Nome: _____ **Data:** _____ **Pontuação:** _____

Proteção de dados e armazenamento empresarial
Fusões de segurança

Ocultação de dados, tokenização, encriptação em repouso vs. em trânsito, cópias de segurança offline

VISÃO GERAL DE APRENDIZAGEM SOBRE PROTEÇÃO DE DADOS

PROTEGIDO
ENCRIPTAÇÃO DE DADOS
Norma AES de 256 bits

CONFORME
NORMAS GLOBAIS
Referenciais RGPD (GDPR) e CCPA

ZERO-TRUST
POLÍTICA DE ACESSO
Autenticação multifator

Bem-vindo! Este conjunto de atividades guia-te pelas normas e controlos de proteção de dados. Vais explorar a encriptação de disco completo, controlos de acesso seguros, cópias de segurança em hardware, postura de segurança na nuvem e técnicas de mascaramento de dados.

PONTOS DE CONTROLO DA FICHA DE TRABALHO

- [ ] **Partes 1-4: Domina a cibersegurança e a prevenção de ameaças.**
- [ ] **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 Cibersegurança da VPN.com

URL: https://www.vpn.com/pt/ciberseguranca/protecao-de-dados/

O teu roteiro de aprendizagem sobre estratégia de proteção de dados

- Distingue as técnicas de ocultação de dados e de tokenização.
- Implementa encriptação em repouso para as unidades de armazenamento e encriptação em trânsito com TLS.
- Concebe sistemas de cópia de segurança offline e isolados da rede para proteção contra ransomware.

INSTRUÇÕES DO GUIA DE PROTEÇÃO DE DADOS

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 proteção de dados. Termina com a atividade bónus Pensa rápido.

PROTEÇÃO DE DADOS E SEGURANÇA DO ARMAZENAMENTO EMPRESARIAL (INTRODUÇÃO)

A proteção de dados salvaguarda os ativos de dados da empresa através de ocultação, tokenização, encriptação de bases de dados em repouso e protocolos de trânsito seguros. Conceber cópias de segurança isoladas da rede ajuda a garantir que as bases de dados principais podem ser restauradas em caso de intrusão ativa.

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

Ponto de controlo 1: Desafio de escolha múltipla

1 **1. Qual é o principal objetivo da ocultação de dados (data masking)?**

- A. Substituir identificadores sensíveis por caracteres fictícios, mas realistas, para proteger a privacidade
- B. Comprimir grandes ficheiros de bases de dados para poupar espaço de armazenamento no servidor físico
- C. Eliminar emails de contacto de clientes antigos de sistemas de cópia de segurança de arquivo
- D. Ocultar o IP público do servidor de base de dados das pesquisas na internet

2 **2. Que mecanismo encripta os ficheiros guardados no disco rígido de um servidor de base de dados?**

- A. Encriptação de disco completo em repouso
- B. Protocolos de handshake de sessão TLS em trânsito
- C. Regras de reencaminhamento de servidores de nomes DNS dinâmico
- D. Autenticação multifator com chaves de hardware

3 **3. O que representa os dados em trânsito?**

- A. Pacotes de dados a circular por routers e comutadores de rede
- B. Registos de transações de bases de dados armazenados numa unidade de cópia de segurança offline
- C. Ficheiros de utilizador arquivados guardados num cofre isolado na cloud
- D. Ficheiros estáticos de configuração do sistema num armazenamento de computador local

4 **4. Porque é que uma cópia de segurança offline regular é essencial para a proteção contra ransomware?**

- A. Fornece uma cópia limpa e offline para restaurar ficheiros sem pagar um resgate
- B. Impede que hackers analisem as configurações de portas abertas
- C. Aumenta as velocidades de largura de banda de transmissão da rede local
- D. Automatiza os registos de adesão ao consentimento de cookies nos navegadores

5 **5. O que faz a tokenização de dados?**

- A. Substitui números de cartão sensíveis por tokens aleatórios não sensíveis
- B. Encaminha o tráfego web através de vários nós onion seguros
- C. Analisa os diretórios do sistema à procura de malware baseado em assinaturas
- D. Audita as horas de sessão dos administradores da base de dados

Ponto de controlo 2: Desafio de verdadeiro ou falso

6 Pergunta 6

6. A ocultação de dados altera permanentemente os registos da base de dados nos ambientes de produção.

- ○ Verdadeiro
- ○ Falso

7 Pergunta 7

7. As cópias de segurança externas devem estar isoladas da rede empresarial principal para evitar a propagação de ransomware.

