Estratégia Concursos

Aula 14

BNB (Analista Bancário) Informática - 2023 (Pré-Edital)

Autor:
Diego Carvalho, Renato da Costa, Equipe Informática e TI

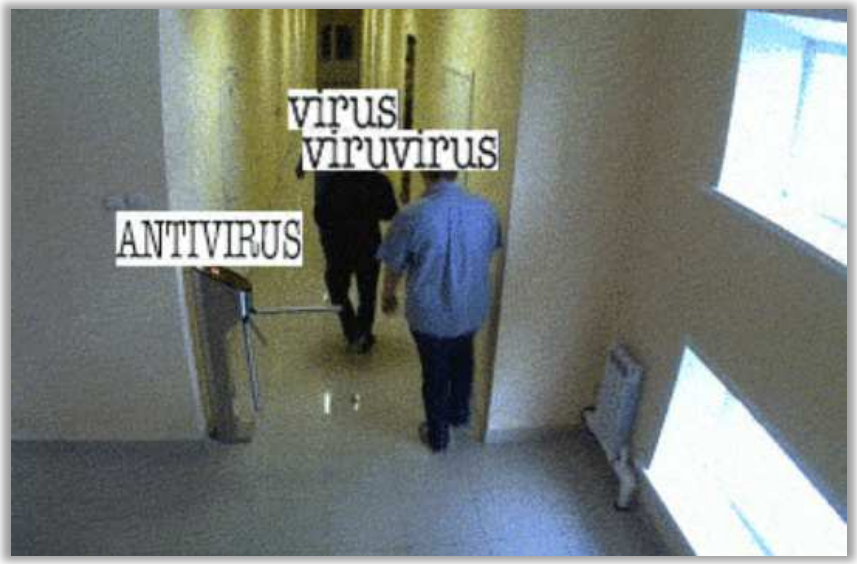
30 de Junho de 2023

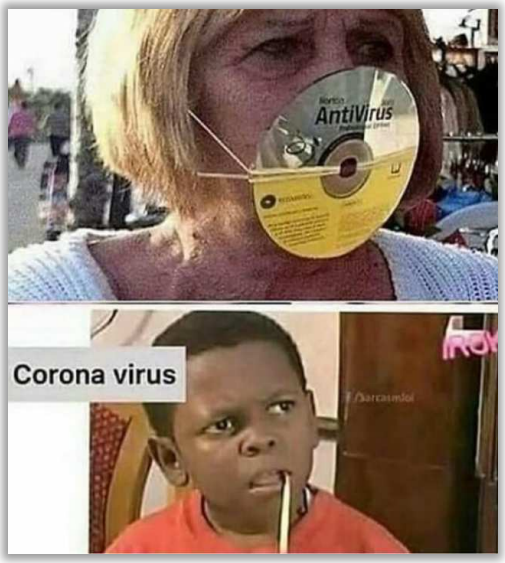
Índice

APRESENTAÇÃO DA AULA

Pessoal, o tema da nossa aula é: **Ferramentas de Proteção e Segurança**. Nós já conhecemos os softwares maliciosos mais comuns e sabemos como são seus processos de infecção e propagação – além disso, nós já sabemos quais são suas ações maliciosas mais comuns. Agora chegou o momento de entender como proteger um computador e uma rede de ações maliciosas. Vem comigo que a aula é tranquilaaaaaaça...

PROFESSOR DIEGO CARVALHO - WWW.INSTAGRAM.COM/PROFESSORDIEGOCARVALHO





Galera, todos os tópicos da aula possuem Faixas de Incidência, que indicam se o assunto cai muito ou pouco em prova. *Diego, se cai pouco para que colocar em aula?* Cair pouco não significa que não cairá justamente na sua prova! A ideia aqui é: se você está com pouco tempo e precisa ver somente aquilo que cai mais, você pode filtrar pelas incidências média, alta e altíssima; se você tem tempo sobrando e quer ver tudo, vejam também as incidências baixas e baixíssimas. *Fechado?*

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

INCIDÊNCIA EM PROVA: BAIXA

INCIDÊNCIA EM PROVA: MÉDIA

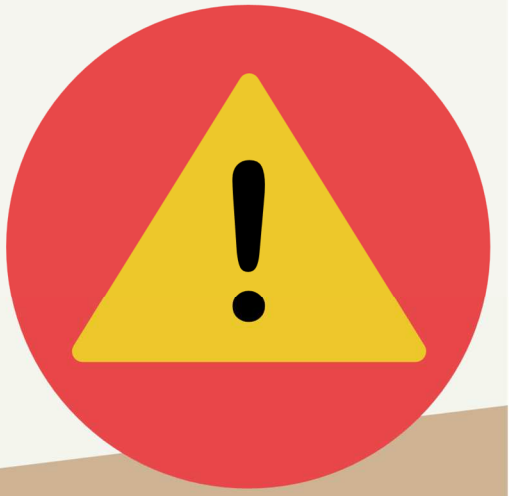
INCIDÊNCIA EM PROVA: ALTA

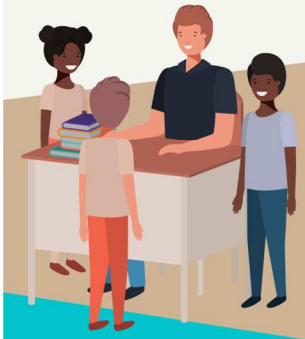
INCIDÊNCIA EM PROVA: ALTÍSSIMA

Além disso, essas faixas não são por banca – é baseado tanto na quantidade de vezes que caiu em prova independentemente da banca e também em minhas avaliações sobre cada assunto...

#ATENÇÃO

Avisos Importantes





O curso abrange todos os níveis de conhecimento...

Esse curso foi desenvolvido para ser acessível a **alunos com diversos níveis de conhecimento diferentes.** Temos alunos mais avançados que têm conhecimento prévio ou têm facilidade com o assunto. Por outro lado, temos alunos iniciantes, que nunca tiveram contato com a matéria ou até mesmo que têm trauma dessa disciplina. A ideia aqui é tentar atingir ambos os públicos - iniciantes e avançados - da melhor maneira possível..

Por que estou enfatizando isso?

O **material completo** é composto de muitas histórias, exemplos, metáforas, piadas, memes, questões, desafios, esquemas, diagramas, imagens, entre outros. Já o **material simplificado** possui exatamente o mesmo núcleo do material completo, mas ele é menor e bem mais objetivo. *Professor, eu devo estudar por qual material?* Se você quiser se aprofundar nos assuntos ou tem dificuldade com a matéria, necessitando de um material mais passo-a-passo, utilize o material completo. Se você não quer se aprofundar nos assuntos ou tem facilidade com a matéria, necessitando de um material mais direto ao ponto, utilize o material simplificado.

Por fim...

O curso contém diversas questões espalhadas em meio à teoria. Essas questões possuem um comentário mais simplificado porque **têm o único objetivo de apresentar ao aluno como bancas de concurso cobram o assunto previamente administrado**. A imensa maioria das questões para que o aluno avalie seus conhecimentos sobre a matéria estão dispostas ao final da aula na lista de exercícios e **possuem comentários bem mais completos, abrangentes e direcionados.**

FERRAMENTAS ANTIMALWARE

Conceitos Básicos

INCIDÊNCIA EM PROVA: ALTA

Ferramentas Antimalware são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador (Ex: Antivírus, Antispyware, Antirootkit e Antitrojan). Ainda que existam ferramentas específicas para os diferentes tipos de códigos maliciosos, muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código depende de cada fabricante e muitos códigos mesclam as características dos demais tipos.

Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o antivírus. **Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso.** Há diversos tipos de programas *antimalware* que diferem entre si das seguintes formas:

- **Método de detecção:** assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características do código) e comportamento (baseia-se no comportamento apresentado) são alguns dos métodos mais comuns.

- **Forma de obtenção**: podem ser gratuitos, experimentais ou pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras e suporte.

- **Execução**: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.

- **Funcionalidades apresentadas**: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e *firewall* pessoal.

Para escolher o *antimalware* que melhor se adapta à necessidade de um usuário, é importante levar em conta o uso que você faz e as características de cada versão. **Observe que não há relação entre o custo e a eficiência de um programa, pois há versões gratuitas que apresentam mais funcionalidades que versões pagas de outros fabricantes.** Cuidados a serem tomados com o *antimalware* escolhido:

CUIDADOS NA ESCOLHA DE ANTIMALWARE
Tenha um *antimalware* instalado em seu computador – há programas online úteis, mas em geral possuem funcionalidades reduzidas;

Utilize programas online quando suspeitar que o *antimalware* local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião;

Configure o *antimalware* para verificar toda extensão de arquivo e para verificar automaticamente arquivos anexados aos e-mails e obtidos pela Internet;

Configure o *antimalware* para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos);

Mantenha o arquivo de assinaturas sempre atualizado (configure o *antimalware* para atualizá-lo automaticamente pela rede, de preferência diariamente);

Mantenha o *antimalware* sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas;

Evite executar simultaneamente diferentes programas *antimalware* – eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção;

Crie um disco de emergência e o utilize-o quando desconfiar que o *antimalware* instalado está desabilitado/comprometido ou que o comportamento do computador está estranho.

(TRT/RS - 2015) Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

Comentários: (a) Errado, um antimalware online só funciona se estiver conectado à internet, logo o ideal é ter um antimalware que esteja ativo independente de estar online ou não; (b) Errado, há outras extensões que também podem causar problemas – inclusive outras extensões executáveis; (c) Errado, é ideal que ele seja configurado para fazer verificações automaticamente discos rígidos e outras mídias; (d) Errado, sugere-se atualizar o antimalware sempre que possível – quanto mais atualizado melhor; (e) Correto, é recomendável evitar a execução simultânea de antimalwares para que eles não entrem em conflito (Letra E).

Antivírus

INCIDÊNCIA EM PROVA: ALTA

Como o próprio nome sugere, o antivírus é uma ferramenta para remover vírus existentes em um computador e combater a infecção por novos vírus. A solução ideal para a ameaça de vírus é a prevenção: em primeiro lugar, não permitir que um vírus entre no sistema. Esse objetivo, em geral, é impossível de se conseguir, embora a prevenção possa reduzir o número de ataques virais bem-sucedidos. Caso não seja possível, recomenda-se seguir os seguintes passos:

FASES	DESCRIÇÃO
DETECÇÃO	Uma vez que a infecção do vírus tenha ocorrido em algum programa de computador, localize o vírus.
IDENTIFICAÇÃO	Uma vez que o vírus tenha sido detectado, identifique qual vírus específico que infectou um programa.
REMOÇÃO	Uma vez o vírus tenha sido identificado, remova todos os traços do vírus do programa infectado e restaure-o ao seu estado original.

Algumas vezes, quando o antivírus encontra um arquivo que considera maligno, ele também oferece a opção colocá-lo em quarentena. *O que é isso, professor?* **A quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto ele aguarda uma confirmação de identificação**. As assinaturas nem sempre são totalmente confiáveis e podem detectar vírus em arquivos inofensivos – falsos-positivos.

Trata-se de uma opção à remoção, uma vez que eventualmente determinados arquivos não podem ser eliminados por possuírem grande valor para o usuário ou por serem considerados importantes para o bom funcionamento de um sistema. Nesse caso, a quarentena permite que o arquivo fique isolado por um período até que desenvolvedores do antivírus possam lançar alguma atualização. *Bacana?*

Ao deixar os arquivos suspeitos em um local isolado e seguro, o antivírus permite que eles eventualmente sejam recuperados mais tarde e também impede que eventuais pragas virtuais realizem qualquer atividade maliciosa. Idealmente, os arquivos na situação de quarentena são

criptografados ou alterados de alguma forma para que ele não possa ser executado e outros antivírus não os identifiquem como um potencial vírus.

(CBTU - 2014) Ao realizar a verificação por meio de um antivírus, um usuário detectou a presença de um vírus no seu computador. Foi orientado por um amigo a não excluir o arquivo infectado de imediato, mas, sim, isolá-lo em uma área sem a execução de suas funções por um determinado período de tempo. Tal recurso é conhecido como:

a) vacina b) maturação c) isolamento d) quarentena

Comentários: o recurso que isola um malware em uma área por um período de tempo é a quarentena (Letra D).

Os principais antivírus do mercado são: Avast, McAfee, Bitdefender, Kaspersky, AVG, ESET, Symantec, Norton, Avira, Comodo, PSafe, entre outros. *Professor, isso cai em prova?* Infelizmente, saber o nome dos principais antivírus do mercado cai em prova. **Agora um ponto que despeeeeeeeeeeenca em prova: é recomendável evitar a execução simultânea de mais de um antimalware (antivírus) em um mesmo computador.**

POR QUE NÃO UTILIZAR MAIS DE UM ANTIMALWARE SIMULTANEAMENTE?

Galera, existem diversos motivos para não utilizar mais de um antimalware simultaneamente. Dentre eles, podemos mencionar: podem ocasionar problemas de desempenho no computador escaneado; podem interferir na capacidade de detecção um do outro; um pode detectar o outro como um possível malware; entre outros. **Dessa forma, recomenda-se evitar a utilização de mais de um antimalware. *Fechado?* ;)**

Vamos falar agora sobre as gerações de antivírus. Os avanços na tecnologia de vírus e antivírus seguem lado a lado. Pesquisas mostram que todos os dias surgem cerca de 220.000 novos tipos de vírus. Os softwares utilitários de antivírus têm evoluído e se tornando mais complexos e sofisticados como os próprios vírus – inclusive antivírus modernos podem detectar até worms, se sua assinatura for conhecida. **Hoje em dia, identificam-se quatro gerações de software antivírus...**

1ª Geração: Detecção baseada em Assinatura

INCIDÊNCIA EM PROVA: ALTA

A assinatura é uma informação usada para detectar pragas. Assim como a assinatura do nome identifica a identidade da pessoa, a assinatura de um vírus é o que o antivírus usa para identificar que uma praga digital está presente em um arquivo. **A assinatura é geralmente um trecho único do código do vírus – estrutura ou padrão de bits**. Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro.

É realizada uma engenharia reversa no software malicioso para entendê-lo. Então é desenvolvida uma maneira de detectá-lo, depois ele é catalogado em uma base de dados e distribuído para todos os clientes do antivírus. Dessa forma, **há um tempo razoável da identificação à atualização da base da dados e esse tempo varia de acordo com fatores como**: complexidade do vírus, tempo para receber a amostra, entre outros.

Por outro lado, as assinaturas permitem detectar códigos maliciosos de um modo muito mais específico, sendo mais eficientes para remover ameaças complexas anteriormente mapeadas. **Além disso, devido a inúmeras técnicas utilizadas pelos atacantes para ofuscar o malware e burlar métodos heurísticos, é necessário – em alguns casos – contar com assinaturas específicas**. *Fechado?*

> **(TCE/ES – 2012)** Em geral, softwares antivírus trabalham com assinaturas de vírus; assim, para um novo vírus ser detectado pelo software, este precisa conhecer a assinatura desse novo vírus.
>
> _____
>
> **Comentários:** é verdade... como ele funciona baseado em uma assinatura conhecida, ele precisa conhecê-la (Correto).

