Nome: _____ Data: _____ Pontuação: _____

Como escolher uma VPN
Ficha de trabalho

Avaliação de fornecedores de VPN, normas de segurança, auditorias e políticas de registo

VISÃO GERAL DE APRENDIZAGEM SOBRE VPN

APRENDENTE
ESTATUTO DE ESTUDANTE
Percurso de defensor de redes

SEGURO
ESTADO DA LIGAÇÃO
Proteger pacotes de dados

ATIVO
PROTEÇÃO CONTRA FUGAS
Proteção contra fugas de DNS e IPv6

Bem-vindo! Este conjunto de atividades guia-te pelos princípios fundamentais das Redes Privadas Virtuais (VPN). Vais explorar como os túneis cifrados protegem os teus dados, como funcionam os protocolos de rede e como identificar e mitigar fugas de privacidade.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina os conceitos e protocolos de VPN.**
- [ ] **Partes 5-7: Resolve puzzles de palavras cruzadas e sopas de letras.**
- [ ] **Partes 8-9: Resolve estudos de caso e o desafio de cifra.**
- [ ] **Parte 10: Revê as páginas de perguntas frequentes básicas e avançadas.**
- [ ] **Parte 11: Explora 10 factos interessantes do mundo real.**
- [ ] **Bónus: desafio Pensa rápido.**

Abrir o Guia de VPN da VPN.com

URL: https://www.vpn.com/pt/vpn/

O teu roteiro de aprendizagem sobre VPN

- Avalia a jurisdição do fornecedor e as políticas de zero registos em matéria de privacidade.
- Compara protocolos de tunelização como o WireGuard e o OpenVPN em termos de velocidade.
- Analisa funcionalidades de segurança como os kill switches e os nós de servidor só com RAM.
- Identifica auditorias de segurança independentes e planos de preços ao fazeres a escolha.
- Seleciona as localizações dos servidores com base na tua velocidade e nas tuas necessidades de desbloqueio geográfico.

INSTRUÇÕES DA FICHA DE SELEÇÃO

Responde às perguntas de escolha múltipla e de verdadeiro/falso, completa as frases de preencher espaços com o banco de palavras, associa as definições e resolve as palavras cruzadas e a sopa de letras. Aplica os teus conhecimentos à escolha de uma infraestrutura VPN segura. Termina com a atividade bónus Pensa rápido.

ESCOLHER UMA VPN (INTRODUÇÃO)

Escolher a VPN certa exige olhar para além do entusiasmo do marketing. Um fornecedor fiável deve ter uma política de zero logs comprovada, protocolos de encriptação seguros e clientes de código aberto. Ao avaliar as funcionalidades de segurança, as jurisdições e o desempenho de velocidade, podes escolher uma VPN que se adeque às tuas necessidades de proteção digital.

LÊ CADA PONTO DE CONTROLO COM ATENÇÃO E ESCOLHE OU ESCREVE A RESPOSTA CORRETA.

Ponto de controlo 1: Desafio de escolha múltipla

1. Qual é o fator-chave ao escolher um fornecedor de VPN seguro?

- A. O número de países com servidores
- B. Uma política de ausência de registos (no-logs) auditada de forma independente
- C. O escalão de preço mensal mais baixo
- D. Patrocínios publicitários chamativos

2. Que protocolo VPN oferece o melhor equilíbrio entre velocidade e capacidade de auditoria?

- A. PPTP (legado)
- B. L2TP/IPSec
- C. OpenVPN apenas sobre TCP
- D. WireGuard

3. Porque devem os utilizadores evitar VPN gratuitas em atividades sensíveis?

- A. São proibidos nos Estados Unidos
- B. Muitas vezes vendem o teu histórico de navegação
- C. Não suportam a navegação web básica
- D. Requerem hardware especial para se ligarem

4. O que determina a jurisdição legal de origem de um fornecedor?

- A. A velocidade da ligação ao servidor
- B. Os tipos de dispositivos suportados
- C. Leis locais que regem a retenção de dados e os mandados de busca
- D. O tema visual da aplicação cliente

5. Qual é o principal objetivo da funcionalidade de «kill switch» de um cliente VPN?

- A. Bloquear o acesso à Internet se a ligação VPN cair
- B. Eliminar todas as aplicações instaladas no dispositivo
- C. Para duplicar a velocidade da ligação ao servidor
- D. Para reiniciar o sistema operativo quando está inativo

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. Uma VPN protege o teu dispositivo contra transferências de software malicioso e ficheiros com vírus.