- ○ Verdadeiro
- ○ Falso

8 Pergunta 8

8. Os certificados SSL/TLS protegem as bases de dados ao encriptar os dados armazenados em repouso em suportes físicos.

- ○ Verdadeiro
- ○ Falso

9 Pergunta 9

9. O Zero Trust Network Access (ZTNA) verifica a identidade de cada utilizador antes de conceder acesso à base de dados.

- ○ Verdadeiro
- ○ Falso

10 Pergunta 10

10. A tokenização baseada em cofre guarda os valores originais dos cartões num cofre de tokens central e seguro.

- ○ 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. Substituir nomes pessoais por marcadores realistas chama-se _____ de dados.

2. Encriptar os blocos de armazenamento físico protege os ativos da base de dados _____ .

3. Os protocolos TLS encriptam os pacotes de dados ativos que circulam em _____ .

4. As permissões baseadas em funções limitam os utilizadores que podem obter _____ à base de dados.

5. Restaurar ficheiros empresariais limpos após uma violação exige um _____ offline seguro.

6. A auditoria das configurações da cloud avalia a _____ de segurança de uma organização.

BANCO DE PALAVRAS DE VOCABULÁRIO

ACESSO BACKUP EM REPOUSO ENCRIPTAÇÃO MASCARAMENTO MINIMIZAÇÃO POSTURA TRÂNSITO

Escreve aqui as tuas respostas:

1. **2.**

3. **4.**

5. **6.**

Ponto de controlo 4: Associação de conceitos de segurança

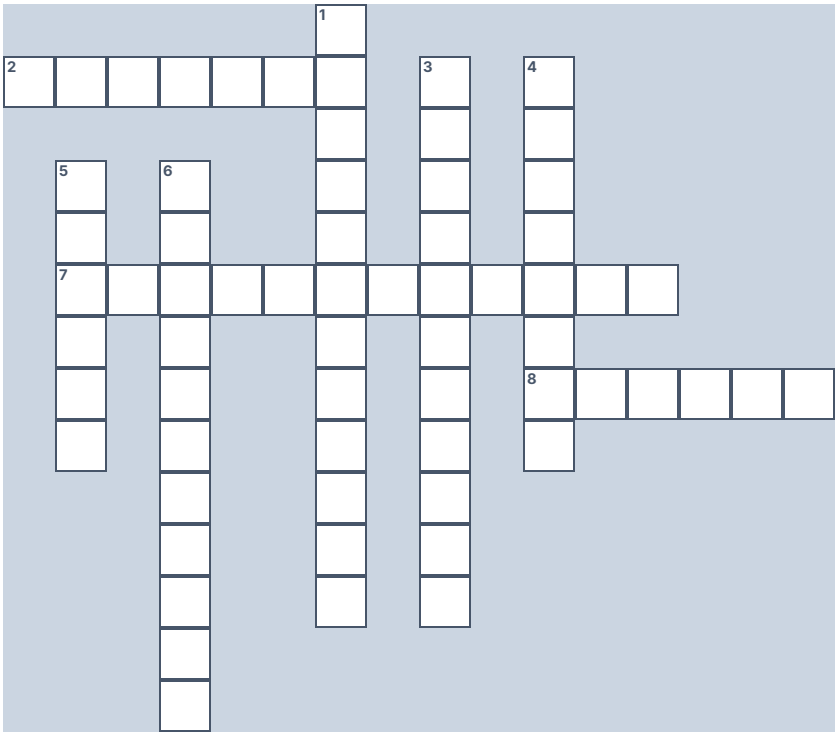
ASSOCIAÇÃO DE DEFINIÇÕES

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

☐	1. ENCRIPTAÇÃO	A	Criar cópias seguras de dados fora das instalações para restaurar em caso de falhas do sistema.
☐	2. CÓPIA DE SEGURANÇA	B	Transformar texto simples em texto cifrado ilegível, para que os dados intercetados permaneçam privados.
☐	3. MINIMIZAÇÃO	C	O estado de segurança coletivo e a preparação de defesa da nuvem de uma organização.
☐	4. ACESSO	D	Cumprir normas regulamentares como o RGPD (GDPR) ou o CCPA na gestão de informações privadas dos utilizadores.
☐	5. POSTURA	E	Incidente de segurança em que dados protegidos são acedidos ou divulgados sem autorização.
☐	6. VIOLAÇÃO	F	Restringir as permissões de leitura e escrita da base de dados a funções de utilizador autenticadas.
☐	7. CONFORMIDADE	G	Substituição de carateres sensíveis em campos de bases de dados para proteger identidades pessoais.
☐	8. OCULTAÇÃO	H	Limitar a recolha de dados pessoais ao mínimo absoluto necessário para as operações.