2ª Geração: Detecção baseada em Heurística

INCIDÊNCIA EM PROVA: MÉDIA

A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável *malware*.

Para tal, ele pode – por exemplo – procurar o início de um loop de criptografia usado em um vírus polimórfico ou verificar a integridade do software, utilizando funções de *hash*. Agora uma informação interessante: a palavra *Heurística* vem de "*Eureka*" – a exclamação atribuída ao matemático Arquimedes ao descobrir uma solução para um problema complexo envolvendo densidade e volume de um corpo. *Eureka* significa *encontrar*, *descobrir, deduzir*!

Em um sentido mais genérico, a palavra *heurística* trata de regras e métodos que conduzem à dedução de uma solução aproximada ou satisfatória para um problema. *E não é a mesma coisa com o antivírus?* Ele busca comparar algumas estruturas e comportamentos com padrões predefinidos com o intuito de indicar a provável presença de um malware. **Eventualmente pode haver alguns falsos-positivos, mas se trata de uma aproximação razoável**.

Em suma, nós podemos afirmar que a detecção baseada em heurística é capaz de identificar possíveis vírus utilizando dados genéricos sobre seus comportamentos. Assim sendo, esta técnica é capaz de detectar vírus genéricos, sem assinatura conhecida, através da comparação com um código conhecido de vírus e, assim, determinar se aquele arquivo ou programa pode ou não ser um vírus. *Compreendido, galera?*

Essa é uma estratégia eficaz, uma vez que a maioria dos códigos maliciosos da Internet são cópias de outros códigos. Ao descobrir um código malicioso, podem ser descobertos muitos outros similares, sem que eles sejam conhecidos. **O principal benefício é a capacidade de detectar novos vírus, antes mesmo que o antivírus conheça e tenha capacidade de evitá-los**. Em outras palavras, é capaz de detectar um novo vírus antes que ele faça algum mal.

(TCE/ES - 2014) Para tentar prevenir uma infecção por vírus ou malware, algumas ferramentas de antivírus procedem à detecção por heurística, técnica de detecção de vírus baseada no comportamento anômalo ou malicioso de um software.

_____

Comentários: perfeito... a detecção por heurística permite identificar vírus desconhecidos de forma proativa – sem depender de assinatura – baseado no comportamento anômalo ou malicioso (Correto).

3ª Geração: Interceptação de Atividade

INCIDÊNCIA EM PROVA: BAIXA

Trata-se de uma tecnologia que identifica um vírus por suas ações, em vez de sua estrutura em um programa infectado. Esses programas têm a vantagem de não ser necessário desenvolver assinaturas e heurísticas para uma ampla variedade de vírus. **É diferente da heurística porque só funciona com programas em execução, enquanto a heurística analisa o próprio arquivo sem a necessidade de executá-lo**.

Funciona como um policial à procura de ações estranhas em um suspeito. **Ele observa o sistema operacional, procurando por eventos suspeitos**. Se o programa antivírus testemunhar uma tentativa de alterar ou modificar um arquivo ou se comunicar pela web, ele poderá agir e avisá-lo da ameaça ou poderá bloqueá-la, dependendo de como você ajusta suas configurações de segurança. Também há uma chance considerável de encontrar falsos-positivos.

Em suma: o antivírus monitora continuamente todos os programas em execução no computador. Cada atividade dos softwares é considerada maliciosa ou inofensiva. Se várias tarefas suspeitas forem realizadas por um mesmo aplicativo, o antivírus irá considerá-lo malicioso. **Caso o vírus se**

comporte de forma semelhante a pragas conhecidas, ele será reconhecido como malicioso sem a necessidade de uma vacina específica.

4ª Geração: Proteção Completa

INCIDÊNCIA EM PROVA: BAIXA

São pacotes compostos por uma série de técnicas antivírus utilizadas em conjunto. Estas incluem componentes de varredura e de interceptação de atividades. Ademais, esse tipo de pacote inclui recurso de controle de acesso, que limita a capacidade dos vírus de penetrar em um sistema e, por consequência, limita a capacidade de um vírus de atualizar arquivos a fim de passar a infecção adiante. Trata-se da geração da maioria dos antivírus atuais.

Next Generation Antivirus (NGAV)

INCIDÊNCIA EM PROVA: BAIXÍSSIMA

Por fim, vamos falar rapidamente sobre o Next Generation Antivirus (NGAV). Para entender o que são e como funcionam os antivírus da nova geração, é preciso focar na sua principal diferença em relação aos antivírus convencionais. Essas soluções que conhecemos há décadas não são "inteligentes"; tudo o que fazem é varrer o sistema em busca de ameaças conhecidas, que constam em listas atualizadas várias vezes ao dia.

O problema é que o tempo entre uma atualização e outra é suficiente para milhares de ataques agirem com sucesso. São ineficazes também contra alguns ataques, nos quais a falha é descoberta e explorada no mesmo dia em que foi identificada sua existência. **Já o NGAV vai além de assinaturas de malwares conhecidas – eles usam análises preditivas, conduzidas por aprendizado de máquina e inteligência artificial para detectar e prevenir ataques de malware.**

Eles podem também identificar comportamentos maliciosos, bem como coletar e analisar dados para determinar as causas raiz de uma vulnerabilidade. **Dessa forma, são capazes de responder a ameaças novas e emergentes que anteriormente não eram detectadas.** Em suma, eles agem com base no comportamento do usuário, verificando em tempo real se cada atividade sua representa – ou não – um risco real.

E faz isso com análises constantes sobre tudo que é feito no dispositivo, usando inteligência artificial e aprendizado de máquina, para determinar o que é seguro ou não. Eles utilizam o conceito de *sandbox*, monitorando e respondendo às táticas, técnicas e procedimentos de invasão. Essa nova tecnologia e arquitetura de software foi criada para preencher a lacuna deixada pelo antivírus comum, levando a proteção a um nível totalmente novo.

O NGAV possui tecnologias de: Anti-Ransomware; Anti-Exploit Prevention; ATP - Advanced Threat Protection; DLP - Data Loss Prevention; Mitigação; Proteção preventiva com Deep Learning; Resposta a Incidentes instantânea; e EDR - Endpoint Detection and Response. **A habilidade em reconhecer e lidar com ameaças de segurança por conta própria é muito mais eficaz em vez de depender de um banco de dados de assinaturas.**

Antispam

INCIDÊNCIA EM PROVA: BAIXA

Os Filtros Antispam já vêm integrados à maioria dos programas de e-mails e permite separar os desejados dos indesejados – os famosos *spams*. A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas *spam* e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens. Ao detectá-las, essas ferramentas alertam para que ele tome as atitudes adequadas para si.

Existem também algumas técnicas de bloqueio de spam (no sentido de classificá-lo como spam e, não, de impedir o seu recebimento) que se baseiam na análise do conteúdo da mensagem. Em geral, são filtros baseados no reconhecimento de padrões do conteúdo que buscam identificar se o *e-mail* pode conter um vírus ou se tem características comuns aos spams. Os filtros de conteúdo mais comuns são os antivírus e os identificadores Bayesianos de spam.

Antispyware

INCIDÊNCIA EM PROVA: BAIXA

Antispyware é um tipo de software projetado para detectar e remover programas de *spyware* indesejados. Spyware é um tipo de *malware* instalado em um computador sem o conhecimento do usuário para coletar informações sobre ele. Isso pode representar um risco de segurança para o usuário, além de degradar o desempenho do sistema, absorvendo o poder de processamento, instalando *software* adicional ou redirecionando a atividade do navegador dos usuários.

(DPE/MT – 2015) Antispyware é um software de segurança que tem o objetivo de detectar e remover spywares, sendo ineficaz contra os adwares.

_____

Comentários: *adwares* são tipos de *spywares*, logo é eficaz também (Errado).

RESUMO

FERRAMENTAS ANTIMALWARE
Ferramentas Antimalware são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador (Ex: Antivírus, Antispyware, Antirootkit e Antitrojan). Apesar de inicialmente eles terem sido criados para atuar especificamente sobre vírus, com o passar do tempo, passaram também a englobar as funcionalidades dos demais programas, fazendo com que alguns deles caíssem em desuso. Há diversos tipos de programas antimalware que diferem entre si sob diversos critérios.

- **Método de detecção:** assinatura (uma lista de assinaturas é usada à procura de padrões), heurística (baseia-se nas estruturas, instruções e características do código) e comportamento (baseia-se no comportamento apresentado) são alguns dos métodos mais comuns.

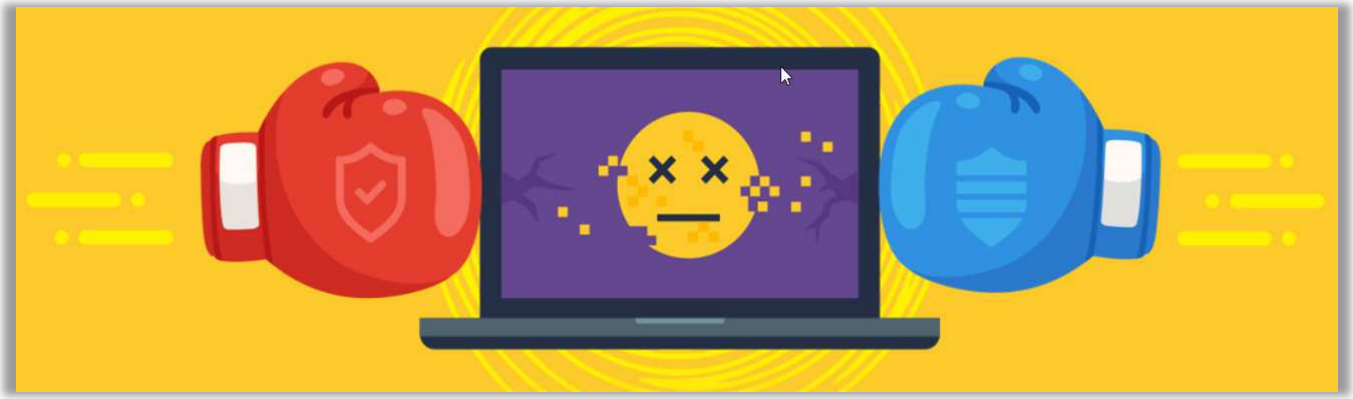
- **Forma de obtenção**: podem ser gratuitos, experimentais ou pagos. Um mesmo fabricante pode disponibilizar mais de um tipo de programa, sendo que a versão gratuita costuma possuir funcionalidades básicas ao passo que a versão paga possui funcionalidades extras e suporte.

- **Execução**: podem ser localmente instalados no computador ou executados sob demanda por intermédio do navegador Web. Também podem ser online, quando enviados para serem executados em servidores remotos, por um ou mais programas.

- **Funcionalidades apresentadas**: além das funções básicas (detectar, anular e remover códigos maliciosos) também podem apresentar outras funcionalidades integradas, como a possibilidade de geração de discos de emergência e *firewall* pessoal.

FASES	DESCRIÇÃO
DETECÇÃO	Uma vez que a infecção do vírus tenha ocorrido em algum programa de computador, localize o vírus.
IDENTIFICAÇÃO	Uma vez que o vírus tenha sido detectado, identifique qual vírus específico que infectou um programa.
REMOÇÃO	Uma vez o vírus tenha sido identificado, remova todos os traços do vírus do programa infectado e restaure-o ao seu estado original.

NÃO É RECOMENDÁVEL UTILIZAR MAIS DE UM ANTIMALWARE SIMULTANEAMENTE



POSSÍVEIS CUIDADOS
Tenha um antimalware instalado em seu computador (programas online, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas).
Utilize programas online quando suspeitar que o antimalware local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local).
Configure o antimalware para verificar toda e qualquer extensão de arquivo.
Configure o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives, CDs, DVDs e discos externos).
Mantenha o arquivo de assinaturas sempre atualizado (configure o antimalware para atualizá-lo automaticamente pela rede, de preferência diariamente).
Mantenha o antimalware sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.
Evite executar simultaneamente diferentes programas antimalware (eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro).
Crie um disco de emergência e o utilize-o quando desconfiar que o antimalware instalado está desabilitado/comprometido ou que o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc).

TIPOS DE ANTIVÍRUS	DESCRIÇÃO
1º GERAÇÃO	Também chamada de Detecção Baseada em Assinatura, ele busca por um trecho único do código do vírus (estrutura ou padrão de bits) chamado de assinatura. Procurando por esse trecho, o antivírus pode detectar o vírus sem precisar analisar o arquivo inteiro. É realizada uma engenharia reversa no software malicioso para entendê-lo. Então é desenvolvida uma maneira de detectá-lo, depois ele é catalogado em uma base de dados e distribuído para todos os clientes do antivírus.

2º GERAÇÃO	Também chamada de Detecção Baseada em Heurística, ele utiliza um conjunto de técnicas para identificar vírus desconhecidos de forma proativa chamada heurística – sem depender de assinatura. Nesta linha, a solução de segurança analisa a estrutura de um arquivo e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça.
3º GERAÇÃO	Também chamada de Interceptação de Atividade, ele utiliza uma tecnologia que identifica um vírus por suas ações, em vez de sua estrutura em um programa infectado. Esses programas têm a vantagem de não ser necessário desenvolver assinaturas e heurísticas para uma ampla variedade de vírus. É diferente da heurística porque só funciona com programas em execução, enquanto a heurística analisa o próprio arquivo sem a necessidade de executá-lo.
4º GERAÇÃO	Também chamado de Proteção Completa, São pacotes compostos por uma série de técnicas antivírus utilizadas em conjunto. Estas incluem componentes de varredura e de interceptação de atividades. Ademais, esse tipo de pacote inclui recurso de controle de acesso, que limita a capacidade dos vírus de penetrar em um sistema e, por consequência, limita a capacidade de um vírus de atualizar arquivos a fim de passar a infecção adiante. Trata-se da geração da maioria dos antivírus atuais.

ANTISPYWARE

- **Antispyware** é um tipo de software projetado para detectar e remover programas de spyware indesejados. Spyware é um tipo de malware instalado em um computador sem o conhecimento do usuário para coletar informações sobre ele. Isso pode representar um risco de segurança para o usuário, além de degradar o desempenho do sistema, absorvendo o poder de processamento, instalando software adicional ou redirecionando a atividade do navegador dos usuários.

ANTISPAM

- **Filtros Antispam** já vêm integrados à maioria dos programas de e-mails e permite separar os desejados dos indesejados – os famosos spams. A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens. Ao detectá-las, essas ferramentas alertam para que ele tome as atitudes adequadas para si.

