PROFISSÃO POLICIAL

Informática

Professor Túlio Queiroz

Informática
Professor Túlio Queiroz

Sumário

PROTEÇÃO, SEGURANÇA E COMPUTAÇÃO NA NUVEM

1 HARDWARE X SOFTWARE

Para iniciarmos o estudo de informática é de fundamental importância que você saiba o conceito básico de Hardware e Software. Esse é o primeiro passo para se fragmentar a informática em partes ao ponto de que se possa entendê-la e assim obter êxito na mesma.

Hardware Vs Software

2 HARDWARE

É a parte física do Computador, ou seja, tudo que eu posso tocar, tudo que for palpável, tudo que pode ser utilizado para matar alguém, por exemplo os periféricos.

Os periféricos se subdividem em três tipos:

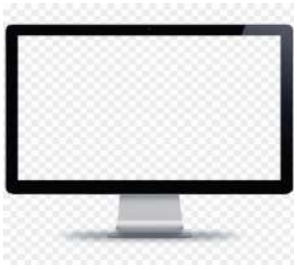
Periféricos de Entrada →

Dispositivos em que o usuário envia dados para o computador, por exemplo, ao digitar um texto o usuário está enviando dados para o mesmo, através do Teclado, outros exemplos de Periféricos de Entrada: Mouse, Scanner, Microfone,Webcam.

Periféricos de Saída →

Dispositivos em que o computador envia mensagens para o usuário, por exemplo ao imprimir uma foto de uma impressora nesse momento o usuário está recebendo um dado do computador, outros exemplos de periféricos de saída: Caixa de Som, Monitor, fone de ouvido.

Dispositivos em que o usuário envia dados para o computador, por exemplo, ao digitar um texto o usuário está enviando dados para o mesmo, através do Teclado, outros exemplos de Periféricos de Entrada: Mouse, Scanner, Microfone,Webcan.



Per. Entrada/Saída Híbridos →

Dispositivos que podem tanto enviar dados para o computador , quanto receber dados do mesmo por exemplo: Pen-drives , HD Externo, CD Rom , DVD-Rom, Impressora MULTIFUNCIONAL. Monitor TouchScreen

Dispositivos de armazenamento →

Dispositivos que podem tanto enviar dados para o computador , quanto receber dados do mesmo por exemplo: Pen-drives , HD Externo, CD Rom , DVD-Rom.

2.1 Processador (CPU)

Erroneamente somos levados a comparar CPU com o gabinete. Então vamos entender o que é cada um e como funcionam.

Gabinete ≠ CPU

"Uma coisa é uma coisa, outra coisa é outra coisa e a mesma coisa é um caminhão cheio de japonês comendo caranguejo" Queiroz, Túlio 2021.

Gabinete

➔ É somente o compartimento ou como algumas bancas chamam "o invólucro" onde será alocado TODOS os outros periféricos do computador como por exemplo a placa mãe, os pentes de memória RAM, a Fonte, inclusive a CPU.

CPU (UCP)

➔É a Unidade de Processamento Central que é considerado o coração do computador, que por sua vez é o dispositivo mais veloz do mesmo, também é considerado o principal componente do computador.

O **processador** se subdivide em Quatro partes:

ULA ➔ Unidade Lógica Aritmética. A ULA é encarregada de resolver ou realizar todo e qualquer cálculo matemática que ocorre no computador.

UC ➔ Unidade Central de Controle (**que as bancas adoram chamar de Unidade Central, CUIDADO!).** É responsável por realizar: Controle de entrada e saída de Dados;

*Controla o funcionamento da CPU;

* Recebe a Instrução do Kernel;

Registradores ➔ Os Registradores por sua vez realizam a tarefa de fazer uma lista de todas as tarefas que são executadas pelo processador.

Cache ➔
- Considerada memória de acesso rápido
- Armazena resultados do processamento;
- Pode ser dividida em níveis: L1, L2 e L3.

2.2 Arquitetura de Processamento

	RISC	CISC
Conjunto de Instruções	SIMPLES	Complexo
Instruções da U.C	POUCAS	Várias
Desempenho do Processo	Melhor	Geralmente Afetado

RISC➔ (Reduced Instruction Set Computer) Computador de consumo de instruções reduzidas;

CISC➔ (Complex Instruction Set Computer) Computador de consume de instruções complexas;

2.3 Velocidade de processamento

Clock

- Tempo de Funcionamento do Processamento
- Medição em **Hertz:** é a unidade de medida, a qual expressa, em termos de ciclos por segundo. Então, 1 hertz é um ciclo (Instrução) por segundo;

- **Overclock**

Forçar o desempenho, por exemplo se fizermos uma analogia com a moto de 50cc vulgo cinquentinha, quando o dono com alta taxa de qi, coloca um motor mais potente e força o desempenho do ciclomotor, momentaneamente é algo bem bacana, mas com o decorrer do tempo pode comprometer o funcionamento do veículo. Da mesma forma é com o processador, quando o usuário força o desempenho.

- **Overflow**

Sobrecarga de dispositivo.

Questão de Entendimento:

01 (IESES|2021)

Sobre os componentes de um computador, verifique as assertivas e assinale a correta.
a) O software corresponde aos componentes físicos do computador, ou seja, são as peças e aparatos eletrônicos que, ao se conectarem, fazem o equipamento funcionar.
b) O hardware é a parte referente aos sistemas que executam as atividades, ou seja, são os programas e aplicativos que fazem com que a máquina funcione.
c) Compreende-se como hardware elementos físicos que formam o equipamento enquanto os programas ou sistemas que fazem o equipamento funcionar são denominados software.
d) Monitor, teclado e mouse são exemplos de software.

Resolução

a) ERRADO. As partes físicas do computador estão relacionadas ao hardware, enquanto o software corresponde às partes lógicas.
b) ERRADO. Sistemas, programas e aplicativos correspondem a parte lógica do computador, ou seja, estão relacionados ao software.
c) CERTO. Elementos físicos correspondem ao hardware, enquanto as partes lógicas estão ligadas ao software.
d) ERRADO. Monitor, teclado e mouse são exemplos de hardware, uma vez que correspondem a parte física do computador.
GABARITO: LETRA C.

02 (INSTITUTO AOCP|2020)
O invólucro onde os componentes eletrônicos como placa de vídeo e placa de som são dispostos em um computador convencional é denominado
a) Memória RAM.
b) CPU.
c) Switch.
d) Gabinete

Resolução

A palavra-chave da questão é INVÓLUCRO e esse corresponde ao gabinete. Não confundam CPU com o Gabinete. **GABARITO LETRA D.**

2.4 Placa mãe (MotherBoard)

A placa mãe ➔ é o dispositivo com maior importância do computador, pois é responsável pela comunicação entre TODOS os componentes, ou seja, absolutamente todos os componentes de Hardware são ligados pela placa mãe. São exemplos de componentes a ela interligados: vários chips, trilhas, capacitores e encaixes.

Chipset ➔ É o principal componente da placa mãe, esse nome é dado ao conjunto de chips (ou circuitos integrados) utilizado na placa mãe e cuja função é realizar diversas funções de hardware, como controle dos barramentos (PCI, AGP e o antigo ISA), controle e acesso à memória, controle da interface IDE e USB...

Barramento

São os caminhos de conexão, basicamente são as trilhas utilizadas para ligação. Barramento é um conjunto de linhas utilizadas para a comunicação que permite com que haja a interligação entre dispositivos tais como: CPU, a memória dentre outros dispositivos.

2.4.1 OnBoard e OffBoard

OnBoard ➔ é o tipo de placa que traz recursos embutido na placa mãe

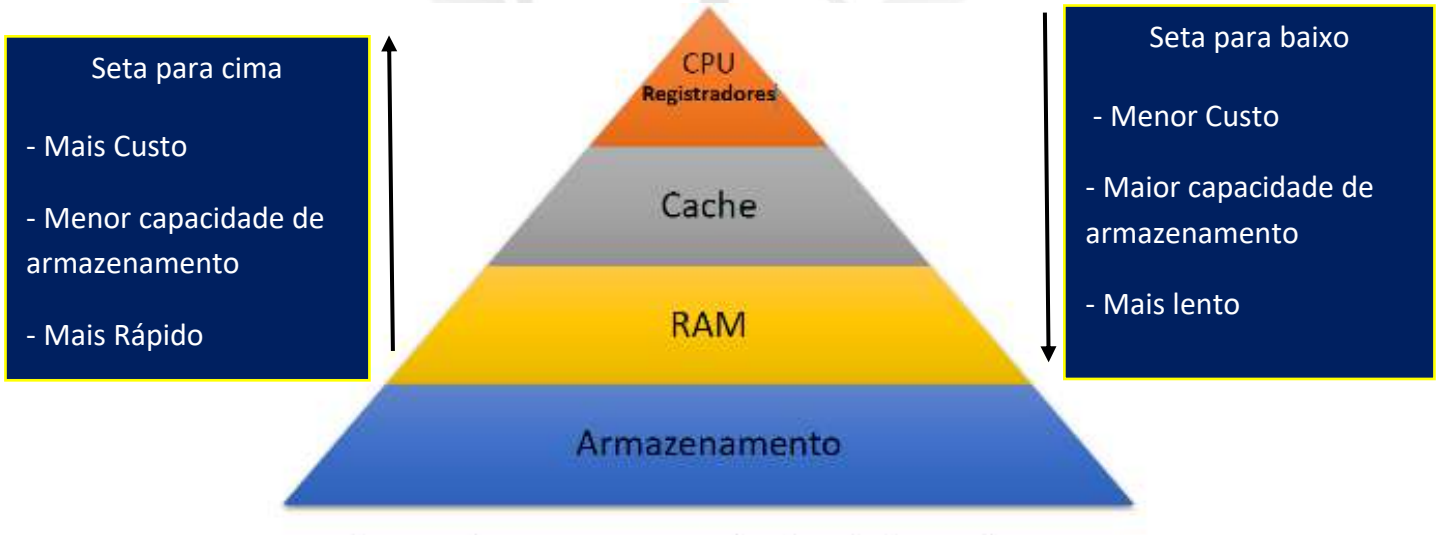
O**ffBoard** ➔ É quando existe uma placa extra (Externa). Grosso modo, é a melhor definição que podemos trazer, mas vamos aprofundar mais um pouco:

As placas onboard são mais comuns, atualmente quase todas as placas mãe tem vídeo onBoard, só que o desempenho não é tão bom assim. Então, para suprir essa necessidade coloca-se uma placa de vídeo offBoard para justamente melhorar o desempenho da parte gráfica.

As placas off-board não possuem seus dispositivos integrados a placa mãe, precisando, portanto, de placas extras com esses dispositivos que serão instalados nos seus respectivos Slots. O seu desempenho é superior as placas On-board pois têm sua própria central de processamento e a transferência superior as que rodam na memória RAM.

2.5 Hierarquia de Memórias

As memórias do computador são organizadas hierarquicamente formando assim uma pirâmide e essa hierarquia se deve a vários quesitos como, por exemplo, a velocidade das memórias, a sua tecnologia sua capacidade e seu custo-benefício. Encontram-se as memórias mais velozes, com maior tecnologia, e bem menor custo relacionado à sua capacidade no pico dessa pirâmide. Já no alicerce encontram-se as memórias com menor custo-benefício, entretanto que suportam a maior quantidade de dados.



