	<input type="checkbox"/>	<input type="checkbox"/>	
Apresenta <i>links</i> para fontes verificadas ou referências	<input type="checkbox"/>	<input type="checkbox"/>	
O autor/criador é conhecido e tem experiência relevante	<input type="checkbox"/>	<input type="checkbox"/>	
A informação pode ser confirmada através de outras fontes fiáveis	<input type="checkbox"/>	<input type="checkbox"/>	
Impacte Emocional e Intenção			
O conteúdo não utiliza linguagem manipuladora ou emocionalmente carregada	<input type="checkbox"/>	<input type="checkbox"/>	
Apresenta a informação de forma objetiva, sem disseminar medo ou teorias da conspiração	<input type="checkbox"/>	<input type="checkbox"/>	
O propósito é educar e não enganar, manipular ou vender um produto de forma antiética	<input type="checkbox"/>	<input type="checkbox"/>	

✓ Veredicto Final

- Seguro e Educativo (Adequado, fiável e informativo)
- Questionável e Requer Cautela (Algum viés, possível desinformação)
- Potencialmente Nocivo (Manipulador, enganador, inapropriado)
- Claramente Perigoso e Enganador (Difunde informações falsas ou prejudiciais)

1.2 Análise do conteúdo das redes sociais - conteúdo digital seguro *versus* prejudicial

DEBATE BASEADO EM CENÁRIOS – ANÁLISE DE CASOS REAIS

👉 **Instruções:** Os participantes debatem exemplos reais de conteúdos enganosos, utilizando o pensamento crítico para avaliar o impacto na literacia digital.

Cenário 1: Publicidade de Influenciadores para Crianças

Um influenciador das redes sociais publica um vídeo intitulado "*Este Suplemento Mágico Tornará o seu Filho Mais Inteligente!*", direcionado a crianças. O vídeo inclui testemunhos dramáticos, não tem qualquer fundamento científico e contém um *link* de afiliado para compras.

Perguntas para reflexão:

1. De que forma este conteúdo manipula emoções para influenciar os mais jovens?
2. Que táticas publicitárias são utilizadas para tornar o produto mais credível?
3. Este tipo de conteúdo deve ser sinalizado como enganador? Porquê?

Cenário 2: Desinformação Viral sobre uma Crise de Saúde

Uma publicação amplamente partilhada afirma que "*Beber água quente previne a COVID-19*", citando um "médico de um laboratório secreto do governo". A publicação não apresenta fontes científicas, mas já tem milhares de partilhas.

Perguntas para reflexão:

1. Como posso verificar se esta afirmação é verdadeira ou falsa?
2. Que danos pode causar a disseminação de desinformação sobre saúde?
3. Que medidas devem os utilizadores responsáveis tomar antes de partilhar publicações deste tipo?

Cenário 3: Vídeo Deepfake de uma Figura Pública

Um vídeo viral mostra um líder mundial a fazer declarações controversas. Mais tarde, descobre-se que foi gerado através de tecnologia de *deepfake* para manipular a sua imagem.

Perguntas para reflexão:

1. Como posso detetar um vídeo *deepfake*?
2. Que impacte pode ter a manipulação de conteúdos multimédia na confiança pública e na democracia?
3. Que ferramentas podem ser utilizadas para verificar a autenticidade de vídeos antes de acreditar neles?

1.2 Análise do conteúdo das redes sociais - conteúdo digital seguro *versus* prejudicial

REFLEXÃO ESCRITA – PRINCIPAIS LIÇÕES SOBRE LITERACIA DIGITAL NAS REDES SOCIAIS

✍ **Instruções:** Os participantes escrevem uma reflexão curta (150-200 palavras) resumindo os conhecimentos adquiridos com a atividade.