MAPA MENTAL

Ferramentas Antimalware

Antivírus

- CRIADO INICIALMENTE PARA REMOVER VÍRUS EXISTENTES NO COMPUTADOR E COMBATER A INFECÇÃO POR NOVOS VÍRUS.
- HOJE, ENGLOBA AS FUNCIONALIDADES DE OUTROS PROGRAMAS, COMO ANTISPYWARES.
- CUIDADOS IMPORTANTES:
  - MANTER O ANTIVÍRUS SEMPRE ATUALIZADO.
  - MANTER O ARQUIVO DE ASSINATURAS SEMPRE ATUALIZADO.
  - CONFIGURAR O ANTIVÍRUS P/ VERIFICAR AUTOMATICAMENTE OS DISCOS RÍGIDOS E AS UNIDADES REMOVÍVEIS (EX: PENDRIVES).
  - EVITAR A EXECUÇÃO SIMULTANEAMENTE DE DIFERENTES ANTIVÍRUS.

GERAÇÕES DE ANTIVÍRUS

1ª GERAÇÃO: DETECÇÃO BASEADA EM ASSINATURA

- A ASSINATURA É UM TRECHO ÚNICO DO CÓDIGO DO VÍRUS (ESTRUTURA OU PADRÃO DE BITS) QUE O ANTIVÍRUS USA PARA IDENTIFICAR QUE UMA PRAGA VIRTUAL ESTÁ PRESENTE EM UM ARQUIVO.
- DESVANTAGEM: LEVA UM CERTO TEMPO PARA QUE O MALWARE SEJA IDENTIFICADO E A BASE DE DADOS SEJA ATUALIZADA COM SUA ASSINATURA.
- VANTAGEM: É MAIS EFICIENTE NA REMOÇÃO DE AMEAÇAS COMPLEXAS ANTERIORMENTE MAPEADAS OU DE MALWARES QUE BURLAM OS MÉTODOS HEURÍSTICOS.

2ª GERAÇÃO: DETECÇÃO BASEADA EM HEURÍSTICA

- A HEURÍSTICA É UM CONJUNTO DE TÉCNICAS P/ IDENTIFICAR VÍRUS DESCONHECIDOS DE FORMA PROATIVA - SEM DEPENDER DE ASSINATURA.
- ANALISA O COMPORTAMENTO DE UM TRECHO DE CÓDIGO P/ DESCOBRIR PADRÕES SUSPEITOS EM SUA ATIVIDADE MALICIOSA.
- É UMA ESTRATÉGIA EFICAZ PORQUE A MAIORIA DOS CÓDIGOS MALICIOSOS DA INTERNET SÃO CÓPIAS DE OUTROS CÓDIGOS.
- DESVANTAGEM: PODE GERAR MAIS FALSOS-POSITIVOS.
- VANTAGEM: É CAPAZ DE IDENTIFICAR VÍRUS NOVOS ANTES QUE ELES GEREM DANOS.

3ª GERAÇÃO: INTERCEPTAÇÃO DE ATIVIDADE

- IDENTIFICA O VÍRUS POR SUAS AÇÕES, EM VEZ DE SUA ESTRUTURA EM UM PROGRAMA INFECTADO.
- DESVANTAGEM: SÓ FUNCIONA COM PROGRAMAS EM EXECUÇÃO, ENQUANTO A HEURÍSTICA ANALISA O ARQUIVO EM SI, SEM NECESSIDADE DE EXECUTÁ-LO.
- VANTAGEM: NÃO É NECESSÁRIO DESENVOLVER ASSINATURAS E HEURÍSTICAS P/ UMA AMPLA VARIEDADE DE VÍRUS.

4ª GERAÇÃO: PROTEÇÃO COMPLETA

- É A GERAÇÃO DA MAIORIA DOS ANTIVÍRUS ATUAIS.
- SÃO PACOTES COMPOSTOS POR UM CONJUNTO DE TÉCNICAS ANTIVÍRUS.
- INCLUEM RECURSO DE CONTROLE DE ACESSO, QUE LIMITA A CAPACIDADE DOS VÍRUS DE PENETRAR EM UM SISTEMA, LIMITANDO SUA CAPACIDADE DE ATUALIZAR ARQUIVOS E, CONSEQUENTEMENTE, DE SE PROPAGAR.

> QUARENTENA:
> - ÁREA VIRTUAL ONDE O ANTIVÍRUS ARMAZENA ARQUIVOS IDENTIFICADOS COMO POSSÍVEIS VÍRUS ENQUANTO ELE AGUARDA CONFIRMAÇÃO.
> - É UMA ALTERNATIVA À REMOÇÃO.
> - ENQUANTO ESTIVEREM ISOLADAS NA QUARENTENA, EVENTUAIS PRAGAS VIRTUAIS FICAM IMPEDIDAS DE REALIZAR QUALQUER ATIVIDADE MALICIOSA.

Antispyware

- SOFTWARE PROJETADO PARA DETECTAR E REMOVER PROGRAMAS DE SPYWARE INDESEJADOS.
  - PODEM SER:
    - SCREENLOGGERS
    - KEYLOGGERS
    - ADWARES

Antispam

- PERMITE SEPARAR OS E-MAILS DESEJADOS DOS INDESEJADOS (SPAMS).
- JÁ VEM INTEGRADO À MAIORIA DOS PROGRAMAS DE E-MAILS.
- GERALMENTE PASSA POR UM PERÍODO DE "TREINAMENTO", EM QUE O USUÁRIO SELECIONA MANUALMENTE E-MAILS QUE CONSIDERA SPAM PARA QUE O FILTRO POSSA APRENDER A DISTINGUI-LOS.


@mapasdathai

QUESTÕES COMENTADAS – CESPE

1. **(CESPE / Prefeitura de Boa Vista-RR - 2023)** Assinale a opção que indica um programa que, se existente no computador, poderá protegê-lo de um arquivo malicioso baixado da Internet:

   a) Lixeira
   b) antivírus
   c) Limpeza de Disco
   d) Explorador de Arquivos.

Comentários:

A questão trata do antivírus, que é um programa essencial para a segurança do computador, pois sua principal função é detectar, bloquear e remover arquivos maliciosos, como vírus, trojans, worms, spyware e outras formas de malware que podem ser baixados acidentalmente ou intencionalmente da internet.

Gabarito: Letra B

---

2. **(CESPE / PO-AL - 2023)** Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

Comentários:

Essas são funções de firewalls e, não, antivírus. Um sistema de firewall pessoal abrangente, quando bem configurado, é capaz de bloquear tentativas de invasão e de exploração de vulnerabilidades do computador do usuário e de possibilitar a identificação das origens dessas tentativas.

Gabarito: Errado

---

3. **(CESPE / TRT8 – 2022)** Certo TRT deseja implementar uma solução de segurança cibernética que combine inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas.

   Com base nessa situação hipotética, assinale a opção que indica a solução requerida.

   a) NGAV.
   b) IPS
   c) IDS
   d) NIST

e) WebProxy

Comentários:

O NGAV (Next Generation Antivirus) é a ferramenta utilizada para combinar inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas. Para entender o que são e como funcionam os antivírus da nova geração, é preciso focar na sua principal diferença em relação aos antivírus convencionais. Essas soluções que conhecemos há décadas não são "inteligentes"; tudo o que fazem é varrer o sistema em busca de ameaças conhecidas, que constam em listas atualizadas várias vezes ao dia.

O problema é que o tempo entre uma atualização e outra é suficiente para milhares de ataques agirem com sucesso. Logo, as ferramentas tradicionais acabam sendo vulneráveis a diversas ameaças. O NGAV atua além de assinaturas de malware conhecidas – eles usam análises preditivas, conduzidas por aprendizado de máquina e inteligência artificial, combinando com inteligência de ameaças para detectar e prevenir ataques de malware.

Podem também identificar comportamentos maliciosos de fontes desconhecidas, bem como coletar e analisar dados para determinar as causas raiz de uma vulnerabilidade. Assim, são capazes de responder a ameaças novas e emergentes que anteriormente não eram detectadas. Em suma, um NGAV age com base no comportamento do usuário, verificando em tempo real se cada atividade sua representa – ou não – um risco.

E faz isso com análises constantes sobre tudo que é feito no dispositivo, usando inteligência artificial e aprendizado de máquina, para determinar o que é seguro ou não.

Gabarito: Letra A

---

4. **(CESPE / PC-AL – 2021)** A heurística é um dos métodos de detecção das ferramentas antimalware – como antivírus, antirootkit e antispyware – que se baseiam nas estruturas, instruções e características que o código malicioso possui para identificá-lo.

Comentários:

Perfeito! A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável malware.

Gabarito: Correto

---

5. **(CESPE / BNB– 2018)** Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes.

Comentários:

Na verdade, scareware é um software malicioso que faz com que os usuários de computadores acessem sites infestados por malware – não se trata de um antivírus!

Gabarito: Errado

---

6. **(CESPE / Polícia Federal – 2018)** Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Comentários:

A heurística é um conjunto de técnicas para identificar vírus desconhecidos de forma proativa – sem depender de assinatura. Nesta linha, a solução de segurança analisa trechos de código e compara o seu comportamento com certos padrões que podem indicar a presença de uma ameaça. Para cada ação executada pelo arquivo é atribuída uma pontuação e assim – se esse número for superior a um determinado valor – será classificado como um provável malware. Antivírus de 2ª Geração realmente utilizam heurísticas para identificar códigos maliciosos.

Gabarito: Correto

---

7. **(CESPE / CRBM – 2018)** O antispyware é conhecido como uma ferramenta complementar ao antivírus que deve ser executada frequentemente para checagem de possíveis ameaças que possam ter contaminado o sistema.

Comentários:

Perfeito... realmente é complementar aos antivírus – atualmente um antimalware integra todas essas ferramentas.

Gabarito: Correto

---

8. **(CESPE / CFO/DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

Comentários:

Elas conseguem - sim - realizar a verificação no conteúdo dos e-mails.

Gabarito: Errado

---

9. **(CESPE / TRE-PI – 2016)** A remoção de códigos maliciosos de um computador pode ser feita por meio de:

a) anti-spyware.
b) detecção de intrusão.
c) anti-spam.
d) anti-phishing.
e) filtro de aplicações.

Comentários:

(a) Correto, forçand a barra, anti-spywares podem remover spywares – que são malwares; (b) Errado, essas são ferramentas de monitoramento e detecção de intrusos em uma rede; (c) Errado, essas ferramentas protegem contra e-mails indesejados; (d) Errado, essas ferramentas protegem contra golpes ou fraudes de para obtenção de dados pessoais ou financeiros; (e) Errado, essas ferramentas permitem controlar acesso e analisar conteúdo de pacotes.

Gabarito: Letra A

---

10. **(CESPE / TRE-MT – 2015)** A função principal de uma ferramenta de segurança do tipo antivírus é:

a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.
b) verificar arquivos que contenham códigos maliciosos.
c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.
d) bloquear sítios de propagandas na Internet.
e) evitar o recebimento de mensagens indesejadas de email, tais como mensagens do tipo spams.

Comentários:

(a) Errado, essa é a função principal de um firewall; (b) Correto, a função principal de um antivírus realmente é verificar arquivos que contenham códigos maliciosos; (c) Errado, antivírus não realizam becapes; (d) Errado, essa é a função principal de um bloqueador de pop-ups; (e) Errado, essa é a função principal de um antispam – alguns antivírus podem exercer essa função, mas não é a sua função principal.

Gabarito: Letra B

---

11. (CESPE / Telebras – 2015) Como os antivírus agem a partir da verificação da assinatura de vírus, eles são incapazes de agir contra vírus cuja assinatura seja desconhecida.

Comentários:

Primeiro, é sempre possível agir isolando o vírus. Segundo, há tipos de antivírus que não necessitam conhecer a assinatura do vírus, eles podem também analisar seu comportamento.

Gabarito: Errado

---

12. (CESPE / TRT-10 Região – 2013) Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

Comentários:

Perfeito, perfeito, perfeito! Recomenda-se manter o antivírus sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.

Gabarito: Correto

---

13. (CESPE / SESA-ES – 2013 – Letra C) O anti-spyware, ao contrário do antivírus, propaga a proteção contra os vírus existentes de maneira semelhante a um antídoto, o que evita a contaminação de outros computadores da rede.

Comentários:

Que viagem é essa? Antispyware protege contra spyware e, não, contra vírus.

Gabarito: Errado

---

14. (CESPE / Banco da Amazônia – 2012) Antispywares são softwares que monitoram as máquinas de possíveis invasores e analisam se, nessas máquinas, há informações armazenadas indevidamente e que sejam de propriedade do usuário de máquina eventualmente invadida.

Comentários:

Na verdade, antispywares são softwares que monitoram as máquinas de possíveis usuários e, não, invasores. Além disso, eles não procuram informações armazenadas e, sim, o programa malicioso que rouba informações do usuário.

Gabarito: Errado

---

15. **(CESPE / Polícia Federal – 2012)** A fim de se proteger do ataque de um spyware — um tipo de vírus (malware) que se multiplica de forma independente nos programas instalados em um computador infectado e recolhe informações pessoais dos usuários —, o usuário deve instalar softwares antivírus e antispywares, mais eficientes que os firewalls no combate a esse tipo de ataque.

Comentários:

Na verdade, spyware não é um tipo de vírus e também não se multiplica de forma independente.

Gabarito: Errado

---

16. **(CESPE / PEFOCE – 2012)** O antivírus, para identificar um vírus, faz uma varredura no código do arquivo que chegou e compara o seu tamanho com o tamanho existente na tabela de alocação de arquivo do sistema operacional. Caso encontre algum problema no código ou divergência de tamanho, a ameaça é bloqueada.

Comentários:

Einh? Como é? A comparação é realizada com o tamanho registrado em um banco de dados criado e mantido pelo próprio antivírus. Não há nenhuma relação com a tabela de alocação de arquivo do sistema operacional. O FAT (File Allocation Table) é uma tabela de utilização do disco rígido que permite ao sistema operacional saber exatamente onde um arquivo está armazenado.

Gabarito: Errado

---

17. **(CESPE / TCE-RO – 2012)** A manutenção da atualização dos antivírus auxilia no combate às pragas virtuais, como os vírus, que são mutantes.

Comentários:

Perfeito! Recomenda-se manter o antimalware/antivírus sempre atualizado, com a versão mais recente e com todas as atualizações existentes aplicadas.

Gabarito: Correto

---

18. **(CESPE / TRE/RJ – 2012)** Recomenda-se utilizar antivírus para evitar phishing-scam, um tipo de golpe no qual se tenta obter dados pessoais e financeiros de um usuário.

Comentários:

Os navegadores podem ajudar a evitar phishing-scam – antivírus não são capazes, por padrão, de realizar essa função.

Gabarito: Errado

---

19. (CESPE / Banco da Amazônia – 2012) As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

Comentários:

A verificação heurística é a capacidade que um antivírus possui de detectar um malware, sem possuir uma vacina específica para ele, isto é, a ideia da heurística é a de antecipar a descoberta de um malware. A questão trata da verificação de assinaturas, que determina as características que levam um arquivo a ser ou não considerado um malware.

