

## **Aula 07**

*TJ-PR (Técnico Judiciário) Passo  
Estratégico de Informática - 2025  
(Pós-Edital)*

Autor:  
**Diego Carvalho**

20 de Agosto de 2025

# Índice

1) Simulado - Segurança da Informação .....	3
2) Simulado - Malwares .....	16
3) Simulado - MS-Excel .....	32



## SIMULADO – SEGURANÇA DA INFORMAÇÃO

### 1. Sobre os princípios de segurança da informação, analise as afirmativas a seguir e escolha a alternativa correta:

- a) A integridade garante que a informação não seja acessada por entidades não autorizadas.
- b) A confidencialidade assegura que os dados transmitidos não sejam alterados durante o processo.
- c) A disponibilidade garante que a informação esteja acessível quando necessária por uma entidade autorizada.
- d) A autenticidade garante que um sistema permaneça operacional, mesmo em caso de falha.
- e) O princípio da irretratabilidade visa garantir que o usuário possa modificar livremente as informações.

### 2. Em relação aos controles de segurança, qual das alternativas abaixo descreve corretamente a diferença entre controles físicos e lógicos?

- a) Controles físicos protegem informações por meio de software, enquanto os controles lógicos utilizam barreiras físicas para impedir acesso.
- b) Controles físicos e lógicos sempre atuam simultaneamente para garantir a proteção de informações.
- c) Controles lógicos limitam o acesso a sistemas de computação, enquanto controles físicos protegem a infraestrutura que contém as informações.
- d) Controles lógicos utilizam trancas, cadeados e vigilantes, enquanto controles físicos empregam criptografia e biometria.
- e) Controles físicos são específicos para ambientes de rede e controles lógicos são usados em ambientes físicos.

### 3. Sobre a Criptografia Simétrica, qual das alternativas abaixo está correta?

- a) A criptografia simétrica utiliza duas chaves: uma pública e outra privada, garantindo autenticidade e confidencialidade.
- b) A criptografia simétrica garante tanto confidencialidade quanto integridade dos dados transmitidos.
- c) Um dos desafios da criptografia simétrica é a necessidade de trocar as chaves de forma segura entre as partes.
- d) O algoritmo RSA é um exemplo de criptografia simétrica, amplamente utilizado em assinaturas digitais.



e) A Criptografia Simétrica é mais lenta e complexa que a Criptografia Assimétrica.

#### **4. Em relação à Criptografia Assimétrica, qual afirmativa está incorreta?**

- a) A Criptografia Assimétrica utiliza duas chaves distintas: uma pública e outra privada.
- b) A chave pública é compartilhada livremente, enquanto a chave privada é mantida em sigilo.
- c) A Criptografia Assimétrica é geralmente mais lenta que a Criptografia Simétrica.
- d) O algoritmo RSA é um exemplo de criptografia assimétrica.
- e) A Criptografia Assimétrica não garante o princípio da autenticidade.

#### **5. Sobre as técnicas criptográficas, identifique a alternativa que descreve corretamente a Criptografia Híbrida:**

- a) A Criptografia Híbrida combina algoritmos de criptografia assimétrica para gerar chaves de sessão para comunicação segura.
- b) A Criptografia Híbrida utiliza apenas algoritmos simétricos e é empregada principalmente em redes locais.
- c) A Criptografia Híbrida é exclusivamente voltada para garantir autenticidade e não emprega criptografia simétrica.
- d) A Criptografia Híbrida combina algoritmos simétricos e assimétricos, sendo a assimétrica utilizada para troca de chaves seguras.
- e) A Criptografia Híbrida não é usada em protocolos de segurança modernos como o SSL.

#### **6. A respeito dos métodos de autenticação, considere as alternativas abaixo. Qual delas descreve corretamente o funcionamento da autenticação baseada no que você é?**

- a) A autenticação baseada no que você é utiliza informações sensíveis como senhas e tokens que devem ser memorizados e gerados pelo usuário, visando maior segurança e integridade dos dados.
- b) Esse método de autenticação envolve a utilização de características físicas únicas de uma pessoa, como impressões digitais ou padrões de retina, que são extremamente difíceis de serem replicadas por terceiros.
- c) No processo de autenticação baseado no que você é, são utilizados cartões inteligentes ou tokens que possuem um microprocessador, garantindo que apenas o usuário com o objeto correto possa acessar o sistema.
- d) A autenticação baseada no que você é depende exclusivamente da combinação de senhas fortes e verificações em duas etapas para garantir a autenticidade do usuário no sistema de informação.



e) Esse método depende principalmente da localização do usuário, identificando sua presença física em determinado local para permitir o acesso a informações e dados confidenciais.

## **7. Sobre as características e aplicação de algoritmos de hash, escolha a alternativa correta.**

a) Os algoritmos de hash transformam dados de qualquer tamanho em uma saída de tamanho variável, podendo variar conforme o tipo de entrada e a complexidade do documento.

b) Uma das principais vulnerabilidades dos algoritmos de hash é que diferentes entradas podem sempre gerar a mesma saída, o que impossibilita a utilização desses algoritmos em assinaturas digitais.

c) Algoritmos de hash são bidirecionais, permitindo que, a partir de uma saída, seja possível reconstruir a entrada original, facilitando o processo de auditoria e verificação de autenticidade.

d) O algoritmo de hash, como o MD5, recebe uma entrada de dados de qualquer tamanho e gera uma saída de tamanho fixo. Mesmo pequenas alterações na entrada resultam em uma mudança significativa na saída.

e) A função hash é utilizada para garantir a confidencialidade da mensagem ao transformá-la em um dado cifrado, impossibilitando qualquer pessoa de verificar a integridade sem descriptografá-la.

## **8. Qual das opções a seguir descreve corretamente o processo de autenticação forte?**

a) A autenticação forte é realizada quando se utiliza um único método de autenticação, como a combinação de nome de usuário e senha, garantindo uma camada extra de segurança ao processo.

b) Trata-se de uma autenticação que utiliza dois métodos de autenticação distintos, como algo que você sabe (senha) e algo que você tem (celular), tornando mais difícil que um atacante tenha acesso a ambos.

c) A autenticação forte baseia-se exclusivamente no uso de tokens físicos e certificados digitais para validar o acesso de usuários a sistemas sensíveis e de alta segurança, garantindo a exclusividade.

d) O uso de biometria associada a senhas é o único método de autenticação considerado forte, visto que esses dois fatores garantem a proteção dos dados e a integridade do usuário autenticado.

e) Nesse processo, o sistema baseia-se principalmente no local físico do usuário, utilizando dispositivos de geolocalização para verificar se o usuário está no lugar correto para acessar os recursos.



**9. Em relação à assinatura digital e o uso da criptografia assimétrica, assinale a alternativa correta:**

- a) A assinatura digital utiliza apenas algoritmos de hash para garantir a confidencialidade da mensagem, impedindo que terceiros visualizem o conteúdo transmitido, sendo amplamente utilizada para criptografar documentos sensíveis.
- b) A criptografia assimétrica é aplicada exclusivamente para garantir a integridade da mensagem. O uso da chave pública serve para verificar se a mensagem não foi alterada durante sua transmissão.
- c) No processo de assinatura digital, a chave privada é utilizada para criptografar o hash da mensagem, garantindo a autenticidade e a integridade, permitindo que o destinatário a verifique com a chave pública.
- d) Assinaturas digitais visam garantir apenas a autenticidade de um documento, não sendo capazes de assegurar a integridade ou irretratabilidade, uma vez que o processo de verificação depende do conteúdo da mensagem.
- e) A assinatura digital com base em hash exige o uso de algoritmos como SHA-1 ou MD5 para criptografar o conteúdo integral da mensagem, garantindo que o destinatário possa verificar a confidencialidade do documento.

**10. Qual das opções descreve corretamente o papel de uma Autoridade Certificadora (AC) no contexto de certificados digitais?**

- a) Uma AC emite e gerencia certificados digitais e está autorizada a revogar certificados, mas não possui a capacidade de assinar digitalmente outros certificados.
- b) Uma AC verifica se o titular do certificado possui a chave privada correspondente à chave pública, assina digitalmente o certificado e o revoga quando necessário.
- c) A AC é responsável apenas pela emissão de certificados digitais, enquanto a revogação e verificação são realizadas por entidades externas como Autoridades de Registro (AR).
- d) A AC é hierarquicamente superior às Autoridades de Registro (AR), e estas têm total autonomia para emitir e revogar certificados digitais sem a supervisão da AC.
- e) A AC é responsável pela criação de chaves públicas e privadas dos usuários e pela autenticação de transações financeiras, mas não desempenha papel na emissão de certificados.



## SIMULADO COMENTADO – SEGURANÇA DA INFORMAÇÃO

### 1. Sobre os princípios de segurança da informação, analise as afirmativas a seguir e escolha a alternativa correta:

- a) A integridade garante que a informação não seja acessada por entidades não autorizadas.
- b) A confidencialidade assegura que os dados transmitidos não sejam alterados durante o processo.
- c) A disponibilidade garante que a informação esteja acessível quando necessária por uma entidade autorizada.
- d) A autenticidade garante que um sistema permaneça operacional, mesmo em caso de falha.
- e) O princípio da irretratabilidade visa garantir que o usuário possa modificar livremente as informações.

#### Comentário:

- (a) Errado. A integridade garante que a informação não seja alterada, não que seja inacessível a entidades não autorizadas, o que é responsabilidade da confidencialidade;
- (b) Errado. A confidencialidade garante que a informação não seja acessada por entidades não autorizadas, enquanto a integridade assegura que os dados não sejam alterados;
- (c) Correto. A disponibilidade garante que a informação ou o sistema esteja acessível para entidades autorizadas quando necessário;
- (d) Errado. A autenticidade refere-se à confirmação da identidade de uma entidade, não à operação do sistema;
- (e) Errado. O princípio da irretratabilidade (ou não repúdio) visa garantir que uma ação, como a assinatura de um documento, não possa ser negada ou desmentida posteriormente.

**Gabarito:** Letra C

### 2. Em relação aos controles de segurança, qual das alternativas abaixo descreve corretamente a diferença entre controles físicos e lógicos?

- a) Controles físicos protegem informações por meio de software, enquanto os controles lógicos utilizam barreiras físicas para impedir acesso.
- b) Controles físicos e lógicos sempre atuam simultaneamente para garantir a proteção de informações.



- c) Controles lógicos limitam o acesso a sistemas de computação, enquanto controles físicos protegem a infraestrutura que contém as informações.
- d) Controles lógicos utilizam trancas, cadeados e vigilantes, enquanto controles físicos empregam criptografia e biometria.
- e) Controles físicos são específicos para ambientes de rede e controles lógicos são usados em ambientes físicos.

#### Comentário:

- (a) Errado. Controles físicos utilizam barreiras físicas, como portas e câmeras de segurança, enquanto controles lógicos usam software para proteger informações, como firewalls e criptografia;
- (b) Errado. Embora possam atuar juntos, não é obrigatório que controles físicos e lógicos atuem simultaneamente;
- (c) Correto. Controles lógicos limitam o acesso a sistemas computacionais, e os controles físicos protegem a infraestrutura, como servidores e equipamentos;
- (d) Errado. Trancas e cadeados são controles físicos, enquanto criptografia e biometria são controles lógicos;
- (e) Errado. Ambos os tipos de controle podem ser aplicados tanto em ambientes físicos quanto digitais.