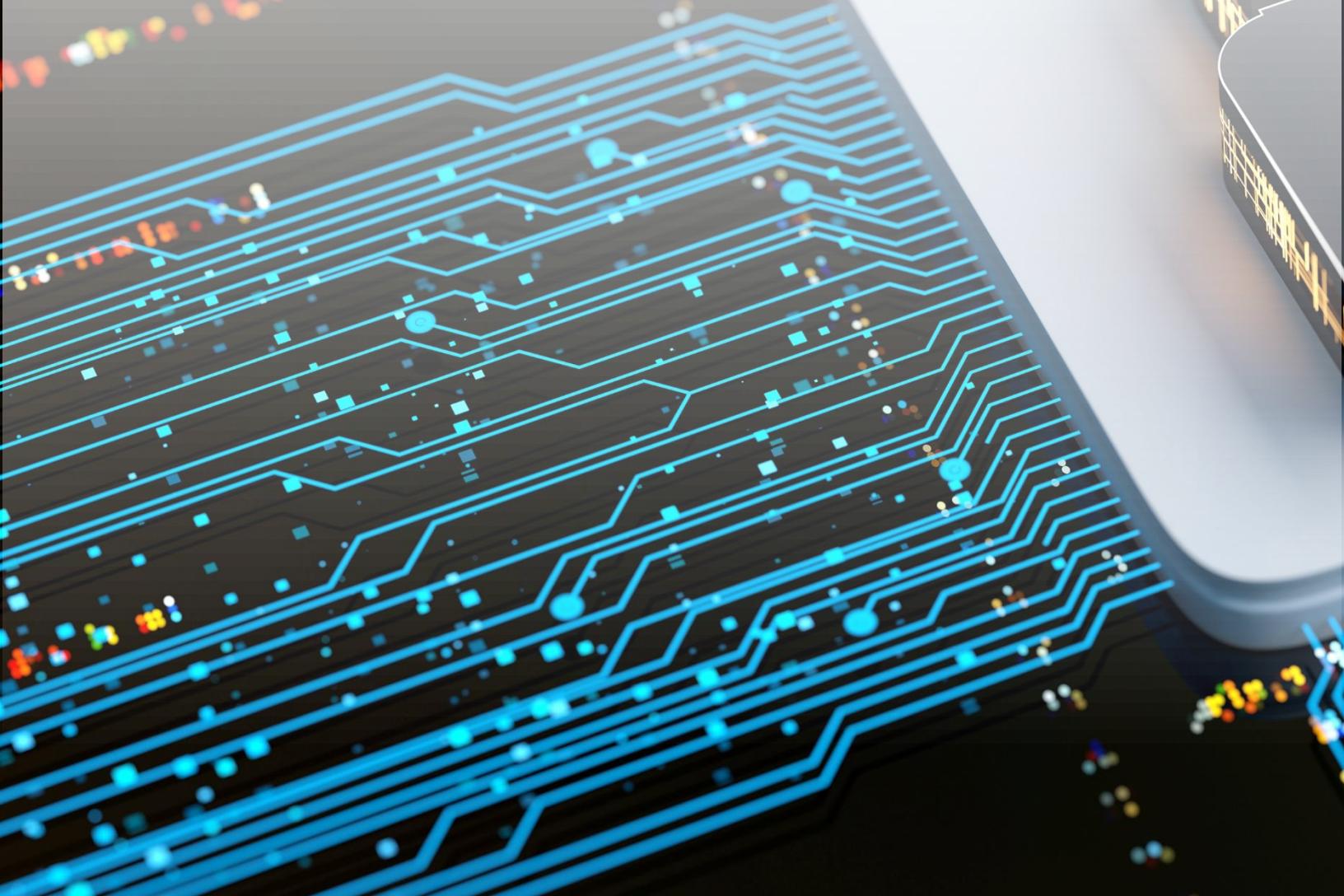
Perguntas para reflexão:

1. Quais são os aspetos mais importantes que aprendeu sobre a avaliação de conteúdos nas redes sociais?
2. Como aplicará estratégias de verificação de factos no seu dia a dia digital?
3. Que conselhos daria a pais e formadores para orientar os menores no uso das redes sociais?
4. Como pode contribuir para combater a desinformação na sua comunidade?



UNIDADE 2.

FUNDAMENTOS DA CIBERSEGURANÇA E MEDIDAS DE SEGURANÇA NA INTERNET



2.1 Workshop sobre os princípios básicos da cibersegurança para educadores de adultos

TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA

Objetivo: Avaliar os conhecimentos dos participantes sobre as noções básicas de cibersegurança.

1. **Verdadeiro ou falso:** Utilizar a mesma palavra-passe em várias contas é uma prática segura.

Resposta: Falso

2. **Escolha múltipla:** Qual das seguintes opções ajuda a evitar o acesso não autorizado a contas online?

A) Utilizar uma palavra-passe simples para facilitar a memorização

B) Ativar a autenticação de dois fatores

C) Partilhar a sua palavra-passe com amigos de confiança

Resposta: B) Ativar a autenticação de dois fatores

3. **Escolha única:** Qual das seguintes opções é um sinal de um e-mail de *phishing*?

A) Solicita informações pessoais com urgência

B) É de uma fonte oficial que não reconhece

C) Tem ligações ou anexos suspeitos

D) Todas as opções anteriores

Resposta: D) Todas as opções anteriores

2.1 Workshop sobre os princípios básicos da cibersegurança para educadores de adultos

FICHA DE REFLEXÃO SOBRE CIBERSEGURANÇA

Objetivo: Incentivar os participantes a refletir sobre o que aprenderam e a planejar como aplicar esse conhecimento.

1. **Identifique dois tipos de ciberameaças** que foram discutidos no workshop.
 - *(Exemplo: Phishing, malware, ransomware, etc.)*
2. **Descreva uma medida de segurança** que aplicou hoje e explique por que razão é essencial.
 - *(Exemplo: Atualizei as palavras-passe para torná-las mais fortes, evitando o acesso não autorizado.)*
3. **Enumere um novo hábito** que tenciona implementar para melhorar a cibersegurança para si e para a sua família.
 - *(Exemplo: Vou ativar a autenticação de dois fatores em todas as contas importantes.)*
4. **Nível de confiança:** Avalie a sua confiança em orientar outras pessoas sobre cibersegurança básica antes e depois do workshop:
 - Antes: Excelente | Bom | Razoável | Precisa de ser melhorado
 - Depois: Excelente | Bom | Razoável | Precisa de ser melhorado

2.1 *Workshop* sobre os princípios básicos da cibersegurança para educadores de adultos

INQUÉRITO SOBRE O *FEEDBACK* E A CONFIANÇA NO *WORKSHOP*

Objetivo: Medir a confiança e a satisfação dos participantes em relação ao workshop.

1. Até que ponto se sente confiante para identificar e gerir as ciberameaças depois do seminário?
 - Muito confiante, Um pouco confiante, Neutro, Não muito confiante, Nada confiante*
2. Em que medida as informações fornecidas neste seminário foram relevantes para as suas necessidades?
 - Muito relevante, Algo relevante, Neutro, Não muito relevante, Nada relevante*
3. Qual foi o conceito mais útil abordado no *workshop*?
 - Resposta aberta*
4. Recomendaria este seminário a outros formadores de adultos? Porquê?
 - Resposta aberta*

2.1 Workshop sobre os princípios básicos da cibersegurança para educadores de adultos

TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA

Objetivo: Avaliar a compreensão dos participantes sobre os conceitos e as melhores práticas de cibersegurança.