Gabarito: Errado

---

20. (CESPE / TJ/AC – 2012) O antispyware é um software que se destina especificamente a detectar e remover spywares, enquanto o antivírus é uma ferramenta que permite detectar e remover alguns programas maliciosos, o que inclui certos tipos de spywares.

Comentários:

Perfeito... antivírus modernos – apesar do nome – permitem detectar e remover diversos tipos de software maliciosos, incluindo spywares.

Gabarito: Correto

---

21. (CESPE / TJ/AC – 2012) As ferramentas antispam permitem combater o recebimento de mensagens consideradas spam e, em geral, baseiam-se na análise do conteúdo das mensagens.

Comentários:

Sendo rigoroso, elas não combatem o recebimento em si – as mensagens indesejadas continuam sendo recebidas, mas elas são classificadas como spam. Em geral, baseiam-se na análise do conteúdo das mensagens. Enfim... caberia recurso!

Gabarito: Correto

---

22. (CESPE / IFB – 2011) Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

Comentários:

Como assim? Eles ajudam muito a reduzir riscos de segurança da informação.

Gabarito: Errado

---

23. (CESPE / FUB – 2009) O aplicativo antivírus original dessa versão do Windows é o Symantec Norton 2003.

Comentários:

Nem precisa saber à qual versão do Windows a questão se refere! Norton é um software antivírus proprietário, que não é nativo de nenhuma versão do MS-Windows.

Gabarito: Errado

QUESTÕES COMENTADAS – FCC

24. (FCC / TRF/4ª Região – 2019) Caso uma praga virtual seja muito forte e sua remoção por meio do processo de deleção de arquivos ou programas infectados possa afetar todo o funcionamento do computador, os antivírus devem executar um processo:

a) para isolar completamente o sistema operacional do sistema de arquivos.
b) para criptografar o arquivo ou programa infectado inteiro, antes renomeando-o em uma cópia com os caracteres $~ na frente de seu nome.
c) que visa manter o sistema operacional suspenso.
d) que visa manter o arquivo ou programa infectado em quarentena.
e) que se incumbe apenas de renomear o arquivo ou programa infectado com os caracteres $~ na frente de seu nome.

Comentários:

(a) Errado. Isso deixaria o sistema operacional inutilizável, logo não ajudaria a resolver o problema; (b) Errado. Isso tornaria o arquivo ou programa inutilizável, logo não ajudaria a resolver o problema; (c) Errado. Isso deixaria o sistema operacional inutilizável, logo não ajudaria a resolver o problema; (d) Correto. Essa é uma maneira de deixar o arquivo isolado em uma área protegida do disco rígido por um período, logo é a ação mais adequada para o problema; (e) Errado. Isso não teria qualquer efeito prático.

Gabarito: Letra D

---

25. (FCC / SEMEF/Manaus – 2019) Um técnico tentou instalar uma aplicação no seu computador, mas o antivírus o impediu mostrando uma mensagem que o programa era legítimo, mas que poderia ser usado por criminosos para danificar o computador ou furtar dados pessoais. Analisando que as perdas que poderiam ser causadas pela execução do software seriam menores do que as perdas causadas pela não execução, o técnico pensou nas seguintes possibilidades para instalar e executar o software:

I. Incluir o software na lista de exclusão do antivírus, ou seja, na lista de programas que o antivírus não deverá verificar.

II. Mudar o nome do software para um nome amigável parecido com o nome recursos legítimos do sistema operacional, a fim de enganar o antivírus no momento da instalação e execução.

III. Desativar/Pausar o antivírus por um tempo determinado, ou seja, pelo tempo necessário para instalar e usar o software para o que necessita.

IV. Colocar o antivírus no modo de verificação apenas de disco rígido, de forma que ele não seja ativado quando perceber um possível malware carregado na memória.

Considerando que o técnico estava utilizando um dos principais antivírus do mercado, permitirá a instalação e execução do software APENAS o que consta em:

a) III.
b) I e III.
c) I e IV.
d) III e IV.
e) I e II.

Comentários:

(I) Correto. Caso ele esteja seguro, poderá incluir o software na lista de exclusão do antivírus de forma que o antivírus não o verifique; (II) Errado. Isso não teria qualquer efeito prático em termos de detecção pelo antivírus, uma vez que ele não verifica o nome do programa; (III) Correto. Caso ele esteja seguro, poderá pausar o antivírus enquanto instala o programa, de modo que o antivírus não impeça a instalação; (IV) Errado. Ao verificar apenas o disco rígido, ele poderá ser detectado normalmente pelo antivírus.

Gabarito: Letra B

---

26. (FCC / TRT/4ª Região – 2015) Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

Comentários:

(a) Errado, o ideal é que haja um antimalware instalado localmente na máquina do usuário – lembrem-se que um malware pode realizar ações maliciosas em um computador mesmo sem acesso à internet; (b) Errado, há diversos outros formatos de arquivos que podem causar danos além dos arquivos executáveis; (c) Errado, ambos devem ser sempre verificados – unidades removíveis, por exemplo, são fontes típicas de contaminação por malwares; (d) Errado, recomenda-se atualizar o antimalware sempre que houver novas atualizações independentemente da atualização do sistema operacional; (e) Correto, recomenda-se utilizar um único programa antimalware, uma vez que eles realmente podem entrar em conflito e afetar o desempenho do computador.

Gabarito: Letra E

---

27. (FCC / MPE/AM – 2013) Com relação à utilização correta de ferramentas antimalware, considere:

I. É aconselhável utilizar programas antimalware on-line quando se suspeitar que o antimalware local esteja desabilitado ou comprometido ou quando se necessitar de uma segunda verificação.

II. Devem ser configuradas para verificar apenas arquivos executáveis, pois são os únicos que podem conter vírus e outros tipos de malware.

III. Deve-se evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

IV. Não é recomendável ter um antimalware instalado no computador, pois os programas on-line além de serem mais eficientes, são suficientes para proteger o computador.

Está correto o que se afirma APENAS em:

a) I, II e III.
b) III e IV.
c) I e III.
d) II e IV.
e) I.

Comentários:

(I) Correto. Recomenda-se utilizar programas online quando suspeitar que o antimalware local esteja desabilitado/comprometido ou quando necessitar de uma segunda opinião (quiser confirmar o estado de um arquivo que já foi verificado pelo antimalware local); (II) Errado. Recomenda-se configurar o *antimalware* para verificar toda e qualquer extensão de arquivo; (III) Correto. Recomenda-se evitar a execução simultânea de diferentes programas antimalware, uma vez que eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de

detecção um do outro; (IV) Errado. Recomenda-se ter um antimalware instalado em seu computador (programas *online*, apesar de bastante úteis, exigem que seu computador esteja conectado à Internet para que funcionem corretamente e podem conter funcionalidades reduzidas).

Gabarito: Letra C

QUESTÕES COMENTADAS – FGV

28.(FGV / CGU – 2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

a) redução de custos e facilidade de atualização;
b) configuração simplificada e fácil instalação de API;
c) monitoramento completo e antivírus atualizado;
d) administração descentralizada e facilidade de integração com novas tecnologias;
e) bloqueio de ações indesejadas e controle no lado do usuário.

Comentários:

Endpoint é qualquer dispositivo, seja ele móvel ou não, desde uma estação de trabalho até notebooks, tablets e celulares, que podem ser conectados a uma rede. Logo, a segurança de endpoint visa assegurar que todos os serviços conectados a uma rede estejam protegidos contra vários tipos de ataques cibernéticos como worms, cavalos de troia, spywares, adwares, etc. Ué, professor... isso não é simplesmente um antivírus? Não...

Enquanto o antivírus é um software que detecta, impede e atua na remoção de programas de software maliciosos, como vírus e worms em PCs – único ou muitos -, a segurança de endpoint cobre toda a infraestrutura. Ele contém não apenas anti-malware, comum entre os antivírus, mas muitas ferramentas de segurança contra diferentes tipos de ameaças. Com ele, é possível manter a integridade dos dispositivos, a autenticação/autorização do usuário, para assim, preservar os endpoints seguros, o que não está incluído no pacote do antivírus.

Entre os benefícios da segurança de endpoint, temos:

- Redução de Custos: ao invés de investir em componentes separados para garantir a proteção de cada dispositivo conectado na rede, o sistema de endpoint reúne os componentes necessários em um só conjunto, o que é muito mais vantajoso financeiramente (Letra A);

- Fácil Instalação: basta instalar e configurar o servidor central que fará a segurança da rede. Assim, os dispositivos só conseguirão acessar a rede a partir da instalação do cliente em seus dispositivos;

- Administração Centralizada: é possível centralizar a rede a partir do sistema gerenciador de segurança, no caso, o endpoint. Assim, o gerente de infraestrutura de TI da empresa ou o parceiro

terceirizado passa a ser o administrador do servidor de endpoint, sendo responsável pelo controle para revogar e conceder permissões de uso, auditar a segurança, obter relatórios, monitorar a rede, entre outros aspectos. Essas ações ocorrem por meio de um orquestrador ou portal de gerenciamento remoto;

- Bloqueio de Ações Indesejadas: apesar de muitas vezes não ser intencional, invasões indesejadas podem ser frequentes no ambiente organizacional. Por exemplo, se um funcionário de uma empresa coloca um pendrive infectado no computador de trabalho, pode causar uma vulnerabilidade no sistema. Por esse motivo, algumas empresas possuem políticas de segurança que impedem que funcionários pluguem dispositivos internos em estações de trabalho. Assim, softwares de segurança de endpoint ajudam a bloquear esse tipo de atividade;

- Fácil integração com novas tecnologias: como o sistema de segurança é apenas um composto, torna-se mais fácil que novas soluções sejam adicionadas ao sistema de forma simples. Assim, as empresas têm acesso às atualizações de forma segura e unificada, de uma vez só, para todos os dispositivos.

Gabarito: Letra A

---

29. (FGV / PC-MA – 2012) Um funcionário em uma viagem de negócios teve de levar em seu notebook arquivos classificados para uma reunião com clientes. Ele foi então aconselhado pelo pessoal de suporte da empresa a instalar um antivírus em sua máquina. Resistindo à orientação recebida, o funcionário argumentou que:

I. O software antivírus deixa minha máquina muito lenta.
II. Eu não preciso de um software antivírus porque eu nunca abro arquivos anexados em e-mails de pessoas que eu não conheço.
III. Tantas pessoas usam a Internet, eu sou apenas um na multidão. Ninguém vai me achar.

São motivos válidos para a não instalação de um programa antivírus:

a) somente a opção I
b) somente a opção II
c) somente a opção III
d) somente as opções I e II
e) nenhuma das opções.

Comentários:

(I) Errado, esse não é um motivo válido porque a máquina não fica muito lenta – ele consome recursos computacionais, mas não deixam a máquina muito lenta; (II) Errado, abrir anexos de e-mail de pessoas conhecidas também pode ocasionar infecções, além disso existem outras formas de contaminação por vírus; (III) Errado, a infecção por malwares pode ocorrer mesmo sem acesso à internet como, por exemplo, através de mídias removíveis.

Gabarito: Letra E

QUESTÕES COMENTADAS – VUNESP

30. (VUNESP / Prefeitura de Palmas-TO – 2023) Tem-se 4 computadores com antivírus instalado, com as seguintes características descritas na tabela a seguir.

Instalação do antivírus: 01.janeiro.2023

Data atual: 23.janeiro.2023

	Computador A	Computador B	Computador C	Computador D
Última atualização de definições de antivírus	01.janeiro.2023	21.janeiro.2023	21.janeiro.2023	Nunca
Última execução do antivírus, fazendo uma varredura completa	01.janeiro.2023	Nunca	22.janeiro.2023	22.janeiro.2023

Considerando que a data atual é 23.janeiro.2023, assinale a alternativa que apresenta o computador que está mais protegido.

a) Computador A.
b) Computador B.
c) Computador C.
d) Computador D.

Comentários:

O computador mais protegido é aquele em que o antivírus teve suas definições atualizadas mais recentemente e em que o antivírus foi executado mais recentemente. Dito isso, trata-se do Computador C. Note que a última atualização de definições do antivírus ocorreu no dia 21 de janeiro e a última execução do antivírus, realizando uma varredura completa foi no dia 22 de janeiro.

Gabarito: Letra C

---

31. (VUNESP / PC-SP – 2022) Visando aumentar a proteção e a segurança dos computadores, diversas ferramentas *antimalware* podem ser utilizadas, como as *antirootkit*, que visam impedir que:

a) sejam capturadas e armazenadas posições do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o *mouse* é clicado.

b) sejam capturadas e armazenadas as teclas digitadas pelo usuário no teclado do computador.

c) um programa se instale para permitir o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

d) um conjunto de programas e técnicas escondam e assegurem a presença de um invasor ou de outro código malicioso em um computador comprometido.

e) um programa execute, além das funções para as quais foi aparentemente projetado, outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Comentários:

(a) Errado, ele não impede a ação de screenloggers; (b) Errado, ele não impede a ação de keyloggers; (c) Errado, ele não impede a ação de backdoors; (d) Correto, antirootkits impedem a ação de rootkits; (e) Errado, ele não impede a ação de trojans.

Gabarito: Letra D

---

32. **(VUNESP / Câmara de Sertãozinho-SP – 2019)** Programas antivírus representam uma importante ferramenta aos usuários de computadores, sendo que tais programas:

a) não atuam sobre arquivos presentes em mídias removíveis, como é o caso de pen drives.

b) não atuam sobre programas com determinadas extensões, como .pdf ou .docx.

c) não atuam sobre programas com tamanho de até 50 KB.

d) devem ser executados somente em dois momentos: quando o computador é ligado e quando é desligado.

e) devem ser mantidos atualizados, assim como as definições de vírus presentes nesses programas.

Comentários:

(a) Errado, eles atuam com ênfase em arquivos presentes em mídias removíveis, uma vez que essa é uma típica fonte de malwares; (b) Errado, eles podem atuar em programas com essas extensões; (c) Errado, não existe essa limitação de tamanho; (d) Errado, o ideal é que sejam executados em tempo real a todo momento; (e) Correto, o ideal é que sejam mantidos atualizados frequentemente assim como as suas definições de vírus.

Gabarito: Letra E

---

33. **(VUNESP / Câmara de Monte Alto - SP – 2019)** Um usuário necessita instalar, em seu computador, um programa antivírus. Duas das possíveis opções que ele pode selecionar para tal finalidade são os programas

a) McAfee e TrueCript.
b) Norton e Predator.
c) Bitdefender e 7-Zip.
d) AVG e Avast.
e) Kaspersky e WinRAR.