Memória Principal (Memória de Leitura)
***RAM**
***ROM**
Memória Intermediária (Não físicas)
***Cache**
***Virtual**
Memória Secundária (Armazenamento)
***HD, CD, DVD, Blu-ray.**

Questão de Entendimento:

03 (APICE|2021)
Na informática, memórias são dispositivos capazes de guardar dados de forma temporária ou permanente. Sobre os diversos tipos de memória, considere as afirmações a seguir:

I.A memória ROM é uma memória somente de leitura e é um tipo de memória volátil, sendo assim, o conteúdo não desaparecerá quando o dispositivo for desligado;

II. Podemos afirmar que um disco rígido (Hard Disk Drive – HDD) é um tipo de memória não volátil. Isto significa que os dados permanecem gravados neste tipo de memória, mesmo com o dispositivo sendo desligado.

III. Uma memória do tipo USB Flash Drive, também conhecida como pen drive, é um tipo de memória não volátil.

IV. A memória RAM é uma memória somente de leitura, cujos dados podem acessados de maneira aleatória e são do tipo não volátil;

Estão CORRETAS APENAS:
a) II, III;
b) I, II e III;
c) III e IV;
d) I, II e IV;
e) I, III e IV.

Resolução

I. A memória ROM é uma memória somente de leitura e é um tipo de memória volátil (não volátil), sendo assim, o conteúdo não desaparecerá quando o dispositivo for desligado;

II. CERTO

III. CERTO

IV. A memória RAM é uma memória somente de leitura (leitura e escrita), cujos dados podem acessados de maneira aleatória e são do tipo não volátil.

GABARITO LETRA A

Questão de Entendimento:

04 (MPE-GO|2021)
A memória RAM é um dos componentes essenciais em todo computador. A função da memória RAM em um computador é:
a) Armazenar os dados de forma permanente, mesmo após o desligamento do computador.
b) Ser utilizada como reserva para o disco rígido, quando o espaço no disco estiver escasso.
c) Armazenar dados relevantes ao funcionamento do sistema, durante a sua operação.
d) Aumentar a memória Cache do processador.

Resolução
As bancas gostam de confundir o conceito de RAM e ROM, cuidado! RAM é a memória principal, volátil (armazenamento temporário) e ROM é a memória não volátil (armazenamento permanente). **GABARITO LETRA C**

2.6 Unidades de Medidas

Bit	Byte	Kilo Byte	Mega Byte	Giga Byte	Tera Byte	Peta Byte	Exa byte	Zetta Byte	Yotta Byte
0 ou 1	8 bits	1024 MBytes	1024 Bytes	1024 Mbytes	1024 Gbyte	1024 TByte	1024 Pbyte	1024 EByte	1024 ZByte

☠ **Bizu Cavernoso da Sofrência**

Unidades de Medida

P→(Pensei) Peta Byte 1024 Tb
T→(Tanto) Tera Byte 1024 Gb
G→(Gostar) Giga Byte 1024 Mb
M→(Mas) Mega Byte 1024 Kb
K→(Kabei) Kilo Byte 1024 B
B→ (Besta) Byte
b→ (bebendo) bit

SSD VS HDD

-Melhor desempenho (Mais rádido)
-Mais resistente à quedas e interferências magnéticas;
-Consome menos energia;
-Mais caro;
-Menor Capacidade de armazenamento
-Menor vida útil;

-Mais barato;
-Maior cap. de armazenamento;
-Maior vida útil;
-Consome mais energia;
-Menos resistente a quedas e interferências magnéticas;
-Pior desempenho (Mais lento)

Questão de Entendimento:

05 (INSTITUTO AOCP|2021)
Considerando as grandezas computacionais, 2 Kilobytes correspondem a quantos bytes?
a) 1024
b) 20486
c) 1000
d) 2048
e) 1048

Resolução
1 kilobyte (KB ou Kbytes) = 1024 bytes; 2 kilobyte (KB ou Kbytes) = 2048 bytes. Lembrando que cada byte possui 8 bits. **GABARITO LETRA D**

06 (VUNESP|2019)
Embora os discos rígidos (HD) sejam ainda muito utilizados, as unidades de estado sólido (SSD) vêm cada vez mais sendo utilizadas. Comparando os HDs convencionais com os SSDs, tem-se que
a) a vida útil dos SSDs é maior do que a dos HDs.
b) o consumo dos SSDs é maior do que o dos HDs.
c) o preço por bit de armazenamento dos SSDs é menor do que o dos HDs.
d) os tempos de leitura e escrita dos SSDs são maiores do que os dos HDs.
e) os SSDs são mais resistentes do que os HDs em relação a movimentos, quedas ou interferências magnéticas.

Resolução
GABARITO LETRA E

3 SOFTWARE

3.1 Conceito de Software

Software nada mais é do que a **Parte Lógica do Computador,** ou seja, tudo que eu **não posso tocar**, tudo que for impalpável.

O mesmo também pode ser considerado um conjunto de instruções lógicas para se executar uma informação/instrução.

Como exemplo de programas, temos algumas subclasses por exemplo:

- as **suítes de escritório** (Word, Excel Power Point),
- um **Browser** que é um navegador de internet (Google Chrome, Mozilla Firefox, Internet Explorer)
- ou um **sistema Operacional** (Windows, Linux).

Abaixo relaciono os tipos de softwares que podem ser cobrados na sua prova.

3.2 Tipos de Software

Bizu Cavernoso Matador (F-A-MA-S) 

F → irmware

Programa Inerente ao HARDWARE. Geralmente, vem com seu conteúdo gravado de fábrica como por exemplo a BIOS (Basic Input/Output System) (SISTEMA BÁSICO DE ENTRADA/SAÍDA). A BIOS é utilizada para executar a inicialização da parte física (Hardware), e para prover serviços de tempo de execução para **sistemas operacionais** e programas. A BIOS vem pré-instalado na memória permanente da placa mãe do **computador** e é o primeiro software a ser executado quando se liga a máquina.

A → plicativos

Podem ser subdivididos em 3 grupos:

Escritórios → Suíte Ms-Office (Word, Excel, Power Point), Suíte Libre Office (Writer, Calc, Impress.).

Utilitários → Nessa classe podemos enquadrar os compactadores de arquivos como por exemplo Winrar, os leitores de PDF,s (Adobe acrobat reader) e as ferramentas Antimalwares.

Entretenimento → Aqui podemos citar o VLC (Reprodutor de Áudio e vídeo), Windows Media Player também da mesma classe.

MA → lwares

São programas maliciosos desenvolvidos com o intuito de causar dados ou realizar alguma prática maléfica ao usuário. Podem ser desenvolvidos por HACKERS (pessoa com bastante conhecimento na área que usa seus conhecimentos para o bem) ou Crackers (pessoa com bastante conhecimento na área que usa seus conhecimentos para o mal).

S → istema operacional

É o Principal programa do computador, é dele a função de realizar todo o gerenciamento do computador tanto a parte de Hardware (Física), quando a parte de Software (Parte Lógica). Também é função do Sistema Operacional ser uma espécie de intermediário entre homem e máquina, deixando assim o sistema mais convidativo.

4 LICENÇAS DE SOFTWARE

Quando falamos em softwares proprietários logo nos remetemos a algo que **não pode ser redistribuído ou modificado**, sem o consentimento de seu criador ou distribuidor. O conceito vai de encontro ao conceito de software livre.

Normalmente, para que se possa: utilizar, copiar, ter acesso ao código-fonte ou redistribuir, o usuário deve realizar uma solicitação de permissão ao proprietário, ou pagar para poder fazê-lo.

> **BIZU CAVERNOSO MATADOR**
>
> Um software proprietário não necessariamente **será pago**, porém manter-se-á sua característica principal de **não disponibilização do código-fonte**.
>
> **Software Proprietário** → é o software que não permite ao usuário acessar o Código Fonte. (receita)

4.1 Software Proprietário

Alguns dos softwares proprietário gratuitos mais conhecidos estão abaixo citados:

- **Google Chrome, Winzip, Avast etc.**

Em contrapartida existe um grande gama de softwares proprietário que são pagos como por exemplo:

- **Microsoft Windows, o Adobe Photoshop, o Mac OS, Corel Draw, Microsoft Office.**

4.2 Software Livre

Já o **software livre** é regido quase que por uma lei. Digamos que seja a Constituição Federal dos Softwares Livres (CF) que nós chamamos de GPL (General Public Licence) que tem por base **4 liberdades:**

Liberdade 00

→ *Liberdade para rodar o programa para quaisquer propósitos. Executar o software seja qualquer finalidade.*

Liberdade 01

→ *Acessar o código-fonte do programa e modificá-lo conforme sua necessidade e distribuir suas melhorias ao público, de modo que elas fiquem disponíveis para a comunidade.*

Liberdade 02

→ *Fazer cópias e distribuí-las para quem desejar de modo que você possa ajudar ao seu próximo.*

Liberdade 03

→ *Melhorar o programa e distribuir suas melhorias ao público, de modo que elas fiquem disponíveis para a comunidade. Para tais ações é indispensável o acesso ao código fonte, por isso todos os softwares livres liberam para os usuários o mesmo.*

BIZU CAVERNOSO MATADOR

Executar (Liberdade 00) acesso para adaptar (Liberdade 01) fazer cópias (Liberdade 02) e melhorar o programa (Liberdade 03).
→ **Executar acesso para adaptar, fazer cópias e melhorar o programa**.

5 LICENÇAS DE SOFTWARE GRATUITO

5.1 Freeware

São programas **distribuídos gratuitamente**, os mesmos que não expiram e você pode **usá-los livremente** e nunca terá que pagar nada por isso.

Nesse tipo, o usuário poderá utilizar de todos os recursos fornecidos pelo fabricante, por um **tempo indeterminado**.

5.2 Shareware

São softwares que após um dado tempo de uso você terá que **pagar para continuar utilizando**. E esse tempo vai ser relativo, ou seja, pode variar de programa para programa. Tal tempo será definido pelo desenvolvedor.

Após número de utilizações, o programa perde algumas ou todas as suas funcionalidades.

E, após este período decorrido, o usuário deverá ou apagá-lo do computador ou registrá-lo através do pagamento de uma taxa ao desenvolvedor.

Vamos resolver uma questão?

Questão de Entendimento:

07 (UFPR|2020|CÂMARA DE CURITIBA-PR|TÉCNICO ADMINISTRATIVO)

Com relação a hardware e software, é correto afirmar:

A) Um Sistema Operacional é uma camada de software que opera entre o hardware e programas.
B) Os aplicativos de edição de texto, reprodução de mídia e editor gráfico são exemplos de hardware.
C) Discos, memórias e portas USB são componentes de software.
D) O software é constituído de aplicativos e de circuitos eletrônicos.
E) A impressora é um exemplo de software, porque depende da instalação de aplicativo específico para funcionar.
F)

Resolução

A) CERTO. Definição correta de sistema operacional.
B) ERRADO. Qualquer aplicativo é software e não hardware.
C) ERRADO. Qualquer peça do computador é item de hardware e não software.
D) ERRADO. Circuitos eletrônicos fazem parte dos itens físicos do computador, ou seja, são itens de hardware.
E) ERRADO. Impressora é um item físico e não um item lógico, ou seja, é hardware e não software.

GABARITO: LETRA A

6 MALWARE

A Primeira definição de Malwares:

É **um software,** porém, entretanto, contudo, todavia, é um **SOFTWARE MALICIOSO**.