1. **Verdadeiro ou falso:** A autenticação de dois fatores fornece uma camada extra de segurança.

Resposta: Verdadeiro

2. **Escolha múltipla:** Quais dos seguintes são sinais de um e-mail de *phishing*?

- A) Saudações genéricas
- B) Hiperligações suspeitas
- C) Pedidos urgentes de dados pessoais
- D) Todas as opções anteriores

Resposta: D) Todas as opções anteriores

3. **Escolha única:** O que deve fazer se suspeitar de um e-mail de *phishing*?

- A) Clicar na hiperligação para verificar o seu conteúdo
- B) Eliminar a mensagem sem comunicar
- C) Comunicar ao seu fornecedor de email

Resposta: C) Comunicar ao seu fornecedor de serviços de email

2.2 Workshop sobre cibersegurança

TESTE DE CONHECIMENTOS SOBRE CIBERSEGURANÇA

Objetivo: Avaliar a compreensão dos participantes sobre as medidas práticas de cibersegurança.

1. **Verdadeiro ou falso:** A ativação da autenticação de dois fatores ajuda a proteger as suas contas online.

Resposta: Verdadeiro

2. **Escolha múltipla:** O que deve fazer para melhorar a privacidade da sua conta nas redes sociais?

- A) Partilhar todas as suas mensagens publicamente
- B) Ajustar as definições de privacidade para limitar quem pode ver o seu conteúdo
- C) Desativar todas as notificações

Resposta: B) Ajustar as definições de privacidade para limitar quem pode ver o seu conteúdo

3. **Verdadeiro ou falso:** Não é necessário verificar as permissões da aplicação após a instalação.

Resposta: Falso

4. **Escolha única:** Qual é um exemplo de boas práticas de cibersegurança?

- A) Utilizar a mesma palavra-passe para todas as suas contas
- B) Atualizar regularmente o seu software e aplicações
- C) Clicar em hiperligações de fontes desconhecidas

Resposta: B) Atualizar regularmente o software e as aplicações

2.2 Workshop sobre cibersegurança

TESTE DE APLICAÇÃO DA CIBERSEGURANÇA

Objetivo: Incentivar os participantes a refletir sobre o que aprenderam e a planejar como aplicar esse conhecimento.

1. Identifique duas práticas de cibersegurança que aprendeu durante o workshop e que tenciona utilizar na sua vida pessoal ou profissional.

(Exemplo: Ativar a autenticação de dois fatores e usar um gestor de palavras-passe.)

2. Descreva uma medida de segurança que aplicou hoje e explique por que razão é essencial.

(Exemplo: Atualizei as definições de privacidade nas redes sociais para limitar o acesso ao meu conteúdo, o que ajuda a proteger os meus dados pessoais.)

3. Enumere um novo hábito que tenciona implementar para melhorar a cibersegurança para si e para a sua família.

(Exemplo: Verificar regularmente as permissões das aplicações instaladas e eliminar aquelas que já não utilizamos.)

4. **Nível de confiança:** Avalie a sua confiança em orientar outras pessoas em matéria de cibersegurança antes e depois do workshop:

- Antes: Excelente, Bom, Razoável, Precisa de ser melhorado
- Depois: Excelente, Bom, Razoável, Precisa de ser melhorado

2.2 Workshop sobre cibersegurança

QUESTIONÁRIO SOBRE CIBERAMEAÇAS

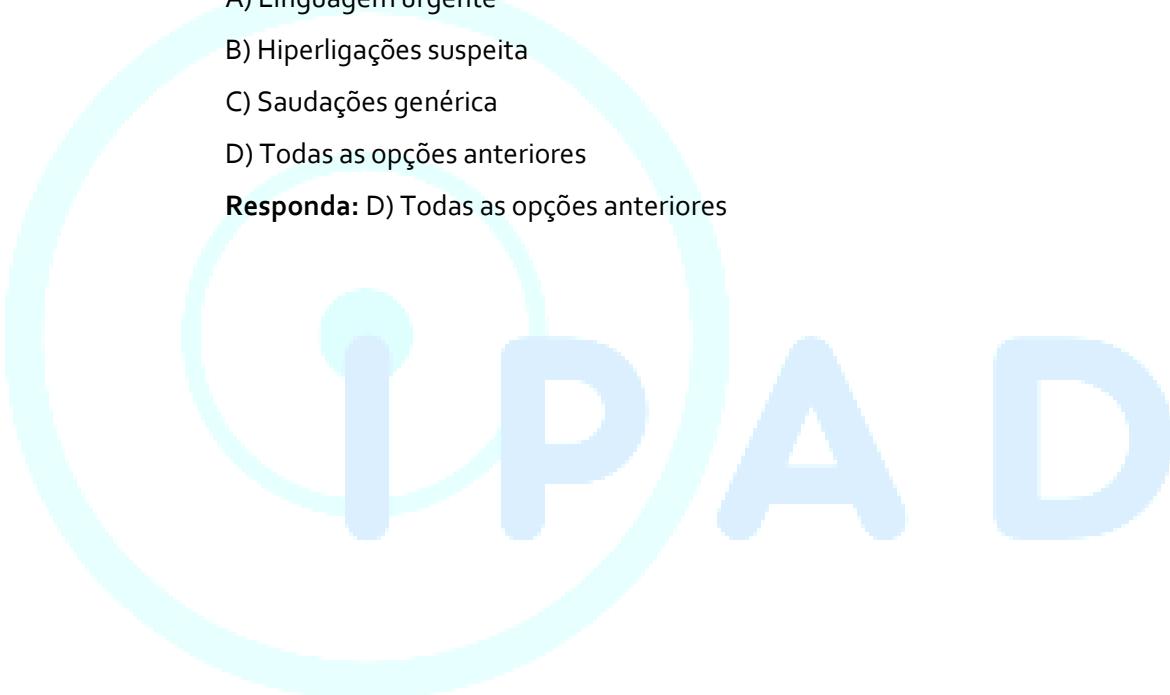
Objetivo: Avaliar a capacidade dos participantes para reconhecer e responder a ciberameaças.