Comentários:

(a) Errado, Truecript é um software de criptografia de disco rígido; (b) Errado, desconheço antivírus chamado Predator; (c) Errado, 7-Zip é um software de compactação/descompactação de arquivos; (d) Correto; (e) Errado, WinRAR é um software de compactação/descompactação de arquivos.

Gabarito: Letra D

---

34. **(VUNESP / Prefeitura de Ribeirão Preto-SP – 2018)** A respeito da execução de um programa antivírus em um computador, é correto afirmar que:

a) somente pode ser feita em intervalos iguais ou maiores do que uma semana.
b) não pode ser feita quando não há Internet de banda larga disponível no computador.
c) só pode ser feita quando ocorre uma atualização do sistema operacional do computador.
d) pode ser programada para ocorrer, por exemplo, uma vez por dia.
e) não pode ser feita em sistemas operacionais instalados há mais de dois anos no computador.

Comentários:

(a) Errado, não só pode como é recomendável que seja feito com alta frequência; (b) Errado, pode ser feito inclusive sem acesso à internet; (c) Errado, pode ser feita independentemente da atualização do sistema operacional; (d) Correto, pode ser programada para ocorrer com qualquer frequência desejada; (e) Errado, não existe essa limitação.

Gabarito: Letra D

QUESTÕES COMENTADAS – CESGRANRIO

35. **(CESGRANRIO / Petrobrás – 2011)** Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o:

a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

Comentários:

(a) Errado, isso é um protocolo de comunicação; (b) Errado, isso é uma mídia de armazenamento; (c) Errado, isso é um protocolo de comunicação; (d) Errado, isso é um formato de distribuição de informações em tempo real; (e) Correto, eles realmente auxiliam na proteção de um computador.

Gabarito: Letra E

QUESTÕES COMENTADAS – DIVERSAS BANCAS

36. **(FUNDATEC / IPE SAÚDE – 2022)** Em segurança da informação, utiliza-se o antivírus para proteção do computador contra vírus, que são códigos maliciosos e podem comprometer o funcionamento da máquina, bem como a integridade dos dados nela armazenados. Quando a remoção de um vírus pode comprometer o funcionamento do computador, o antivírus adota o seguinte procedimento:

a) Coloca o vírus em quarentena durante um tempo, enquanto busca por mais problemas relacionados a ele.
b) Apaga o vírus imediatamente e conserta os danos causados pela sua remoção.
c) Solicita que o usuário repare todos os arquivos comprometidos pelo vírus utilizando outra ferramenta.
d) Não toma providência alguma, pois, ao remover o vírus, o computador pode ficar instável.
e) Desliga imediatamente o computador para que o vírus não contamine outros programas.

Comentários:

Em regra, quando um antivírus detecta uma ameaça, há a opção de remoção ou envio para a quarentena. Como a questão afirmou que a remoção pode afetar o funcionamento do computador, o item não pode ser removido, então ele deve ser movido para a quarentena. Lembrando que a quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto aguarda uma confirmação de identificação.

Gabarito: Letra A

---

37. **(IDIB / Ministério da Economia – 2021)** São softwares que detectam e removem programas maliciosos, como vírus e worms, protegendo os sistemas de computador contra essas ameaças. Assinale a alternativa que apresenta um desses programas:

a) Pipefy
b) Asana
c) Comodo
d) Avant
e) Acrobat

Comentários:

(a) Errado, esse é um software para gerenciamento de fluxos de trabalho; (b) Errado, esse é um software para gerenciamento de equipes e projetos; (c) Correto; (d) Errado, desconheço software com esse nome – acredito que a banca quis confundir com Avast; (e) Errado, esse é um software para leitura de PDF.

Gabarito: Letra C

---

38. (QUADRIX / CONRERP/2ª Região – 2019) O software antivírus, após sua instalação e configuração, não necessita de ser atualizado pelo fabricante, pois já contém uma lista de assinaturas válidas e consegue eliminar todas as formas de vírus.

Comentários:

Ele precisa – sim – ser atualizado pelo fabricante! Aliás, essa atualização deve ocorrer com alta frequência, uma vez que novas ameaça surgem diariamente no mundo inteiro. Dessa forma, a lista de assinaturas válidas deve ser constantemente revisitada.

Gabarito: Errado

---

39. (OBJETIVA / Prefeitura de Tupanci do Sul - RS – 2019) Atenção! Para responder às questões de Informática, a menos que seja explicitamente informado o contrário, considerar que os programas mencionados encontram-se na versão Português-BR e em sua configuração padrão de instalação, possuem licença de uso, o mouse está configurado para destros, um clique ou duplo clique correspondem ao botão esquerdo do mouse, e teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Dessa forma, as teclas de atalho, os menus, os submenus, as barras, os ícones e os demais itens que compõem os programas abordados nesta prova encontram-se na configuração padrão.

Em conformidade com a Cartilha de Segurança para Internet, sobre mecanismos de segurança, assinalar a alternativa que preenche a lacuna abaixo CORRETAMENTE:

Ferramentas _____ são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

a) pop-up's
b) backups
c) antispam
d) antimalware

Comentários:

As ferramentas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador são as ferramentas antimalware.

Gabarito: Letra D

---

40. (IBADE / SAAE de Vilhena - RO – 2019) Qual dos softwares abaixo é um Anti-Virus?

a) Avast
b) Excel
c) Squirrel
d) WinRAR
e) WinZip

Comentários:

(a) Correto, é um antivírus; (b) Errado, é uma ferramenta de planilha eletrônica; (c) Errado, esse é um recurso de webmail do Linux; (d) Errado, essa é uma ferramenta de compactação de arquivos; (e) Errado, essa é uma ferramenta de compactação de arquivos.

Gabarito: Letra A

---

41. (IADES / CAU-MT – 2019) O antivírus tem como responsabilidade proteger o computador de potenciais arquivos maliciosos:

a) A capacidade de detecção de novas ameaças de um antivírus independe de ele estar atualizado.
b) O antivírus tem como principal responsabilidade proteger a navegação do usuário na internet.
c) São tão importantes para o funcionamento de um computador que todas essas máquinas já vêm com um antivírus previamente instalado.
d) Quando um antivírus está ativado, o computador está seguro contra qualquer tipo de ataque.
e) Uma das capacidades do antivírus é inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

Comentários:

(a) Errado, novos vírus surgem todos os dias, logo suas assinaturas precisam ser identificadas para atualizar a base de dados dos antivírus de modo que ele fique atualizado e consiga detectar novas ameaças; (b) Errado, sua principal responsabilidade é proteger computadores de malwares e, não, a navegação na internet; (c) Errado, não é obrigatório ter um antivírus para o funcionamento de um computador, logo eles não são necessariamente pré-instalados; (d) Errado, ele não é infalível; (e) Correto, ele realmente é capaz de inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

Gabarito: Letra E

---

42. (UECE-CEV / DETRAN/CE – 2018) Um software antivírus é um programa responsável por:

a) dividir os recursos da máquina entre os processos em execução.

b) prevenir, procurar, detectar e remover programas maliciosos.
c) arranjar em espaço contíguo os arquivos contidos em disco.
d) realizar a atualização do sistema operacional.

Comentários:

(a) Errado, essa não é uma função de antivírus; (b) Correto, essa é uma função típica de antivírus; (c) Errado, essa não é uma função de antivírus; (d) Errado, essa não é uma função de antivírus;

Gabarito: Letra B

---

43. (FAPEC / UFMS – 2018) A prevenção, detecção e a eliminação de vírus são feitos por aplicativos denominados antivírus. É um exemplo de antivírus:

a) AVG.
b) FTP.
c) Keylogger.
d) Spam.
e) Malware.

Comentários:

(a) Correto, esse é um exemplo de software antivírus; (b) Errado, isso é um exemplo protocolo de comunicação; (c) Errado, isso é um exemplo de software malicioso; (d) Errado, esse é uma mensagem eletrônica indesejável; (e) Errado, isso é um software malicioso.

Gabarito: Letra A

---

44. (CPCON / Prefeitura de São José dos Pinhais-PB – 2018) Alguns softwares de antivírus têm se popularizado bastante e construído marcas sólidas e facilmente reconhecíveis por seus usuários. NÃO é um exemplo de software antivírus:

a) McAfee.
b) NetBeans.
c) Avast.
d) Kaspersky.
e) Norton.

Comentários:

(a) Correto, trata-se de um exemplo de software antivírus; (b) Errado, trata-se de uma ferramenta de programação; (c) Correto, trata-se de um exemplo de software antivírus; (d) Correto, trata-se de um exemplo de software antivírus; (e) Correto, trata-se de um exemplo de software antivírus.

Gabarito: Letra B

---

45. (IF-CE / IF-CE – 2017) São ações desejáveis em um programa de antivírus:

a) proteção contra arquivos infectados de e-mail e varredura à procura de vírus em tempo real.
b) verificação contínua de defeitos de discos rígidos e varredura à procura de vírus em tempo real.
c) alerta de instalação de aplicativos infectados e impedimento de formatação de disco rígido.
d) proteção contra arquivos infectados de e-mail e atualização de softwares aplicativos.
e) atualização automática do programa de antivírus e criptografia de mensagens de e-mail.

Comentários:

(a) Correto, é altamente desejável que ele seja capaz de verificar e-mails, uma vez que essa é uma fonte típica de contaminação por malwares – de preferência, em tempo real; (b) Errado. Ele não é utilizado para detectar defeitos de discos rígidos; (c) Errado. Ele não deve impedir a formatação de disco rígido; (d) Errado. Ele não deve ser utilizado para atualizar softwares aplicativos; (e) Errado. Ele não deve criptografar mensagens de e-mail.

Gabarito: Letra A

---

46. (IESES / Prefeitura de São José do Cerrito – 2017) O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de:

a) Gerenciamento de Banco de Dados.
b) Antivírus.
c) Backup.
d) Processamento de Textos.

Comentários:

O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de... antivírus.

Gabarito: Letra B

---

47. (QUADRIX / CRB 6ª Região – 2017) Em um ambiente público, com um microcomputador e um sistema operacional para desktop com acesso à internet, as diversas vulnerabilidades e falhas de segurança são uma constante preocupação ao usuário, seja navegando na internet ou acessando o microcomputador. Qual das seguintes alternativas auxilia um usuário padrão a se proteger de vírus e programas maliciosos?

a) Backup.
b) PROXY.
c) Planilhas eletrônicas.
d) Antivírus.
e) Rede IP.

Comentários:

O software utilizado para auxiliar um usuário padrão a se proteger de vírus e outros programas maliciosos é também chamado de... antivírus.

Gabarito: Letra D

48.(CS-UFG / UFG – 2017) Antivírus são programas de computador voltados para a eliminação e o controle de pragas virtuais, tais como:

a) spyware e firewall.
b) spam e boot.
c) worms e cavalos de Troia.
d) macro e log.

Comentários:

(a) Errado, Firewall é uma ferramenta de proteção e segurança; (b) Errado, boot é o nome dado a inicialização de um sistema operacional; (c) Correto, ambos podem ser eliminados ou controlados por softwares antivírus; (d) Errado, macro é um conjunto de instruções e log é o processo de registro de informações.

Gabarito: Letra C

49.(IBADE / IPERON-RO – 2017) Um usuário precisa instalar em seu microcomputador um software antivírus de mercado, para se prevenir de ataques. Um software dessa categoria é o:

a) Media Player.
b) Switcher.
c) Kaspersky.
d) Adware.
e) Broadsheeet.

Comentários:

(a) Errado, isso é um exemplo de player de vídeo; (b) Errado, isso não existe; (c) Correto, isso é um exemplo de software antivírus; (d) Errado, isso é um exemplo de software malicioso; (e) Errado, isso não existe.

Gabarito: Letra C

---

50. (QUADRIX / CFO-DF – 2017) Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

Comentários:

Filtros Antispam vêm integrado à maioria dos webmails e clientes de e-mails para separar os e-mails desejados dos indesejados (chamados de spams). A maioria dos filtros passa por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro "aprende" a distinguir as mensagens. Para realizar esse procedimento, ele precisa ter acesso ao conteúdo desses e-mails.

Gabarito: Errado

---

51. (IF/PA / IF/PA – 2016) O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o:

a) Antivírus.
b) Firewall.
c) Filtro Antispam.
d) Filtro de janelas de pop-up.
e) Algoritmo criptográfico.

Comentários:

O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o Filtro Antispam.

Gabarito: Letra C

---

52. (IDECAN / UE-RN – 2016) O software responsável por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados denomina-se:

a) Rootkit.
b) Antivírus.
c) Backdoor.
d) Keylogger.

Comentários:

(a) Errado, isso é um exemplo de software mal-intencionado; (b) Correto, antivírus são softwares responsáveis por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados; (c) Errado, isso é um exemplo de software mal-intencionado; (d) Errado, isso é um exemplo de software mal-intencionado;

Gabarito: Letra B

---

53. **(UFCG / UFCG – 2016)** Antivirus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus de computadores. São exemplos de antivirus disponíveis no mercado, EXCETO:

a) Avira Free Antivirus.
b) AVG AntiVirus.
c) Comodo.
d) Windows Defender.
e) Formoid.

Comentários:

(a) Correto, trata-se de um exemplo de antivírus; (b) Correto, trata-se de um exemplo de antivírus; (c) Correto, trata-se de um exemplo de antivírus; (d) Correto, trata-se de um exemplo de antivírus e antispyware nessa época; (e) Errado, isso não é um exemplo de antivírus.

Gabarito: Letra E

---

54. **(CRO-SC / CRO-SC – 2016)** São exemplos de programas antivírus todos os seguintes, EXCETO:

a) Karspersky
b) Avast
c) Quicken
d) AVG

Comentários:

(a) Correto, esse é um exemplo de programa antivírus; (b) Correto, esse é um exemplo de programa antivírus; (c) Errado, esse não é um exemplo de programa antivírus; (d) Correto, esse é um exemplo de programa antivírus.

Gabarito: Letra C

---

55. (COPEVE-UFAL / UFAL – 2016) Após a detecção de um vírus, normalmente os softwares antivírus oferecem duas opções para o usuário: deletar ou colocar em quarentena. Nesse contexto, quando é mais indicado colocar o arquivo em quarentena, ao invés de apagá-lo?

a) Quando o arquivo infectado é considerado importante para o bom funcionamento do sistema ou de grande valor para o usuário.

b) Quando o antivírus foi capaz de remover completamente o vírus do arquivo infectado, a fim de ficar um tempo em observação.

c) Quando o arquivo infectado possui tamanho longo, normalmente acima de 20MB, a fim de otimizar o tempo de execução do antivírus.

d) É sempre mais indicado excluir definitivamente o arquivo, caso contrário, o vírus volta à ativa na próxima vez que o computador for reiniciado.

e) Quando o arquivo infectado é um executável totalmente desconhecido que não pertence ao sistema operacional nem a nenhum software instalado pelo usuário.