- ◯ Verdadeiro
- ◯ Falso

7 Pergunta 7

7. Auditorias independentes de empresas como a Deloitte verificam as alegações de zero registos.

- ◯ Verdadeiro
- ◯ Falso

8 Pergunta 8

8. As leis do país de origem de um fornecedor não afetam a privacidade dos dados dos utilizadores.

- ◯ Verdadeiro
- ◯ Falso

9 Pergunta 9

9. O código compacto do WireGuard é mais fácil de auditar do que o do OpenVPN.

- ◯ Verdadeiro
- ◯ Falso

10 Pergunta 10

10. As VPN gratuitas vendem frequentemente publicidade ou rastreiam os utilizadores para cobrir os custos dos servidores.

- ◯ Verdadeiro
- ◯ Falso

Ponto de controlo 3: Inserção de termos-chave

Lê cada frase abaixo e preenche o espaço em branco com o termo correto do banco de palavras.

1. Uma política de _____ verificada de forma independente compromete o fornecedor de VPN a não registar o teu historial online.

2. O moderno protocolo _____ oferece alta velocidade e usa uma base de código muito pequena.

3. Uma funcionalidade de segurança chamada _____ interrompe todo o tráfego se a ligação VPN falhar de repente.

4. Avaliar a _____ legal de um fornecedor determina se este está sujeito a tratados de vigilância.

5. A utilização de _____ ajuda a evitar que os dados dos utilizadores persistam após um reinício.

6. Verificar uma política de conhecimento zero exige uma _____ de segurança por terceiros, feita por empresas de renome.

BANCO DE PALAVRAS DE VOCABULÁRIO

AUDITORIA FIVE EYES JURISDIÇÃO KILL SWITCH SERVIDORES RAM
VPN GRATUITA WIREGUARD ZERO LOGS

Escreve aqui as tuas respostas:

1. **2.**

3. **4.**

5. **6.**

Ponto de controlo 4: Associação de conceitos de rede

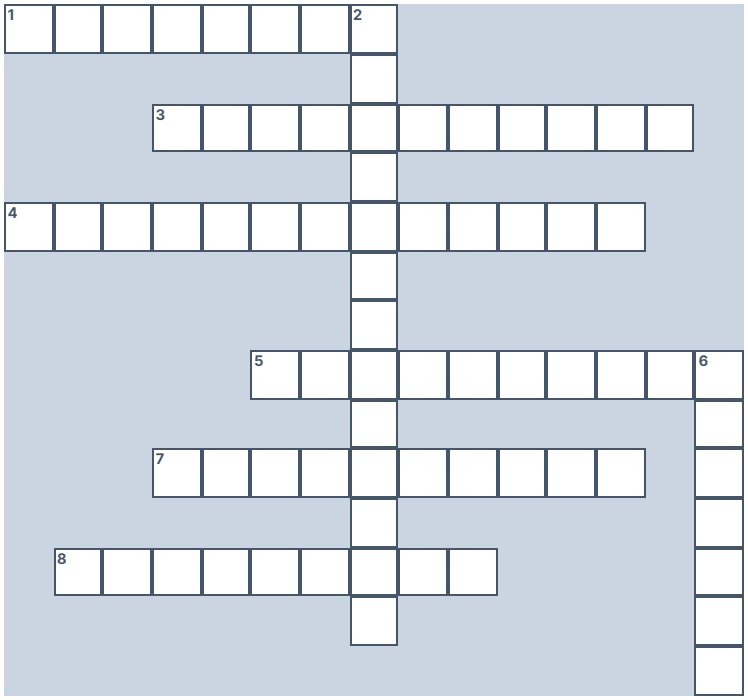
ASSOCIAÇÃO DE DEFINIÇÕES

Associa cada termo de vocabulário da esquerda à sua definição correta da direita, escrevendo a letra correspondente (A-H) na caixa de preenchimento.

☐	1. WireGuard	A	Serviço de ligação de alto risco que se rentabiliza frequentemente através do registo e da venda de dados de navegação.
☐	2. Registos auditados	B	Mecanismo de segurança que bloqueia o encaminhamento de Internet se o túnel seguro se desligar.
☐	3. Jurisdição	C	Aliança internacional de partilha de informações entre os EUA, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia.
☐	4. Kill switch	D	Infraestrutura de hardware que funciona com memória volátil, pelo que os dados não são guardados em disco.
☐	5. Five Eyes	E	A região geográfica que rege as obrigações legais do fornecedor de VPN.
☐	6. VPN gratuita	F	Protocolo moderno e rápido que utiliza cerca de 4000 linhas de código altamente auditável.
☐	7. Servidores só com RAM	G	Protocolo de código aberto maduro e amplamente auditado, com uma base de código muito maior do que a do WireGuard.
☐	8. OpenVPN	H	Alegação de privacidade verificada por empresas independentes de cibersegurança.