Ponto de controlo 5: Palavras cruzadas

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



HORIZONTAIS

2. Estado coletivo de segurança e prontidão de defesa da cloud de uma organização (7)

7. Cumprimento de normas regulamentares como o RGPD ou o CCPA na gestão de informação privada dos utilizadores (12)

8. Restringir as permissões de leitura e escrita da base de dados a funções de utilizador autenticadas (6)

VERTICAIS

1. Substituição de carateres sensíveis nos campos da base de dados para proteger identidades pessoais (12)

3. Transformar texto simples em texto cifrado ilegível para que os dados intercetados permaneçam privados (11)

4. Incidente de segurança em que dados protegidos são acedidos ou divulgados sem autorização (8)

5. Criação de cópias seguras externas dos dados para restauro em caso de falhas do sistema (6)

6. Limitar a recolha de dados pessoais ao mínimo absoluto necessário para as operações (11)

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

2 horizontal: Estado coletivo de segurança e prontidão de defesa da cloud de uma organização (7 letras):

7 horizontal: Cumprimento de normas regulamentares como o RGPD ou o CCPA na gestão de informação privada dos utilizadores (12 letras):

8 horizontal: Restringir as permissões de leitura e escrita da base de dados a funções de utilizador autenticadas (6 letras):

VERTICAIS

1 vertical: Substituição de carateres sensíveis nos campos da base de dados para proteger identidades pessoais (12 letras):

3 vertical: Transformar texto simples em texto cifrado ilegível para que os dados intercetados permaneçam privados (11 letras):

4 vertical: Incidente de segurança em que dados protegidos são acedidos ou divulgados sem autorização (8 letras):

5 vertical: Criação de cópias seguras externas dos dados para restauro em caso de falhas do sistema (6 letras):

6 vertical: Limitar a recolha de dados pessoais ao mínimo absoluto necessário para as operações (11 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.

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

LISTA DE PALAVRAS DE VOCABULÁRIO

ENCRIPTACAO BACKUP MINIMIZACAO ACESSO POSTURA VIOLACAO CONFORMIDADE MASCARAMENTO

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. ENCRIPTACAO**
- **B. BACKUP**
- **C. MINIMIZACAO**
- **D. ACESSO**
- **E. POSTURA**
- **F. VIOLACAO**
- **G. CONFORMIDADE**
- **H. MASCARAMENTO**

DEFINIÇÕES E CAMPOS DE ASSOCIAÇÃO

_____ 1. Incidente de segurança em que dados protegidos são acedidos ou divulgados sem autorização.

_____ 2. Substituição de carateres sensíveis nos campos da base de dados para proteger identidades pessoais.

_____ 3. Restringir as permissões de leitura e escrita da base de dados a funções de utilizador autenticadas.

_____ 4. Estado coletivo de segurança e prontidão de defesa da cloud de uma organização.

_____ 5. Cumprimento de normas regulamentares como o RGPD ou o CCPA na gestão de informação privada dos utilizadores.

_____ 6. Limitar a recolha de dados pessoais ao mínimo absoluto necessário para as operações.

_____ 7. Transformar texto simples em texto cifrado ilegível para que os dados intercetados permaneçam privados.

_____ 8. Criação de cópias seguras externas dos dados para restauro em caso de falhas do sistema.

Ponto de controlo 7: Desafio de palavras baralhadas

Desembaralha as letras abaixo para revelar conceitos e termos essenciais de cibersegurança. Escreve as tuas respostas nas caixas de resposta fornecidas.