- 1. Verdadeiro ou falso:** Um e-mail legítimo do seu banco pedirá sempre a sua palavra-passe.
Responda: Falso

- 2. Escolha múltipla:** Qual das seguintes opções é um sinal de um e-mail de *phishing*?

- A) Linguagem urgente
- B) Hipergigações suspeita
- C) Saudações genérica
- D) Todas as opções anteriores

Responda: D) Todas as opções anteriores



2.3 Workshop de identificação e prevenção de ciberameaças

FICHA DE TRABALHO SOBRE CIBERAMEAÇAS

Objetivo: Avaliar a capacidade dos participantes para identificar ameaças e propor estratégias de prevenção.

1. Descreva a ameaça cibernética que analisou e os principais indicadores que identificou.
2. Enumere as medidas que tomaria para evitar ser vítima desta ameaça.



2.3 Workshop de identificação e prevenção de ciberameaças

INQUÉRITO DE FEEDBACK DO WORKSHOP

Objetivo: Medir a confiança e a satisfação dos participantes com a atividade.

1. Qual é o seu grau de confiança na identificação de ciberameaças depois desta sessão

- A) Muito confiante
- B) Um pouco confiante
- C) Neutro
- D) Não muito confiante
- E) Nada confiante

2. Qual foi a parte mais útil desta atividade?

(Resposta aberta)



UNIDADE 3.

COMPREENDER OS AMBIENTES ONLINE DE MENORES



3.1 Navegar no mundo digital – como as redes sociais moldam as nossas vidas

QUESTIONÁRIO PÓS-ATIVIDADE

Pew Research Center?

- A) Instagram
- B) Snapchat
- C) Facebook
- D) Twitter

Qual a percentagem de adolescentes que utilizam o YouTube, de acordo com o Pew Research Center?

- A) 75%
- B) 85%
- C) 93%
- D) 98%

Quais das seguintes plataformas dominam atualmente o uso das redes sociais entre menores? (Selecione todas as opções corretas)

- A) TikTok
- B) LinkedIn
- C) Snapchat
- D) Instagram

Verdadeiro ou Falso: A higiene digital envolve práticas que ajudam a manter os dados sensíveis seguros e protegidos contra-ataques cibernéticos.

- A) Verdadeiro
- B) Falso

Qual o termo utilizado para descrever o folclore digital transmitido através da internet?

- A) Meme
- B) Netlore
- C) Conteúdo viral
- D) Digimoto

Respostas

- C) Facebook
- C) 93%
- A) TikTok, C) Snapchat, D) Instagram
- A) Verdadeiro
- B) Netlore



3.2 Manter-se resiliente online - lidar com o *cyberbullying* e o assédio

QUESTIONÁRIO PÓS-ATIVIDADE

Quais dos seguintes são potenciais riscos do mundo digital para menores? (Selecione todas as opções corretas)

- A) Vantagens económicas e profissionais
- B) *Cyberbullying* e assédio
- C) Oportunidades de aprendizagem e crescimento
- D) Exposição a conteúdos inadequados

Verdadeiro ou Falso: O termo “fosso geracional” refere-se às diferenças de opiniões, valores, entre outros, entre pessoas mais jovens e mais velhas

- A) Verdadeiro
- B) Falso

Quais são as principais estratégias para intervir em casos de *cyberbullying*? (Selecione todas as opções corretas)

- A) Garantir a segurança do menor
- B) Ignorar o problema
- C) Documentar e reportar o abuso
- D) Repreender a vítima sobre como deveria ter respondido

Qual o primeiro passo para responder ao *cyberbullying*?

- A) Denunciar o agressor à polícia
- B) Garantir a segurança do menor
- C) Bloquear imediatamente o agressor
- D) Repreender o menor sobre o seu comportamento online

Verdadeiro ou Falso: A empatia não é necessária ao discutir *cyberbullying*

- A) Verdadeiro
- B) Falso

Respostas

- B) *Cyberbullying* e assédio, d) Exposição a conteúdos inadequados
- A) Verdadeiro
- A) Garantir a segurança do menor, c) Documentar e reportar o abuso
- B) Garantir a segurança do menor
- B) Falso



3.3 Segurança online para menores - utilização inteligente e segura da Internet

QUESTIONÁRIO PÓS-ATIVIDADE

Que termo descreve o método pelo qual a informação é convertida num código secreto para ocultar o seu significado real?

- A) Ocultação de dados
- B) Esteganografia
- C) Encriptação
- D) Desencriptação

O que são *cookies* no contexto da internet?