Ponto de controlo 5: Palavras cruzadas

Resolve as palavras cruzadas escrevendo letras nas caixas brancas ativas. Os números correspondem às pistas abaixo.



HORIZONTAIS

1. Aliança internacional de partilha de informações entre EUA, Reino Unido, Canadá, Austrália e Nova Zelândia (8)

3. Serviço de ligação de alto risco que muitas vezes rentabiliza registando e vendendo dados de navegação (11)

4. Garantia de privacidade verificada por empresas de cibersegurança independentes (13)

5. A região geográfica que rege as obrigações legais do fornecedor de VPN (10)

7. Mecanismo de segurança que bloqueia o encaminhamento de internet se o túnel seguro se desligar (10)

8. Protocolo moderno e rápido, com cerca de 4000 linhas de código facilmente auditável (9)

VERTICAIS

2. Infraestrutura de hardware que funciona inteiramente em memória volátil, impedindo o armazenamento de dados (13)

6. Protocolo de código aberto maduro e amplamente auditado, com uma base de código muito maior do que a do WireGuard (7)

Ponto de controlo 5, alternativa: Pistas acessíveis das palavras cruzadas

Os utilizadores de leitores de ecrã e de teclado podem escrever as respostas das palavras cruzadas diretamente nos campos de texto abaixo.

HORIZONTAIS

1 horizontal: Aliança internacional de partilha de informações entre EUA, Reino Unido, Canadá, Austrália e Nova Zelândia (8 letras):

3 horizontal: Serviço de ligação de alto risco que muitas vezes rentabiliza registando e vendendo dados de navegação (11 letras):

4 horizontal: Garantia de privacidade verificada por empresas de cibersegurança independentes (13 letras):

5 horizontal: A região geográfica que rege as obrigações legais do fornecedor de VPN (10 letras):

7 horizontal: Mecanismo de segurança que bloqueia o encaminhamento de internet se o túnel seguro se desligar (10 letras):

8 horizontal: Protocolo moderno e rápido, com cerca de 4000 linhas de código facilmente auditável (9 letras):

VERTICAIS

2 vertical: Infraestrutura de hardware que funciona inteiramente em memória volátil, impedindo o armazenamento de dados (13 letras):

6 vertical: Protocolo de código aberto maduro e amplamente auditado, com uma base de código muito maior do que a do WireGuard (7 letras):

Ponto de controlo 6: Sopa de letras

Encontra os 8 termos-chave de vocabulário escondidos na grelha abaixo. As palavras podem estar na horizontal, na vertical ou na diagonal.

M Z M K V R U A S W J M M H H
A N O A C I D S I R U J H R F
R K T L F I V E E Y E S R W H
S B U F Y O Y N W S H T X A P
E U N N Z O P I Q T I P V U O
R U U K A V E P M K A N V G G
O P Q X N Y J K V J Y W Y P J
D I Z E I D R A U G E R I W J
I N P A E I A S A J F W E K Z
V O H C T I W S L L I K K E K
R L O G S A U D I T A D O S Q
E N J A F O K N D N C D H I B
S A V P N G R A T U I T A P R
L P W T I Y F Y S G X W H F R
T N U K R D T S L P L M S H K

LISTA DE PALAVRAS DE VOCABULÁRIO

WIREGUARD
LOGSAUDITADOS
JURISDICAO
KILLSWITCH
FIVEEYES
VPNGRATUITA
SERVIDORESRAM
OPENVPN

Ponto de controlo 6, alternativa: Associação acessível de vocabulário

Associa cada um dos 8 termos de vocabulário da sopa de letras à sua definição correta, escrevendo a letra (A-H) no espaço em branco.

TERMOS DE VOCABULÁRIO

- **A. WIREGUARD**
- **B. LOGSAUDITADOS**
- **C. JURISDICAO**
- **D. KILLSWITCH**
- **E. FIVEEYES**
- **F. VPNGRATUITA**
- **G. SERVIDORESRAM**
- **H. OPENVPN**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Aliança internacional de partilha de informações entre EUA, Reino Unido, Canadá, Austrália e Nova Zelândia.

_____ 2. Protocolo moderno e rápido, com cerca de 4000 linhas de código facilmente auditável.

_____ 3. Protocolo de código aberto maduro e amplamente auditado, com uma base de código muito maior do que a do WireGuard.