Comentários:

(a) Correto. Se o arquivo for importante, recomenda-se colocá-lo em quarentena; (b) Errado. Nesse caso, é melhor removê-lo; (c) Errado, o tamanho é irrelevante para essa decisão; (d) Errado, por vezes o arquivo pode ser importante tanto para o usuário quanto para o sistema; (e) Errado, mesmo sendo um arquivo executável, pode ser um falso-positivo.

Gabarito: Letra A

---

56. (IADES / ELETROBRÁS – 2015) Os arquivos de computador podem ser contaminados por vírus. A forma mais comum de contaminação ocorre por meio de mensagens eletrônicas (e-mail). Para evitar contaminações e realizar a recuperação de arquivos contaminados, são utilizados os programas antivírus. A esse respeito, é correto afirmar que a área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador denomina-se:

a) lixeira.
b) disco rígido.
c) pasta spam.
d) área de trabalho.
e) quarentena.

Comentários:

A área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador é denominada... quarentena.

Gabarito: Letra E

---

57. **(INAZ DO PARÁ / Prefeitura de Terra Alta – 2015)** Atualmente, a informação representa o maior bem dentro de qualquer organização; assim, existem diversas formas de se garantir a proteção da mesma. Dentre os diversos procedimentos existentes, assinale qual pode ser considerada a forma mais segura para proteção desta informação:

a) Backup.
b) Firewall.
c) Ifconfig.
d) Antivírus.
e) Dump.

Comentários:

Questão horrorosa! Dependendo do critério utilizado, backup, firewall e antivírus podem ser consideradas formas seguras em certo nível para proteção de informação.

Gabarito: Letra D

---

58. **(COSEAC / CLIN – 2015)** São normalmente funcionalidades de um software antivírus as abaixo relacionadas, EXCETO:

a) impedir que um hacker explore vulnerabilidades em seu sistema.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) verificar continuamente os discos rígidos e discos removíveis.

Comentários:

(a) Errado, essa seria uma possível funcionalidade de firewalls; (b) Correto, analisar downloads é uma função comum de antivírus; (c) Correto, procurar programas maliciosos em anexos de e-mails é uma função comum de antivírus; (d) Correto, verificar discos rígidos e removíveis é uma função comum de antivírus.

Gabarito: Letra A

---

59. **(PR-4 UFRJ/ UFRJ – 2015)** Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar vírus de um computador. São exemplos de antivírus:

a) AVG, Avast e Avira.
b) AVG, Hoax e FTP.
c) Hoax, Avast e Avira.
d) Spam, Keylogger e AVG.
e) Spam, Avast e Hoax.

Comentários:

(a) Correto, todos são exemplos de antivírus; (b) Errado, Hoax é um boato e FTP é um protocolo; (c) Errado, Hoax é um boato; (d) Errado, Spam é uma mensagem de e-mail indesejada e Keylogger é um software malicioso; (e) Errado, Spam é uma mensagem de e-mail indesejada e Hoax é um boato.

Gabarito: Letra A

---

60. (FUNIVERSA / SEAP-DF – 2015) Um dos procedimentos de segurança da informação é instalar no computador o anti-spyware e o antivírus, pois o anti-spyware é um aplicativo que complementa o antivírus.

Comentários:

De fato, antivírus não têm uma eficácia tão boa no combate aos spywares. Dessa forma, para manter o computador com uma proteção razoável, é interessante usar um antispyware, que complementa a ação do antivírus, combatendo os programas maliciosos que o antivírus tem problemas em combater.

Gabarito: Correto

---

61. (UFBA / UFOB – 2014) Para identificar um vírus, o antivírus faz uma comparação entre o arquivo que chega por algum meio de entrada e uma biblioteca de informações sobre os vários tipos de vírus, o que explica a importância de manter o antivírus sempre atualizado.

Comentários:

Perfeito! Essa biblioteca é chamada de arquivo de assinaturas. É bastante recomendável manter o arquivo de assinaturas sempre atualizado. Recomenda-se também configurar o antimalware para atualizá-lo automaticamente pela rede e, de preferência, diariamente.

Gabarito: Correto

---

62. (FUMARC / Câmara Municipal de Mariana/MG – 2014) São exemplos de softwares antivírus, EXCETO:

a) Avast.
b) AVG.
c) Kaspersky.
d) Microsoft Windows Defender, disponível no Windows 7.

Comentários:

(a) Correto, é um exemplo de software antivírus; (b) Correto, é um exemplo de software antivírus; (c) Correto, é um exemplo de software antivírus; (d) Errado, ele era apenas um antispyware na época dessa questão.

Gabarito: Letra D

---

63. (CETRO / FUNDAÇÃO CASA – 2014) Sobre os softwares antivírus, assinale a alternativa correta.

a) Algumas empresas mantêm softwares antivírus em seus websites e oferecem os serviços do software via Internet.
b) Cada antivírus protege contra um único tipo de software malicioso.
c) Cada antivírus utiliza somente uma estratégia de detecção de softwares maliciosos.
d) Não existem antivírus que protejam os computadores em tempo real.
e) A única coisa que o antivírus consegue fazer é detectar o vírus e eliminar os arquivos infectados.

Comentários:

(a) Correto, existem antivírus online capazes de escanear arquivos; (b) Errado, antivírus protegem contra diversos tipos de softwares maliciosos; (c) Errado, antivírus utilizam diversas estratégias de detecção de softwares maliciosos; (d) Errado, existem diversos antivírus capazes de proteger computadores em tempo real; (e) Errado, ele pode colocá-lo em quarentena.

Gabarito: Letra A

---

64. (COSEAC / Prefeitura de Niterói/RJ – 2014) São funções rotineiras de um programa antivírus as abaixo relacionadas, EXCETO:

a) identificar e eliminar vírus e outros tipos de malwares.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) possibilitar a atualização das assinaturas de novos vírus de forma automática.
e) efetuar o controle de configuração dos softwares na rede.

Comentários:

(a) Correto, programas antivírus têm como função identificar e eliminar vírus e outros tipos de malwares; (b) Correto, programas antivírus têm como função analisar downloads da Internet; (c) Correto, programas antivírus têm como função procurar programas maliciosos em anexos de e-mails; (d) Correto, programas antivírus têm função de possibilitar a atualização de assinaturas de novos vírus de forma automática; (e) Errado, programas antivírus não realizam controle de configuração de softwares na rede – essa não é uma de suas funções.

Gabarito: Letra E

---

65. (BIO-RIO / Prefeitura de Três Rios – 2014) Atualmente, com o objetivo de evitar a contaminação dos computadores é necessário instalar um software antivírus na máquina. Dois exemplos de antivírus são:

a) McAfee e Shirink
b) Safari e Linkedin
c) Avast e Psafe
d) AVG e Winrar
e) Bing e Android.

Comentários:

(a) Errado, Shirink não existe; (b) Errado, Safari é um navegador e Linkedin é uma rede social; (c) Correto, ambos são softwares antivírus; (d) Errado, Winrar é um compactador/descompactador de arquivos; (e) Errado, Bing é uma ferramenta de busca e Android é um sistema operacional móvel.

Gabarito: Letra C

---

66. (MPE-RS / MPE-RS – 2014) Código Malicioso é o termo genérico usado para referir programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Qual das alternativas abaixo NÃO apresenta um tipo de código malicioso?

a) Antivírus.
b) Bot.
c) Worm.
d) Spyware
e) Cavalo de Tróia.

Comentários:

(a) Correto, trata-se de um software para proteção contra código malicioso; (b) Errado, trata-se de um exemplo de código malicioso; (c) Errado, trata-se de um exemplo de código malicioso; (d)

Errado, trata-se de um exemplo de código malicioso; (e) Errado, trata-se de um exemplo de código malicioso.

Gabarito: Letra A

---

67. (BIO-RIO / EMGEPRON– 2014) A instalação de um antivírus em um microcomputador é de suma importância para o seu funcionamento satisfatório, no que diz respeito à segurança dos dados e ao próprio desempenho da máquina. Dois exemplos de programas antivírus são:

a) iTunes e Avast!
b) Avast! e McAfee
c) McAfee e WinZip
d) WinZip e iTunes.

Comentários:

(a) Errado, iTunes é um player de música; (b) Correto, ambos são programas antivírus; (c) Errado, WinZip é um compactador/descompactar de arquivos; (d) Errado, WinZip é um compactador e descompactar de arquivos, e iTunes é um player de música.

Gabarito: Letra B

---

68. (UFBA / UFBA – 2013) A instalação e o uso de programas "antivírus" aumentam a segurança dos arquivos armazenados no computador.

Comentários:

Perfeito! Eles ajudam bastante a melhorar o nível de segurança dos arquivos armazenados em um computador.

Gabarito: Correto

---

69. (AOCP / Colégio Pedro II – 2013) Antivírus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus do computador. Assinale a alternativa que NÃO representa um antivírus.

a) Avast.
b) AVG.
c) Microsoft Security Essentials.
d) Kaspersky.
e) WinRAR.

Comentários:

(a) Correto, trata-se de um antivírus; (b) Correto, trata-se de um antivírus; (c) Correto, trata-se de um antivírus; (d) Correto, trata-se de um antivírus; (e) Errado, trata-se de compactador e descompactador de arquivos.

Gabarito: Letra E

---

70. (FUNCAB / SC/CE – 2013) O software antivírus é um software da categoria dos(as):

a) sistemas operacionais.
b) linguagens de programação.
c) softwares utilitários.
d) firmwares.
e) softwares aplicativos.

Comentários:

Antivírus é um tipo de software utilitário, isto é, são utilizados para suprir deficiências dos sistemas operacionais, melhorando seus recursos.

Gabarito: Letra C

---

71. (FUNCAB / CODATA – 2013) Sobre sistemas antivírus, é correto afirmar:

a) Garantem integralmente a segurança das informações em seu computador.
b) Distribuem os arquivos contaminados pela rede do seu computador, visando a enfraquecer o vírus.
c) Por padrão, movem para a lixeira arquivos contaminados do seu computador.
d) Os programas antivírus examinam os arquivos antes de abri-los e notificam o usuário do computador, caso encontrem um arquivo potencialmente não seguro.
e) garantem a recuperação de arquivos danificados por Cavalo de Troia.

Comentários:

(a) Errado, eles não garantem integralmente a segurança das informações de um computador; (b) Errado, eles impedem a distribuição de arquivos contaminados; (c) Errado, eles notificam o usuário para que ele decida o que fazer; (d) Correto, eles realmente examinam o arquivo e notificam o usuário quando encontram arquivos potencialmente perigosos; (e) Errado, não há garantia de recuperação de arquivos infelizmente.

Gabarito: Letra D

---

72. **(CETRO / Prefeitura de Manaus – 2012)** Quanto ao processo de quarentena, que alguns softwares antivírus oferecem, é correto afirmar que:

a) quarentena é uma área separada em um disco rígido.

b) apesar de isolar os arquivos, a quarentena não consegue impedir que outros arquivos sejam infectados pelo software suspeito.

c) somente o software antivírus tem a capacidade de colocar um software suspeito em quarentena.

d) após determinado tempo, os arquivos em quarentena são eliminados automaticamente.

e) arquivos em quarentena sempre são eliminados do computador, já que não existe solução para o problema deles (infecção).

Comentários:

(a) Correto, quarentena é uma área virtual onde o antivírus armazena arquivos identificados como possíveis vírus enquanto ele aguarda uma confirmação de identificação; (b) Errado, ela consegue – sim – impedir que outros arquivos sejam infectados porque ela isola o arquivo que infecta; (c) Errado, um usuário pode colocar um software suspeito em quarentena manualmente; (d) Errado, eles não são eliminados até que o usuário o deseje; (e) Errado, eles não são necessariamente eliminados do computador.

Gabarito: Letra A

---

73. **(FUNCAB / SESC-BA – 2012)** Considere que o técnico da área de suporte da empresa na qual você trabalha tenha detectado, em seu computador, um Cavalo de Troia. O recurso de computador que pode ter auxiliado nessa localização foi:

a) Ferramenta de Busca Google
b) Firewall
c) Sistema Antivírus
d) Gerenciador de Tarefas.
e) Fragmentador.

Comentários:

O recurso de computador que pode ter auxiliado na localização de um software malicioso como um Cavalo de Troia é o Sistema Antivírus.

Gabarito: Letra C

---

74. (UECE-CEV / SEPLAG-CE – 2011) O software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos é denominado:

a) Bloco de Notas.
b) Microsoft Office.
c) Windows Explorer.
d) Antivírus.

Comentários:

(a) Errado, isso é um editor de texto; (b) Errado, isso é uma suíte de ferramentas de escritório; (c) Errado, isso é um navegador web; (d) Correto, isso é um software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos.

Gabarito: Letra D

---

75. (PONTUA / TRE-SC – 2011) Os sistemas antivírus são programas que têm o objetivo de detectar e, então, anular ou eliminar os vírus encontrados no computador. Marque V (Verdadeiro) e F (Falso) para os exemplos de programas antivírus:

( ) Norton.
( ) WinZip.
( ) McAfee.
( ) Kaspersky.
( ) Word.

A sequência CORRETA, de cima para baixo, é:

a) F – F – V – V – V.
b) V – F – V – V – F.
c) F – V – F – F – V.
d) V – V – V – V – F.

Comentários:

(V) Norton é um exemplo de programa antivírus; (F) WinZip é um compactador/descompactador de arquivos; (V) McAfee é um exemplo de programa antivírus; (V) Kaspersky é um exemplo de programa antivírus; (F) Word é um processador de texto.

Gabarito: Letra B

---

76. **(FUNCAB / Prefeitura de Porto Velho/RO – 2009)** Às vezes, os sistemas Antivírus detectam vírus desconhecidos que não podem ser eliminados com o conjunto de ferramentas disponíveis. Qual a função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados no seu computador?

a) Scanear;
b) Colocar em quarentena;
c) Reparar;
d) Congela;
e) Purgar.

Comentários:

A função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados em um computador é chamada de... quarentena.

Gabarito: Letra B

Lista de Questões – CESPE

1. **(CESPE / Prefeitura de Boa Vista-RR - 2023)** Assinale a opção que indica um programa que, se existente no computador, poderá protegê-lo de um arquivo malicioso baixado da Internet:

   a) Lixeira
   b) antivírus
   c) Limpeza de Disco
   d) Explorador de Arquivos.

2. **(CESPE / PO-AL - 2023)** Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

3. **(CESPE / TRT8 – 2022)** Certo TRT deseja implementar uma solução de segurança cibernética que combine inteligência artificial, detecção comportamental e algoritmos de aprendizado de máquina para antecipar e prevenir ameaças conhecidas e desconhecidas.

   Com base nessa situação hipotética, assinale a opção que indica a solução requerida.

   a) NGAV.
   b) IPS
   c) IDS
   d) NIST
   e) WebProxy

4. **(CESPE / PC-AL – 2021)** A heurística é um dos métodos de detecção das ferramentas antimalware – como antivírus, antirootkit e antispyware – que se baseiam nas estruturas, instruções e características que o código malicioso possui para identificá-lo.