**Gabarito:** Letra C

### 3. Sobre a Criptografia Simétrica, qual das alternativas abaixo está correta?

- a) A criptografia simétrica utiliza duas chaves: uma pública e outra privada, garantindo autenticidade e confidencialidade.
- b) A criptografia simétrica garante tanto confidencialidade quanto integridade dos dados transmitidos.
- c) Um dos desafios da criptografia simétrica é a necessidade de trocar as chaves de forma segura entre as partes.
- d) O algoritmo RSA é um exemplo de criptografia simétrica, amplamente utilizado em assinaturas digitais.
- e) A Criptografia Simétrica é mais lenta e complexa que a Criptografia Assimétrica.

#### Comentário:

- (a) Errado. A criptografia simétrica utiliza uma única chave secreta compartilhada entre as partes, não duas chaves (pública e privada), que são características da criptografia assimétrica;





- (b) Errado. A criptografia simétrica garante a confidencialidade, mas não necessariamente a integridade dos dados, que é uma função adicional;
- (c) Correto. Um dos principais desafios da criptografia simétrica é a necessidade de trocar a chave secreta de forma segura entre as partes envolvidas;
- (d) Errado. O RSA é um exemplo de criptografia assimétrica, não simétrica;
- (e) Errado. A criptografia simétrica é geralmente mais rápida e menos complexa do que a criptografia assimétrica.

**Gabarito:** Letra C

#### 4. Em relação à Criptografia Assimétrica, qual afirmativa está incorreta?

- a) A Criptografia Assimétrica utiliza duas chaves distintas: uma pública e outra privada.
- b) A chave pública é compartilhada livremente, enquanto a chave privada é mantida em sigilo.
- c) A Criptografia Assimétrica é geralmente mais lenta que a Criptografia Simétrica.
- d) O algoritmo RSA é um exemplo de criptografia assimétrica.
- e) A Criptografia Assimétrica não garante o princípio da autenticidade.

#### Comentário:

- (a) Correto. A criptografia assimétrica usa um par de chaves: uma pública e outra privada, que são diferentes entre si;
- (b) Correto. A chave pública é compartilhada, e a chave privada deve ser mantida secreta pelo proprietário;
- (c) Correto. A criptografia assimétrica é, de fato, mais lenta que a simétrica devido à complexidade dos cálculos envolvidos;
- (d) Correto. O algoritmo RSA é amplamente utilizado como um exemplo de criptografia assimétrica;
- (e) Incorreto. A criptografia assimétrica pode garantir autenticidade, especialmente em assinaturas digitais, onde a chave privada é usada para gerar a assinatura, e a chave pública é usada para verificá-la.

**Gabarito:** Letra E

#### 5. Sobre as técnicas criptográficas, identifique a alternativa que descreve corretamente a Criptografia Híbrida:

- a) A Criptografia Híbrida combina algoritmos de criptografia assimétrica para gerar chaves de sessão para comunicação segura.



- b) A Criptografia Híbrida utiliza apenas algoritmos simétricos e é empregada principalmente em redes locais.
- c) A Criptografia Híbrida é exclusivamente voltada para garantir autenticidade e não emprega criptografia simétrica.
- d) A Criptografia Híbrida combina algoritmos simétricos e assimétricos, sendo a assimétrica utilizada para troca de chaves seguras.
- e) A Criptografia Híbrida não é usada em protocolos de segurança modernos como o SSL.

### Comentário:

- (a) Errado. A criptografia híbrida utiliza algoritmos assimétricos e simétricos, mas a chave de sessão usada para comunicação segura é criptografada com um algoritmo assimétrico, e não gerada por ele;
- (b) Errado. A criptografia híbrida combina algoritmos simétricos e assimétricos, e não utiliza apenas algoritmos simétricos;
- (c) Errado. A criptografia híbrida usa tanto criptografia simétrica quanto assimétrica e pode garantir tanto autenticidade quanto confidencialidade;
- (d) Correto. A criptografia híbrida combina algoritmos simétricos (para criptografia de dados) e assimétricos (para troca segura de chaves de sessão);
- (e) Errado. A criptografia híbrida é amplamente utilizada em protocolos modernos como SSL e TLS.

**Gabarito:** Letra D

### 6. A respeito dos métodos de autenticação, considere as alternativas abaixo. Qual delas descreve corretamente o funcionamento da autenticação baseada no que você é?

- a) A autenticação baseada no que você é utiliza informações sensíveis como senhas e tokens que devem ser memorizados e gerados pelo usuário, visando maior segurança e integridade dos dados.
- b) Esse método de autenticação envolve a utilização de características físicas únicas de uma pessoa, como impressões digitais ou padrões de retina, que são extremamente difíceis de serem replicadas por terceiros.
- c) No processo de autenticação baseado no que você é, são utilizados cartões inteligentes ou tokens que possuem um microprocessador, garantindo que apenas o usuário com o objeto correto possa acessar o sistema.



d) A autenticação baseada no que você é depende exclusivamente da combinação de senhas fortes e verificações em duas etapas para garantir a autenticidade do usuário no sistema de informação.

e) Esse método depende principalmente da localização do usuário, identificando sua presença física em determinado local para permitir o acesso a informações e dados confidenciais.

### Comentário:

(a) Errado. A autenticação baseada no que você é utiliza características biométricas, não senhas ou tokens, que são usados em outros métodos de autenticação;

(b) Correto. A autenticação baseada no que você é refere-se a características físicas únicas, como impressões digitais e padrões de retina, difíceis de serem falsificados;

(c) Errado. Cartões inteligentes e tokens estão relacionados à autenticação baseada no que você tem, não no que você é;

(d) Errado. A combinação de senhas fortes e verificações em duas etapas está relacionada a outros métodos de autenticação, como o que você sabe e o que você tem;

(e) Errado. A autenticação baseada na localização refere-se ao método de "onde você está", não ao que você é.

**Gabarito:** Letra B

## 7. Sobre as características e aplicação de algoritmos de hash, escolha a alternativa correta.

a) Os algoritmos de hash transformam dados de qualquer tamanho em uma saída de tamanho variável, podendo variar conforme o tipo de entrada e a complexidade do documento.

b) Uma das principais vulnerabilidades dos algoritmos de hash é que diferentes entradas podem sempre gerar a mesma saída, o que impossibilita a utilização desses algoritmos em assinaturas digitais.

c) Algoritmos de hash são bidirecionais, permitindo que, a partir de uma saída, seja possível reconstruir a entrada original, facilitando o processo de auditoria e verificação de autenticidade.

d) O algoritmo de hash, como o MD5, recebe uma entrada de dados de qualquer tamanho e gera uma saída de tamanho fixo. Mesmo pequenas alterações na entrada resultam em uma mudança significativa na saída.

e) A função hash é utilizada para garantir a confidencialidade da mensagem ao transformá-la em um dado cifrado, impossibilitando qualquer pessoa de verificar a integridade sem descriptografá-la.



### Comentário:

- (a) Errado. Os algoritmos de hash geram uma saída de tamanho fixo, independentemente do tamanho da entrada de dados;
- (b) Errado. A principal vulnerabilidade são as colisões (duas entradas diferentes gerando a mesma saída), mas isso não ocorre "sempre". Além disso, algoritmos de hash são amplamente utilizados em assinaturas digitais;
- (c) Errado. Algoritmos de hash são unidirecionais, ou seja, não é possível reconstruir a entrada a partir da saída;
- (d) Correto. Algoritmos de hash, como o MD5, geram uma saída de tamanho fixo e uma pequena mudança na entrada resulta em uma saída completamente diferente (efeito avalanche);
- (e) Errado. A função hash não garante confidencialidade, mas sim integridade, permitindo verificar se os dados foram alterados.

**Gabarito:** Letra D

### 8. Qual das opções a seguir descreve corretamente o processo de autenticação forte?

- a) A autenticação forte é realizada quando se utiliza um único método de autenticação, como a combinação de nome de usuário e senha, garantindo uma camada extra de segurança ao processo.
- b) Trata-se de uma autenticação que utiliza dois métodos de autenticação distintos, como algo que você sabe (senha) e algo que você tem (celular), tornando mais difícil que um atacante tenha acesso a ambos.
- c) A autenticação forte baseia-se exclusivamente no uso de tokens físicos e certificados digitais para validar o acesso de usuários a sistemas sensíveis e de alta segurança, garantindo a exclusividade.
- d) O uso de biometria associada a senhas é o único método de autenticação considerado forte, visto que esses dois fatores garantem a proteção dos dados e a integridade do usuário autenticado.
- e) Nesse processo, o sistema baseia-se principalmente no local físico do usuário, utilizando dispositivos de geolocalização para verificar se o usuário está no lugar correto para acessar os recursos.

### Comentário:

- (a) Errado. A utilização de um único método de autenticação, como senha, não caracteriza autenticação forte, que requer múltiplos fatores;



- (b) Correto. A autenticação forte utiliza dois ou mais fatores distintos, como algo que você sabe (senha) e algo que você tem (celular), dificultando o acesso para atacantes;
- (c) Errado. Embora tokens físicos e certificados digitais possam ser usados, a autenticação forte não se limita a esses métodos;
- (d) Errado. A combinação de biometria e senhas é um método eficaz, mas não é o único método de autenticação forte;
- (e) Errado. A geolocalização pode ser um fator adicional, mas, sozinha, não caracteriza a autenticação forte.

**Gabarito:** Letra B

**9. Em relação à assinatura digital e o uso da criptografia assimétrica, assinale a alternativa correta:**

- a) A assinatura digital utiliza apenas algoritmos de hash para garantir a confidencialidade da mensagem, impedindo que terceiros visualizem o conteúdo transmitido, sendo amplamente utilizada para criptografar documentos sensíveis.
- b) A criptografia assimétrica é aplicada exclusivamente para garantir a integridade da mensagem. O uso da chave pública serve para verificar se a mensagem não foi alterada durante sua transmissão.
- c) No processo de assinatura digital, a chave privada é utilizada para criptografar o hash da mensagem, garantindo a autenticidade e a integridade, permitindo que o destinatário a verifique com a chave pública.
- d) Assinaturas digitais visam garantir apenas a autenticidade de um documento, não sendo capazes de assegurar a integridade ou irretratabilidade, uma vez que o processo de verificação depende do conteúdo da mensagem.
- e) A assinatura digital com base em hash exige o uso de algoritmos como SHA-1 ou MD5 para criptografar o conteúdo integral da mensagem, garantindo que o destinatário possa verificar a confidencialidade do documento.

**Comentário:**

- (a) Errado. A assinatura digital utiliza algoritmos de hash para garantir integridade, e a criptografia assimétrica para garantir autenticidade e não repúdio, não confidencialidade;
- (b) Errado. A criptografia assimétrica é usada para garantir autenticidade, integridade e não repúdio, não apenas integridade;
- (c) Correto. No processo de assinatura digital, a chave privada é usada para criptografar o hash da mensagem, garantindo autenticidade e integridade, enquanto a chave pública permite a verificação da assinatura;



- (d) Errado. Assinaturas digitais garantem autenticidade, integridade e não repúdio, não apenas autenticidade;
- (e) Errado. O hash não criptografa o conteúdo da mensagem, e a assinatura digital não garante confidencialidade, mas sim integridade e autenticidade.