1. ITANPAECCOR
2. MOIMAINCAZI
3. TPUASRO
4. DIONMERADCOF
5. KCPBUA
6. SSAEOC
7. VOACAILO
8. MSANAOMRATEC

Atividade bónus: Pensa rápido

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

1	Coisas de que fazes cópia de segurança			
2	Palavras relacionadas com cibersegurança			
3	Pessoas autorizadas a ver dados sensíveis			
4	Formas de apagar dados em segurança			
5	Locais onde os dados são armazenados			
6	Coisas que devem ser encriptadas			
7	Dados que um hospital tem de proteger			
8	Tipos de cópia de segurança			
9	Informações que nunca deves partilhar			
10	Sinais de alerta num email			
11	Hábitos seguros que podes começar hoje			
12	Pessoas a quem podes pedir ajuda de TI			
13	Dispositivos que podem ser hackeados			
14	Formas de proteger dados			
15	Coisas que podem destruir dados			

Ponto de controlo 8: Estudos de caso de cibersegurança

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

ESTUDO DE CASO 1: ATUALIZAÇÃO DA ENCRIPTAÇÃO EM REPOUSO DE BASES DE DADOS EMPRESARIAIS



Cenário: Um retalhista online guarda bases de dados de transações em armazenamento cloud sem encriptação total do disco. Uma auditoria de conformidade recente assinalou isto como um risco grave de segurança de dados à luz do CCPA. Cria uma arquitetura de recuperação.

Questão para debate: Analisa os riscos de conformidade com o CCPA e propõe uma estratégia de encriptação em repouso.

ESTUDO DE CASO 2: CONTENÇÃO DE RANSOMWARE E RESTAURO DE DADOS



Cenário: Um ataque de ransomware ativo está a encriptar unidades de rede numa rede local empresarial. O administrador detetou a infeção cedo. Planeia os passos de contenção e recuperação.

Questão para debate: Detalha as ações imediatas de contenção e planeia um processo de restauro seguro.

Ponto de controlo 9: Decifrar o código

Um profissional de cibersegurança protege os ativos de rede contra agentes de ameaça online. Usa a chave Letra-Número abaixo para decifrar a mensagem, escrevendo as letras correspondentes nos espaços em branco.

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

16	18	15	20	5	7	5		15	19		20	5	21	19		4	1	4	15	19
3	15	13		3	15	14	20	18	15	12	15	19		19	5	7	21	18	15	19

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 cibersegurança (Parte A)

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q1: O que é a proteção de dados?

É o processo de proteger dados pessoais e empresariais contra acesso não autorizado, perda ou corrupção através de controlos técnicos.

Q2: Porque é que a encriptação de disco completo é importante?

Protege os blocos de dados armazenados em unidades físicas, impedindo que alguém leia os dados se roubar fisicamente o disco rígido.

Q3: Qual é a diferença entre encriptação em repouso e em trânsito?

A encriptação em repouso protege os ficheiros guardados nas unidades, enquanto a encriptação em trânsito protege os pacotes de rede ativos que passam pelos routers.

Q4: O que é a ocultação de dados (data masking)?

Substitui dados sensíveis (como números de cartões de crédito) por dados fictícios mas realistas para testes, sem expor registos reais.

Q5: Porque é importante a cópia de segurança offline?

Mantém uma cópia limpa dos teus ficheiros isolada da rede, o que ajuda a proteger as tuas cópias de segurança contra a encriptação por ransomware.

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

Revê perguntas e respostas comuns sobre a mitigação de ameaças online.

Q6: O que é um cofre de tokenização de dados?

Uma base de dados segura e isolada que associa tokens aleatórios aos valores sensíveis originais (como os números principais de cartões de crédito).

Q7: O que significa acesso a bases de dados com Zero Trust?

Significa verificar a identidade e o estado do dispositivo de cada utilizador em cada início de sessão, em vez de confiar em quem está dentro da rede.

Q8: Como protege o TLS os dados em trânsito?

O TLS encripta o conteúdo da sessão TCP, impedindo que agentes maliciosos em redes públicas intercetem ou modifiquem pacotes em trânsito.

Q9: O que é a auditoria de acesso a bases de dados?

O registo contínuo de consultas à base de dados e de inícios de sessão para detetar padrões de acesso não autorizado ou anomalias de segurança.

Q10: O que é uma auditoria da postura de segurança na nuvem?

Um processo que analisa configurações na nuvem para identificar portas abertas, regras de acesso mal configuradas e lacunas de conformidade de segurança.