5. **(CESPE / BNB– 2018)** Entre as categorias de antivírus disponíveis gratuitamente, a mais confiável e eficiente é o scareware, pois os antivírus dessa categoria fazem uma varredura nos arquivos e são capazes de remover 99% dos vírus existentes.

6. **(CESPE / Polícia Federal – 2018)** Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

7. **(CESPE / CRBM – 2018)** O antispyware é conhecido como uma ferramenta complementar ao antivírus que deve ser executada frequentemente para checagem de possíveis ameaças que possam ter contaminado o sistema.

8. **(CESPE / CFO/DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

9. **(CESPE / TRE-PI – 2016)** A remoção de códigos maliciosos de um computador pode ser feita por meio de:

a) anti-spyware.
b) detecção de intrusão.
c) anti-spam.
d) anti-phishing.
e) filtro de aplicações.

10. **(CESPE / TRE-MT – 2015)** A função principal de uma ferramenta de segurança do tipo antivírus é:

a) monitorar o tráfego da rede e identificar possíveis ataques de invasão.
b) verificar arquivos que contenham códigos maliciosos.
c) fazer becape de segurança dos arquivos considerados críticos para o funcionamento do computador.
d) bloquear sítios de propagandas na Internet.
e) evitar o recebimento de mensagens indesejadas de email, tais como mensagens do tipo spams.

11. **(CESPE / Telebras – 2015)** Como os antivírus agem a partir da verificação da assinatura de vírus, eles são incapazes de agir contra vírus cuja assinatura seja desconhecida.

12. **(CESPE / TRT-10 Região – 2013)** Um computador em uso na Internet é vulnerável ao ataque de vírus, razão por que a instalação e a constante atualização de antivírus são de fundamental importância para se evitar contaminações.

13. **(CESPE / SESA-ES – 2013 – Letra C)** O anti-spyware, ao contrário do antivírus, propaga a proteção contra os vírus existentes de maneira semelhante a um antídoto, o que evita a contaminação de outros computadores da rede.

14. **(CESPE / Banco da Amazônia – 2012)** Antispywares são softwares que monitoram as máquinas de possíveis invasores e analisam se, nessas máquinas, há informações armazenadas indevidamente e que sejam de propriedade do usuário de máquina eventualmente invadida.

15. **(CESPE / Polícia Federal – 2012)** A fim de se proteger do ataque de um spyware — um tipo de vírus (malware) que se multiplica de forma independente nos programas instalados em um computador infectado e recolhe informações pessoais dos usuários —, o usuário deve instalar softwares antivírus e antispywares, mais eficientes que os firewalls no combate a esse tipo de ataque.

16. **(CESPE / PEFOCE – 2012)** O antivírus, para identificar um vírus, faz uma varredura no código do arquivo que chegou e compara o seu tamanho com o tamanho existente na tabela de alocação de arquivo do sistema operacional. Caso encontre algum problema no código ou divergência de tamanho, a ameaça é bloqueada.

17. **(CESPE / TCE-RO – 2012)** A manutenção da atualização dos antivírus auxilia no combate às pragas virtuais, como os vírus, que são mutantes.

18. **(CESPE / TRE/RJ – 2012)** Recomenda-se utilizar antivírus para evitar phishing-scam, um tipo de golpe no qual se tenta obter dados pessoais e financeiros de um usuário.

19. **(CESPE / Banco da Amazônia – 2012)** As ferramentas de antivírus que realizam a verificação do tipo heurística detectam somente vírus já conhecidos, o que reduz a ocorrência de falsos positivos.

20. **(CESPE / TJ/AC – 2012)** O antispyware é um software que se destina especificamente a detectar e remover spywares, enquanto o antivírus é uma ferramenta que permite detectar e remover alguns programas maliciosos, o que inclui certos tipos de spywares.

21. **(CESPE / TJ/AC – 2012)** As ferramentas antispam permitem combater o recebimento de mensagens consideradas spam e, em geral, baseiam-se na análise do conteúdo das mensagens.

22. **(CESPE / IFB – 2011)** Ferramentas como firewall e antivírus para estação de trabalho não ajudam a reduzir riscos de segurança da informação.

23. **(CESPE / FUB – 2009)** O aplicativo antivírus original dessa versão do Windows é o Symantec Norton 2003.

LISTA DE QUESTÕES – FCC

24. (FCC / TRF/4ª Região – 2019) Caso uma praga virtual seja muito forte e sua remoção por meio do processo de deleção de arquivos ou programas infectados possa afetar todo o funcionamento do computador, os antivírus devem executar um processo:

a) para isolar completamente o sistema operacional do sistema de arquivos.
b) para criptografar o arquivo ou programa infectado inteiro, antes renomeando-o em uma cópia com os caracteres $~ na frente de seu nome.
c) que visa manter o sistema operacional suspenso.
d) que visa manter o arquivo ou programa infectado em quarentena.
e) que se incumbe apenas de renomear o arquivo ou programa infectado com os caracteres $~ na frente de seu nome.

25. (FCC / SEMEF/Manaus – 2019) Um técnico tentou instalar uma aplicação no seu computador, mas o antivírus o impediu mostrando uma mensagem que o programa era legítimo, mas que poderia ser usado por criminosos para danificar o computador ou furtar dados pessoais. Analisando que as perdas que poderiam ser causadas pela execução do software seriam menores do que as perdas causadas pela não execução, o técnico pensou nas seguintes possibilidades para instalar e executar o software:

I. Incluir o software na lista de exclusão do antivírus, ou seja, na lista de programas que o antivírus não deverá verificar.

II. Mudar o nome do software para um nome amigável parecido com o nome recursos legítimos do sistema operacional, a fim de enganar o antivírus no momento da instalação e execução.

III. Desativar/Pausar o antivírus por um tempo determinado, ou seja, pelo tempo necessário para instalar e usar o software para o que necessita.

IV. Colocar o antivírus no modo de verificação apenas de disco rígido, de forma que ele não seja ativado quando perceber um possível malware carregado na memória.

Considerando que o técnico estava utilizando um dos principais antivírus do mercado, permitirá a instalação e execução do software APENAS o que consta em:

a) III.
b) I e III.
c) I e IV.
d) III e IV.
e) I e II.

26. (FCC / TRT/4ª Região – 2015) Ferramentas antimalware, como os antivírus, procuram detectar, anular ou remover os códigos maliciosos de um computador. Para que estas ferramentas possam atuar preventivamente, diversos cuidados devem ser tomados, por exemplo:

a) utilizar sempre um antimalware online, que é mais atualizado e mais completo que os locais.

b) configurar o antimalware para verificar apenas arquivos que tenham a extensão .EXE.

c) não configurar o antimalware para verificar automaticamente os discos rígidos e as unidades removíveis (como pen-drives e discos externos), pois podem ser uma fonte de contaminação que o usuário não percebe.

d) atualizar o antimalware somente quando o sistema operacional for atualizado, para evitar que o antimalware entre em conflito com a versão atual do sistema instalado.

e) evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

27. (FCC / MPE/AM – 2013) Com relação à utilização correta de ferramentas antimalware, considere:

I. É aconselhável utilizar programas antimalware on-line quando se suspeitar que o antimalware local esteja desabilitado ou comprometido ou quando se necessitar de uma segunda verificação.

II. Devem ser configuradas para verificar apenas arquivos executáveis, pois são os únicos que podem conter vírus e outros tipos de malware.

III. Deve-se evitar executar simultaneamente diferentes programas antimalware, pois eles podem entrar em conflito, afetar o desempenho do computador e interferir na capacidade de detecção um do outro.

IV. Não é recomendável ter um antimalware instalado no computador, pois os programas on-line além de serem mais eficientes, são suficientes para proteger o computador.

Está correto o que se afirma APENAS em:

a) I, II e III.
b) III e IV.
c) I e III.
d) II e IV.
e) I.

LISTA DE QUESTÕES – FGV

28.(FGV / CGU – 2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

a) redução de custos e facilidade de atualização;
b) configuração simplificada e fácil instalação de API;
c) monitoramento completo e antivírus atualizado;
d) administração descentralizada e facilidade de integração com novas tecnologias;
e) bloqueio de ações indesejadas e controle no lado do usuário.

29.(FGV / PC-MA – 2012) Um funcionário em uma viagem de negócios teve de levar em seu notebook arquivos classificados para uma reunião com clientes. Ele foi então aconselhado pelo pessoal de suporte da empresa a instalar um antivírus em sua máquina. Resistindo à orientação recebida, o funcionário argumentou que:

I. O software antivírus deixa minha máquina muito lenta.
II. Eu não preciso de um software antivírus porque eu nunca abro arquivos anexados em e-mails de pessoas que eu não conheço.
III. Tantas pessoas usam a Internet, eu sou apenas um na multidão. Ninguém vai me achar.

São motivos válidos para a não instalação de um programa antivírus:

a) somente a opção I
b) somente a opção II
c) somente a opção III
d) somente as opções I e II
e) nenhuma das opções.

LISTA DE QUESTÕES – VUNESP

30. (VUNESP / Prefeitura de Palmas-TO – 2023) Tem-se 4 computadores com antivírus instalado, com as seguintes características descritas na tabela a seguir.

Instalação do antivírus: 01.janeiro.2023

Data atual: 23.janeiro.2023

	Computador A	Computador B	Computador C	Computador D
Última atualização de definições de antivírus	01.janeiro.2023	21.janeiro.2023	21.janeiro.2023	Nunca
Última execução do antivírus, fazendo uma varredura completa	01.janeiro.2023	Nunca	22.janeiro.2023	22.janeiro.2023

Considerando que a data atual é 23.janeiro.2023, assinale a alternativa que apresenta o computador que está mais protegido.

a) Computador A.
b) Computador B.
c) Computador C.
d) Computador D.

31. (VUNESP / PC-SP – 2022) Visando aumentar a proteção e a segurança dos computadores, diversas ferramentas *antimalware* podem ser utilizadas, como as *antirootkit*, que visam impedir que:

a) sejam capturadas e armazenadas posições do cursor e a tela apresentada no monitor, nos momentos em que o mouse é clicado, ou a região que circunda a posição onde o *mouse* é clicado.

b) sejam capturadas e armazenadas as teclas digitadas pelo usuário no teclado do computador.

c) um programa se instale para permitir o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

d) um conjunto de programas e técnicas escondam e assegurem a presença de um invasor ou de outro código malicioso em um computador comprometido.

e) um programa execute, além das funções para as quais foi aparentemente projetado, outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

32. **(VUNESP / Câmara de Sertãozinho-SP – 2019)** Programas antivírus representam uma importante ferramenta aos usuários de computadores, sendo que tais programas:

a) não atuam sobre arquivos presentes em mídias removíveis, como é o caso de pen drives.

b) não atuam sobre programas com determinadas extensões, como .pdf ou .docx.

c) não atuam sobre programas com tamanho de até 50 KB.

d) devem ser executados somente em dois momentos: quando o computador é ligado e quando é desligado.

e) devem ser mantidos atualizados, assim como as definições de vírus presentes nesses programas.

33. **(VUNESP / Câmara de Monte Alto - SP – 2019)** Um usuário necessita instalar, em seu computador, um programa antivírus. Duas das possíveis opções que ele pode selecionar para tal finalidade são os programas

a) McAfee e TrueCript.
b) Norton e Predator.
c) Bitdefender e 7-Zip.
d) AVG e Avast.
e) Kaspersky e WinRAR.

34. **(VUNESP / Prefeitura de Ribeirão Preto-SP – 2018)** A respeito da execução de um programa antivírus em um computador, é correto afirmar que:

a) somente pode ser feita em intervalos iguais ou maiores do que uma semana.
b) não pode ser feita quando não há Internet de banda larga disponível no computador.
c) só pode ser feita quando ocorre uma atualização do sistema operacional do computador.
d) pode ser programada para ocorrer, por exemplo, uma vez por dia.
e) não pode ser feita em sistemas operacionais instalados há mais de dois anos no computador.

LISTA DE QUESTÕES – CESGRANRIO

35. **(CESGRANRIO / Petrobrás – 2011)** Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o:

a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

LISTA DE QUESTÕES – DIVERSAS BANCAS

36. **(FUNDATEC / IPE SAÚDE – 2022)** Em segurança da informação, utiliza-se o antivírus para proteção do computador contra vírus, que são códigos maliciosos e podem comprometer o funcionamento da máquina, bem como a integridade dos dados nela armazenados. Quando a remoção de um vírus pode comprometer o funcionamento do computador, o antivírus adota o seguinte procedimento:

a) Coloca o vírus em quarentena durante um tempo, enquanto busca por mais problemas relacionados a ele.
b) Apaga o vírus imediatamente e conserta os danos causados pela sua remoção.
c) Solicita que o usuário repare todos os arquivos comprometidos pelo vírus utilizando outra ferramenta.
d) Não toma providência alguma, pois, ao remover o vírus, o computador pode ficar instável.
e) Desliga imediatamente o computador para que o vírus não contamine outros programas.

37. **(IDIB / Ministério da Economia – 2021)** São softwares que detectam e removem programas maliciosos, como vírus e worms, protegendo os sistemas de computador contra essas ameaças. Assinale a alternativa que apresenta um desses programas:

a) Pipefy
b) Asana
c) Comodo
d) Avant
e) Acrobat

38. **(QUADRIX / CONRERP/2ª Região – 2019)** O software antivírus, após sua instalação e configuração, não necessita de ser atualizado pelo fabricante, pois já contém uma lista de assinaturas válidas e consegue eliminar todas as formas de vírus.

39. **(OBJETIVA / Prefeitura de Tupanci do Sul - RS – 2019)** Atenção! Para responder às questões de Informática, a menos que seja explicitamente informado o contrário, considerar que os programas mencionados encontram-se na versão Português-BR e em sua configuração padrão de instalação, possuem licença de uso, o mouse está configurado para destros, um clique ou duplo clique correspondem ao botão esquerdo do mouse, e teclar corresponde à operação de pressionar uma tecla e, rapidamente, liberá-la, acionando-a apenas uma vez. Dessa forma, as teclas de atalho, os menus, os submenus, as barras, os ícones e os demais itens que compõem os programas abordados nesta prova encontram-se na configuração padrão.

Em conformidade com a Cartilha de Segurança para Internet, sobre mecanismos de segurança, assinalar a alternativa que preenche a lacuna abaixo CORRETAMENTE:

Ferramentas _____ são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador. Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

a) pop-up's
b) backups
c) antispam
d) antimalware

40. **(IBADE / SAAE de Vilhena - RO – 2019)** Qual dos softwares abaixo é um Anti-Virus?

a) Avast
b) Excel
c) Squirrel
d) WinRAR
e) WinZip

41. **(IADES / CAU-MT – 2019)** O antivírus tem como responsabilidade proteger o computador de potenciais arquivos maliciosos:

a) A capacidade de detecção de novas ameaças de um antivírus independe de ele estar atualizado.
b) O antivírus tem como principal responsabilidade proteger a navegação do usuário na internet.
c) São tão importantes para o funcionamento de um computador que todas essas máquinas já vêm com um antivírus previamente instalado.
d) Quando um antivírus está ativado, o computador está seguro contra qualquer tipo de ataque.
e) Uma das capacidades do antivírus é inspecionar os anexos do correio eletrônico, procurando por possíveis ameaças.