**Gabarito:** Letra C

**10. Qual das opções descreve corretamente o papel de uma Autoridade Certificadora (AC) no contexto de certificados digitais?**

- a) Uma AC emite e gerencia certificados digitais e está autorizada a revogar certificados, mas não possui a capacidade de assinar digitalmente outros certificados.
- b) Uma AC verifica se o titular do certificado possui a chave privada correspondente à chave pública, assina digitalmente o certificado e o revoga quando necessário.
- c) A AC é responsável apenas pela emissão de certificados digitais, enquanto a revogação e verificação são realizadas por entidades externas como Autoridades de Registro (AR).
- d) A AC é hierarquicamente superior às Autoridades de Registro (AR), e estas têm total autonomia para emitir e revogar certificados digitais sem a supervisão da AC.
- e) A AC é responsável pela criação de chaves públicas e privadas dos usuários e pela autenticação de transações financeiras, mas não desempenha papel na emissão de certificados.

**Comentário:**

- (a) Errado. A Autoridade Certificadora (AC) tem a capacidade de assinar digitalmente outros certificados e também gerenciá-los e revogá-los quando necessário;
- (b) Correto. A AC verifica a posse da chave privada correspondente à chave pública, assina digitalmente o certificado e também pode revogá-lo se necessário;
- (c) Errado. A AC é responsável pela emissão e revogação de certificados digitais, enquanto a Autoridade de Registro (AR) auxilia na verificação e identificação dos solicitantes;
- (d) Errado. As Autoridades de Registro (AR) não têm autonomia para emitir ou revogar certificados sem a supervisão da AC;
- (e) Errado. A AC não cria chaves públicas e privadas para os usuários, mas valida e emite certificados digitais para garantir a autenticidade das chaves.

**Gabarito:** Letra B



## GABARITO – SEGURANÇA DA INFORMAÇÃO

1. LETRA C
2. LETRA C
3. LETRA C
4. LETRA E
5. LETRA D
6. LETRA B
7. LETRA D
8. LETRA B
9. LETRA C
10. LETRA B



## SIMULADO – MALWARES

**1. Os vírus de computador se propagam de diversas formas e podem causar grandes danos ao sistema infectado. Qual das alternativas a seguir descreve corretamente o comportamento e as características de um vírus de computador?**

- a) Um vírus é autossuficiente, podendo se propagar pela rede sem depender da execução de um arquivo hospedeiro, tornando-o similar a um worm.
- b) O vírus realiza duas tarefas principais: primeiro, replica-se para outros programas, depois executa seu código malicioso, que pode variar desde exibir uma mensagem na tela até destruir arquivos do sistema.
- c) O vírus se instala na MBR (Master Boot Record) de dispositivos de armazenamento, sendo ativado apenas na inicialização do sistema e infectando arquivos executáveis somente após o carregamento do sistema operacional.
- d) Vírus de script são sempre benignos, executando funcionalidades limitadas e inofensivas em arquivos como macros do Excel e não representando risco significativo à integridade dos dados do sistema infectado.
- e) Todos os vírus têm as mesmas características e operam independentemente do sistema operacional, sendo igualmente destrutivos em qualquer plataforma, como Windows, Linux e Mac OS.

**2. Sobre as diferentes formas de infecção e propagação de malwares, qual alternativa está correta?**

- a) Malware se propaga apenas por mídias físicas, como pendrives, sendo impossível a infecção por e-mails ou páginas da web sem interação do usuário.
- b) A infecção por malwares ocorre exclusivamente quando um arquivo infectado é baixado e executado diretamente pelo usuário, sem a necessidade de o computador estar vulnerável.
- c) Um dos principais vetores de infecção é a execução de arquivos infectados obtidos por meio de anexos de e-mails, mídias removíveis, redes sociais ou páginas web comprometidas, e eles podem ser ativados ao abrir o arquivo.
- d) O malware só é capaz de infectar o sistema operacional quando executado em modo de segurança, pois o antivírus fica desabilitado nesse modo e não pode detectar a infecção em tempo real.
- e) A infecção por malware ocorre apenas em sistemas Windows, já que sistemas como Linux e Mac OS são completamente imunes a vírus e outros códigos maliciosos.





**3. Considerando os diferentes tipos de spyware, qual das alternativas abaixo descreve corretamente a funcionalidade de um spyware?**

- a) Spywares têm como principal objetivo infectar arquivos executáveis e impedir que o sistema operacional seja inicializado corretamente, similar aos vírus de boot, sendo que a coleta de informações do usuário é uma ação secundária.
- b) Spywares, como keyloggers e screenloggers, são utilizados para monitorar a atividade do usuário, capturando dados como teclas digitadas ou imagens da tela, e enviam essas informações a um atacante sem o conhecimento do usuário.
- c) Ao contrário de outros malwares, os spywares não comprometem a privacidade dos dados do usuário, sendo usados apenas para fins publicitários, como a exibição de anúncios e promoções por meio de pop-ups ou banners.
- d) Um spyware precisa sempre ser instalado manualmente pelo usuário, sem exceções, e sua função primária é permitir o acesso remoto a dados sensíveis do sistema infectado, tornando-o vulnerável a ataques diretos.
- e) Spywares não necessitam da execução explícita de um arquivo para serem instalados no sistema e, diferentemente de adwares, não utilizam a navegação do usuário para coletar informações e exibir propagandas.

**4. Considerando as fases de execução de um vírus, qual das alternativas descreve corretamente a sequência e o funcionamento de cada fase?**

- a) A fase de dormência ocorre após a propagação e ativação, sendo o momento em que o vírus entra em repouso, aguardando a ação do antivírus para continuar a infecção no sistema.
- b) Na fase de propagação, o vírus infecta arquivos específicos de segurança, como firewalls e antivírus, antes de replicar-se para outros sistemas, garantindo maior dificuldade de detecção.
- c) A fase de ativação ocorre quando o vírus se replica para outros programas, contaminando arquivos do sistema sem realizar qualquer ação até a presença de outro malware no sistema infectado.
- d) Na fase de ação, o vírus executa sua carga útil, que pode variar de ações benignas, como exibir mensagens na tela, até ações destrutivas, como apagar arquivos essenciais do disco rígido.
- e) Vírus passam diretamente da fase de dormência para a fase de ação, sem a necessidade de propagação, infectando o sistema por meio de atualizações automáticas de softwares instalados.

**5. O worm é um malware autorreplicante que se propaga de forma automática entre computadores. Qual das alternativas descreve corretamente o comportamento e o processo de infecção de um worm?**



- a) Worms precisam de interação direta do usuário para se replicar, infectando arquivos executáveis no sistema para garantir a continuidade de sua propagação, semelhante aos vírus tradicionais.
- b) Worms são capazes de explorar vulnerabilidades em programas instalados, propagando-se automaticamente entre computadores na rede, consumindo muitos recursos e degradando o desempenho, sem precisar de um arquivo hospedeiro.
- c) O worm é incapaz de se replicar por conta própria e depende de ataques direcionados realizados por hackers para se espalhar, atacando sistemas exclusivamente por meio de mensagens de phishing e anexos de e-mails.
- d) Um worm se instala em programas já existentes no sistema, agindo apenas após a execução do programa hospedeiro, e, diferentemente dos vírus, não afeta diretamente o desempenho da rede ou o consumo de recursos.
- e) Worms infectam sistemas através de mídias removíveis, exigindo a presença de um programa antivírus desatualizado para se propagar, o que limita sua ação a máquinas que não estão conectadas à internet.

**6. Sobre os Bots e Botnets, qual alternativa descreve corretamente seu funcionamento e as ações que podem ser realizadas por uma Botnet?**

- a) Bots são incapazes de replicar-se automaticamente, dependendo de outros tipos de malware para serem instalados. Eles não realizam ações maliciosas diretamente, mas fornecem informações sobre vulnerabilidades.
- b) Um Botnet é formado por zumbis, computadores controlados remotamente, usados para coordenar ataques distribuídos, enviar spam, e furtar dados sem o conhecimento do usuário. A potência da Botnet depende do número de zumbis conectados.
- c) Bots são exclusivamente utilizados para ataques de negação de serviço (DoS), sendo incapazes de coletar informações sensíveis ou enviar spam. Sua principal função é derrubar servidores web.
- d) Ao contrário dos Worms, Bots necessitam ser instalados diretamente pelo usuário, já que não possuem mecanismos de propagação automática e só podem se comunicar com o atacante via e-mails.
- e) Botnets são redes autônomas que não necessitam de um controlador, funcionando de forma independente e desorganizada, apenas propagando spam e vírus sem ações coordenadas específicas.

**7. Os Trojans são malwares que agem de forma disfarçada, executando funções maliciosas sem o conhecimento do usuário. Qual das alternativas descreve corretamente as características de um Trojan Horse?**



- a) Trojans são semelhantes a Worms na medida em que não precisam ser executados pelo usuário e podem se propagar automaticamente pela rede, instalando-se em outros computadores sem interação.
- b) Trojans se disfarçam de programas úteis, mas, ao serem executados, podem abrir portas para que o invasor controle remotamente o computador ou instale outros malwares, como backdoors e spyware.
- c) Ao contrário de outros malwares, Trojans são incapazes de coletar informações sensíveis, sendo usados apenas para desferir ataques de negação de serviço ou corromper arquivos do sistema.
- d) A principal forma de infecção de um Trojan é por meio da autoexecução em redes sociais ou compartilhamento de arquivos em nuvem, replicando-se automaticamente como os Worms.
- e) Trojans são inofensivos enquanto não são acionados por uma data específica, sendo programados para ativar-se apenas após uma condição de tempo, o que os diferencia de vírus e Worms.

**8. Ransomwares têm se tornado uma ameaça crescente, com diferentes tipos capazes de bloquear o acesso a dados do usuário. Qual das alternativas descreve corretamente o funcionamento de um ransomware e as melhores práticas para proteção?**

- a) Ransomware Locker impede apenas o acesso à rede, sem afetar o acesso local ao sistema operacional ou aos arquivos armazenados. Ele só pode ser removido formatando o disco rígido do computador.
- b) O Ransomware Crypto criptografa os arquivos do usuário, impedindo o acesso a dados críticos, e o pagamento do resgate não garante a devolução dos dados. Fazer backups regularmente é uma das principais estratégias de proteção.
- c) Ransomwares são incapazes de afetar sistemas conectados à nuvem ou dispositivos em rede, já que sua propagação é limitada a um único computador local, e eles não utilizam criptografia para bloquear arquivos.
- d) A propagação de Ransomware ocorre exclusivamente por meio de e-mails, e o uso de antivírus atualizado é suficiente para garantir a proteção completa contra esse tipo de ameaça, sem necessidade de backups frequentes.
- e) Uma vez infectado por um Ransomware, o pagamento do resgate é sempre a maneira mais eficaz de garantir a recuperação dos dados, pois os atacantes devolvem o acesso imediatamente após o pagamento.