- A) Um tipo de *malware*
- B) Pequenos ficheiros usados por servidores web para guardar informações de navegação
- C) Um tipo de encriptação
- D) Uma forma de *cyberbullying*

Quais das seguintes são boas práticas de higiene digital? (Selecione todas as opções corretas)

- A) Utilizar palavras-passe fortes e únicas
- B) Atualizar regularmente o software
- C) Partilhar palavras-passe com amigos
- D) Ativar a autenticação de dois fatores

Verdadeiro ou Falso: Os emails de *phishing* são sempre fáceis de identificar porque contêm erros ortográficos óbvios

- A) Verdadeiro
- B) Falso

Qual das seguintes é um exemplo de uma palavra-passe forte?

- A) 123456
- B) Password123
- C) T!ger\$RunF@st2024
- D) O seu nome seguido do seu ano de nascimento

Respostas

- C) Encriptação
- B) Pequenos ficheiros usados por servidores web para guardar informações de navegação
- A) Utilizar palavras-passe fortes e únicas, b) Atualizar regularmente o software, d) Ativar a autenticação de dois fatores
- B) Falso
- C) T!ger\$RunF@st2024





UNIDADE 4.

NAVEGAR NAS DEFINIÇÕES DE PRIVACIDADE
E SEGURANÇA



4.1 Workshop de sensibilização para a privacidade destinado às famílias

TESTE DE SENSIBILIZAÇÃO PARA A PRIVACIDADE

Este questionário pode ser utilizado no final do *workshop* para avaliar a compreensão dos participantes sobre os principais conceitos de privacidade e as melhores práticas.

1. **Verdadeiro ou falso:** A partilha de informações pessoais online acarreta sempre riscos, especialmente para os menores.

Resposta: Verdadeiro

2. **Escolha múltipla:** Qual das seguintes opções ****NÃO**** é uma ação recomendada para proteger a privacidade online?

- A) Utilizar palavras-passe fortes e únicas
- B) Partilhar regularmente atualizações sobre a sua localização
- C) Ativar a autenticação de dois fatores
- D) Limitar as informações pessoais partilhadas nas redes sociais

Resposta: B) Partilhar regularmente atualizações sobre a sua localização

3. **Verdadeiro ou falso:** É importante rever as definições de privacidade regularmente, uma vez que as plataformas de redes sociais atualizam frequentemente as suas definições e funcionalidades.

Resposta: Verdadeiro

4. **Escolha única:** Quais destas ações podem ajudar a proteger a privacidade online de um menor?

- A) Partilhar publicamente os resultados escolares
- B) Publicar as rotinas diárias nas redes sociais
- C) Limitar as mensagens com informações identificáveis
- D) Marcar os menores em fotografias públicas

Resposta: C) Limitar as mensagens com informações identificáveis

5. **Escolha múltipla:** Quais são as boas práticas para proteger uma pegada digital?

- A) Pensar bem antes de publicar
- B) Verificar as definições de privacidade nas plataformas
- C) Utilizar a mesma palavra-passe para todas as contas
- D) Rever regularmente as mensagens marcadas

Respostas: A), B), e D)

4.1 Workshop de sensibilização para a privacidade destinado às famílias

INQUÉRITO SOBRE O FEEDBACK E A CONFIANÇA DO WORKSHOP

Esta ficha de trabalho incentiva as famílias a refletir sobre o que aprenderam no workshop e como planeiam aplicá-lo nas suas atividades diárias online.

1. Enumere três riscos de privacidade associados à partilha de informações pessoais online
Resposta aberta
2. Que definições de privacidade ou hábitos online está mais interessado em alterar ou melhorar depois deste workshop?
Resposta aberta
3. Como é que vai abordar os debates sobre privacidade com os membros da sua família, especialmente com os menores?
Resposta aberta
4. Avalie o seu conhecimento atual da privacidade online dos membros da família (antes do workshop):
Excelente
Muito Bom
Bom
Precisa de ser melhorado
5. Avalie a sua compreensão atual da privacidade online para os membros da família (após o seminário):
Excelente
Muito Bom
Bom
Precisa de ser melhorado
6. Que medidas tenciona tomar para aumentar a consciência da privacidade na sua família?
Resposta aberta

4.1 Workshop de sensibilização para a privacidade destinado às famílias

INQUÉRITO SOBRE O *FEEDBACK* E A CONFIANÇA DO WORKSHOP

Este inquérito avalia a confiança dos participantes na aplicação de estratégias de privacidade e a sua satisfação geral com o conteúdo do *workshop*.

1. Até que ponto se sente confiante na sua capacidade de debater e gerir a privacidade online com a sua família?
 - Muito confiante
 - Relativamente confiante
 - Neutro
 - Não muito confiante
 - Nada confiante
2. As informações fornecidas durante o *workshop* foram relevantes para as necessidades da sua família?
 - Sim, muito relevante
 - Relativamente relevante
 - Neutro
 - Não muito relevante
 - Nada relevante
3. Avalie a eficácia do *workshop* para o ajudar a compreender os riscos da partilha excessiva online.
 - Excelente
 - Boa
 - Média
 - Reduzida
4. Que tópico ou conceito foi mais útil para si no *workshop*?
 - Resposta aberta
5. Recomendaria este *workshop* a outras pessoas que pretendam aprender sobre privacidade e segurança online para as suas famílias?
 - Sim
 - Não
 - Explique a sua escolha

4.2 Análise da pegada digital

PERGUNTAS DE REFLEXÃO

Depois de concluir a atividade, os participantes devem responder às seguintes perguntas de reflexão:

1. De que aspetos da sua pegada digital tinha conhecimento antes desta atividade?
 - Resposta aberta*

2. Houve alguma surpresa ou descoberta inesperada na análise da sua pegada digital?
 - Sim
 - Não
 - Em caso afirmativo, queira explicar:

3. De que forma é que o conhecimento da sua pegada digital afeta a forma como abordará as suas atividades online no futuro?
 - Resposta aberta*

4. Que ação específica irá tomar para gerir ou reduzir a sua pegada digital?
 - Resposta aberta*

5. Até que ponto se sente confortável para explicar o conceito de pegadas digitais a outras pessoas?
 - Muito confortável
 - Um pouco confortável
 - Nada confortável

4.2 Análise da pegada digital

FICHA DE AUTOAVALIAÇÃO

Os participantes podem utilizar esta lista de verificação para avaliar as suas práticas atuais em matéria de pegada digital. Instruções: Assinale cada afirmação que se aplica a si.