42. **(UECE-CEV / DETRAN/CE – 2018)** Um software antivírus é um programa responsável por:

a) dividir os recursos da máquina entre os processos em execução.
b) prevenir, procurar, detectar e remover programas maliciosos.
c) arranjar em espaço contíguo os arquivos contidos em disco.
d) realizar a atualização do sistema operacional.

43. **(FAPEC / UFMS – 2018)** A prevenção, detecção e a eliminação de vírus são feitos por aplicativos denominados antivírus. É um exemplo de antivírus:

a) AVG.
b) FTP.

c) Keylogger.
d) Spam.
e) Malware.

44. (CPCON / Prefeitura de São José dos Pinhais-PB – 2018) Alguns softwares de antivírus têm se popularizado bastante e construído marcas sólidas e facilmente reconhecíveis por seus usuários. NÃO é um exemplo de software antivírus:

a) McAfee.
b) NetBeans.
c) Avast.
d) Kaspersky.
e) Norton.

45. (IF-CE / IF-CE – 2017) São ações desejáveis em um programa de antivírus:

a) proteção contra arquivos infectados de e-mail e varredura à procura de vírus em tempo real.
b) verificação contínua de defeitos de discos rígidos e varredura à procura de vírus em tempo real.
c) alerta de instalação de aplicativos infectados e impedimento de formatação de disco rígido.
d) proteção contra arquivos infectados de e-mail e atualização de softwares aplicativos.
e) atualização automática do programa de antivírus e criptografia de mensagens de e-mail.

46. (IESES / Prefeitura de São José do Cerrito – 2017) O software que utilizaríamos para protegermos nossos arquivos de programas maliciosos que desejassem controlar nosso computador são da categoria de softwares de:

a) Gerenciamento de Banco de Dados.
b) Antivírus.
c) Backup.
d) Processamento de Textos.

47. (QUADRIX / CRB 6ª Região – 2017) Em um ambiente público, com um microcomputador e um sistema operacional para desktop com acesso à internet, as diversas vulnerabilidades e falhas de segurança são uma constante preocupação ao usuário, seja navegando na internet ou acessando o microcomputador. Qual das seguintes alternativas auxilia um usuário padrão a se proteger de vírus e programas maliciosos?

a) Backup.
b) PROXY.
c) Planilhas eletrônicas.
d) Antivírus.
e) Rede IP.

48. **(CS-UFG / UFG – 2017)** Antivírus são programas de computador voltados para a eliminação e o controle de pragas virtuais, tais como:

a) spyware e firewall.
b) spam e boot.
c) worms e cavalos de Troia.
d) macro e log.

49. **(IBADE / IPERON-RO – 2017)** Um usuário precisa instalar em seu microcomputador um software antivírus de mercado, para se prevenir de ataques. Um software dessa categoria é o:

a) Media Player.
b) Switcher.
c) Kaspersky.
d) Adware.
e) Broadsheeet.

50. **(QUADRIX / CFO-DF – 2017)** Embora as ferramentas AntiSpam sejam muito eficientes, elas não conseguem realizar uma verificação no conteúdo dos e-mails.

51. **(IF/PA / IF/PA – 2016)** O software que já vem integrado à maioria dos programas leitores de e-mails e que permite separar os e-mails desejados dos indesejados (como, por exemplo, propagandas) é o:

a) Antivírus.
b) Firewall.
c) Filtro Antispam.
d) Filtro de janelas de pop-up.
e) Algoritmo criptográfico.

52. **(IDECAN / UE-RN – 2016)** O software responsável por detectar, evitar e atuar na neutralização ou remoção de programas mal-intencionados denomina-se:

a) Rootkit.
b) Antivírus.
c) Backdoor.
d) Keylogger.

53. **(UFCG / UFCG – 2016)** Antivirus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus de computadores. São exemplos de antivirus disponíveis no mercado, EXCETO:

a) Avira Free Antivirus.

b) AVG AntiVirus.
c) Comodo.
d) Windows Defender.
e) Formoid.

54. **(CRO-SC / CRO-SC – 2016)** São exemplos de programas antivírus todos os seguintes, EXCETO:

a) Karspersky
b) Avast
c) Quicken
d) AVG

55. **(COPEVE-UFAL / UFAL – 2016)** Após a detecção de um vírus, normalmente os softwares antivírus oferecem duas opções para o usuário: deletar ou colocar em quarentena. Nesse contexto, quando é mais indicado colocar o arquivo em quarentena, ao invés de apagá-lo?

a) Quando o arquivo infectado é considerado importante para o bom funcionamento do sistema ou de grande valor para o usuário.

b) Quando o antivírus foi capaz de remover completamente o vírus do arquivo infectado, a fim de ficar um tempo em observação.

c) Quando o arquivo infectado possui tamanho longo, normalmente acima de 20MB, a fim de otimizar o tempo de execução do antivírus.

d) É sempre mais indicado excluir definitivamente o arquivo, caso contrário, o vírus volta à ativa na próxima vez que o computador for reiniciado.

e) Quando o arquivo infectado é um executável totalmente desconhecido que não pertence ao sistema operacional nem a nenhum software instalado pelo usuário.

56. **(IADES / ELETROBRÁS – 2015)** Os arquivos de computador podem ser contaminados por vírus. A forma mais comum de contaminação ocorre por meio de mensagens eletrônicas (e-mail). Para evitar contaminações e realizar a recuperação de arquivos contaminados, são utilizados os programas antivírus. A esse respeito, é correto afirmar que a área de armazenamento em que os programas antivírus costumam guardar os arquivos contaminados de um computador denomina-se:

a) lixeira.
b) disco rígido.
c) pasta spam.
d) área de trabalho.
e) quarentena.

57. **(INAZ DO PARÁ / Prefeitura de Terra Alta – 2015)** Atualmente, a informação representa o maior bem dentro de qualquer organização; assim, existem diversas formas de se garantir a proteção da mesma. Dentre os diversos procedimentos existentes, assinale qual pode ser considerada a forma mais segura para proteção desta informação:

a) Backup.
b) Firewall.
c) Ifconfig.
d) Antivírus.
e) Dump.

58. **(COSEAC / CLIN – 2015)** São normalmente funcionalidades de um software antivírus as abaixo relacionadas, EXCETO:

a) impedir que um hacker explore vulnerabilidades em seu sistema.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) verificar continuamente os discos rígidos e discos removíveis.

59. **(PR-4 UFRJ/ UFRJ – 2015)** Os antivírus são programas de computador concebidos para prevenir, detectar e eliminar vírus de um computador. São exemplos de antivírus:

a) AVG, Avast e Avira.
b) AVG, Hoax e FTP.
c) Hoax, Avast e Avira.
d) Spam, Keylogger e AVG.
e) Spam, Avast e Hoax.

60. **(FUNIVERSA / SEAP-DF – 2015)** Um dos procedimentos de segurança da informação é instalar no computador o anti-spyware e o antivírus, pois o anti-spyware é um aplicativo que complementa o antivírus.

61. **(UFBA / UFOB – 2014)** Para identificar um vírus, o antivírus faz uma comparação entre o arquivo que chega por algum meio de entrada e uma biblioteca de informações sobre os vários tipos de vírus, o que explica a importância de manter o antivírus sempre atualizado.

62. **(FUMARC / Câmara Municipal de Mariana/MG – 2014)** São exemplos de softwares antivírus, EXCETO:

a) Avast.
b) AVG.
c) Kaspersky.
d) Microsoft Windows Defender, disponível no Windows 7.

63. **(CETRO / FUNDAÇÃO CASA – 2014)** Sobre os softwares antivírus, assinale a alternativa correta.

a) Algumas empresas mantêm softwares antivírus em seus websites e oferecem os serviços do software via Internet.
b) Cada antivírus protege contra um único tipo de software malicioso.
c) Cada antivírus utiliza somente uma estratégia de detecção de softwares maliciosos.
d) Não existem antivírus que protejam os computadores em tempo real.
e) A única coisa que o antivírus consegue fazer é detectar o vírus e eliminar os arquivos infectados.

64. **(COSEAC / Prefeitura de Niterói/RJ – 2014)** São funções rotineiras de um programa antivírus as abaixo relacionadas, EXCETO:

a) identificar e eliminar vírus e outros tipos de malwares.
b) analisar downloads da Internet.
c) procurar programas maliciosos nos anexos dos e-mails.
d) possibilitar a atualização das assinaturas de novos vírus de forma automática.
e) efetuar o controle de configuração dos softwares na rede.

65. **(BIO-RIO / Prefeitura de Três Rios – 2014)** Atualmente, com o objetivo de evitar a contaminação dos computadores é necessário instalar um software antivírus na máquina. Dois exemplos de antivírus são:

a) McAfee e Shirink
b) Safari e Linkedin
c) Avast e Psafe
d) AVG e Winrar
e) Bing e Android.

66. **(MPE-RS / MPE-RS – 2014)** Código Malicioso é o termo genérico usado para referir programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Qual das alternativas abaixo NÃO apresenta um tipo de código malicioso?

a) Antivírus.
b) Bot.
c) Worm.
d) Spyware
e) Cavalo de Tróia.

67. **(BIO-RIO / EMGEPRON– 2014)** A instalação de um antivírus em um microcomputador é de suma importância para o seu funcionamento satisfatório, no que diz respeito à segurança dos dados e ao próprio desempenho da máquina. Dois exemplos de programas antivírus são:

a) iTunes e Avast!
b) Avast! e McAfee
c) McAfee e WinZip
d) WinZip e iTunes.

68. **(UFBA / UFBA – 2013)** A instalação e o uso de programas "antivírus" aumentam a segurança dos arquivos armazenados no computador.

69. **(AOCP / Colégio Pedro II – 2013)** Antivírus são programas de computador desenvolvidos para prevenir, detectar e eliminar vírus do computador. Assinale a alternativa que NÃO representa um antivírus.

a) Avast.
b) AVG.
c) Microsoft Security Essentials.
d) Kaspersky.
e) WinRAR.

70. **(FUNCAB / SC/CE – 2013)** O software antivírus é um software da categoria dos(as):

a) sistemas operacionais.
b) linguagens de programação.
c) softwares utilitários.
d) firmwares.
e) softwares aplicativos.

71. **(FUNCAB / CODATA – 2013)** Sobre sistemas antivírus, é correto afirmar:

a) Garantem integralmente a segurança das informações em seu computador.
b) Distribuem os arquivos contaminados pela rede do seu computador, visando a enfraquecer o vírus.
c) Por padrão, movem para a lixeira arquivos contaminados do seu computador.
d) Os programas antivírus examinam os arquivos antes de abri-los e notificam o usuário do computador, caso encontrem um arquivo potencialmente não seguro.
e) garantem a recuperação de arquivos danificados por Cavalo de Troia.

72. **(CETRO / Prefeitura de Manaus – 2012)** Quanto ao processo de quarentena, que alguns softwares antivírus oferecem, é correto afirmar que:

a) quarentena é uma área separada em um disco rígido.

b) apesar de isolar os arquivos, a quarentena não consegue impedir que outros arquivos sejam infectados pelo software suspeito.

c) somente o software antivírus tem a capacidade de colocar um software suspeito em quarentena.

d) após determinado tempo, os arquivos em quarentena são eliminados automaticamente.

e) arquivos em quarentena sempre são eliminados do computador, já que não existe solução para o problema deles (infecção).

73. **(FUNCAB / SESC-BA – 2012)** Considere que o técnico da área de suporte da empresa na qual você trabalha tenha detectado, em seu computador, um Cavalo de Troia. O recurso de computador que pode ter auxiliado nessa localização foi:

a) Ferramenta de Busca Google
b) Firewall
c) Sistema Antivírus
d) Gerenciador de Tarefas.
e) Fragmentador.

74. **(UECE-CEV / SEPLAG-CE – 2011)** O software concebido com o objetivo de prevenir, detectar e eliminar programas maliciosos é denominado:

a) Bloco de Notas.
b) Microsoft Office.
c) Windows Explorer.
d) Antivírus.

75. **(PONTUA / TRE-SC – 2011)** Os sistemas antivírus são programas que têm o objetivo de detectar e, então, anular ou eliminar os vírus encontrados no computador. Marque V (Verdadeiro) e F (Falso) para os exemplos de programas antivírus:

( ) Norton.
( ) WinZip.
( ) McAfee.
( ) Kaspersky.
( ) Word.

A sequência CORRETA, de cima para baixo, é:

a) F – F – V – V – V.
b) V – F – V – V – F.
c) F – V – F – F – V.
d) V – V – V – V – F.

76. **(FUNCAB / Prefeitura de Porto Velho/RO – 2009)** Às vezes, os sistemas Antivírus detectam vírus desconhecidos que não podem ser eliminados com o conjunto de ferramentas disponíveis. Qual a função existente nos sistemas antivírus que permite isolar arquivos potencialmente infectados no seu computador?

a) Scanear;
b) Colocar em quarentena;
c) Reparar;
d) Congela;
e) Purgar.

GABARITO

1. B
2. ERRADO
3. LETRA A
4. CORRETO
5. ERRADO
6. CORRETO
7. CORRETO
8. ERRADO
9. LETRA A
10. LETRA B
11. ERRADO
12. CORRETO
13. ERRADO
14. ERRADO
15. ERRADO
16. ERRADO
17. CORRETO
18. ERRADO
19. ERRADO
20. CORRETO
21. CORRETO
22. ERRADO
23. ERRADO
24. LETRA D
25. LETRA B
26. LETRA E
27. LETRA C
28. LETRA A
29. LETRA E
30. LETRA C
31. LETRA D
32. LETRA E
33. LETRA D
34. LETRA D
35. LETRA E
36. LETRA A
37. LETRA C
38. ERRADO
39. LETRA D
40. LETRA A
41. LETRA E
42. LETRA B
43. LETRA A
44. LETRA B
45. LETRA A
46. LETRA B
47. LETRA D
48. LETRA C
49. LETRA C
50. ERRADO
51. LETRA C
52. LETRA B
53. LETRA E
54. LETRA C
55. LETRA A
56. LETRA E
57. LETRA D
58. LETRA A
59. LETRA A
60. CORRETO
61. CORRETO
62. LETRA D
63. LETRA A
64. LETRA E
65. LETRA C
66. LETRA A
67. LETRA B
68. CORRETO
69. LETRA E
70. LETRA C
71. LETRA D
72. LETRA A
73. LETRA C
74. LETRA D
75. LETRA B
76. LETRA B

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.