**9. Sobre as características e funcionamento de um Trojan Horse, qual alternativa está correta?**



- a) Um Trojan Horse, ao contrário dos vírus, se replica automaticamente pela rede e precisa de um programa hospedeiro para se propagar, inserindo cópias de si mesmo em outros arquivos e infectando o sistema sem a interação do usuário.
- b) Diferente dos bots, os trojans não permitem acesso remoto ao computador infectado, funcionando apenas para a destruição de dados ou alteração de configurações sem possibilitar o controle externo pelo atacante.
- c) O Trojan Horse se disfarça como um software legítimo ou útil, mas contém funções maliciosas ocultas que são executadas sem o conhecimento do usuário, possibilitando o acesso remoto ao sistema e a coleta de dados confidenciais.
- d) Trojans são especialmente projetados para infectar sistemas operacionais específicos, como Windows, e são incapazes de infectar dispositivos que utilizam sistemas como Linux ou Mac OS, o que limita sua propagação.
- e) Um Trojan não pode ser distribuído por e-mails ou anexos de arquivos. Sua propagação ocorre exclusivamente por downloads automáticos em sites comprometidos, que o instalam sem a necessidade de intervenção do usuário.

**10. Phishing é um tipo de golpe que envolve a obtenção de dados pessoais e financeiros. Qual das alternativas explica corretamente o conceito e as técnicas utilizadas no phishing?**

- a) Phishing é uma técnica que consiste em ataques diretos ao servidor de e-mail do usuário, onde o atacante intercepta e altera o conteúdo de mensagens reais, solicitando dados sigilosos de forma disfarçada.
- b) Phishing se caracteriza pelo envio de mensagens que aparentam ser de instituições legítimas, como bancos, para induzir o usuário a fornecer dados confidenciais por meio de páginas falsas ou anexos maliciosos.
- c) No Phishing, o usuário é induzido a instalar malware em seu sistema por meio de mensagens de texto, e o atacante pode acessar o dispositivo remotamente após a instalação de spyware disfarçado de atualização de sistema.
- d) A principal forma de prevenção contra Phishing é manter o sistema operacional atualizado, uma vez que ataques de phishing só ocorrem em sistemas desatualizados e sem antivírus instalado.
- e) Phishing depende exclusivamente do uso de redes sociais para se propagar e tem como alvo usuários que clicam em links de anúncios falsos exibidos em suas timelines, sem envolver e-mails ou outros métodos de comunicação.



## SIMULADO COMENTADO – MALWARES

**1. Os vírus de computador se propagam de diversas formas e podem causar grandes danos ao sistema infectado. Qual das alternativas a seguir descreve corretamente o comportamento e as características de um vírus de computador?**

- a) Um vírus é autossuficiente, podendo se propagar pela rede sem depender da execução de um arquivo hospedeiro, tornando-o similar a um worm.
- b) O vírus realiza duas tarefas principais: primeiro, replica-se para outros programas, depois executa seu código malicioso, que pode variar desde exibir uma mensagem na tela até destruir arquivos do sistema.
- c) O vírus se instala na MBR (Master Boot Record) de dispositivos de armazenamento, sendo ativado apenas na inicialização do sistema e infectando arquivos executáveis somente após o carregamento do sistema operacional.
- d) Vírus de script são sempre benignos, executando funcionalidades limitadas e inofensivas em arquivos como macros do Excel e não representando risco significativo à integridade dos dados do sistema infectado.
- e) Todos os vírus têm as mesmas características e operam independentemente do sistema operacional, sendo igualmente destrutivos em qualquer plataforma, como Windows, Linux e Mac OS.

**Comentário:**

- (a) Errado. Um vírus depende da execução de um arquivo hospedeiro para se propagar. Worms, por outro lado, são autossuficientes e se propagam pela rede sem precisar de um hospedeiro;
- (b) Correto. Um vírus realiza duas tarefas principais: ele se replica para outros programas ou arquivos e, posteriormente, executa seu código malicioso, que pode causar desde efeitos leves até danos graves, como destruição de arquivos;
- (c) Errado. Embora alguns vírus possam se instalar na MBR, nem todos seguem esse comportamento. Além disso, vírus podem infectar arquivos executáveis mesmo sem atuar na MBR;
- (d) Errado. Vírus de script podem ser maliciosos e representar riscos, como a execução de macros mal-intencionadas, que podem comprometer a integridade dos dados;
- (e) Errado. Vírus têm diferentes características e dependem do sistema operacional, podendo ser mais destrutivos em determinadas plataformas.

**Gabarito:** Letra B



## 2. Sobre as diferentes formas de infecção e propagação de malwares, qual alternativa está correta?

- a) Malware se propaga apenas por mídias físicas, como pendrives, sendo impossível a infecção por e-mails ou páginas da web sem interação do usuário.
- b) A infecção por malwares ocorre exclusivamente quando um arquivo infectado é baixado e executado diretamente pelo usuário, sem a necessidade de o computador estar vulnerável.
- c) Um dos principais vetores de infecção é a execução de arquivos infectados obtidos por meio de anexos de e-mails, mídias removíveis, redes sociais ou páginas web comprometidas, e eles podem ser ativados ao abrir o arquivo.
- d) O malware só é capaz de infectar o sistema operacional quando executado em modo de segurança, pois o antivírus fica desabilitado nesse modo e não pode detectar a infecção em tempo real.
- e) A infecção por malware ocorre apenas em sistemas Windows, já que sistemas como Linux e Mac OS são completamente imunes a vírus e outros códigos maliciosos.

### Comentário:

- (a) Errado. Malware pode se propagar tanto por mídias físicas quanto por e-mails, páginas da web, downloads e outros vetores online, sem depender exclusivamente de mídias físicas;
- (b) Errado. Embora a interação do usuário seja um fator comum, malwares podem explorar vulnerabilidades do sistema sem a necessidade de execução direta pelo usuário;
- (c) Correto. Anexos de e-mails, mídias removíveis, redes sociais e páginas web comprometidas são vetores comuns de infecção. O malware pode ser ativado ao abrir um arquivo infectado, mesmo que pareça legítimo;
- (d) Errado. O modo de segurança é projetado para ajudar na remoção de malwares, pois muitos deles não são executados nesse ambiente, e o antivírus pode continuar funcionando dependendo da configuração;
- (e) Errado. Sistemas como Linux e Mac OS não são imunes a malwares, embora sejam menos visados em comparação ao Windows.

**Gabarito:** Letra C

## 3. Considerando os diferentes tipos de spyware, qual das alternativas abaixo descreve corretamente a funcionalidade de um spyware?

- a) Spywares têm como principal objetivo infectar arquivos executáveis e impedir que o sistema operacional seja inicializado corretamente, similar aos vírus de boot, sendo que a coleta de informações do usuário é uma ação secundária.



b) Spywares, como keyloggers e screenloggers, são utilizados para monitorar a atividade do usuário, capturando dados como teclas digitadas ou imagens da tela, e enviam essas informações a um atacante sem o conhecimento do usuário.

c) Ao contrário de outros malwares, os spywares não comprometem a privacidade dos dados do usuário, sendo usados apenas para fins publicitários, como a exibição de anúncios e promoções por meio de pop-ups ou banners.

d) Um spyware precisa sempre ser instalado manualmente pelo usuário, sem exceções, e sua função primária é permitir o acesso remoto a dados sensíveis do sistema infectado, tornando-o vulnerável a ataques diretos.

e) Spywares não necessitam da execução explícita de um arquivo para serem instalados no sistema e, diferentemente de adwares, não utilizam a navegação do usuário para coletar informações e exibir propagandas.

### Comentário:

(a) Errado. Spywares não têm como objetivo principal infectar arquivos executáveis ou impedir a inicialização do sistema; eles se focam em monitorar atividades e coletar informações pessoais;

(b) Correto. Spywares, como keyloggers e screenloggers, monitoram atividades do usuário, capturando informações como teclas digitadas e imagens da tela, e enviam esses dados a um atacante sem que o usuário perceba;

(c) Errado. Embora alguns spywares possam exibir anúncios (como adwares), muitos comprometem a privacidade do usuário ao coletar informações sensíveis para fins maliciosos;

(d) Errado. Spywares podem ser instalados sem a intervenção direta do usuário, por meio de downloads ocultos ou vulnerabilidades, e não dependem de instalação manual;

(e) Errado. Spywares podem ser instalados sem a execução explícita de um arquivo, mas eles frequentemente coletam informações sobre a navegação do usuário.

**Gabarito:** Letra B

### 4. Considerando as fases de execução de um vírus, qual das alternativas descreve corretamente a sequência e o funcionamento de cada fase?

a) A fase de dormência ocorre após a propagação e ativação, sendo o momento em que o vírus entra em repouso, aguardando a ação do antivírus para continuar a infecção no sistema.

b) Na fase de propagação, o vírus infecta arquivos específicos de segurança, como firewalls e antivírus, antes de replicar-se para outros sistemas, garantindo maior dificuldade de detecção.





c) A fase de ativação ocorre quando o vírus se replica para outros programas, contaminando arquivos do sistema sem realizar qualquer ação até a presença de outro malware no sistema infectado.

d) Na fase de ação, o vírus executa sua carga útil, que pode variar de ações benignas, como exibir mensagens na tela, até ações destrutivas, como apagar arquivos essenciais do disco rígido.

e) Vírus passam diretamente da fase de dormência para a fase de ação, sem a necessidade de propagação, infectando o sistema por meio de atualizações automáticas de softwares instalados.

### Comentário:

(a) Errado. A fase de dormência é opcional e não ocorre após a propagação e ativação. Nessa fase, o vírus fica inativo até que uma condição específica o acione, mas não aguarda o antivírus para continuar a infecção;

(b) Errado. Na fase de propagação, o vírus se replica e infecta arquivos ou sistemas, mas não tem como alvo principal firewalls e antivírus. Ele visa replicar-se silenciosamente para evitar detecção;

(c) Errado. Na fase de ativação, o vírus executa sua carga maliciosa com base em uma condição específica, e não apenas se replica. A replicação ocorre na fase de propagação;

(d) Correto. Na fase de ação, o vírus executa sua carga útil, que pode variar desde ações inofensivas, como exibir mensagens, até ações destrutivas, como apagar arquivos ou corromper sistemas;

(e) Errado. A fase de propagação é necessária para que o vírus se espalhe. A fase de dormência é opcional, e a infecção não ocorre apenas por meio de atualizações automáticas.

**Gabarito:** Letra D

### 5. O worm é um malware autorreplicante que se propaga de forma automática entre computadores. Qual das alternativas descreve corretamente o comportamento e o processo de infecção de um worm?

a) Worms precisam de interação direta do usuário para se replicar, infectando arquivos executáveis no sistema para garantir a continuidade de sua propagação, semelhante aos vírus tradicionais.

b) Worms são capazes de explorar vulnerabilidades em programas instalados, propagando-se automaticamente entre computadores na rede, consumindo muitos recursos e degradando o desempenho, sem precisar de um arquivo hospedeiro.

c) O worm é incapaz de se replicar por conta própria e depende de ataques direcionados realizados por hackers para se espalhar, atacando sistemas exclusivamente por meio de mensagens de phishing e anexos de e-mails.





d) Um worm se instala em programas já existentes no sistema, agindo apenas após a execução do programa hospedeiro, e, diferentemente dos vírus, não afeta diretamente o desempenho da rede ou o consumo de recursos.

e) Worms infectam sistemas através de mídias removíveis, exigindo a presença de um programa antivírus desatualizado para se propagar, o que limita sua ação a máquinas que não estão conectadas à internet.