_____ 4. Serviço de ligação de alto risco que muitas vezes rentabiliza registando e vendendo dados de navegação.

_____ 5. Mecanismo de segurança que bloqueia o encaminhamento de internet se o túnel seguro se desligar.

_____ 6. Infraestrutura de hardware que funciona inteiramente em memória volátil, impedindo o armazenamento de dados.

_____ 7. A região geográfica que rege as obrigações legais do fornecedor de VPN.

_____ 8. Garantia de privacidade verificada por empresas de cibersegurança independentes.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de VPN. Escreve as tuas respostas nas caixas de texto preenchíveis.

1. UGEIWARDR
2. AIJUSOICDR
3. EIFEYSEV
4. DAERRIMORSSEV
5. TDOGIASUADLOS
6. CSLITKIWHL
7. URVPTAITNAG
8. PNNOPVE

Atividade bónus: Pensa rápido

3 RESPOSTAS POR CATEGORIA. GANHA QUEM COMPLETAR PRIMEIRO A LISTA.

1	Coisas que uma VPN consegue esconder			
2	Coisas que importam mais do que o preço			
3	Locais onde ler análises de VPN			
4	Coisas de que uma VPN não te consegue proteger			
5	Perguntas para uma equipa de vendas de VPN			
6	Coisas que o teu fornecedor de internet consegue ver			
7	Itens da tua lista de verificação ao escolher uma VPN			
8	Locais onde usarias uma VPN			
9	Sinais de alerta num fornecedor de VPN			
10	Palavras relacionadas com privacidade			
11	Coisas que testarias primeiro			
12	Promessas que um bom fornecedor de VPN faz			
13	Razões para usar uma VPN quando viajas			
14	Dispositivos que podem usar uma VPN			
15	Mitos sobre as VPN			

Ponto de controlo 8: Estudos de caso de VPN

Aplica os conceitos que aprendeste para resolver os cenários reais abaixo.

SARAH (ESTUDANTE NO CAFÉ)

👩‍💻 "Olá! Estou sentada no Coffee & Bytes. Há uma rede pública sem proteção chamada 'Free_Wi-Fi_No_Password'. Quero iniciar sessão no e-mail da escola e enviar o meu trabalho, mas receio os hackers. Quais são os riscos de usar esta rede sem VPN e como é que uma VPN protege os meus dados?"

ALEX (ESTUDANTE VIAJANTE)

👩‍💻 "Ai, não! Estou a viajar no estrangeiro para um projeto e a tentar ver um documentário de biologia alojado num servidor no meu país. Mas o site diz 'Este vídeo não está disponível na tua localização atual.' Porque é que estou bloqueado e como pode uma VPN ajudar-me a vê-lo?"

Ponto de controlo 9: Decifrar o código

Para concluíres a tua formação em guia de seleção, decifra esta mensagem oculta sobre a escolha de infraestrutura segura.

CHAVE DE ENCRIPTAÇÃO DE LETRAS PARA NÚMEROS

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

3 15 13 16 1 18 1 15 19 20 5 21 19

18 5 12 1 20 15 18 9 15 19 3 15 13 21 13

19 9 19 20 5 13 1 19 5 7 21 18 15

Mensagem decifrada:

DICA: CADA NÚMERO REPRESENTA A POSIÇÃO DESSA LETRA NO ALFABETO (P. EX., 1 = A, 2 = B, 26 = Z).

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte A)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q1: O que é uma VPN e como funciona?

Uma Rede Privada Virtual (VPN) encripta a tua ligação à Internet e encaminha o teu tráfego através de um servidor remoto seguro. Isto oculta o teu endereço IP público e limita o que os observadores da rede local e o teu ISP podem ver sobre o tráfego encaminhado pelo túnel VPN.

Q2: Porque devo utilizar uma VPN?

Uma VPN protege a tua privacidade digital, protege a tua ligação em redes Wi-Fi públicas (como cafés ou aeroportos), pode reduzir a limitação baseada na atividade quando o ISP não consegue identificar o tipo de tráfego encriptado, contorna restrições geográficas para aceder a conteúdos globais e ajuda a proteger recursos de trabalho remoto.

Q3: Uma VPN torna-me completamente anónimo online?

Não. Embora uma VPN oculte o teu endereço IP e encripte o tráfego, podes continuar a ser rastreado através de cookies do navegador, contas ativas (como Google ou Facebook), identificação por impressão digital do navegador ou se o teu fornecedor de VPN registar os teus dados.

Q4: Uma VPN vai tornar a minha ligação à Internet mais lenta?