Qual a principal Função do Malware?

Causar Danos e esses danos podem ser de **três tipos**:

→ **LÓGICO**

Vamos pensar no seguinte exemplo: o Usuário está acessando uma página da web de repente a mesma é fechada.

Outro exemplo: Sem que o usuário ordene páginas são abertas, computador desligado, dados perdidos, computador fica lento, sem motivo aparente o computador reinicia, dentre outros.

→ **FÍSICO**

Suponhamos que um processador rode a 20km/h (estamos supondo, ok?!). E um Malware faz com que ele rode a 100km/h ou seja 5X mais do que a sua capacidade. O mesmo irá danificar e isso é um exemplo de um **dano Físico** que pode ser causado pelo Malware.

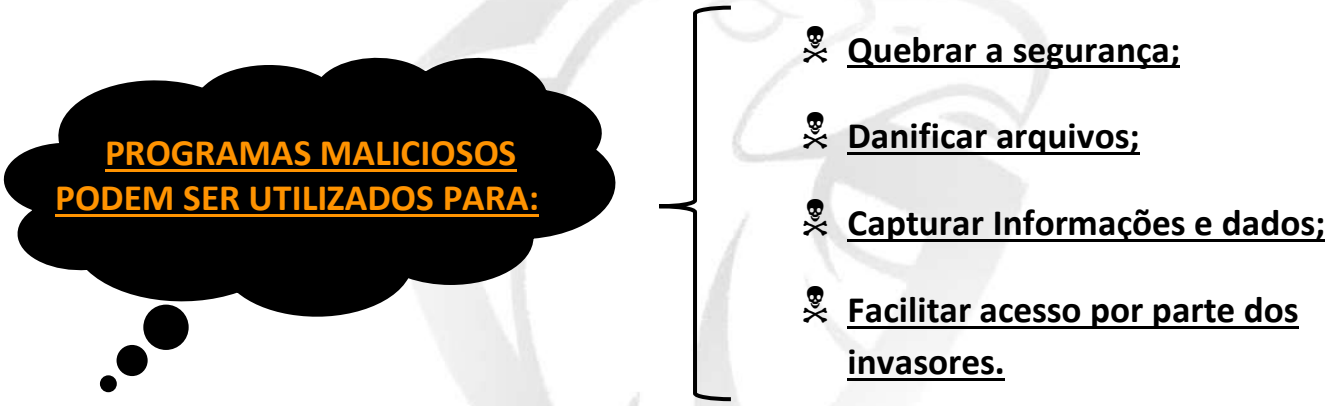
→ **MORAL**

Digamos que o usuário tenha fotos íntimas em seu computador ou smartphone e de alguma forma um usuário utilizando um tipo de malware tem acesso à foto e a

publica nas redes Sociais (Facebook, WhatsApp, Instagram etc.). Esse é um exemplo de um **dano Moral** que pode ser causado pelo Malware.

BIZU CAVERNOSO

TODO **VÍRUS** É UM **MALWARE**, MAS NEM TODO **MALWARE** É **VÍRUS**.



Um Malware pode ser desenvolvido tanto por Hackers, quanto por Crackers.
¬- **"Ain, mais professor qual a diferença?"**

Hackers e Crackers são pessoas com vasto conhecimento na área de TI (Tecnologia da informação), mas que utilizam de formas distintas. Por exemplo: o hacker é o cara do bem, e o Cracker é o cara do mal.

> **Hacker:** usa de todo conhecimento técnico para invadir sistemas com alto nível de segurança e quando obtém êxito, mostra os resultados ao proprietário que o contratou, para que as falhas sejam sanadas.

Cracker: usa seu conhecimento para obter vantagem ilícita, roubar dados, obter dados bancários etc.

6.1 Tipos de Malwares

Abaixo a lista de Malwares mais cobrados pelas bancas organizadores de concursos policiais:

- BOT,
- EXPLOIT,
- BACKDOOR,
- WORM,
- VÍRUS,
- TROJAN HORSE (Cavalo de Tróia),
- SPYWARE,
- ADWARE,
- ROOTKIT,
- E RANSOMWARE.

6.1.1 Bot

A Definição de bot parte do nome *Robot* que significa robô em inglês e é um robô controlado a distância. É uma espécie de acesso remoto **NÂO AUTORIZADO**! O usuário não sabe que está sendo lesado.

FICA ALERTA, GUERREIRO(A)!

Não confundir BOT com o Acesso remoto autorizado, que nesse caso o usuário tem total conhecimento da "invasão".

Uma característica que vale salientar pois os elaboradores misturam conceitos na hora da sua prova:

BOT X WORM

Bot pode ser confundido com o **Worm** devido algumas características serem semelhantes. Como por exemplo, um bot pode se replicar e, também, é autoexecutável, mas dispõe de mecanismos de comunicação com o invasor, permitindo que a máquina seja controlada remotamente.

- "**Ain, mais professor como vou diferenciar na hora da prova?"**
O bot tem como intuito com salientado acima de permitir o acesso remoto.

6.1.2 Exploit

Exploit um explorador de falhas e/ou comportamentos.

6.1.3 Backdoor

Esse malware abre uma porta dos fundos para o computador espião.

Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

6.1.4 Vírus

Vírus nada mais são do que pequenos programas desenvolvidos com o objetivo de causar algum dano ao usuário do computador.

NECESSITA da ação do usuário e precisa de um programa para se hospedar. Ao contrário do que é pregado por aí, o vírus **pode sim se replicar**, ou seja, criar cópias de **si mesmo** pelo computador. Só que ele faz isso **dentro dos arquivos**, e não diretamente como faz o worm, sem a necessidade de um hospedeiro.

Abaixo listo alguns dos tipos de vírus mais comuns de serem abordados na sua prova:

Vírus de Boot
→ Corrompe os dados da inicialização do Sistema Operacional.

Vírus de script
→ escrito em linguagem de script, como VBScript e JavaScript, e recebido ao acessar uma página web ou por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. **Pode ser automaticamente executado**.

Vírus de Macro
→ tipo específico de vírus de script, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõe o Microsoft Office (Excel, Word e PowerPoint, entre outros).

Vírus Sthealth
→ É um malware complexo que se esconde (fica invisível) depois de infectar um computador. Uma vez escondido, ele copia as informações de dados não infectados para si mesmo e retransmite-as para o software antivírus durante uma verificação.

Vírus de Hardware

- Ataca arquivos e pastas;
- Dispositivos de armazenamento: Pendrive, HD Externo;
- Transforma arquivos em atalhos.

Vírus Polimórfico (Mutante)

- Capaz de alterar suas características a cada novo ataque;
- Dificilmente detectado.

Os vírus são divididos em 3 partes:

• **Mecanismo de infecção:** É também conhecido como vetor de infecção. São os meios pelos quais um vírus se propaga, permitindo-o a sua reprodução;

• **Mecanismo de ativação:** condição que determina quando a carga útil é ativada ou entregue. Às vezes, pode ser citado como bomba lógica;

• **Carga útil:** componente que executa uma atividade maliciosa. Embora nem todos os vírus tenham carga útil, algumas cargas são consideradas extremamente perigosas. Também é conhecida como carga destrutiva

Vírus SEMPRE precisa de um hospedeiro (não é autossuficiente). O único que consegue "ver" o vírus é o antivírus.

6.1.5 Worm

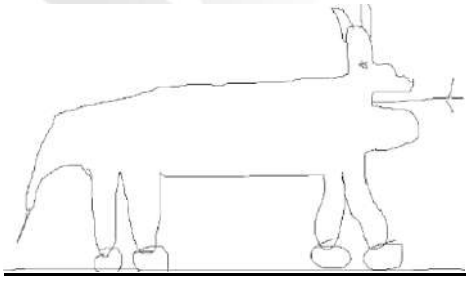
Worm é um programa independente que envia cópias de si mesmo de computador para computador, com capacidade de se auto propagar através de redes. Ele explora a vulnerabilidade de programas e sistemas ou falhas na configuração de softwares instalados.

Não Necessita: →

- Da ação do usuário
- De um hospedeiro (programa para se alojar).

OBSERVAÇÃO: O **worm não é um vírus**, pois não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Observe que é um arquivo executável – autossuficiente. Não necessita de um hospedeiro, como o vírus.

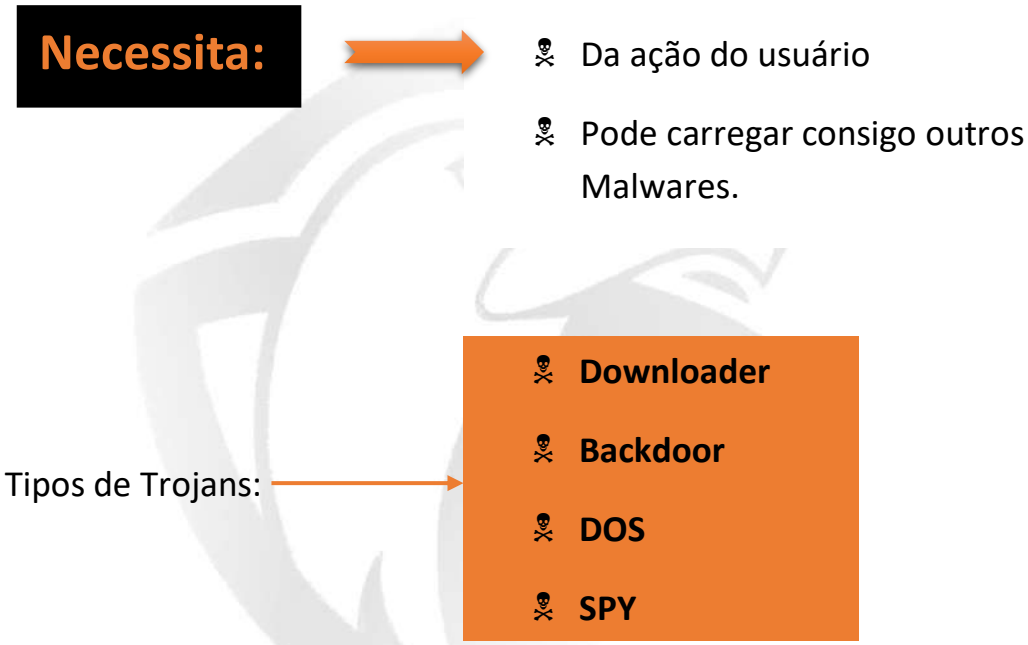
6.1.6 Trojan Horse (Cavalo De Tróia)



O cavalo de Troia é um malware (programa malicioso) que ataca como na famosa história do Cavalo de Troia, entrando disfarçado no computador e criando uma

porta para uma possível invasão; e é fácil de ser enviado, clicando na ID do computador e enviando para qualquer outro computador.

Tem como objetivo manter-se oculto, enquanto baixam e instalam ameaças mais robustas em computadores. Podem ser transportados em arquivos de música, mensagens de e-mail, escondidos em downloads e sites maliciosos, aproveitando as vulnerabilidades do navegador utilizado para instalar a praga no computador (parece ser uma coisa, mas é outra).



6.1.7 SPYWARE

Programa espião de computador, que tem o objetivo de observar (espiar) e roubar informações pessoais do usuário que utiliza o PC em que o programa está instalado, retransmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

Os Spywares podem ser divididos em 3 grupos:

Bizu Cavernoso

3 Espiãs Demais:
- **Alex (Adware)**
- **Sam (Screenlogger)**
- **Klover (Keylogger)**

- **ADWARE** → Anúncios e/ou propagandas. Utiliza costumes do usuário como por exemplo: visitar sites de compras, quando o mesmo for em suas redes sociais o produto aparece lá de forma "mágica".