### Comentário:

(a) Errado. Worms não dependem de interação do usuário nem de infectar arquivos executáveis para se propagar. Eles se espalham automaticamente pela rede, diferentemente dos vírus tradicionais;

(b) Correto. Worms exploram vulnerabilidades em sistemas ou redes e se propagam automaticamente entre computadores conectados, consumindo recursos e degradando o desempenho da rede, sem a necessidade de um arquivo hospedeiro;

(c) Errado. Worms se replicam por conta própria, sem a necessidade de ataques direcionados por hackers. Eles podem se espalhar automaticamente por vulnerabilidades de rede, sem depender de phishing;

(d) Errado. Worms não precisam de um programa hospedeiro para se replicar, diferentemente dos vírus, e podem impactar o desempenho da rede e dos sistemas;

(e) Errado. Embora possam ser transmitidos via mídias removíveis, worms se propagam principalmente pela rede e não dependem de programas antivírus desatualizados para sua propagação.

**Gabarito:** Letra B

### 6. Sobre os Bots e Botnets, qual alternativa descreve corretamente seu funcionamento e as ações que podem ser realizadas por uma Botnet?

a) Bots são incapazes de replicar-se automaticamente, dependendo de outros tipos de malware para serem instalados. Eles não realizam ações maliciosas diretamente, mas fornecem informações sobre vulnerabilidades.

b) Um Botnet é formado por zumbis, computadores controlados remotamente, usados para coordenar ataques distribuídos, enviar spam, e furtar dados sem o conhecimento do usuário. A potência da Botnet depende do número de zumbis conectados.

c) Bots são exclusivamente utilizados para ataques de negação de serviço (DoS), sendo incapazes de coletar informações sensíveis ou enviar spam. Sua principal função é derrubar servidores web.



d) Ao contrário dos Worms, Bots necessitam ser instalados diretamente pelo usuário, já que não possuem mecanismos de propagação automática e só podem se comunicar com o atacante via e-mails.

e) Botnets são redes autônomas que não necessitam de um controlador, funcionando de forma independente e desorganizada, apenas propagando spam e vírus sem ações coordenadas específicas.

### Comentário:

(a) Errado. Bots são instalados por meio de várias técnicas, como downloads maliciosos, mas podem se replicar automaticamente e realizar ações maliciosas diretamente, como o controle remoto de sistemas;

(b) Correto. Uma Botnet é formada por "zumbis" (computadores infectados e controlados remotamente) que são usados para coordenar ataques distribuídos, enviar spam, e furtar dados sem o conhecimento do usuário. A eficiência da Botnet aumenta com o número de zumbis conectados;

(c) Errado. Bots podem ser usados em diversas atividades maliciosas, como envio de spam, coleta de informações sensíveis, e não apenas em ataques de negação de serviço (DoS);

(d) Errado. Bots podem ser instalados automaticamente por malwares e se comunicam com o atacante via diversos canais, como servidores de comando e controle (C&C), não apenas por e-mails;

(e) Errado. Botnets são controladas remotamente por um atacante (ou controlador), que emite comandos para realizar ações coordenadas, como ataques DDoS, roubo de dados ou propagação de malware.

**Gabarito:** Letra B

### **7. Os Trojans são malwares que agem de forma disfarçada, executando funções maliciosas sem o conhecimento do usuário. Qual das alternativas descreve corretamente as características de um Trojan Horse?**

a) Trojans são semelhantes a Worms na medida em que não precisam ser executados pelo usuário e podem se propagar automaticamente pela rede, instalando-se em outros computadores sem interação.

b) Trojans se disfarçam de programas úteis, mas, ao serem executados, podem abrir portas para que o invasor controle remotamente o computador ou instale outros malwares, como backdoors e spyware.

c) Ao contrário de outros malwares, Trojans são incapazes de coletar informações sensíveis, sendo usados apenas para desferir ataques de negação de serviço ou corromper arquivos do sistema.



d) A principal forma de infecção de um Trojan é por meio da autoexecução em redes sociais ou compartilhamento de arquivos em nuvem, replicando-se automaticamente como os Worms.

e) Trojans são inofensivos enquanto não são acionados por uma data específica, sendo programados para ativar-se apenas após uma condição de tempo, o que os diferencia de vírus e Worms.

### Comentário:

(a) Errado. Ao contrário dos worms, Trojans precisam ser executados pelo usuário e não se propagam automaticamente pela rede. Eles são instalados sob o disfarce de software legítimo;

(b) Correto. Trojans se disfarçam de programas úteis ou inofensivos, mas ao serem executados, podem abrir portas para controle remoto, instalação de backdoors, spyware, e outros malwares, permitindo que um invasor tenha acesso ao sistema;

(c) Errado. Trojans são usados para uma variedade de ações maliciosas, incluindo o roubo de informações sensíveis, instalação de outros malwares e criação de backdoors, e não apenas para ataques de negação de serviço;

(d) Errado. Trojans não se replicam automaticamente. Eles geralmente são baixados ou executados manualmente, muitas vezes disfarçados como programas legítimos;

(e) Errado. Embora alguns Trojans possam ser programados para ativação em uma data específica, sua principal característica é o disfarce e não a execução baseada em condições temporais, como ocorre em outros tipos de malwares, como logic bombs.

**Gabarito:** Letra B

### 8. Ransomwares têm se tornado uma ameaça crescente, com diferentes tipos capazes de bloquear o acesso a dados do usuário. Qual das alternativas descreve corretamente o funcionamento de um ransomware e as melhores práticas para proteção?

a) Ransomware Locker impede apenas o acesso à rede, sem afetar o acesso local ao sistema operacional ou aos arquivos armazenados. Ele só pode ser removido formatando o disco rígido do computador.

b) O Ransomware Crypto criptografa os arquivos do usuário, impedindo o acesso a dados críticos, e o pagamento do resgate não garante a devolução dos dados. Fazer backups regularmente é uma das principais estratégias de proteção.

c) Ransomwares são incapazes de afetar sistemas conectados à nuvem ou dispositivos em rede, já que sua propagação é limitada a um único computador local, e eles não utilizam criptografia para bloquear arquivos.



d) A propagação de Ransomware ocorre exclusivamente por meio de e-mails, e o uso de antivírus atualizado é suficiente para garantir a proteção completa contra esse tipo de ameaça, sem necessidade de backups frequentes.

e) Uma vez infectado por um Ransomware, o pagamento do resgate é sempre a maneira mais eficaz de garantir a recuperação dos dados, pois os atacantes devolvem o acesso imediatamente após o pagamento.

### Comentário:

(a) Errado. Ransomware Locker bloqueia o acesso ao sistema operacional, mas não afeta arquivos individuais diretamente. A formatação não é a única forma de remoção, e existem ferramentas que podem ajudar a desbloquear o sistema;

(b) Correto. Ransomware Crypto criptografa os arquivos do usuário, impedindo o acesso a dados importantes. Mesmo com o pagamento do resgate, não há garantia de recuperação dos dados. A melhor prática é manter backups regulares em locais seguros e utilizar soluções de segurança atualizadas;

(c) Errado. Ransomwares podem afetar sistemas em rede ou na nuvem, e criptografam arquivos, bloqueando o acesso. Eles podem se propagar por dispositivos conectados;

(d) Errado. Embora e-mails sejam um vetor comum, ransomwares também se propagam por downloads maliciosos, vulnerabilidades de sistemas e outros métodos. Backups e medidas adicionais são essenciais para proteção;

(e) Errado. O pagamento do resgate não garante a recuperação dos dados, pois os atacantes nem sempre devolvem o acesso. A recomendação é não pagar o resgate e depender de backups e soluções de segurança.

**Gabarito:** Letra B

### 9. Sobre as características e funcionamento de um Trojan Horse, qual alternativa está correta?

a) Um Trojan Horse, ao contrário dos vírus, se replica automaticamente pela rede e precisa de um programa hospedeiro para se propagar, inserindo cópias de si mesmo em outros arquivos e infectando o sistema sem a interação do usuário.

b) Diferente dos bots, os trojans não permitem acesso remoto ao computador infectado, funcionando apenas para a destruição de dados ou alteração de configurações sem possibilitar o controle externo pelo atacante.

c) O Trojan Horse se disfarça como um software legítimo ou útil, mas contém funções maliciosas ocultas que são executadas sem o conhecimento do usuário, possibilitando o acesso remoto ao sistema e a coleta de dados confidenciais.



d) Trojans são especialmente projetados para infectar sistemas operacionais específicos, como Windows, e são incapazes de infectar dispositivos que utilizam sistemas como Linux ou Mac OS, o que limita sua propagação.

e) Um Trojan não pode ser distribuído por e-mails ou anexos de arquivos. Sua propagação ocorre exclusivamente por downloads automáticos em sites comprometidos, que o instalam sem a necessidade de intervenção do usuário.

### Comentário:

(a) Errado. Um Trojan Horse não se replica automaticamente nem depende de um programa hospedeiro, diferentemente dos vírus. Ele precisa ser executado manualmente pelo usuário e não se propaga sozinho pela rede;

(b) Errado. Muitos trojans, especialmente aqueles com backdoors, permitem acesso remoto ao computador infectado, facilitando o controle externo pelo atacante, além de outras ações maliciosas;

(c) Correto. Um Trojan Horse disfarça-se como um software legítimo, mas contém funções maliciosas que executam atividades sem o conhecimento do usuário, como o acesso remoto e a coleta de dados confidenciais;

(d) Errado. Embora trojans sejam mais comuns em sistemas Windows, eles também podem infectar outros sistemas, como Linux e Mac OS, dependendo da sua engenharia;

(e) Errado. Trojans podem ser distribuídos por e-mails, anexos ou downloads maliciosos, e não apenas por sites comprometidos. Eles geralmente requerem interação do usuário para serem instalados.

**Gabarito:** Letra C

### 10. Phishing é um tipo de golpe que envolve a obtenção de dados pessoais e financeiros. Qual das alternativas explica corretamente o conceito e as técnicas utilizadas no phishing?

a) Phishing é uma técnica que consiste em ataques diretos ao servidor de e-mail do usuário, onde o atacante intercepta e altera o conteúdo de mensagens reais, solicitando dados sigilosos de forma disfarçada.

b) Phishing se caracteriza pelo envio de mensagens que aparentam ser de instituições legítimas, como bancos, para induzir o usuário a fornecer dados confidenciais por meio de páginas falsas ou anexos maliciosos.

c) No Phishing, o usuário é induzido a instalar malware em seu sistema por meio de mensagens de texto, e o atacante pode acessar o dispositivo remotamente após a instalação de spyware disfarçado de atualização de sistema.



d) A principal forma de prevenção contra Phishing é manter o sistema operacional atualizado, uma vez que ataques de phishing só ocorrem em sistemas desatualizados e sem antivírus instalado.

e) Phishing depende exclusivamente do uso de redes sociais para se propagar e tem como alvo usuários que clicam em links de anúncios falsos exibidos em suas timelines, sem envolver e-mails ou outros métodos de comunicação.