Sim, ligeiramente. O processo de encriptação e a distância física ao servidor VPN acrescentam latência e sobrecarga. O impacto varia consoante o fornecedor, o protocolo, a distância ao servidor, o dispositivo e as condições da rede.

Q5: Como ganha dinheiro?

Verifica o modelo de negócio. As subscrições, os escalões freemium e a venda de dados afetam todos o grau de confiança que podes ter numa VPN, e um serviço que nunca recolhe os teus dados não os pode vender. Lê primeiro a política de privacidade. [1]

Ponto de controlo 10: Perguntas frequentes básicas sobre VPN (Parte B)

Revê as perguntas e respostas mais comuns que os potenciais clientes colocam sobre a utilização de redes privadas virtuais.

Q6: Posso usar uma VPN gratuita?

As VPN gratuitas podem depender de publicidade, de funcionalidades limitadas, de análises de utilização, de limites de dados ou de outros modelos de rentabilização. Os utilizadores devem consultar a política de privacidade, a propriedade, as auditorias e o modelo de negócio do fornecedor antes de as utilizar.

Q7: O que é uma política de «não guardar registos» (no-logs)?

Uma política de não registos descreve que dados de atividade e de ligação um fornecedor afirma não reter. O âmbito exato varia, pelo que os leitores devem consultar a política e as conclusões de auditorias independentes.

Q8: Como escolho a melhor VPN?

Procura políticas de não registo auditadas, protocolos robustos (WireGuard, OpenVPN), localizações de servidores seguras, velocidades rápidas, servidores apenas com RAM, uma funcionalidade de kill switch e uma jurisdição fora de alianças de partilha de informações (como as 5/9/14 Eyes).

Q9: Posso usar uma VPN no meu telemóvel e na smart TV?

Sim. Os fornecedores de VPN modernos oferecem aplicações dedicadas para iOS, Android, macOS, Windows, Linux e smart TV, bem como configurações em routers para proteger todos os dispositivos da tua rede doméstica.

Q10: O que é um Kill Switch?

Um Kill Switch é uma funcionalidade de segurança que desliga automaticamente o teu dispositivo da Internet se a ligação VPN cair. Isto evita a fuga dos teus dados não encriptados ou do teu IP real.

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte C)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q1: Qual é a diferença entre WireGuard, OpenVPN e IKEv2?

O WireGuard é um protocolo moderno e leve (apenas cerca de 4000 linhas de código) que oferece velocidades elevadas e tempos de ligação rápidos. O OpenVPN é um protocolo de código aberto muito seguro e testado em batalha. O IKEv2 é excelente para dispositivos móveis graças à capacidade de voltar a ligar-se rapidamente ao mudar de rede.

Q2: O que é o encaminhamento de VPN dupla ou Multi-Hop?

O Multi-Hop encaminha o teu tráfego através de dois ou mais servidores VPN em sequência. Isto acrescenta uma segunda camada de encriptação e ajuda a manter o teu endereço IP real oculto do segundo salto se um servidor for comprometido.

Q3: O que é a fuga de WebRTC e como a evita uma VPN?

O WebRTC é um protocolo de navegador que pode revelar os teus endereços IP local e público reais, mesmo quando uma VPN está ativa. As VPN premium bloqueiam ou falsificam os pedidos WebRTC nas suas aplicações para computador/telemóvel e nas extensões de navegador.

Q4: O que são servidores só com RAM e porque são importantes?

Os servidores tradicionais gravam dados em discos rígidos, que podem ser apreendidos ou comprometidos. Os servidores só com RAM (sem disco) funcionam inteiramente em memória volátil (RAM). Quando o servidor é reiniciado ou desligado, os dados guardados na memória são apagados.

Q5: Como contorna a ofuscação os bloqueios de VPN?

A ofuscação (ou "Stealth VPN") disfarça os pacotes de tráfego VPN para parecerem tráfego web HTTPS normal (porta 443). Isto ajuda a contornar a inspeção profunda de pacotes (DPI) usada por governos ou redes escolares/de escritório para bloquear VPN.

Ponto de controlo 10: Perguntas frequentes avançadas sobre VPN (Parte D)

Explora aspetos técnicos e estruturais das redes privadas virtuais e dos protocolos de tunneling seguro.

Q6: O que é o split tunneling e quando devo usá-lo?

O split tunneling permite escolher quais as aplicações que passam pelo túnel VPN encriptado e quais as que se ligam diretamente à internet. Usa-o para encaminhar aplicações bancárias sensíveis pela VPN enquanto os jogos locais se ligam diretamente, evitando a latência acrescentada pela VPN.