1. Revejo regularmente as minhas publicações online para garantir que correspondem à minha imagem digital desejada
2. Tenho conhecimento das definições de privacidade das minhas contas nas redes sociais e ajusto-as em conformidade
3. Tenho cuidado ao partilhar informações pessoais online
4. Elimino regularmente conteúdos antigos ou desatualizados que já não me representam
5. Estou ciente do meu perfil público nos motores de busca e monitorizo-o periodicamente

Interpretação da pontuação:

- **4-5 declarações verificadas:** É proativo na gestão da sua pegada digital
- **2-3 afirmações verificadas:** Tem alguma consciência, mas poderia beneficiar de mais atenção à gestão da pegada digital
- **0-1 afirmação verificada:** Considerar a possibilidade de tomar mais medidas para controlar e gerir a sua presença digital

4.3 Role-play sobre definições de privacidade

FICHA DE ANÁLISE DE CENÁRIOS

Os participantes preencherão a ficha de trabalho com as respostas com base no cenário de dramatização atribuído.

1. Qual foi a pessoa que lhe foi atribuída (por exemplo, pai, adolescente, profissional)?
 - *Persona:*

2. Descreva as definições de privacidade que escolheu para esta pessoa e por que razão são adequadas.
 - *Resposta aberta*

3. Que desafios ou preocupações encontrou ao selecionar as definições de privacidade para esta pessoa?
 - *Resposta aberta*

4. Quais são os riscos potenciais se esta pessoa não gerir bem as suas definições de privacidade?
 - *Resposta aberta*

5. Qual é o seu grau de confiança para orientar outras pessoas na configuração de definições de privacidade semelhantes?
 - Muito confiante
 - Um pouco confiante
 - Nada confiante

4.3 Role-play sobre definições de privacidade

FORMULÁRIO DE FEEDBACK DA DRAMATIZAÇÃO

Após a atividade, os participantes preenchem este formulário de *feedback* para refletir sobre a sua abordagem e os resultados da aprendizagem.

1. Considerou o exercício de dramatização útil para compreender a importância das definições de privacidade?
 - Sim
 - Não

2. Qual foi a informação mais valiosa que obteve ao configurar as definições de privacidade para a persona que lhe foi atribuída?
 - Resposta aberta*

3. Sentir-se-ia confortável para ajudar alguém a definir as definições de privacidade nas redes sociais? Porquê ou porque não?
 - Resposta aberta*

4. Classifique a relevância desta atividade para ajudar as famílias a navegar nas definições de privacidade:
 - Muito relevante
 - Moderadamente relevante
 - Nada relevante

5. Que apoio ou informações adicionais o ajudariam a sentir-se mais confiante para aconselhar as famílias sobre as definições de privacidade?
 - Resposta aberta*



UNIDADE 5.

NETIQUETA: PROMOVER A PARTICIPAÇÃO NA SOCIEDADE E A CAPACITAÇÃO



5.1 Analisar as interações online

ANÁLISE DE CENÁRIOS

Esta rubrica oferece uma estrutura organizada para avaliar a análise de cada grupo de cenários de interação online. Antes de iniciar a atividade, forneça exemplos claros e explique os critérios de forma detalhada. Use a rubrica como um guia para promover o debate e a recolha de *feedback*. Pode ajustar os critérios, adicionando ou removendo itens, conforme os objetivos de aprendizagem e os tipos de cenários trabalhados.