### Comentário:

(a) Errado. Phishing não envolve ataques diretos ao servidor de e-mail, mas sim mensagens fraudulentas que tentam enganar o usuário para obter dados confidenciais;

(b) Correto. Phishing se caracteriza pelo envio de mensagens fraudulentas que se passam por instituições legítimas, como bancos, para induzir o usuário a fornecer dados confidenciais em páginas falsas ou por meio de anexos maliciosos;

(c) Errado. Embora mensagens possam conter malware, o phishing geralmente visa coletar dados pessoais ou financeiros via páginas falsas, não necessariamente instalar malware;

(d) Errado. Manter o sistema atualizado ajuda, mas a principal defesa contra phishing é a educação do usuário e o cuidado ao clicar em links e fornecer informações em páginas suspeitas;

(e) Errado. Phishing pode ocorrer por e-mails, SMS (smishing), redes sociais e outros meios, não se limita ao uso de redes sociais ou anúncios falsos.

**Gabarito:** Letra B



## GABARITO – MALWARES

1. LETRA B
2. LETRA C
3. LETRA B
4. LETRA C
5. LETRA B
6. LETRA B
7. LETRA B
8. LETRA B
9. LETRA C
10. LETRA B



## SIMULADO – MS-EXCEL

### 1. Qual das alternativas representa corretamente a diferença entre as funções INT() e TRUNCAR() ao lidar com números negativos?

- a) A função TRUNCAR() sempre arredonda o número para o inteiro mais próximo, enquanto INT() apenas descarta a parte decimal, sem arredondamento.
- b) A função INT() arredonda sempre para o número inteiro mais baixo, afastando-se do zero, enquanto TRUNCAR() apenas remove a parte decimal sem arredondar o valor, independentemente do sinal do número.
- c) Ambas as funções se comportam da mesma forma com números negativos, retornando sempre o valor absoluto do número com a parte decimal truncada.
- d) A função TRUNCAR() transforma o número em seu equivalente positivo antes de truncar, enquanto INT() mantém o sinal original ao arredondar.
- e) INT() e TRUNCAR() apresentam resultados idênticos para números negativos, pois ambas se limitam a descartar a parte decimal, sem qualquer arredondamento adicional.

### 2. A função ARRED() possui uma lógica de arredondamento particular, especialmente quando o parâmetro é negativo. Qual das alternativas descreve corretamente o processo de arredondamento com base nos múltiplos mais próximos?

- a) Quando o parâmetro é negativo, a função ARRED() sempre arredonda para o próximo múltiplo de 10, 100 ou 1000, dependendo da quantidade de dígitos fracionários a serem arredondados.
- b) Com um parâmetro negativo, ARRED() sempre arredonda para baixo, ignorando o valor fracionário e retornando o múltiplo de 10 mais próximo do número fornecido.
- c) Quando o parâmetro é negativo, ARRED() simplesmente remove a parte decimal, sem arredondar para qualquer múltiplo, o que pode resultar em perda de precisão significativa no cálculo.
- d) Ao utilizar um parâmetro negativo, a função ARRED() se comporta como a função TRUNCAR(), ignorando qualquer múltiplo e retornando o número truncado sem arredondamento.
- e) A função ARRED() arredonda para o múltiplo mais próximo de acordo com o parâmetro negativo, onde -1 arredonda para 10, -2 para 100 e assim por diante, eliminando as casas decimais e arredondando o valor ao múltiplo correspondente.

### 3. Sobre a função MOD(), que retorna o resto de uma divisão, qual das opções descreve corretamente o comportamento da função ao lidar com números negativos?





- a) A função MOD() sempre retorna o valor absoluto do resto, independentemente do sinal do divisor, assegurando que o resultado seja positivo.
- b) O comportamento da função MOD() depende exclusivamente do dividendo, ignorando o sinal do divisor, e retorna sempre um valor positivo.
- c) MOD() retorna o resto da divisão, mas o sinal do resultado será sempre o mesmo que o do divisor, mesmo quando o dividendo for negativo.
- d) Quando o divisor é negativo, a função MOD() sempre retorna um valor negativo, independentemente do sinal do dividendo, refletindo o comportamento da divisão inteira.
- e) MOD() não pode lidar com números negativos e retornará um erro quando o dividendo ou divisor tiver sinal negativo, pois a função não suporta tais operações.

**4. A função CONT.NÚM() retorna a quantidade de células que contêm números. Qual das alternativas descreve corretamente como essa função trata diferentes tipos de dados no intervalo selecionado?**

- a) A função CONT.NÚM() considera números, textos e valores booleanos, retornando o total de células preenchidas, sem diferenciar os tipos de dados contidos nas células.
- b) A função CONT.NÚM() retorna a quantidade total de células preenchidas, independentemente de conterem texto, números ou valores booleanos, desde que não estejam vazias.
- c) Ao utilizar CONT.NÚM(), células com valores booleanos são contadas como "1" se forem verdadeiras e ignoradas se forem falsas, enquanto números e textos são contabilizados normalmente.
- d) CONT.NÚM() conta apenas células que contenham números ou datas, ignorando células com texto ou booleanos, pois esses não são considerados números pela função.
- e) CONT.NÚM() contabiliza apenas as células que contêm valores booleanos, datas ou números negativos, ignorando quaisquer outros tipos de valores no intervalo especificado.

**5. A função CONT.SES() é útil para contar células que atendem a múltiplos critérios. Qual das alternativas abaixo explica corretamente o funcionamento dessa função em relação aos critérios especificados?**

- a) A função CONT.SES() retorna a quantidade de células que atendem a todos os critérios especificados nos intervalos, não contando as células que atendem apenas a um dos critérios.
- b) CONT.SES() conta as células que atendem a pelo menos um critério especificado no intervalo de valores, ignorando aquelas que não cumprem todos os critérios.



c) CONT.SES() soma os valores das células que atendem a qualquer critério dentro de um intervalo, independentemente de quantos critérios são atendidos simultaneamente.

d) CONT.SES() só considera o primeiro critério especificado, ignorando os demais, retornando a quantidade de células que atendem exclusivamente a esse critério.

e) A função CONT.SES() conta a quantidade de células que atendem apenas aos critérios de texto, ignorando critérios relacionados a números ou datas no intervalo.

**6. A função PROCV() é amplamente utilizada para localizar valores em uma tabela, com base em um valor de referência na primeira coluna de um intervalo. Qual das alternativas descreve corretamente o uso da função e o comportamento do parâmetro de exatidão?**

a) A função PROCV() localiza o valor exato apenas quando o parâmetro [Exatidão] é definido como VERDADEIRO. Caso contrário, a função retorna um valor aleatório da tabela que esteja mais próximo do valor procurado.

b) Se o parâmetro [Exatidão] for omitido, o PROCV() assume automaticamente o valor FALSO e retorna o valor mais próximo, não sendo necessário que a primeira coluna do intervalo esteja ordenada.

c) Quando o parâmetro [Exatidão] é definido como FALSO, a função retorna apenas valores exatos, independentemente de a coluna estar ou não ordenada. Se o valor não for encontrado, retornará um erro.

d) A função PROCV() retorna o valor da última coluna da matriz caso o parâmetro [Exatidão] seja definido como VERDADEIRO, mesmo que o valor procurado não esteja presente na primeira coluna do intervalo de pesquisa.

e) Definir o parâmetro [Exatidão] como VERDADEIRO permite que a função retorne o valor anterior ao valor exato encontrado, desde que a primeira coluna esteja ordenada. Se estiver desordenada, a função retornará um erro.

**7. A função PROCH() é utilizada para pesquisar um valor na linha superior de uma tabela e retornar o valor correspondente em uma linha especificada. Qual das afirmações abaixo descreve corretamente o uso dessa função?**

a) PROCH() é equivalente ao PROCV(), mas busca valores na horizontal, localizando um valor na primeira coluna e retornando o valor correspondente na linha selecionada.

b) A função PROCH() retorna um valor exato na linha selecionada, independentemente de o valor procurado estar na linha superior, desde que o parâmetro [Exatidão] seja configurado como FALSO.

c) Quando o parâmetro [Exatidão] é definido como VERDADEIRO, a função PROCH() pode retornar o valor mais próximo ao procurado na linha superior, contanto que os dados estejam ordenados de forma crescente.



d) PROCH() é adequada para tabelas em que os valores estão dispostos verticalmente e permite procurar dados em uma coluna específica de uma linha selecionada.

e) A função PROCH() requer que os valores na linha superior da matriz estejam ordenados apenas quando o parâmetro [Exatidão] for omitido, retornando assim o valor mais próximo ao procurado.

**8. A função SE() é uma das funções mais utilizadas para tomar decisões lógicas com base em um teste. Qual das alternativas descreve corretamente o comportamento da função SE() em diferentes cenários?**

a) A função SE() sempre retorna o valor "VERDADEIRO" se o teste lógico for igual a zero. Se o teste retornar qualquer outro valor numérico, o resultado será "FALSO", independentemente dos valores fornecidos.

b) SE() permite retornar dois resultados diferentes, sendo um valor para o caso de o teste lógico ser verdadeiro e outro valor para quando o teste for falso. O teste deve sempre envolver comparação entre números inteiros.

c) SE() retorna o valor do segundo argumento apenas se o teste lógico for falso, ignorando o terceiro argumento. Se o teste for verdadeiro, retorna automaticamente "VERDADEIRO" sem considerar os outros argumentos.

d) A função SE() é capaz de retornar um valor numérico ou textual como resultado, dependendo do teste lógico. O teste pode envolver qualquer tipo de dado, incluindo texto, números ou expressões booleanas.

e) Quando a função SE() recebe mais de dois argumentos, ela retorna o primeiro valor correspondente à primeira condição verdadeira e ignora o restante da fórmula, simplificando assim a análise de múltiplas condições.

**9. A função CONCATENAR() é utilizada para unir diferentes cadeias de texto em uma única sequência. Qual das alternativas apresenta corretamente o uso dessa função, considerando diferentes formas de concatenação?**

a) Ao utilizar a função CONCATENAR(), é necessário inserir manualmente qualquer separador entre as cadeias de texto, como espaços ou vírgulas, utilizando aspas para representar esses caracteres.

b) A função CONCATENAR() permite juntar cadeias de texto sem precisar incluir espaços entre os valores concatenados, pois o Excel insere automaticamente os espaços necessários entre as palavras.

c) CONCATENAR() pode ser substituída pelo operador "+" no Excel, que realiza a junção de textos com a adição de caracteres especiais automaticamente, como tabulações ou quebras de linha.



d) CONCATENAR() permite combinar valores numéricos e textuais sem a necessidade de conversão, sendo que o resultado é sempre formatado em maiúsculas, independentemente da formatação original do texto.

e) O uso de CONCATENAR() exige que as células de referência contenham textos no formato de string. Caso contrário, a função retornará um erro de tipo, não sendo possível concatenar valores numéricos diretamente.