- **SCREENLOGGER** → Captura os quadros da tela (Bate o Retrato) onde o mouse clicar (Teclado Virtual).

- **KEYLOGGER** → Captura senhas digitadas através do teclado. (Teclado Físico).

6.1.8 Rootkit

Consiste em um malware que comunica aos outros malwares quando o antivírus está chegando, os ajuda a esconder-se e em seguida se esconde, ou seja, é um programa muito difícil de ser encontrado.

Criado para esconder ou camuflar a existência de certos processos ou programas de métodos normais de detecção e permitir acesso exclusivo a um computador e suas informações.

6.1.9 Ransomware

É um tipo de programa malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O valor a ser cobrado vai ser definido pelo atacante.

Existem dois tipos de ransomware:

- ***Locker*:** impede que você acesse o **equipamento** infectado.
- ***Crypto*:** impede que você acesse os **dados armazenados** no equipamento infectado, geralmente usando criptografia.

Além de infectar o equipamento o ransomware também costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também.

Tudo que vimos na nossa aula é baseada na Cartilha de Segurança para Internet do CERT.Br e normas ABNT NBR ISO/IEC 27002:2013, fontes constantes das principais bancas de concurso.

Desse modo, é sempre interessante buscar por esses arquivos na internet, caso tenha alguma dúvida.

Vamos resolver questões para reforçar nosso aprendizado sobre malwares?

Questão de Entendimento:

08 (CEBRASPE|2019|PRF|POLICIAL RODOVIÁRIO FEDERAL)

No acesso a uma página *web* que contenha o código de um vírus de *script*, pode ocorrer a execução automática desse vírus, conforme as configurações do navegador.

Certo ( ) Errado ( )

Resolução

O vírus obrigatoriamente precisa ser executado pelo usuário (em regra). Porém, existem a exceção do vírus de script que pode ser executado automaticamente. Além disso, normalmente, quando a banca Cebraspe utiliza na questão as palavras ''...Conforme as configurações...'' o gabarito está correto (bizu).
CERTO

09 (CEBRASPE|2021|PC-AL|ESCRIVÃO DE POLÍCIA|PROVA ANULADA)

Julgue o item seguinte, relativo à organização de arquivos e suas premissas de segurança.

A grande diferença entre vírus e *worms* está na forma como eles se propagam: o vírus, ao contrário do *worm*, não se propaga por meio da inclusão de cópias de si mesmo em outros programas, mas pela execução direta de uma de suas cópias.

Certo ( ) Errado ( )

Resolução

Ambos propagam cópias de si mesmos, porém o worm faz isso automaticamente, enquanto o vírus faz isso mediante a execução pelo usuário.
ERRADO.

7 ATAQUES E PRAGAS

Conhecemos praga como toda espécie que se desenvolve sem ordem específica e que podem destruir ou prejudicar propriedades humanas. No digital isso não é diferente.

Assim, podemos dizer que as pragas virtuais **são programas maliciosos** que se espalham em **softwares** e **arquivos desprotegidos**.

7.1 Tipos de ataques e pragas

ENGENHARIA SOCIAL

- É a arte de enganar. Normalmente, um engenheiro social é condenado por estelionato e/ou falsidade ideológica. Pois, para realizar suas artimanhas ele se passa por outras pessoas e com um bom papo convence-as a fornecer dados, que por vezes não tem muito significado para a pessoa que os está fornecendo ao Engenheiro Social.

PHISHING

- Phishing é uma expressão derivada do termo **pescar** em inglês, pois o que esse tipo de ataque faz é induzir o usuário a informar seus dados pessoais através de páginas da Internet ou e-mails falsos. Criam **páginas semelhantes à original**, com promoções bem abaixo do preço convencional, ludibriando o usuário, que por sua vez, insere seus dados com intuito de comprar um produto abaixo do valor, e acaba se f* ferrando.

VISHING

- é um ataque que **ocorre por meio do telefone**, seja por meio de chamadas ou mensagens de texto, utilizando a boa-fé das pessoas, "premiando-a" de alguma forma.

PHARMING

- é um **tipo específico de phishing**, com a diferença que no pharming o tráfego de um site legítimo é manipulado para **direcionar usuários para sites falsos**, que vão instalar softwares maliciosos nos computadores dos visitantes ou coletar dados pessoais, tais como senhas ou informações financeiras.

FRAUDE DE ANTECIPAÇÃO DE RECURSOS OU ADVANCE FEE FRAUD

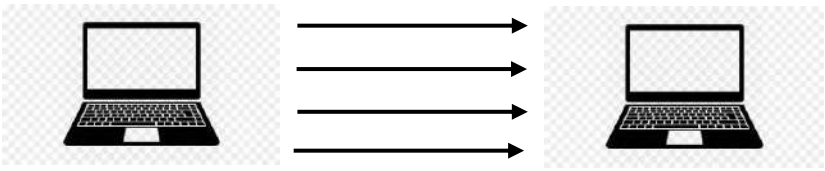
- É aquela no qual um(a) golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um **pagamento adiantado**, com a promessa de futuramente receber algum tipo de benefício. É só lembrar de político.

BRUTE FORCE

- O outro tipo de ataque bem comum é o ataque Brute Force ou força bruta, que realiza uma **busca exaustiva de chave**. É um ataque considerado criptoanalítico que pode, em teoria, ser usado contra quaisquer dados criptografados (salvo para dados criptografados de uma maneira segura). Ele realiza uma verificação sistemática de todas as possibilidades de chaves e senhas até que as corretas sejam encontradas.

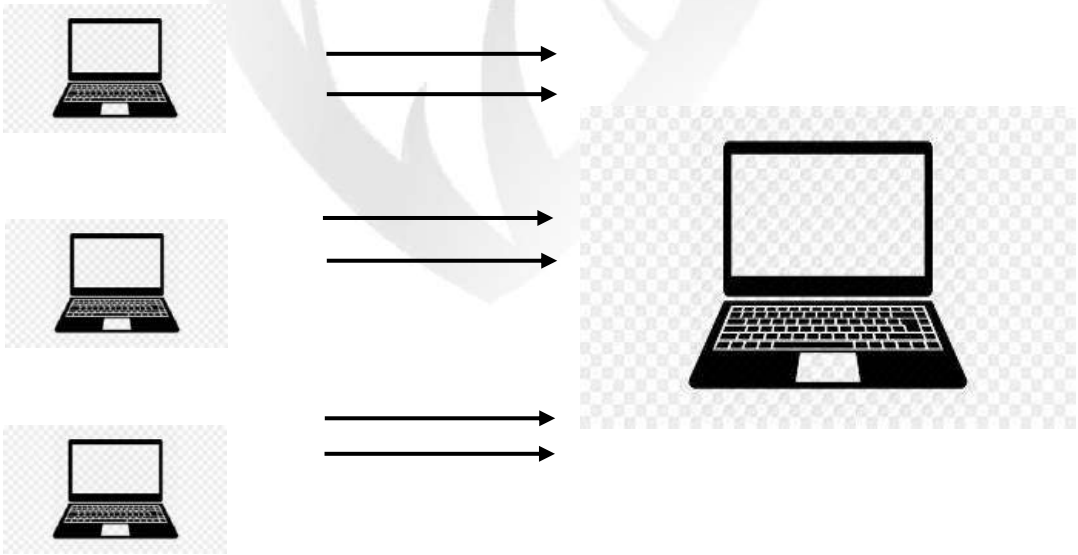
DoS (DENIAL OF SERVICE OU NEGAÇÃO DE SERVIÇO)

- é um **ataque individual**, geralmente com o intuito de tornar-se um serviço inoperante para o usuário. O objetivo do ataque DoS não é roubar informações, mas sim tornar o servidor da página indisponível.



DDoS (DISTRIBUITED DENIAL OF SEVICE)

- é um **ataque realizado em massa**, utiliza-se de vários computadores contaminados que dispara solicitações de acesso a determinados sites ou serviços, derrubando o serviço.
- Nesses casos, as tarefas de ataque de negação de serviço são distribuídas a um exército de máquinas escravizadas. Por isso, denomina-se um ataque distribuído de **negação de serviço**.



SPAM

- é uma prática que tem como finalidade divulgar **propagandas por e-mail**, ou mesmo utilizar de e-mails que chamem a atenção do usuário e incentivem ele a encaminhar para inúmeros outros contatos, para que, com isso, levantem uma lista de contatos que pode ser vendida na Internet ou mesmo utilizada para encaminhar mais propagandas.

  Tipos de Spam:
  - Propaganda
  - Hoax (boato falso e alarmista)
  - Filantrópicos
  - Correntes

SPOOFING

- Nesse ataque o **remetente** é que é **fraudado**. Um exemplo comum é você receber um e-mail de você mesmo, sem tê-lo enviado. Os servidores possibilitam realizar esse procedimento facilmente, pois é uma necessidade para serviços rotineiros de sites, em que o servidor envia um e-mail de uma conta, mas envia para o usuário os dados do cabeçalho do e-mail como se fosse de outro endereço.

DEFACEMENT

- Também conhecido como **pichação**, é o ataque que consiste em alterar ou inserir dados nos sites normalmente usados como forma de protesto ou **mostrar que o site possui segurança fraca** ou inexistente.

8 PROCEDIMENTOS E APLICATIVOS DE SEGURANÇA

8.1 Antimalwares

São programas que tem como intuito realizar a prevenção contra os ataques e ações de Malwares(Programas Maliciosos).

Esses programas auxiliam na segurança de um computador, como, por exemplo, Antivírus, Antispyware, Antirootkit e Antitrojan, que reparam o sistema ou programas, procuram e apagam pragas instaladas nos computadores do usuário, depende qual seja a ação necessária para aquele momento.

O que poderíamos considerar como ideal para um bom procedimento de segurança é que cada máquina possua apenas um programa Antimalware, já que pode haver conflito entre as configurações estabelecidas, mas nada impede que o usuário instale vários programas de segurança de sua preferência.

Usar mais que um Antimalware ao mesmo tempo é diferente de usar um Antimalware com um Firewall em conjunto, por exemplo, que são ferramentas distintas, mas que, em todos os casos, ambas as ferramentas cooperam para a segurança da informação.

8.2 Antivírus

Os softwares Antivírus são os mais completos nessa categoria de defesa e estão voltados mais especificamente para controle de pragas virtuais, os Malwares, embora sua constituição fosse voltada para controle de vírus, primariamente; com

o passar do tempo, ele acabou sendo incorporado a um Antimalware em geral, mas o nome Antivírus permaneceu.

Toda vez que o usuário executa um arquivo no computador, ele passará por uma Análise Comportamental, que são as práticas de análise que um antivírus realiza no arquivo como métodos de detecção de um Malware.

Escaneamento em 1ª Geração

➔ Buscando pela assinatura do malware (Retrato Falado) é realizado um comparativo com uma lista de assinaturas já existentes no programa Antivírus e que são instaladas e atualizadas todas as vezes que o programa for atualizado.