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

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q1: Como funciona a encriptação de envelope?

Encripta os dados com uma chave de dados e depois encripta essa chave de dados com uma chave mestra, simplificando o armazenamento e a rotação de chaves.

Q2: O que é a encriptação homomórfica?

Um método avançado de encriptação que permite realizar operações diretamente sobre dados encriptados sem os desencriptar primeiro.

Q3: Porque é que se utiliza encriptação ao nível das colunas numa base de dados?

Encripta individualmente colunas sensíveis específicas (como os números de segurança social), protegendo-as mesmo que os administradores obtenham acesso geral de leitura à tabela.

Q4: O que é a prevenção de perda de dados (DLP)?

Software que monitoriza os pontos de saída da rede para detetar e bloquear transferências de saída não autorizadas de ficheiros sensíveis.

Q5: Como protegem as cópias de segurança de escrita única e leitura múltipla (WORM) contra ransomware?

As cópias de segurança WORM impedem que os ficheiros sejam eliminados ou modificados durante um período definido, o que evita que o ransomware encripte as cópias de segurança existentes.

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

Explora aspetos técnicos avançados das estruturas de segurança, da análise de malware e da conformidade de dados.

Q6: Qual é o risco da reutilização de chaves?

Reutilizar a mesma chave criptográfica em diferentes bases de dados significa que o comprometimento de uma única chave expõe todas as bases de dados.

Q7: Como melhora a tokenização de bases de dados a conformidade com o CCPA?

Os tokens pseudonimizam registos em sistemas de não produção e limitam a exposição a violações, mas os dados tokenizados continuam a poder ser informação pessoal.

Q8: Porque é crítica a classificação de dados?

Classifica os ficheiros por nível de sensibilidade, ajudando as organizações a aplicar a encriptação e os controlos de acesso mais fortes aos dados de alto risco.

Q9: Qual é o papel da rotação de chaves?

Atualizar regularmente as chaves de encriptação limita a quantidade de dados históricos expostos se uma única chave vier a ser quebrada.

Q10: Como é que os enclaves seguros protegem as consultas à base de dados em memória?

Os enclaves seguros isolam as operações de consulta em blocos de memória protegidos pelo CPU, impedindo que os administradores do anfitrião vejam texto em claro na RAM.

Parte 11: 10 factos e perspetivas do mundo real sobre cibersegurança

Revê factos reais sobre violações de segurança, mecanismos de defesa e normas de conformidade.

1. PERSPETIVA SOBRE SEGURANÇA

O RGPD (GDPR) entrou em vigor em maio de 2018, alterando a forma como os sites globais gerem os consentimentos de cookies e os registos de dados pessoais.

2. PERSPETIVA SOBRE SEGURANÇA

Uma coima por violação do RGPD (GDPR) pode atingir 20 milhões de euros ou 4% do volume de negócios global, o que representa uma exposição jurídica substancial. [4]

3. PERSPETIVA SOBRE SEGURANÇA

A CCPA entrou em vigor em janeiro de 2020, estabelecendo direitos pioneiros dos consumidores em matéria de privacidade digital nos Estados Unidos.

4. PERSPETIVA SOBRE SEGURANÇA

A minimização de dados reduz o espaço ocupado pela base de dados, diminuindo os custos de funcionamento do servidor e o impacto de uma violação.

5. PERSPETIVA SOBRE SEGURANÇA

A destruição criptográfica resolve o desafio da eliminação de cópias de segurança ao eliminar as chaves em vez de editar ficheiros históricos de fitas de cópia de segurança.

6. PERSPETIVA SOBRE SEGURANÇA

A maioria dos países em todo o mundo já promulgou leis de proteção de dados pessoais para proteger os direitos de privacidade dos consumidores.

7. PERSPETIVA SOBRE SEGURANÇA

Os formulários de consentimento com caixas pré-selecionadas estão expressamente proibidos pelas definições regulamentares europeias de privacidade de dados.

8. PERSPETIVA SOBRE SEGURANÇA

O RGPD (GDPR) exige a comunicação de violações de dados pessoais à autoridade de controlo no prazo de 72 horas após o conhecimento, sempre que possível. [3]

9. PERSPETIVA SOBRE SEGURANÇA

Aplicar hash às palavras-passe com algoritmos lentos como o bcrypt ou o Argon2 torna muito mais difícil a quebra offline de hashes roubados. [6]

10. PERSPETIVA SOBRE SEGURANÇA

Os dados em repouso representam ficheiros de bases de dados guardados, enquanto os dados em trânsito abrangem pacotes que se deslocam ativamente pelos routers da rede.