**10. A função DIA.DA.SEMANA() é utilizada para identificar o dia da semana correspondente a uma data. Qual das alternativas explica corretamente o funcionamento dessa função?**

a) DIA.DA.SEMANA() retorna um número inteiro entre 1 e 5, representando os dias úteis da semana, com base em uma data inserida ou um número de série que representa uma data específica.

b) A função DIA.DA.SEMANA() retorna o dia correspondente da semana para qualquer data fornecida, mas requer que o usuário insira manualmente o código que representa o início da semana (por exemplo, 1 para segunda-feira).

c) DIA.DA.SEMANA() retorna um valor numérico entre 1 (domingo) e 7 (sábado) por padrão, permitindo que o usuário altere a configuração para iniciar a contagem a partir de qualquer outro dia da semana, como segunda-feira.

d) A função DIA.DA.SEMANA() permite o cálculo apenas de dias úteis e ignora automaticamente finais de semana, retornando um erro para datas que caem no sábado ou domingo.

e) DIA.DA.SEMANA() converte automaticamente qualquer valor numérico em uma data válida do calendário gregoriano, retornando o dia correspondente de acordo com o formato local configurado no Excel.



## SIMULADO COMENTADO – MS-EXCEL

### 1. Qual das alternativas representa corretamente a diferença entre as funções INT() e TRUNCAR() ao lidar com números negativos?

- a) A função TRUNCAR() sempre arredonda o número para o inteiro mais próximo, enquanto INT() apenas descarta a parte decimal, sem arredondamento.
- b) A função INT() arredonda sempre para o número inteiro mais baixo, afastando-se do zero, enquanto TRUNCAR() apenas remove a parte decimal sem arredondar o valor, independentemente do sinal do número.
- c) Ambas as funções se comportam da mesma forma com números negativos, retornando sempre o valor absoluto do número com a parte decimal truncada.
- d) A função TRUNCAR() transforma o número em seu equivalente positivo antes de truncar, enquanto INT() mantém o sinal original ao arredondar.
- e) INT() e TRUNCAR() apresentam resultados idênticos para números negativos, pois ambas se limitam a descartar a parte decimal, sem qualquer arredondamento adicional.

#### Comentário:

- (a) Errado. A função TRUNCAR() não arredonda o número, ela apenas remove a parte decimal. A função INT() também não arredonda, mas ela sempre "arredonda para baixo", afastando-se do zero, no caso de números negativos;
- (b) Correto. A função INT() arredonda sempre para o número inteiro mais baixo, ou seja, em direção a números mais negativos. Já TRUNCAR() apenas remove a parte decimal, sem alterar o valor do número inteiro, independentemente do sinal;
- (c) Errado. As funções INT() e TRUNCAR() se comportam de forma diferente com números negativos. INT() arredonda para o número inteiro mais baixo, enquanto TRUNCAR() apenas remove a parte decimal;
- (d) Errado. A função TRUNCAR() não transforma o número em seu equivalente positivo antes de truncar, ela apenas remove a parte decimal, mantendo o sinal original;
- (e) Errado. INT() e TRUNCAR() apresentam resultados diferentes para números negativos, pois INT() arredonda para o número mais baixo, enquanto TRUNCAR() apenas remove a parte decimal.

**Gabarito:** Letra B



**2. A função ARRED() possui uma lógica de arredondamento particular, especialmente quando o parâmetro é negativo. Qual das alternativas descreve corretamente o processo de arredondamento com base nos múltiplos mais próximos?**

- a) Quando o parâmetro é negativo, a função ARRED() sempre arredonda para o próximo múltiplo de 10, 100 ou 1000, dependendo da quantidade de dígitos fracionários a serem arredondados.
- b) Com um parâmetro negativo, ARRED() sempre arredonda para baixo, ignorando o valor fracionário e retornando o múltiplo de 10 mais próximo do número fornecido.
- c) Quando o parâmetro é negativo, ARRED() simplesmente remove a parte decimal, sem arredondar para qualquer múltiplo, o que pode resultar em perda de precisão significativa no cálculo.
- d) Ao utilizar um parâmetro negativo, a função ARRED() se comporta como a função TRUNCAR(), ignorando qualquer múltiplo e retornando o número truncado sem arredondamento.
- e) A função ARRED() arredonda para o múltiplo mais próximo de acordo com o parâmetro negativo, onde -1 arredonda para 10, -2 para 100 e assim por diante, eliminando as casas decimais e arredondando o valor ao múltiplo correspondente.

**Comentário:**

- (a) Errado. O ARRED() não arredonda automaticamente para múltiplos de 10, 100 ou 1000 apenas com base no parâmetro negativo. Ele segue uma lógica específica de arredondamento baseada no valor do parâmetro;
- (b) Errado. A função ARRED() não arredonda sempre para baixo com parâmetros negativos. Ela arredonda para o múltiplo mais próximo, que pode ser para cima ou para baixo, dependendo do valor do número;
- (c) Errado. ARRED() não remove simplesmente a parte decimal com parâmetro negativo, ele arredonda para o múltiplo correspondente, mantendo precisão no processo;
- (d) Errado. ARRED() e TRUNCAR() têm comportamentos diferentes. ARRED() arredonda para o múltiplo mais próximo, enquanto TRUNCAR() apenas remove a parte decimal sem arredondar;
- (e) Correto. Quando o parâmetro de ARRED() é negativo, a função arredonda para o múltiplo mais próximo de acordo com a posição indicada: -1 arredonda para o múltiplo de 10 mais próximo, -2 para o de 100, e assim por diante. Esse processo elimina as casas decimais e arredonda ao múltiplo correspondente.

**Gabarito:** Letra E

**3. Sobre a função MOD(), que retorna o resto de uma divisão, qual das opções descreve corretamente o comportamento da função ao lidar com números negativos?**



- a) A função MOD() sempre retorna o valor absoluto do resto, independentemente do sinal do divisor, assegurando que o resultado seja positivo.
- b) O comportamento da função MOD() depende exclusivamente do dividendo, ignorando o sinal do divisor, e retorna sempre um valor positivo.
- c) MOD() retorna o resto da divisão, mas o sinal do resultado será sempre o mesmo que o do divisor, mesmo quando o dividendo for negativo.
- d) Quando o divisor é negativo, a função MOD() sempre retorna um valor negativo, independentemente do sinal do dividendo, refletindo o comportamento da divisão inteira.
- e) MOD() não pode lidar com números negativos e retornará um erro quando o dividendo ou divisor tiver sinal negativo, pois a função não suporta tais operações.

#### Comentário:

- (a) Errado. A função MOD() não retorna sempre o valor absoluto do resto. O sinal do resultado depende do sinal do dividendo, e não necessariamente será positivo;
- (b) Errado. O comportamento de MOD() não ignora o sinal do divisor, mas sim depende do sinal do dividendo. O valor retornado pode ser positivo ou negativo, conforme o dividendo;
- (c) Correto. A função MOD() retorna o resto da divisão, e o sinal do resultado será o mesmo que o do dividendo, mesmo quando o divisor for negativo;
- (d) Errado. MOD() não retorna um valor negativo apenas com base no divisor ser negativo. O sinal do resultado segue o sinal do dividendo, não o do divisor;
- (e) Errado. A função MOD() pode lidar com números negativos e não gera erro. Ela retorna o valor corretamente com base nas regras de divisão e no sinal do dividendo.

**Gabarito:** Letra C

#### 4. A função CONT.NÚM() retorna a quantidade de células que contêm números. Qual das alternativas descreve corretamente como essa função trata diferentes tipos de dados no intervalo selecionado?

- a) A função CONT.NÚM() considera números, textos e valores booleanos, retornando o total de células preenchidas, sem diferenciar os tipos de dados contidos nas células.
- b) A função CONT.NÚM() retorna a quantidade total de células preenchidas, independentemente de conterem texto, números ou valores booleanos, desde que não estejam vazias.





c) Ao utilizar CONT.NÚM(), células com valores booleanos são contadas como "1" se forem verdadeiras e ignoradas se forem falsas, enquanto números e textos são contabilizados normalmente.

d) CONT.NÚM() conta apenas células que contenham números ou datas, ignorando células com texto ou booleanos, pois esses não são considerados números pela função.

e) CONT.NÚM() contabiliza apenas as células que contêm valores booleanos, datas ou números negativos, ignorando quaisquer outros tipos de valores no intervalo especificado.

### Comentário:

(a) Errado. A função CONT.NÚM() não conta textos nem valores booleanos. Ela se limita a contar células que contenham números, como inteiros, decimais e datas (que são armazenadas como números);

(b) Errado. CONT.NÚM() não conta todas as células preenchidas. Ela ignora células com textos ou booleanos e considera apenas aquelas com números;

(c) Errado. CONT.NÚM() não trata valores booleanos como números. Ela ignora completamente células que contenham valores booleanos;

(d) Correto. CONT.NÚM() conta apenas células que contêm números ou datas, ignorando células com texto ou valores booleanos, pois esses não são considerados números para a função;

(e) Errado. CONT.NÚM() não conta valores booleanos e considera qualquer número (positivo ou negativo) e datas, mas ignora outros tipos de valores.

**Gabarito:** Letra D

### 5. A função CONT.SES() é útil para contar células que atendem a múltiplos critérios. Qual das alternativas abaixo explica corretamente o funcionamento dessa função em relação aos critérios especificados?

a) A função CONT.SES() retorna a quantidade de células que atendem a todos os critérios especificados nos intervalos, não contando as células que atendem apenas a um dos critérios.

b) CONT.SES() conta as células que atendem a pelo menos um critério especificado no intervalo de valores, ignorando aquelas que não cumprem todos os critérios.

c) CONT.SES() soma os valores das células que atendem a qualquer critério dentro de um intervalo, independentemente de quantos critérios são atendidos simultaneamente.

d) CONT.SES() só considera o primeiro critério especificado, ignorando os demais, retornando a quantidade de células que atendem exclusivamente a esse critério.





e) A função CONT.SES() conta a quantidade de células que atendem apenas aos critérios de texto, ignorando critérios relacionados a números ou datas no intervalo.

### Comentário:

(a) Correto. CONT.SES() retorna a quantidade de células que atendem a todos os critérios especificados. Se uma célula não atender a um dos critérios, ela não será contada;

(b) Errado. A função CONT.SES() não conta células que atendem a pelo menos um critério. Ela exige que todas as condições especificadas sejam atendidas simultaneamente;

(c) Errado. CONT.SES() não soma valores. Ela apenas conta as células que atendem a todos os critérios, sem realizar operações de soma;

(d) Errado. CONT.SES() considera todos os critérios especificados, não apenas o primeiro. Uma célula só será contada se atender a todos os critérios;

(e) Errado. CONT.SES() não se limita a critérios de texto. Ela pode usar critérios relacionados a números, datas e texto, conforme o que for especificado.