2ª Geração

➔ Busca pela Heurística, ou seja, as características do Malware. Após essa análise, os arquivos serão executados corretamente, por não serem Malwares, ou colocados em quarentena, quando suspeitos de serem Malwares e não possuírem naquele momento uma forma apta de combatê-los. **Os arquivos enviados para quarentena aguardam até que o programa antivírus receba novas atualizações do fabricante com as possíveis maneiras de limpar o arquivo contaminado**. Caso não haja ações suficientes para a recuperação do arquivo contaminado, o programa antivírus irá apagá-lo do computador, para que o sistema não seja mais contaminado.

8.3 Firewall (Parede de Fogo)

Firewall é uma barreira protetora entre o usuário e a rede (Internet, intranet ou Extranet)

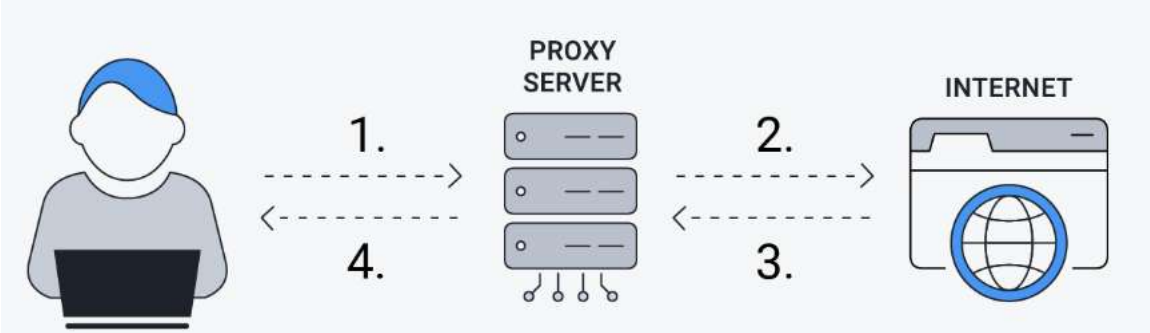
- Controla os dados que entram e saem a nível de rede;
- PRF/porteiro
- Restritivo (nada pode a não ser que se crie uma exceção)

- Filtrar; restringir, bloquear, monitorar, controlar;
- Pode ser implementado via hardware (*appliance*) e também via software;

OBSERVAÇÃO: Firewall não combate malware já instalados

8.3.1 Proxy

Aplicação do Firewall. Atua como intermediário entre todas as requisições que eu faço e a internet.



8.4 Backup

Cópia de segurança. Salvar um arquivo em pelo menos 2 locais geograficamente distintos.

Questão de Entendimento:

10 Em relação a vírus, Worms e pragas virtuais, para garantir a segurança da informação, é suficiente instalar e manter atualizados antivírus.

Certo ( ) Errado ( )

Resolução

Não é absoluto, mas é suficiente. **CERTO**

11 A função principal de uma ferramenta de segurança do tipo antivírus é verificar arquivos que contenham códigos maliciosos.

Certo ( ) Errado ( )

Resolução

CERTO

12 Acerca de antivírus e softwares maliciosos, julgue o próximo item. Como os antivírus agem a partir da verificação da assinatura de vírus, eles são incapazes de agir contra vírus cuja assinatura seja desconhecida.

Certo ( ) Errado ( )

Resolução

ERRADO. Ele pode buscar pela heurística.

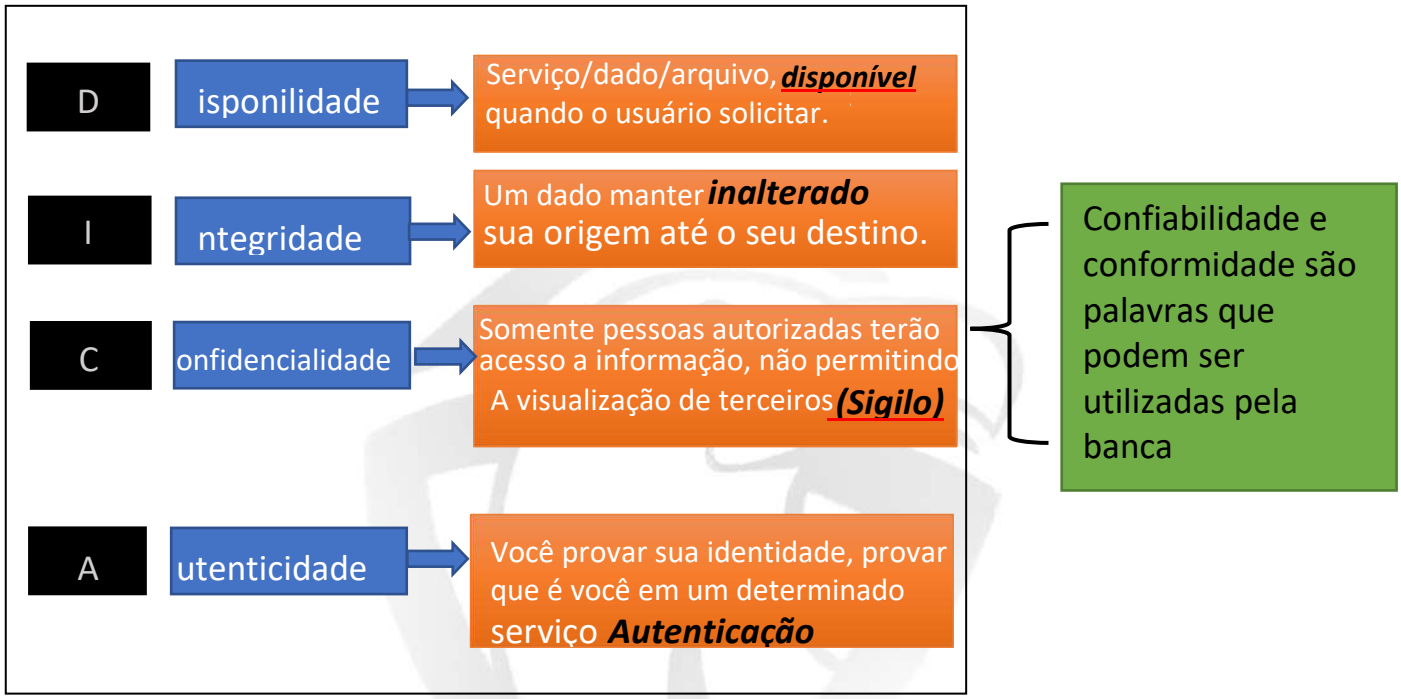
13 Acerca das redes de computadores e segurança, julgue o item que segue. Os aplicativos de antivírus com escaneamento de segunda geração utilizam técnicas heurísticas para identificar códigos maliciosos.

Certo ( ) Errado ( )

Resolução

CERTO. 1ª geração busca a assinatura do vírus e 2ª geração busca a heurística.

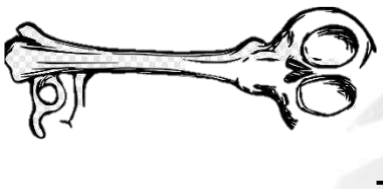
9 SEGURANÇA DA INFORMAÇÃO



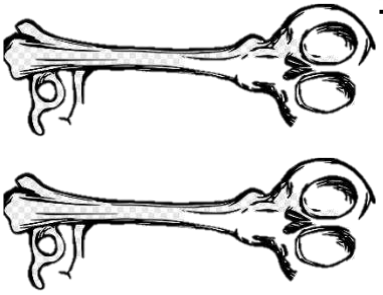
9.1 Criptografia

A criptografia, palavra que tem origem nos termos gregos kryptós (escondido) e gráphein (escrita), é uma área de estudo que analisa princípios e técnicas para transformar uma informação, como um arquivo de texto, em um código cifrado, o qual não possibilita a leitura, pois é ilegível, sendo compilada apenas pelo seu emissor e receptor, que são os elementos que detém as chaves (códigos) para criptografar e reverter a criptografia, garantindo com isso a confidencialidade, pois se for interceptada por outra pessoa, não poderá ser lida.

Nesse sentido, esse ramo da matemática visa o estudo dos métodos para garantir o sigilo da informação, por meio da utilização de duas chaves possíveis, a pública e a privada, gerando duas formas de criptografia:



SIMÉTRICA→ PALAVRA ESCRITA COM UM "S", ENTÃO TEM UMA ÚNICA CHAVE, ENTÃO A MESMA CHAVE USADA PARA CIFRAR, SERÁ USADA PARA DECIFRAR.
TAMBÉM CHAMADA DE CRIPTOGRAFIA



ASSIMÉTRICA→PALAVRA ESCRITA COM DOIS "S", ENTÃO UTILIZA CHAVES DISTINTAS PARA CIFRAR E DECIFRAR A INFORMAÇÃO.
TAMBÉM CHAMADA DE CRIPTOGRAFIA DE CHAVE PÚBLICA.

Questão de Entendimento:

14 A segurança da informação baseia-se em três pilares: Confidencialidade, Integridade e Disponibilidade. Com base nessa informação, analise as afirmativas a seguir:

I. Garantir o acesso por pessoa ou dispositivo devidamente autorizados a todo o hardware, software e dados sempre que necessário.
II. As informações devem ser armazenadas da forma como foram criadas, de modo que não sejam corrompidas ou danificadas.
III. As informações não poderão ser vistas ou utilizadas sem as devidas autorizações de acesso por pessoas ou dispositivos.

Assinale a alternativa que apresente a ordem correta de associação com os três pilares da segurança da informação.

A) I – Disponibilidade, II – Integridade, III – Confidencialidade
B) I – Confidencialidade, II – Integridade, III – Disponibilidade
C) I – Integridade, II – Confidencialidade, III – Disponibilidade
D) I – Confidencialidade, II – Disponibilidade, III – Integridade
E) I – Disponibilidade, II –Confidencialidade, III – Integridade

15 O recurso que estuda os princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, com o objetivo de dificultar a leitura de pessoas não autorizadas, denomina-se

A) Backup.
B) Webgrafia.
C) criptografia.
D) quarentena.