Q7: Como funciona a confidencialidade de encaminhamento (Perfect Forward Secrecy)?

O PFS garante que é gerada uma chave de encriptação única e temporária para cada sessão. Mesmo que uma chave privada seja comprometida no futuro, não pode ser usada para decifrar sessões passadas ou futuras, porque estas usaram chaves independentes.

Q8: O que são as alianças 5/9/14 Eyes e porque me devem interessar?

A jurisdição pode afetar o processo legal que um fornecedor pode enfrentar, mas o risco prático para a privacidade depende também dos dados que o fornecedor conserva, da sua arquitetura técnica, da propriedade, dos relatórios de transparência e do historial de auditorias.

Q9: O que é a proteção contra fugas de DNS?

A proteção contra fugas de DNS força o teu dispositivo a enviar as consultas de pesquisa de sites (consultas DNS) através dos servidores DNS privados e encriptados da VPN, em vez dos servidores do teu ISP. Isto impede o teu ISP de rastrear os sites que visitas.

Q10: Porque é importante verificar quem gere e apoia uma VPN?

A reputação importa. Pesquisa os proprietários e os líderes da empresa, procura auditorias públicas de terceiros e verifica o que dizem os especialistas independentes em segurança e a imprensa antes de confiares nela. [1]

Parte 11: 10 factos interessantes sobre VPN e perspetivas do mundo real

Revê estes factos e conhecimentos reais, muito valiosos, sobre a história, o mercado e a tecnologia das VPN.

1. PRIMEIRO PROTOCOLO VPN

O PPTP (Point-to-Point Tunneling Protocol), um dos primeiros protocolos VPN, criado por um grupo liderado pela Microsoft na década de 1990, é hoje considerado inseguro, pelo que as VPN modernas usam WireGuard ou OpenVPN. [1]

2. AVALIAÇÃO DE MERCADO

O mercado global de VPN tem registado um crescimento rápido, impulsionado pelo aumento das necessidades de trabalho remoto e das exigências de segurança das empresas.

3. REVOLUÇÃO WIREGUARD

O WireGuard tem um código muito simplificado e concebido para a eficiência, o que o torna mais fácil de auditar quanto a vulnerabilidades de segurança do que os protocolos tradicionais. [3]

4. NORMAS DE AUDITORIA RIGOROSAS

Os principais fornecedores de VPN contratam empresas como a Deloitte, a KPMG ou a PwC para verificar as alegações de não registo, e empresas de segurança como a Cure53 para testar as suas aplicações e servidores. [4]

5. ORIGENS DA ALIANÇA 5-EYES

A parceria de informações Five Eyes, formada pelos EUA, Reino Unido, Canadá, Austrália e Nova Zelândia, nasceu da cooperação em informações de sinais entre os Aliados durante a Segunda Guerra Mundial.

6. INSPEÇÃO PROFUNDA DE PACOTES

As firewalls avançadas implementam a inspeção profunda de pacotes (DPI) para analisar os metadados dos pacotes de rede e bloquear as características normais das ligações VPN.

7. UTILIZAÇÃO EMPRESARIAL

Muitas organizações dão aos funcionários remotos uma VPN para acederem a sistemas internos, como bases de dados, o que faz das VPN uma ferramenta de segurança comum no local de trabalho.

8. VPN DESCENTRALIZADAS

As VPN descentralizadas (dVPN) distribuem o tráfego por uma rede de nós geridos por pares, reduzindo a dependência de um único fornecedor centralizado.

9. ANONIMATO TOR VS. VPN

Uma VPN encaminha o tráfego através de um único fornecedor, enquanto o Tor (The Onion Router) envia o tráfego por três relays voluntários (de entrada, intermédio, de saída) para maximizar a privacidade. [5]

10. CUSTO DAS FUGAS DE DADOS

Combinar uma VPN com um modelo de acesso zero trust, que verifica cada utilizador e dispositivo, ajuda as organizações a proteger os dados e a limitar os danos de violações de dados.

Referências técnicas e fontes

Publicações citadas, especificações criptográficas e normas oficiais de documentos utilizadas ao longo desta ficha de trabalho.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.
https://ssd.eff.org/module/choosing-vpn-thats-right-you

[2] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.
https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[4] Yahoo Finance. (2026). NordVPN passes its no-logs assurance assessment for the sixth time.
https://finance.yahoo.com/news/nordvpn-passes-no-logs-assurance-140000101.html

[5] Tor Project. (n.d.). Overview.
https://support.torproject.org/about-tor/how-tor-works/overview/

Soluções: Avaliar fornecedores de VPN, normas de segurança, auditorias e políticas de registos

1 **Política de registos auditada** PROTOCOLOS — **Resposta correta: B**

NOTA PARA O PROFESSOR

Uma política de não registos auditada de forma independente é a forma mais prática de verificar as alegações de privacidade de conhecimento zero de um fornecedor. O marketing apelativo ou as alegações do próprio não são suficientes. Citação: Deloitte Advisory, Cure53 Audit.