**Gabarito:** Letra A

**6. A função PROCV() é amplamente utilizada para localizar valores em uma tabela, com base em um valor de referência na primeira coluna de um intervalo. Qual das alternativas descreve corretamente o uso da função e o comportamento do parâmetro de exatidão?**

a) A função PROCV() localiza o valor exato apenas quando o parâmetro [Exatidão] é definido como VERDADEIRO. Caso contrário, a função retorna um valor aleatório da tabela que esteja mais próximo do valor procurado.

b) Se o parâmetro [Exatidão] for omitido, o PROCV() assume automaticamente o valor FALSO e retorna o valor mais próximo, não sendo necessário que a primeira coluna do intervalo esteja ordenada.

c) Quando o parâmetro [Exatidão] é definido como FALSO, a função retorna apenas valores exatos, independentemente de a coluna estar ou não ordenada. Se o valor não for encontrado, retornará um erro.

d) A função PROCV() retorna o valor da última coluna da matriz caso o parâmetro [Exatidão] seja definido como VERDADEIRO, mesmo que o valor procurado não esteja presente na primeira coluna do intervalo de pesquisa.

e) Definir o parâmetro [Exatidão] como VERDADEIRO permite que a função retorne o valor anterior ao valor exato encontrado, desde que a primeira coluna esteja ordenada. Se estiver desordenada, a função retornará um erro.



### Comentário:

- (a) Errado. Quando o parâmetro [Exatidão] é definido como VERDADEIRO, a função PROCV() retorna o valor mais próximo (não aleatório), mas apenas se a primeira coluna estiver ordenada. O valor exato é retornado quando [Exatidão] é FALSO;
- (b) Errado. Se o parâmetro [Exatidão] for omitido, o PROCV() assume o valor VERDADEIRO, não FALSO, e espera que a primeira coluna esteja ordenada para retornar o valor mais próximo ou o valor exato, se encontrado;
- (c) Correto. Quando [Exatidão] é definido como FALSO, o PROCV() retorna apenas valores exatos. Se o valor exato não for encontrado, a função retornará um erro. Não há necessidade de a coluna estar ordenada neste caso;
- (d) Errado. O PROCV() retorna o valor de uma coluna especificada pelo argumento "número do índice da coluna", não necessariamente da última coluna, e depende do valor encontrado na primeira coluna;
- (e) Errado. Definir [Exatidão] como VERDADEIRO permite que a função retorne o valor mais próximo ao procurado, se não encontrar o exato. A coluna precisa estar ordenada, mas a função não retorna o valor anterior ao encontrado.

**Gabarito:** Letra C

### 7. A função PROCH() é utilizada para pesquisar um valor na linha superior de uma tabela e retornar o valor correspondente em uma linha especificada. Qual das afirmações abaixo descreve corretamente o uso dessa função?

- a) PROCH() é equivalente ao PROCV(), mas busca valores na horizontal, localizando um valor na primeira coluna e retornando o valor correspondente na linha selecionada.
- b) A função PROCH() retorna um valor exato na linha selecionada, independentemente de o valor procurado estar na linha superior, desde que o parâmetro [Exatidão] seja configurado como FALSO.
- c) Quando o parâmetro [Exatidão] é definido como VERDADEIRO, a função PROCH() pode retornar o valor mais próximo ao procurado na linha superior, contanto que os dados estejam ordenados de forma crescente.
- d) PROCH() é adequada para tabelas em que os valores estão dispostos verticalmente e permite procurar dados em uma coluna específica de uma linha selecionada.
- e) A função PROCH() requer que os valores na linha superior da matriz estejam ordenados apenas quando o parâmetro [Exatidão] for omitido, retornando assim o valor mais próximo ao procurado.

### Comentário:



- (a) Errado. PROCH() é similar ao PROCV(), mas busca valores na linha superior de uma tabela e retorna o valor correspondente em uma linha específica, não em uma coluna;
- (b) Errado. PROCH() retorna um valor correspondente a um valor encontrado na linha superior. Se o parâmetro [Exatidão] for FALSO, a função retorna apenas o valor exato, não qualquer valor de outra linha;
- (c) Correto. Quando o parâmetro [Exatidão] é VERDADEIRO, PROCH() pode retornar o valor mais próximo ao procurado, desde que os valores na linha superior estejam ordenados em ordem crescente;
- (d) Errado. PROCH() é usada para tabelas em que os valores estão dispostos horizontalmente. Ela busca na linha superior e retorna um valor de uma linha específica, não em uma coluna;
- (e) Errado. Quando o parâmetro [Exatidão] é omitido, PROCH() assume o valor VERDADEIRO, e os valores na linha superior devem estar ordenados para que o valor mais próximo possa ser retornado.

**Gabarito:** Letra C

**8. A função SE() é uma das funções mais utilizadas para tomar decisões lógicas com base em um teste. Qual das alternativas descreve corretamente o comportamento da função SE() em diferentes cenários?**

- a) A função SE() sempre retorna o valor "VERDADEIRO" se o teste lógico for igual a zero. Se o teste retornar qualquer outro valor numérico, o resultado será "FALSO", independentemente dos valores fornecidos.
- b) SE() permite retornar dois resultados diferentes, sendo um valor para o caso de o teste lógico ser verdadeiro e outro valor para quando o teste for falso. O teste deve sempre envolver comparação entre números inteiros.
- c) SE() retorna o valor do segundo argumento apenas se o teste lógico for falso, ignorando o terceiro argumento. Se o teste for verdadeiro, retorna automaticamente "VERDADEIRO" sem considerar os outros argumentos.
- d) A função SE() é capaz de retornar um valor numérico ou textual como resultado, dependendo do teste lógico. O teste pode envolver qualquer tipo de dado, incluindo texto, números ou expressões booleanas.
- e) Quando a função SE() recebe mais de dois argumentos, ela retorna o primeiro valor correspondente à primeira condição verdadeira e ignora o restante da fórmula, simplificando assim a análise de múltiplas condições.

**Comentário:**



- (a) Errado. A função SE() não retorna "VERDADEIRO" automaticamente se o teste for zero. Ela avalia a expressão lógica fornecida e retorna o valor correspondente ao resultado do teste, que pode ser "VERDADEIRO" ou "FALSO", conforme definido nos argumentos;
- (b) Errado. A função SE() permite retornar dois resultados diferentes com base no teste lógico, mas o teste não precisa envolver apenas números inteiros. Ele pode envolver comparações com qualquer tipo de dado, como números, texto ou expressões booleanas;
- (c) Errado. Se o teste lógico for verdadeiro, a função SE() retorna o segundo argumento (o valor associado ao "verdadeiro"), e não "VERDADEIRO" por padrão. O terceiro argumento é usado quando o teste for falso;
- (d) Correto. A função SE() pode retornar valores numéricos, textuais ou outros, dependendo do teste lógico. O teste pode envolver qualquer tipo de dado, como texto, números ou expressões booleanas;
- (e) Errado. SE() aceita apenas três argumentos. Para múltiplas condições, é necessário usar funções aninhadas ou outras abordagens como SEERRO ou SE() combinada com outras funções.

**Gabarito:** Letra D

**9. A função CONCATENAR() é utilizada para unir diferentes cadeias de texto em uma única sequência. Qual das alternativas apresenta corretamente o uso dessa função, considerando diferentes formas de concatenação?**

- a) Ao utilizar a função CONCATENAR(), é necessário inserir manualmente qualquer separador entre as cadeias de texto, como espaços ou vírgulas, utilizando aspas para representar esses caracteres.
- b) A função CONCATENAR() permite juntar cadeias de texto sem precisar incluir espaços entre os valores concatenados, pois o Excel insere automaticamente os espaços necessários entre as palavras.
- c) CONCATENAR() pode ser substituída pelo operador "+" no Excel, que realiza a junção de textos com a adição de caracteres especiais automaticamente, como tabulações ou quebras de linha.
- d) CONCATENAR() permite combinar valores numéricos e textuais sem a necessidade de conversão, sendo que o resultado é sempre formatado em maiúsculas, independentemente da formatação original do texto.
- e) O uso de CONCATENAR() exige que as células de referência contenham textos no formato de string. Caso contrário, a função retornará um erro de tipo, não sendo possível concatenar valores numéricos diretamente.

**Comentário:**



- (a) Correto. Na função CONCATENAR(), é necessário inserir manualmente qualquer separador, como espaços ou vírgulas. Para adicionar espaços entre as palavras, por exemplo, deve-se usar " " (aspas com espaço);
- (b) Errado. A função CONCATENAR() não insere automaticamente espaços entre os textos concatenados. Se o espaço for necessário, ele deve ser adicionado manualmente usando aspas com espaço (" ");
- (c) Errado. O operador de concatenação no Excel é &, não +. O & permite unir textos sem adicionar automaticamente caracteres especiais como tabulações ou quebras de linha;
- (d) Errado. CONCATENAR() permite combinar valores numéricos e textuais, mas o resultado não é formatado automaticamente em maiúsculas. A função não altera a formatação original dos textos;
- (e) Errado. CONCATENAR() pode concatenar tanto valores numéricos quanto textuais. Se uma célula contiver um número, ele será convertido para texto automaticamente sem gerar erro.

**Gabarito:** Letra A

**10. A função DIA.DA.SEMANA() é utilizada para identificar o dia da semana correspondente a uma data. Qual das alternativas explica corretamente o funcionamento dessa função?**

- a) DIA.DA.SEMANA() retorna um número inteiro entre 1 e 5, representando os dias úteis da semana, com base em uma data inserida ou um número de série que representa uma data específica.
- b) A função DIA.DA.SEMANA() retorna o dia correspondente da semana para qualquer data fornecida, mas requer que o usuário insira manualmente o código que representa o início da semana (por exemplo, 1 para segunda-feira).
- c) DIA.DA.SEMANA() retorna um valor numérico entre 1 (domingo) e 7 (sábado) por padrão, permitindo que o usuário altere a configuração para iniciar a contagem a partir de qualquer outro dia da semana, como segunda-feira.
- d) A função DIA.DA.SEMANA() permite o cálculo apenas de dias úteis e ignora automaticamente finais de semana, retornando um erro para datas que caem no sábado ou domingo.
- e) DIA.DA.SEMANA() converte automaticamente qualquer valor numérico em uma data válida do calendário gregoriano, retornando o dia correspondente de acordo com o formato local configurado no Excel.

**Comentário:**

- (a) Errado. DIA.DA.SEMANA() retorna um número entre 1 e 7 por padrão, representando todos os dias da semana, e não apenas os dias úteis;



- (b) Errado. DIA.DA.SEMANA() não requer que o usuário insira manualmente o código que representa o início da semana. Ele tem uma configuração padrão e opções para alterar o dia inicial da semana, mas o código é opcional;
- (c) Correto. DIA.DA.SEMANA() retorna um número entre 1 (domingo) e 7 (sábado) por padrão. O usuário pode alterar essa configuração para iniciar a semana em outro dia, como segunda-feira, usando um argumento adicional na função;
- (d) Errado. DIA.DA.SEMANA() não ignora finais de semana e não retorna erros para datas que caem no sábado ou domingo. Ela identifica qualquer dia da semana;
- (e) Errado. DIA.DA.SEMANA() trabalha com datas válidas, mas não converte automaticamente qualquer valor numérico em uma data. A data precisa estar em um formato reconhecível como uma data válida.

**Gabarito:** Letra C



## GABARITO – MS-EXCEL

1. LETRA B
2. LETRA E
3. LETRA C
4. LETRA D
5. LETRA A
6. LETRA C
7. LETRA C
8. LETRA D
9. LETRA A
10. LETRA C





# ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.