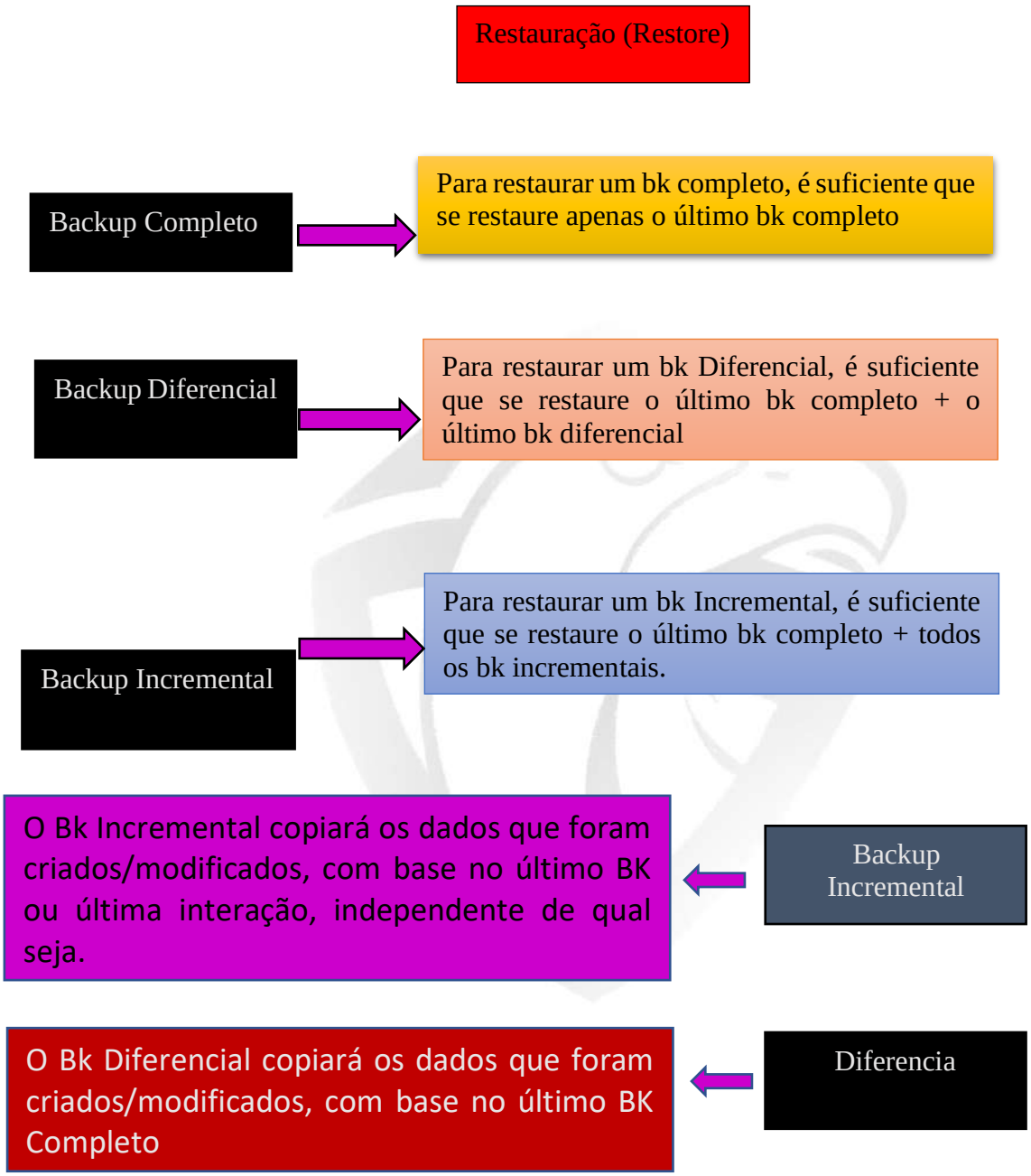
16 Para o estabelecimento de padrões de segurança, um dos princípios críticos é a necessidade de se verificar a legitimidade de uma comunicação, de uma transação ou de um acesso a algum serviço. Esse princípio refere-se à

A) confidencialidade.
B) autenticidade.
C) integridade.
D) conformidade.
E) disponibilidade.

17 A criptografia é um dos elementos principais para garantir a segurança em redes de computadores. Quando o remetente e destinatário precisam compartilhar uma mesma chave secreta para criptografar e descriptografar as mensagens, é correto afirmar que se está utilizando o sistema de chaves:

a) combinadas.
b) escondidas.
c) assimétricas.
d) simétricas.
e) criptografadas.

9.2 Restauração



Questão de Entendimento:

18 Backup é um termo inglês que tem o significado de cópia de segurança. Como se chama o backup que contém apenas os arquivos que foram criados ou modificados a partir do último backup realizado, e que, depois de fazer a cópia do arquivo, desmarca o atributo (flag) de arquivamento?

a) Diferencial
b)Incremental
c) Completo
d) Seletivo

19 As cópias de segurança (backup) são imprescindíveis nas organizações. Elas podem ser armazenadas de diversas formas. O tipo de backup onde cópias são feitas apenas dos arquivos que foram modificados desde a última interação é denominado:

A) Backup cumulativo.
B) Backup diferencial.
C) Backup incremental.
D) Backup completo.

20 Uma rotina de backup de uma determinada empresa consiste na utilização de backups normais e incrementais. Acerca de desse cenário, assinale a alternativa correta:

A) Para a recuperação do sistema no caso de acontecer algum problema, deve-se recuperar primeiramente o último backup normal e todos os backups incrementais seguintes até o dia em que o problema aconteceu.
B) O primeiro backup incremental deve sempre ser mantido porque sem ele não é possível recuperar os backups normais posteriores.
C) Antes de realizar um backup normal, é necessário que seja realizado pelo menos um backup incremental.
D) Não será necessário recuperar nenhum backup normal se os incrementais são realizados diariamente.
E) Caso se utilize apenas um conjunto para backups normais, recomenda-se que esse backup nunca seja apagado, por questões de segurança e de atualização dos dados presentes no backup.

9.3 Certificado Digital

O Certificado digital que ao contrário da Assinatura Digital, não há validade jurídica por não conter uma terceira parte confiável envolvida.
O certificado digital tem validade jurídica justamente por haver essa terceira parte confiável e independente, que é a organização pública ou privada a qual cria o certificado digital que por sua vez é regulamentado pela Medida Provisória **2200/02**,

O certificado digital nada mais é do que um arquivo de forma digital que contém informações sobre um emissor → (quem emite e informação) (no qual pode ser pessoa física ou jurídica) por meio da chave pública referente à chave privada que deve ser de posse exclusiva do receptor → (que é quem recebe a informação), do conteúdo em que foi solicitado tal certificado.

9.3.1 Elementos do certificado digital

As Informações pessoais que deverão ser referentes ao emissor (entidade) para o qual o certificado foi emitido
Ex: (nome,CPF/CNPJ, e-mail, endereço etc.).

Uma chave pública vinculada à chave privada de posse da entidade especificada no certificado digital emitido.

- O prazo de validade do certificado.
- Número de série do certificado.
- O chamado “centro de revogação” que geralmente é uma URL para LCR.

9.4 Assinatura Digital

Quando falamos assinatura digital, embora seja considerado um importante instrumento de segurança na transmissão de dados, o mesmo por sua vez não tem validade jurídica no Brasil, devido ao fato de ser uma relação entre duas pessoas (emissor e receptor), ou seja, não tendo uma terceira parte independente envolvida.

A assinatura digital representa um método de autenticação de informação enviada digitalmente, e tem a mesma relação da assinatura propriamente dita. A principal diferença é que a assinatura digital, que é criada pelo Emissor, tem como objetivo a comprovação do autor da mensagem, se o emissor é de fato o dito cujo que desenvolveu a mensagem. O que, quando confirmado, impede o emissor de repudiar o conteúdo como não tenha sido ele o autor.

Seguem abaixo quais critérios a assinatura digital visa garantir

- Autenticidade.
- Integridade.
- Irretratabilidade (Não repúdio).

9.4.1 Legislação

A Medida Provisória nº 2.200-2, de 24 de agosto de 2001 define as regras para a criação da ICP-Brasil:

> *Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileiras - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras, integrada pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro - AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

As informações obrigatórias são **Número de série** e **Prazo de validade.**

Questão de Entendimento:

21 Preencha a lacuna e assinale a alternativa correta. Um (a) _____ se usado(a) de forma maliciosa e instalado(a) pode permitir estabelecer conexões cifradas com sites fraudulentos, sem que o navegador emita alertas indicativos de risco.

A) certificado EV SSL
B) certificado auto-assinado
C) criptografia de chaves assimétricas
D) criptografia de chave simétrica

22 Certificados Eletrônicos, no Brasil, são emitidos:

A) por autoridades certificadoras;
B) pela Receita Federal;
C) pela Polícia Federal;
D) pelas prefeituras;
E) pelos cartórios.

Questão de Entendimento:

23 Para que serve um Certificado Digital?

A) Para atribuir a um documento a autenticidade, confidencialidade, integridade e não repúdio.
B) Para que um documento não pegue vírus.
C) Para o Firewall criptografar as informações de um documento.
D) Evitar o conflito de hardware.
E) Colocar um programa na "queue" do sistema operacional.

24 O certificado digital, emitido por uma Autoridade Certificadora (AC), visa a prover uma identidade virtual que permite a identificação segura e inequívoca do ator de uma mensagem ou transação feita em meios eletrônicos. Dentre as informações presentes no certificado digital, emitido por uma AC para um indivíduo, existe a

A) chave privada da AC
B) chave pública da AC
C) chave privada do indivíduo
D) chave pública do indivíduo
E) assinatura digital do indivíduo

9.4.2 Aplicação da Assinatura Digital

Os principais navegadores de internet do mercado trabalham com assinatura digital tais como: Mozilla, Chrome, Opera. Isso pode muitas vezes não ser perceptível para o usuário, mas é recorrente na navegação em diversos sites. Cada browser tem sua própria forma de identificação, e no caso do Google Chrome, por exemplo, a identificação segue abaixo:

- **Cadeados verdes - Identificam certificados reconhecidos.**
- **Cadeados amarelos - Identificam problemas na certificação.**
- **Cadeados vermelhos - Não identificados.**

9.4.3 Funcionamento da Assinatura Digital

O usuário pode utilizar dos diversos métodos fornecidos para assinar um documento digital, e pela necessidade de aumentar os níveis de segurança na internet, esses modos estão constantemente em alteração e consequentemente em evolução. Centralmente, as assinaturas digitais têm dois elementos, o hash (resumo do conteúdo) e a encriptação desse mesmo hash.

- Primeiro é gerado resumo criptografado do conteúdo por meio de algoritmos, e esses reduzem as mensagens. Depois, esse resumo, denominado hash, é analisado sobre as características que seguem abaixo:
- Não pode haver vínculo entre a mensagem original e o hash, para que essa não seja encontrada facilmente.
- Mesmo que seja gerado por meio de um algoritmo padrão, o hash deve dar a impressão de ser aleatório, e é eficaz quando consegue identificar a alteração de um bit da mensagem original para a que chega até o receptor.

Não deve existir hash vinculado a mais conteúdo com assinatura digital, por essa razão ele deve manter a característica de exclusividade.

Questão de Entendimento:

25 A segurança de redes de computadores representa uma necessidade cada vez mais presente no mundo moderno. Sobre conceitos relacionados a esse tipo de segurança, assinale a alternativa CORRETA.

A) A criptografia é uma técnica utilizada para garantir a confidencialidade da informação transmitida.

B) O controle de autenticidade visa garantir que o acesso à informação seja feito apenas por agentes (pessoas ou máquinas) autorizados.

C) Um firewall é um recurso exclusivamente de hardware, que garante a segurança de uma rede a partir da filtragem de toda informação que chega a essa rede.

D) A assinatura digital é uma técnica que objetiva substituir a assinatura convencional, garantido apenas a autenticidade de quem envia uma mensagem.

E) Vírus é um termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

26 A assinatura digital tem entre suas características principais:

A) exigir que o usuário compareça a uma AR com a documentação necessária para cadastramento

B) garantir a confidencialidade dos dados, não sendo necessário nenhum método adicional

C) fornecer uma prova inegável de que uma mensagem veio de um emissor

D) coexistir em dois modelos: malha de confiança e hierárquico

27 Um dos benefícios fornecidos por assinaturas digitais de documentos eletrônicos é a possibilidade de verificar que o conteúdo assinado não foi alterado em trânsito. Ou seja, a possibilidade de verificar que um terceiro que teve acesso ao conteúdo antes que o mesmo chegasse em seu destinatário não alterou os dados. Esse conceito é chamado de

A) imutabilidade.
B) integridade.
C) persistência.
D) não repúdio.
E) autenticação.