Referências técnicas e fontes

O guia de estudo e os puzzles interativos são compilados a partir das normas globais do NIST, da OWASP e de conformidade em matéria de privacidade de dados.

REFERÊNCIAS ACADÉMICAS E DO SETOR

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Soluções: Ponto de controlo 1 - Escolha múltipla

1 Pergunta 1

Resposta correta: A

NOTA PARA O PROFESSOR

Qual é o principal objetivo da ocultação de dados (data masking)? → Substituir identificadores sensíveis por caracteres fictícios, mas realistas, para proteger a privacidade

2 Pergunta 2

Resposta correta: A

NOTA PARA O PROFESSOR

Que mecanismo encripta os ficheiros guardados no disco rígido de um servidor de base de dados? → Encriptação de disco completo em repouso

3 Pergunta 3

Resposta correta: A

NOTA PARA O PROFESSOR

O que representa os dados em trânsito? → Pacotes de dados a circular por routers e comutadores de rede

4 Pergunta 4

Resposta correta: A

NOTA PARA O PROFESSOR

Porque é que uma cópia de segurança offline regular é essencial para a proteção contra ransomware? → Fornece uma cópia limpa e offline para restaurar ficheiros sem pagar um resgate

5 Pergunta 5

Resposta correta: A

NOTA PARA O PROFESSOR

O que faz a tokenização de dados? → Substitui números de cartão sensíveis por tokens aleatórios não sensíveis

Soluções: Ponto de controlo 2 - Verdadeiro ou falso

6 Pergunta 6

Resposta correta: Falso

NOTA PARA O PROFESSOR

O mascaramento altera cópias de teste ou oculta valores no momento da consulta; os registos de produção permanecem inalterados.

7 Pergunta 7

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

As cópias de segurança externas devem estar isoladas da rede empresarial principal para evitar a propagação de ransomware.

8 Pergunta 8

Resposta correta: Falso

NOTA PARA O PROFESSOR

Os certificados TLS protegem os dados em trânsito; os dados em repouso precisam de encriptação de disco, de ficheiros ou de base de dados.

9 Pergunta 9

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

O Zero Trust Network Access (ZTNA) verifica a identidade de cada utilizador antes de conceder acesso à base de dados.

10 Pergunta 10

Resposta correta: Verdadeiro

NOTA PARA O PROFESSOR

A tokenização baseada em cofre guarda os valores originais num cofre de tokens seguro que associa cada token aos respetivos dados.

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

B 1. ENCRIPTAÇÃO	A 2. CÓPIA DE SEGURANÇA	H 3. MINIMIZAÇÃO	F 4. ACESSO
C 5. POSTURA	E 6. VIOLAÇÃO	D 7. CONFORMIDADE	G 8. OCULTAÇÃO

PONTO DE CONTROLO 3: SOLUÇÕES – TERMOS-CHAVE

1 MASCARAMENTO	2 EM REPOUSO	3 TRÂNSITO	4 ACESSO
5 BACKUP	6 POSTURA		

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

1 F – VIOLACAO	2 H – MASCARAMENTO	3 D – ACESSO	4 E – POSTURA
5 G – CONFORMIDADE	6 C – MINIMIZACAO	7 A – ENCRIPTACAO	8 B – BACKUP

NOTAS DE DEBATE PARA PROFESSORES

Termos-chave:
Verifica se os alunos sabem explicar ENCRIPTAÇÃO, CÓPIA DE SEGURANÇA e MINIMIZAÇÃO 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.