Rubrica de análise de cenários

Atividade: Analisar as interações online

Nome do grupo: _____

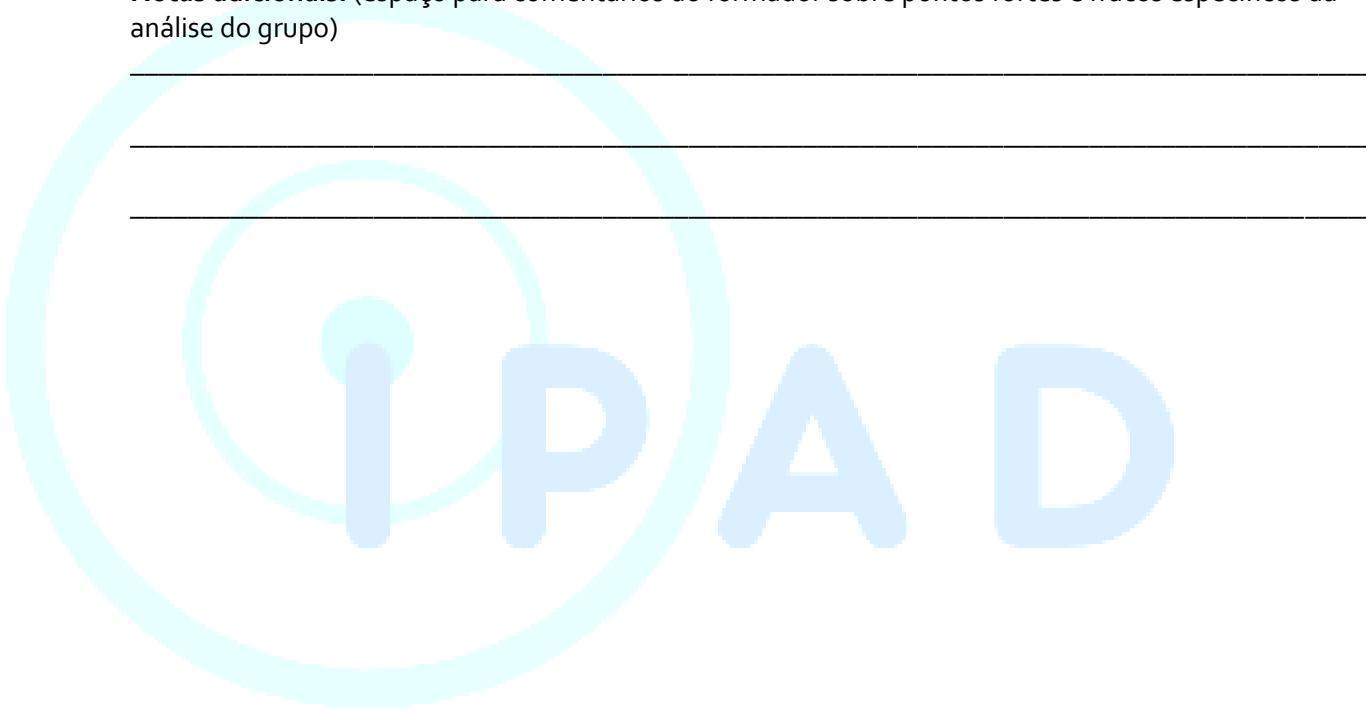
Número do cenário: _____

Critérios	Excelente (4 pontos)	Bom (3 pontos)	Razoável (2 pontos)	Fraco (1 ponto)
Identificação do tipo de comunicação	Identifica corretamente o tipo de comunicação online (e-mail, publicação em redes sociais, fórum, etc.).	Identifica corretamente o tipo de comunicação na maioria dos cenários.	Identifica o tipo de comunicação em alguns cenários, mas com imprecisões.	Não consegue identificar com precisão o tipo de comunicação na maioria dos cenários.
Identificação de violações da netiqueta	Identifica todas as violações da netiqueta com explicações claras e fundamentadas.	Identifica a maioria das violações da netiqueta com explicações adequadas.	Identifica algumas violações, mas as explicações são insuficientes ou pouco claras.	Não identifica a maioria das violações ou deixa de explicar adequadamente as identificadas.
Explicação dos princípios da netiqueta	Oferece explicações claras, precisas e detalhadas sobre os princípios de netiqueta violados.	Fornece explicações na maior parte das vezes corretas sobre os princípios violados.	Dá explicações incompletas ou com algumas imprecisões sobre os princípios relevantes.	Não apresenta explicações adequadas ou relevantes sobre os princípios violados.
Consequências das ações	Prevê com exatidão e detalhe as potenciais consequências negativas das ações descritas no cenário.	Prevê a maioria das consequências negativas de forma adequada.	Prevê algumas consequências, mas com análises incompletas ou imprecisas.	Não identifica ou analisa corretamente a maioria das consequências negativas.
Qualidade global da análise	A análise é completa, perspicaz, bem estruturada e apresentada de forma clara e organizada.	A análise é, em geral, completa e bem estruturada, apesar de pequenas incoerências.	A análise apresenta falta de profundidade ou organização em alguns aspectos.	A análise é superficial, desorganizada e pouco clara.

Pontuação:

- **16-20 pontos:** Excelente compreensão da netiqueta e da sua aplicação.
- **12-15 pontos:** Boa compreensão da netiqueta, com pequenas áreas a melhorar.
- **8-11 pontos:** Compreensão razoável da netiqueta; são necessárias áreas significativas para melhorar.
- **4-7 pontos:** Fraca compreensão da netiqueta; é necessária uma revisão substancial e um estudo mais aprofundado.

Notas adicionais: (espaço para comentários do formador sobre pontos fortes e fracos específicos da análise do grupo)



5.2 Criar um guia de netiqueta para as famílias

QUESTIONÁRIO DE AUTORREFLEXÃO

Este modelo de autorreflexão foi criado para ajudar os formandos a avaliar sua contribuição, aprendizagem, compreensão da netiqueta e sua relevância dentro do contexto familiar. Certifique-se de reservar tempo suficiente para que os participantes preencham o questionário com atenção. Considere torná-lo anônimo para promover respostas mais honestas e sinceras.

Autorreflexão: Criar um guia de netiqueta para as famílias

Nome: _____

Data: _____

Parte 1: A minha contribuição para a atividade

- Descreva o seu papel e as suas contribuições no seio do seu grupo. Quais foram as tarefas específicas que realizou? Como acredita que a sua participação ajudou no sucesso global da criação do guia?
- Quais foram os seus pontos fortes durante o trabalho de grupo? Reflita sobre as suas competências, como capacidade de investigação, redação, comunicação, organização, criatividade ou resolução de problemas.
- Em que domínios poderia ter melhorado a sua contribuição? Seja honesto e específico. Que pontos precisam de ajustes? Como poderia ter sido um membro mais eficaz da equipa?
- Reflita sobre a sua colaboração com os membros do grupo. O que funcionou bem no trabalho em equipa? Que desafios enfrentaram? Como lidaram com esses desafios para alcançar os objetivos do grupo?