2 **Superioridade do WireGuard** LATÊNCIA — **Resposta correta: D**

NOTA PARA O PROFESSOR

O WireGuard oferece um encaminhamento de ligações moderno e rápido no espaço do kernel, com um código compacto (cerca de 4000 linhas), o que torna as auditorias muito eficientes. Citação: IETF Protocol RFC, WireGuard Project.

3 **Pergunta 3** — **Resposta correta: B**

NOTA PARA O PROFESSOR

As VPN gratuitas também pagam servidores, e a FTC avisa que algumas aplicações VPN partilham dados de utilizadores com terceiros, por exemplo para apresentar anúncios.

4 **Jurisdições legais** CONTROLOS DE ENCAMINHAMENTO — **Resposta correta: C**

NOTA PARA O PROFESSOR

A jurisdição determina se a VPN está sujeita a leis de vigilância, a obrigações locais de conservação de dados e a mandados judiciais secretos do governo. Citação: Privacy Rights Clearinghouse.

5 **Proteção do kill switch** PRIVACIDADE — **Resposta correta: A**

NOTA PARA O PROFESSOR

O kill switch corta imediatamente o encaminhamento do adaptador de rede do sistema se o túnel falhar, evitando a exposição do IP real e fugas de DNS. Fonte: IETF Tunnel RFC.

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 **Limitações do software malicioso** MASCARAMENTO DE IP — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Uma VPN fornece um canal encriptado seguro, mas não analisa os dados transportados nem os ficheiros. É necessário software antivírus para bloquear software malicioso. Citação: Deloitte Advisory.

7 **Auditoria independente** VELOCIDADES — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Os relatórios de auditoria verificam as configurações do software dos servidores, a conformidade da configuração apenas em RAM e a ausência de bases de dados de registos. Citação: Deloitte Advisory, Cure53 Audit.

8 **Pergunta 8** — **Resposta correta: Falso**

NOTA PARA O PROFESSOR

Os fornecedores têm de cumprir as leis do seu país de origem, que podem incluir regras de conservação de dados e ordens para entregar os dados que detêm.

9 **Tamanho da base de código do protocolo** FIREWALLS — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Uma base de código mais pequena reduz a superfície de ataque potencial e facilita às equipas de segurança a verificação da integridade do protocolo. Citação: WireGuard Project.

10 **Monetização com anúncios** SEM REGISTOS — **Resposta correta: Verdadeiro**

NOTA PARA O PROFESSOR

Sem taxas de subscrição, as VPN gratuitas dependem da mineração de dados, da criação de perfis de tráfego e da injeção de anúncios no navegador para gerar receitas. Citação: EDRi Retention Guidelines.

Soluções de vocabulário e grelha de avaliação

Grelha de classificação do professor: atribui 1 ponto por cada correspondência correta (8 pontos no total) e por cada termo de contexto (6 pontos no total).

PONTO DE CONTROLO 4: SOLUÇÕES – ASSOCIAÇÃO DE CONCEITOS

F 1. WireGuard	H 2. Registos auditados	E 3. Jurisdição	B 4. Kill switch
C 5. Five Eyes	A 6. VPN gratuita	D 7. Servidores só com RAM	G 8. OpenVPN

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 ZERO LOGS	2 WIREGUARD	3 KILL SWITCH	4 JURISDIÇÃO
5 SERVIDORES RAM	6 AUDITORIA		

PONTO DE CONTROLO 6, ALTERNATIVA: SOLUÇÕES – ASSOCIAÇÃO DE PALAVRAS

1 E – FIVEEYES	2 A – WIREGUARD	3 H – OPENVPN	4 F – VPNGRATUITA
5 D – KILLSWITCH	6 G – SERVIDORESRAM	7 C – JURISDICAO	8 B – LOGSAUDITADOS

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar WireGuard, Registos auditados e Jurisdição por palavras suas e dar um exemplo de cada.

Estudos de caso:
Pede aos alunos que justifiquem as recomendações com factos da ficha e não com suposições.

Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

M	Z	M	K	V	R	U	A	S	W	J	M	M	H	H
A	N	O	A	C	I	D	S	I	R	U	J	H	R	F
R	K	T	L	F	I	V	E	E	Y	E	S	R	W	H
S	B	U	F	Y	O	Y	N	W	S	H	T	X	A	P
E	U	N	N	Z	O	P	I	Q	T	I	P	V	U	O
R	U	U	K	A	V	E	P	M	K	A	N	V	G	G
O	P	Q	X	N	Y	J	K	V	J	Y	W	Y	P	J
D	I	Z	E	I	D	R	A	U	G	E	R	I	W	J
I	N	P	A	E	I	A	S	A	J	F	W	E	K	Z
V	O	H	C	T	I	W	S	L	L	I	K	K	E	K
R	L	O	G	S	A	U	D	I	T	A	D	O	S	Q
E	N	J	A	F	O	K	N	D	N	C	D	H	I	B
S	A	V	P	N	G	R	A	T	U	I	T	A	P	R
L	P	W	T	I	Y	F	Y	S	G	X	W	H	F	R
T	N	U	K	R	D	T	S	L	P	L	M	S	H	K

SOLUÇÃO DAS PALAVRAS CRUZADAS

F	I	V	E	E	Y	E	S							
							E							
			V	P	N	G	R	A	T	U	I	T	A	
							V							
L	O	G	S	A	U	D	I	T	A	D	O	S		
							D							
							O							
				J	U	R	I	S	D	I	C	A	O	
							E						P	
			K	I	L	L	S	W	I	T	C	H	E	
							R						N	
	W	I	R	E	G	U	A	R	D				V	
							M						P	
													N	

GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

1 horizontal: FIVEEYES Aliança internacional de partilha de informações entre EUA, Reino Unido, Canadá, Austrália e Nova Zelândia (8 letras)

3 horizontal: VPNGRATUITA Serviço de ligação de alto risco que muitas vezes rentabiliza registando e vendendo dados de navegação (11 letras)

4 horizontal: LOGSAUDITADOS Garantia de privacidade verificada por empresas de cibersegurança independentes (13 letras)

5 horizontal: JURISDICAO A região geográfica que rege as obrigações legais do fornecedor de VPN (10 letras)

7 horizontal: KILLSWITCH Mecanismo de segurança que bloqueia o encaminhamento de internet se o túnel seguro se desligar (10 letras)

8 horizontal: WIREGUARD Protocolo moderno e rápido, com cerca de 4000 linhas de código facilmente auditável (9 letras)

VERTICAIS

2 vertical: SERVIDORESRAM Infraestrutura de hardware que funciona inteiramente em memória volátil, impedindo o armazenamento de dados (13 letras)

6 vertical: OPENVPN Protocolo de código aberto maduro e amplamente auditado, com uma base de código muito maior do que a do WireGuard (7 letras)

Palavras baralhadas e soluções da cifra

Chave de correção da atividade de reordenação de letras do vocabulário e do Desafio do Código Secreto.

CHAVE DE SOLUÇÕES DAS PALAVRAS EMBARALHADAS

1. UGEIWARDR — **WIREGUARD**
2. AIJUSOICDR — **JURISDICAO**
3. EIFEYSEV — **FIVEEYES**
4. DAERRIMORSSEV — **SERVIDORESRAM**
5. TDOGIASUADLOS — **LOGSAUDITADOS**
6. CSLITKIWHL — **KILLSWITCH**
7. URVPTAITNAG — **VPNGRATUITA**
8. PNNOPVE — **OPENVPN**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"COMPARA OS TEUS RELATORIOS COM UM SISTEMA SEGURO"

Soluções dos estudos de caso

A Cenário A: Segurança em redes públicas

SNIFFING E ENCRIPTAÇÃO · O dilema da Sarah

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Riscos: Captura de pacotes, intercetação de dados e ataques man-in-the-middle. Alguém na mesma rede do café poderia capturar os dados de início de sessão ou o ficheiro dos trabalhos de casa dela.
- Proteção da VPN: encripta o conteúdo dos pacotes de rede, tornando ilegível o tráfego intercetado no túnel para quem espia passivamente a rede local, quando a VPN está corretamente configurada.

B Cenário B: Aceder a recursos bloqueados

BLOQUEIO GEOGRÁFICO E IP · O dilema do Alex

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Motivo do bloqueio: a plataforma de streaming usa bloqueio geográfico, que associa o endereço IP local do viajante ao seu país físico e o bloqueia com base nas licenças territoriais.
- Como a VPN ajuda: mascara a localização real dele, encaminhando o tráfego por um servidor no seu país de origem. O site vê o IP do país de origem, o que permite o acesso.