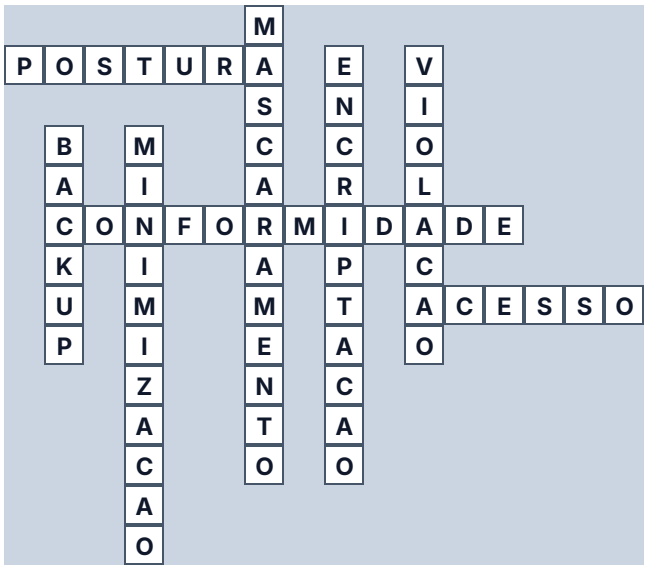
Avaliação das fontes:
Pede aos alunos que confirmem pelo menos uma afirmação nas fontes da ficha e discutam porque é que números, preços e regras podem mudar com o tempo.

Soluções dos puzzles e notas para o professor

SOLUÇÃO DO CAÇA-PALAVRAS

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

SOLUÇÃO DAS PALAVRAS CRUZADAS



GUIA DO PROFESSOR PARA AS SOLUÇÕES DAS PALAVRAS CRUZADAS

HORIZONTAIS

2 horizontal: POSTURA Estado coletivo de segurança e prontidão de defesa da cloud de uma organização (7 letras)

7 horizontal: CONFORMIDADE Cumprimento de normas regulamentares como o RGPD ou o CCPA na gestão de informação privada dos utilizadores (12 letras)

8 horizontal: ACESSO Restringir as permissões de leitura e escrita da base de dados a funções de utilizador autenticadas (6 letras)

VERTICAIS

1 vertical: MASCARAMENTO Substituição de carateres sensíveis nos campos da base de dados para proteger identidades pessoais (12 letras)

3 vertical: ENCRIPTACAO Transformar texto simples em texto cifrado ilegível para que os dados intercetados permaneçam privados (11 letras)

4 vertical: VIOLACAO Incidente de segurança em que dados protegidos são acedidos ou divulgados sem autorização (8 letras)

5 vertical: BACKUP Criação de cópias seguras externas dos dados para restauro em caso de falhas do sistema (6 letras)

6 vertical: MINIMIZACAO Limitar a recolha de dados pessoais ao mínimo absoluto necessário para as operações (11 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. ITANPAECCOR — **ENCRIPTACAO**
2. MOIMAINCAZI — **MINIMIZACAO**
3. TPUASRO — **POSTURA**
4. DIONMERADCOF — **CONFORMIDADE**
5. KCPBUA — **BACKUP**
6. SSAEOC — **ACESSO**
7. VOACAILO — **VIOLACAO**
8. MSANAOMRATEC — **MASCARAMENTO**

CHAVE DO DESAFIO DO CÓDIGO SECRETO

"PROTEGE OS TEUS DADOS COM CONTROLOS SEGUROS"

Soluções dos estudos de caso

A Estudo de caso 1: Atualização da encriptação em repouso de bases de dados empresariais

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise de cenário: Um retalhista online guarda bases de dados de transações em armazenamento na nuvem sem encriptação de disco completo. Uma auditoria de conformidade recente assinalou isto como um grave risco de segurança de dados à luz do CCPA. Concebe uma arquitetura de recuperação.
- Estratégia e solução recomendadas: Implementar encriptação de disco completo AES-256 em repouso em todos os sistemas de ficheiros. Usar um Key Management Service (KMS) centralizado com rotação automática e aplicar políticas IAM rigorosas para controlar o acesso à desencriptação.

B Estudo de caso 2: Contenção de ransomware e restauro de dados

Solução para o professor

CRITÉRIO DE CLASSIFICAÇÃO

As respostas dos alunos devem abranger os seguintes pontos:

- Análise do cenário: Um ataque de ransomware ativo está a encriptar unidades de rede numa rede local empresarial. O administrador detetou a infeção cedo. Planeia os passos de contenção e recuperação.
- Estratégia e solução recomendadas: Isolar imediatamente o segmento comprometido. Formatar os pontos finais afetados e restaurar a partir da cópia de segurança offline WORM (write-once-read-many) mais recente. Verificar a integridade da cópia antes de voltar a ligar os sistemas.