Parte 2: A minha aprendizagem e compreensão

- Antes desta atividade, o que entendia por netiqueta? Como era a sua percepção sobre o conceito de netiqueta? De que forma essa compreensão se alterou ou aprofundou com o que aprendeu?
- Quais são os três aspetos mais importantes que aprendeu sobre netiqueta durante esta atividade? Liste e explique brevemente as três lições mais valiosas que adquiriu, destacando por que as considera fundamentais.
- Como vai aplicar o que aprendeu sobre netiqueta nas suas próprias interações online e na sua família? Forneça exemplos práticos de como pretende adotar as boas práticas de netiqueta nas suas interações online e no ambiente familiar.
- Qual é a importância de ter diretrizes claras de netiqueta nas famílias? Reflita sobre o papel das diretrizes em diferentes contextos online em que as famílias interagem (redes sociais, mensagens, grupos). Explique como acredita que a netiqueta pode fortalecer as relações familiares.
- Quais são as potenciais consequências da ausência de diretrizes claras em matéria de netiqueta nas famílias? Analise os impactes negativos que podem surgir quando não há regras ou orientações claras sobre comportamento online no seio familiar.

Parte 3: Reflexões gerais

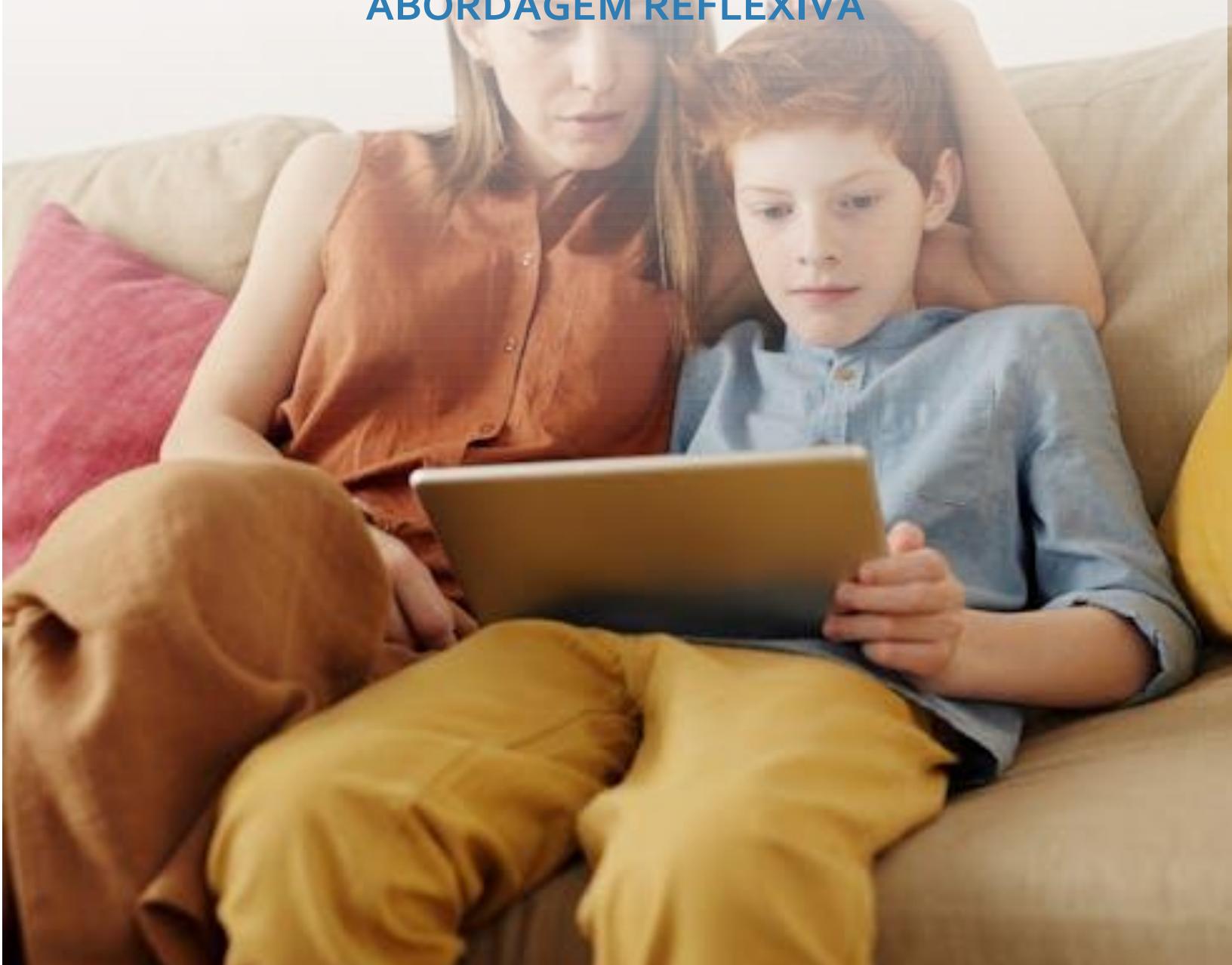
- Qual foi o aspetto mais valioso desta atividade para si?
- Quais foram os maiores desafios que enfrentou durante esta atividade? Como é que os ultrapassou?
- Que sugestões tem para melhorar esta atividade no futuro?





UNIDADE 6.

MEDIAÇÃO PARENTAL PARA UMA
ABORDAGEM REFLEXIVA





Parceria