28 É propriedade de uma Assinatura Digital, além de Autenticidade e Integridade:

A) Quebras.
B) Irretratabilidade.
C) Derivação.
D) Motivação.
E) Data.

29 Os critérios garantidos pela assinatura digital são os da autenticidade, da integridade e da irretratabilidade.

Certo ( ) Errado ( )

30 Ícones em navegadores, como o Google Chrome, indica o nível de segurança existente nos sites da internet.

Certo ( ) Errado ( )

10 CLOUD COMPUTING (COMPUTAÇÃO EM NUVENS)

Cloud Computing refere-se ao armazenamento, edição e aplicação de softwares se utilizando de servidores da Internet ou Intranet.

Quando é utilizado a nuvem para armazenamento e edição, não existe a necessidade de dispositivos de armazenamento em massa tais como: pen-drives,Cd, Blu-ray , HD, etc. E essa situação traz várias vantagens para quem faz uso desses serviços.

10.1 Principais vantagens de Cloud Computing

- **Disponibilidade** – As informações (Dados) ficando gravados nos servidores da Internet ou da Intranet, o uso pode ser feito de múltiplos pontos, sendo necessário apenas o acesso à internet.

- **Serviços sobre demanda** (on demand) – O uso e contratação do serviço, ou mesmo a utilização de algum aplicativo on-line, só são feitos quando existe real demanda de trabalho por parte do usuário de tal serviço.

- **Escalabilidade** – É possível, de acordo com a necessidade de uso, aumentar o espaço para armazenamento ou atualizar o serviço fornecido .

- **Segurança** – Os dados salvos nas nuvens ficam armazenados em servidores corporativos, ou seja, os níveis de segurança são geralmente mais elevados do que os encontrados em computadores de uso pessoal.

Mas como todo serviço também apresenta as suas desvantagens.

10.2 Principais desvantagens de Cloud Computing

- **Comprometimento de dados**
- **Velocidade de acesso**
- **Custo**
- **Disponibilidade**

10.3 Tipos de Clouds Computings

Podem existir algumas classificações e tipos de Cloud, e essa se dá pela natureza do serviço e objetivos da empresa que é a provedora Cloud. Abaixo listaremos os tipos de Cloud Computing existentes:

- Cloud Privado
- Cloud Público
- Cloud em Comunidade
- Cloud Híbrido_

Questão de Entendimento:

31 De acordo com os conceitos de cloud computing julgue a assertiva a seguir: No serviço de Cloud Computing, o usuário mantem total autonomia frente aos servidores da internet.

Certo ( ) Errado ( )

32 De acordo com os conceitos de cloud computing julgue a assertiva a seguir: Serviços privados de Cloud são aqueles em que apenas empresas privadas podem oferecer serviços aos usuários, terceirizando o acesso.

Certo ( ) Errado ( )

33 De acordo com os conceitos de cloud computing julgue a assertiva a seguir: O serviço de cloud computing tem como característica a escalabilidade, podendo gradativamente agregar mais espaço de armazenamento e tecnologia.

Certo ( ) Errado ( )

10.3.1Sistema de Cloud Computing

O sistema de Cloud Computing faz referência ao uso de sistemas computacionais, armazenamento, processamento, segurança, sem que esses recursos estejam fisicamente no computador do usuário.

O serviço de nuvem pode ser oferecido de diversas maneiras, desde um simples espaço para armazenamento de dados, até um serviço que disponibiliza programas que podem ser acessados de qualquer lugar do mundo desde que haja conexão com internet, ou um serviço completo de infraestrutura computacional, processamento, memória, armazenamento, segurança.

Existem diversos tipos de serviços fornecidos e uma tipologia de arquitetura como por exemplo:

A) IaaS – Infrastructure As A Service (Infraestrutura Como Serviço)

Esse tipo de nuvem o próprio usuário faz a adesão de uma infraestrutura que já vem pronta, tanto hardware como software (“máquinas virtuais”). Nesse serviço contratado, o usuário possui total controle sobre os recursos aderidos e se desejar pode fazer uso desses recursos sempre que quiser, bastando apenas do uso da Internet.

As grandes empresas que necessitam de um servidor controlador de acesso ou servidor de segurança, mas que não há necessidade de instalar um computador, utilizam muito esse tipo específico de serviço. Exemplo de empresas que prestam esse tipo de serviço é a Amazon, Google Cloud Platform e a IBM.

B) SaaS – Software As A Service (Software como Serviço)

Já esse tipo específico é muito usado para acesso de softwares sem haver a necessidade destes estarem instalados na máquina do cliente. Quando o usuário recebe um e-mail com anexos do tipo .docx ou .pdf e consegue abrir o conteúdo desses anexos no próprio navegador de internet sem a necessidade de ter instalado na máquina o Word ou um leitor de .pdf.

Outro serviço muito utilizado na Tipologia SaaS é o de armazenamento de dados na nuvem Cloud Storage (armazenamento em nuvem), onde o usuário contrata um serviço de armazenamento em nuvem e utiliza programas específicos do serviço contratado para gerenciar os arquivos armazenados ou utiliza o próprio navegador de Internet para poder acessar seus recursos salvos em nuvem. Exemplos de empresas que prestam esse tipo de serviço são Dropbox, iCloud, google docs.

C) PaaS – Platforme As A Service (plataforma como Serviço)

Essa tipologia por sua vez é usada basicamente para desenvolvimento de programas, justamente para os garotos de programa, brincadeira a parte com essa tipologia não há necessidade de instalar na máquina do usuário os programas necessários para isso.

Esse tipo de nuvem é bastante aderido por empresas de desenvolvimento de software, pois em grandes projetos os desenvolvedores podem estar em lugares diferentes do mundo e com isso é possível utilizar sempre o mesmo serviço para continuar o desenvolvimento sem a necessidade de ficar transportando o que já foi programado por todos os lados, já que toda estrutura necessária é disponibilizada na tipologia PaaS. Exemplo de empresas que prestam esse tipo de serviço é a Azure, Drupal, Squarespace.

10.3.2Nuvem Pública

- Os servidores são alocados em data centers externos.
- É um serviço de nuvem terceirizado.
- Serviço gerenciado pelo provedor de nuvem.
- Geralmente usadas para: Web e-mail, aplicativos de escritório online, armazenamento etc.

Vantagens

- Redução de custos – não há necessidade de comprar hardware ou software.
- Sem manutenção – seu provedor de serviços fornece a manutenção.
- Escalabilidade.
- Alta confiabilidade.

10.3.3Nuvem Privada

- Recursos usados exclusivamente por uma única empresa ou organização.
- Localizada fisicamente na organização ou hospedada por um provedor de serviços terceirizado dedicado.
- Recursos são mantidos na rede privada
- Geralmente usadas por órgãos governamentais, instituições financeiras e outras organizações de grande porte.

Vantagens

- Maior flexibilidade – personalizar o ambiente de nuvem para atender a necessidades específicas.
- Segurança aprimorada – serviço não compartilhado. Maior de controle e segurança.
- Alta escalabilidade.

10.3.4Nuvem Híbrida

Assim como o nome sugere, nuvem mista ou nuvem híbrida é quando uma empresa ou organização utiliza os recursos de nuvem pública e nuvem privada ao mesmo tempo.

Na teoria, esse tipo de nuvem seria o modelo mais indicado para as empresas, pois esse tipo de implementação oferece muitos recursos de operação. Mas, a implantação desse tipo de serviço em nuvem é mais cara que a nuvem pública ou

privada, pois ao mesclar os dois tipos de implantação em nuvem, o recurso pode se tornar economicamente inviável para Pequenas e Médias Empresas

Questão de Entendimento:

34 Considere hipoteticamente que Ana, analista do Conselho de Arquitetura e Urbanismo, emitiu um parecer de caráter público e, após a aprovação dele por instâncias superiores, disponibilizou-o, em formato PDF, no Google Drive, para acesso de todos os respectivos colegas de trabalho. No caso apresentado, o tipo de serviço que Ana utilizou se denomina

A) armazenamento em nuvem.
B) armazenamento por correio eletrônico.
C) armazenamento em pen drive.
D) upload em rede social.

35 A computação em nuvem, ou cloud computing, trata a computação como um serviço oferecido por meio da internet de forma gratuita ou paga. A esse respeito, assinale a alternativa correspondente à categoria de cloud computing em que os softwares Google Docs e Gmail são classificados.

A) Documentação de serviços
B) Software como serviço
C) Infraestrutura de redes sociais
D) Redes sociais como serviço
E) Hardware como serviço

36 A respeito de computação em nuvem, julgue o próximo item. A computação em nuvem do tipo software as a service (SaaS) possibilita que o usuário acesse aplicativos e serviços de qualquer local usando um computador conectado à Internet.

Certo ( ) Errado ( )

37 Um analista utiliza um conjunto de aplicativos de escritório (google docs) que não estão instalados em seu computador, mas em servidores espalhados em pontos diversos da internet. Além de acessar os aplicativos, guarda também os documentos produzidos por meio deles nesses servidores, de forma a poder acessá-los a partir de qualquer computador com acesso à internet. O analista utiliza um tipo de computação em nuvem conhecido como

A) DEVELOPMENT AS A SERVICE.
B) SOFTWARE AS A SERVICE.
C) PLATAFORM AS A SERVICE.
D) INFRASTRUCTURE AS A SERVICE.
E) COMMUNICATION AS A SERVICE.

11 QUESTÕES DE RENDIMENTO

01 (AOCP|2020|PREFEITURA DE CARIACICA-ES|ASSISTENTE)

Considerando que é necessário anexar um arquivo de 12 bytes em um sistema Web que aceita apenas arquivos com tamanho máximo de 10 bytes, qual programa deve ser utilizado para resolver esse problema?

A) Adobe Reader.
B) Winrar.
C) Outlook Express.
D) Conexão para a Área de Trabalho Remota.

02 (IBFC|2019|IDAM|ASSISTENTE TÉCNICO)

Relacione a coluna de números com o respectivo componente da coluna de letras e selecione a resposta correta:

(1) Hardware
(2) Software

(A) banco de dados
(B) memórias RAM e ROM
(C) placa-mãe
(D) editor de texto

A) 1AD - 2BC
B) 1AC - 2BD
C) 1BD - 2AC
D) 1BC - 2AD

03 (FUMARC|2022|PC-MG|ANALISTA DA POLÍCIA CIVIL)

Considerando os fundamentos de licenças GPL, existem quatro liberdades que caracterizam um software livre. Analise os itens a seguir e identifique-os com (**V**) ou (**F**) conforme sejam verdadeiros ou falsos, em relação a estas liberdades.

( ) A liberdade de usar o software para qualquer finalidade.
( ) A liberdade de mudar o software de acordo com as suas necessidades.
( ) A liberdade de compartilhar o software somente quando o seu código fonte não for divulgado.
( ) A liberdade de compartilhar as mudanças que você faz.

A sequência **CORRETA**, de cima para baixo, é:

A) F, F, V, F.
B) V, F, F, V.
C) V, F, V, V.
D) V, V, F, V.

04 (AOCP|2018|ITEP-RN|AGENTE DE NECRÓPSIA)

Assinale a alternativa que apresenta uma definição correta de Software.

A) São as partes concretas do computador, isto é, os componentes como: gabinete, teclado, mouse, impressora, memória, CPU.
B) São programas destinados a causar danos, alterações ou roubo de informações no computador em que estão instalados.
C) São programas instalados em um computador, os quais realizam uma ou mais tarefas.
D) São programas feitos diretamente no hardware de computadores.
E) São programas leves (*soft*), ou seja, que não requerem alto poder de processamento de um computador.

05 (FGV|2017|ALERJ|ESPECIALISTA LEGISLATIVO)

Segundo a Cartilha de Segurança para Internet (http://cartilha.cert.br/malware/), códigos maliciosos (malware) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Sobre códigos maliciosos, é correto afirmar que:

A) spyware é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim;
B) backdoor é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador;
C) bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente;
D) rootkit é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
E) worm é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

06 (FCC|2016|PREFEITURA DE TERESINA-PI|AUDITOR FISCAL)

Um funcionário de uma empresa percebeu que seu computador estava sendo controlado remotamente sem seu consentimento, quando foi notificado pelo administrador da rede que, a partir de seu computador, estavam sendo enviados spams, realizados ataques de negação de serviço e propagação de outros códigos maliciosos. Com base nestas características e ações, conclui-se que o computador deve estar infectado por um

A) vírus.
B) rootkit.
C) keylogger.
D) spyware.
E) bot.

07 (FCC|2017|TRE-SP|TÉCNICO JUDICIÁRIO)

Em uma situação hipotética, um tipo de código malicioso foi detectado no TRE-SP e tinha a característica de ser controlado pelo invasor via processo de infecção e propagação automática. Ele explorava diversas vulnerabilidades existentes em programas instalados. Foi verificado, ainda, que a comunicação entre os infectados e o invasor ocorria de várias formas, via servidores Web, canais IRC, redes tipo P2P, entre outros meios e eram recebidos, automaticamente, pela rede. Um Programador de Sistemas analisou estas características e observou que os computadores atingidos ficavam semelhantes a zumbis (*zombie computer*) pelo fato de serem controlados remotamente, sem o conhecimento de seu usuário. Trata-se de um código malicioso conhecido como

A) Trojan DoS.
B) Screenlogger.
C) Rootkit.
D) Keylogger.
E) Bot.

08 (UFES|2019|UFES|JORNALISTA)

Segundo Machado (2014), aos programas de computador que se duplicam e passam de um sistema para outro, sem necessidade de um arquivo hospedeiro, a fim de atacar um sistema qualquer e explorar uma vulnerabilidade específica nesse sistema, dá-se o nome de

A) Trojan.
B) Worm.
C) Vírus.
D) Spyware.
E) Backdoor.

09 (FUNCERN|2019|PREFEITURA DE APODI-RN|AGENTE COMUNITÁRIO)

Os malwares são programas maliciosos cujo objetivo é roubar informações ou contaminar os computadores. O malware que tem a capacidade de se propagar na rede de computadores é o

A) vírus.
B) worm.
C) netmal.
D) trojan.

10 (FUNCERN|2019|PREFEITURA DE APODI-RN|AGENTE COMUNITÁRIO)

Quanto à Segurança da Informação analise as afirmativas abaixo e assinale a alternativa correta.

I. Spyware, mais conhecidos como antivírus, são softwares específicos para a devida Segurança da Informação individual e corporativa.
II. Trojan é um tipo de programa malicioso que pode entrar em um computador disfarçado como um programa comum e legítimo.
III. Malware são programas de computador destinados a infiltrar-se em um sistema de computador de forma ilícita, com o intuito de causar danos, alterações ou roubo de informações.

A) Apenas as afirmativas I e II são tecnicamente verdadeiras
B) Apenas as afirmativas II e III são tecnicamente verdadeiras
C) Apenas as afirmativas I e III são tecnicamente verdadeiras
D) As afirmativas I, II e III são tecnicamente verdadeiras

11 (CEBRASPE|2018|PF|ESCRIVÃO)

Uma das partes de um vírus de computador é o mecanismo de infecção, que determina quando a carga útil do vírus será ativada no dispositivo infectado.

Certo ( ) Errado ( )

12 (CEBRASPE|2013|PRF|POLICIAL RODOVIÁRIO FEDERAL)

Ao contrário de um vírus de computador, que é capaz de se autorreplicar e não necessita de um programa hospedeiro para se propagar, um worm não pode se replicar automaticamente e necessita de um programa hospedeiro.

Certo ( ) Errado ( )

13 (CEBRASPE|2022|PC-RO|AGENTE DE POLÍCIA)

Um tipo de *malware* que, ao infectar um computador, pode tanto criptografar dados de arquivos individuais quanto corromper algumas funções básicas do computador, realizando uma extorsão cuja recuperação é feita mediante algum tipo de resgate, é o

A) *backdoor.*
B) *rootkit.*
C) *screenlogger.*
D) *ransomware.*
E) *spyware.*

14 (CEBRASPE|2021|PC-DF|ESCRIVÃO DE POLÍCIA)

A respeito de segurança e proteção na Internet, julgue o item que se segue.

Para que as pragas virtuais denominadas *worms* ataquem o computador em uso, é necessário que se execute um arquivo do tipo **.bat**.

Certo ( ) Errado ( )

15 (CEBRASPE|2021|PRF|POLICIAL RODOVIÁRIO FEDERAL)

A respeito de segurança e de *cloud computing*, julgue o item subsequente.

Ransomware é um programa malicioso de computador que se propaga por meio da inserção de cópias de si mesmo em arquivos criptografados.

Certo ( ) Errado ( )

16 (CEBRASPE|2018|PF|PERITO CRIMINAL FEDERAL)

Julgue o item a seguir, em relação às características de *software* malicioso.

Formatos comuns de arquivos, como, por exemplo, .docx ou .xlsx, são utilizados como vetor de infecção por *ransomware*, um tipo de *software* malicioso que encripta os dados do usuário e solicita resgate.

Certo ( ) Errado ( )

17 (CEBRASPE|2018|PF|ESCRIVÃO DA POLÍCIA FEDERAL)

Acerca de redes de computadores e segurança, julgue o item que segue.

Uma das partes de um vírus de computador é o mecanismo de infecção, que determina quando a carga útil do vírus será ativada no dispositivo infectado.

Certo ( ) Errado ( )

18 (FAU|2017|PARANÁ COMUNICAÇÃO|TÉCNICO EM TI)

Relacione as colunas e assinale a alternativa que apresenta a sequência correta de cima para baixo:

1ª COLUNA
1 - Phishing.
2 - Advance fee fraud.
3 - Hoax.

2ª COLUNA
( ) É um tipo de fraude na qual o golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.
( ) É uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.
( ) É um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.

A) 3, 2, 1.
B) 2, 1, 3.
C) 2, 3, 1.
D) 1, 2, 3.

19 (FCC|2017|TRE-SP|ANALISTA JUDICIÁRIO-ANÁLISE DE SISTEMAS)

O funcionário de uma empresa recebeu, pelo webmail, uma mensagem supostamente do banco no qual tem conta, informando que ele havia sido sorteado e ganhara um prêmio de um milhão de reais. Para resgatar o prêmio, o funcionário foi orientado a clicar em um link e digitar seus dados pessoais e bancários. Após seguir as orientações e enviar os dados digitados, percebeu que o endereço do banco era falso, mas muito semelhante ao endereço verdadeiro. O funcionário foi vítima de um tipo de fraude conhecida como

A) defacing.
B) worming.

C) phishing.
D) keylogging.
E) Joking.

---

20 (IDECAN|2019)
Com base nos conceitos de hardware e software, analise as afirmativas a seguir:

I. O Software Básico de Entrada e Saída (BIOS) é gravado na memória ROM. Assim, não é possível desinstalar o BIOS do computador, apenas atualizá-lo ou modificar as opções permitidas.

II. O touchpad de um notebook é considerado um dispositivo de entrada/saída sensível ao toque.

III. A menor unidade de medida do computador é o bit, que é representado por 0 (zeros) e 1 (uns); um conjunto de 8 (oito) bits equivale a um byte, que representa um caractere.

Assinale:
a) se somente a afirmativa I estiver correta.
b) se somente as afirmativas II e III estiverem corretas.
c) se somente a afirmativa III estiver correta.
d) se somente as afirmativas I e III estiverem corretas.
e) se somente a afirmativa II estiver correta.

---

21 (IBGP|2021)
"Considerada um tipo de memória mais rápida e cara para se armazenar um dado. Tipicamente utilizadas como um dispositivo de armazenamento temporário". O trecho apresentado define CORRETAMENTE a memória do tipo:
a) Cache.

b) EEPROM
c) Registradores.
d) RAM.

---

22 (IFSUL RIO-GRANDENSE|2019)
O termo memória, em informática, refere-se aos componentes que armazenam dados no computador. Dentre as memórias utilizadas, qual geralmente é utilizada para fornecer as instruções de inicialização do computador ao processador?
a) HD
b) RAM
c) ROM
d) SATA

---

23 (IDECAN|2019)
Em relação à capacidade de armazenamento de dados, o mercado disponibiliza hoje uma série de opções de mídias. Entre as mais conhecidas estão as mídias CD, DVD e Blu-Ray. A respeito desta última, assinale a alternativa que indica corretamente a máxima capacidade de uma mídia Blu-Ray do tipo duas camadas.
a) 700 Mb
b) 4.7 Gb
c) 50 Gb
d) 8.5 Gb
e) 850 Mb

---

24 (CETAP|2019)
5 TB (Terra bytes) equivalem a:
A) 5120 MB

B) 5000 GB.
C) 5000 MB.
D) 5120 GB.

25 (FCC|2019)
Foi especificada a aquisição de um microcomputador com uma porta USB-C. Essa porta apresenta como uma de suas características
a) a transferência de dados de até 1 Gbps, insuficiente para a transmissão de vídeos de padrão 4K para monitores externos ao computador.
b) compatibilidade mecânica com as portas USB 3.1.
c) permitir que a carga de dispositivos, como smartphones, seja mais lenta, pois esse padrão fornece menos potência do que portas USB 3.1.
d) possuir encaixe simétrico sem polarização, podendo ser encaixado de qualquer um de seus lados.
e) suportar cargas de até 10 W.

26 (FCC|2019)
Um técnico de manutenção de microcomputadores de uma empresa precisa substituir o seu disco rígido (HD) com padrão SATA e capacidade de armazenamento de 1 t B, que apresenta defeito. O computador faz o uso intenso desse disco e permanece em operação continuamente (24 horas, todos os dias). Esse técnico cogita substituir esse HD por uma unidade de estado sólido (SSD) com a mesma capacidade de armazenamento. Sobre essa substituição, é correto afirmar que o SSD
a) apresenta um consumo de energia superior ao do HD, podendo exigir a substituição da fonte de alimentação por uma de maior capacidade.
b) apresentará como desvantagem, em relação ao HD, uma vida útil inferior, pois o número de gravações em cada célula é limitado.
c) apresenta, atualmente, um custo para a capacidade requerida equivalente ao dos HDs convencionais.

d) exigirá cuidados especiais na instalação, como blindagem da unidade SSD, que é mais sensível a interferências magnéticas do que os HDs.
e) não pode ser utilizado, pois as unidades SSD possuem apenas conexão padrão IDE.

---

27 (CF-UFG|2019)
Os dispositivos para armazenamento de dados com tecnologia do tipo SSD (do inglês: Solid State Drive) estão substituindo gradativamente os tradicionais dispositivos com tecnologia do tipo magnética. Em comparação à tecnologia do tipo magnética, a SSD apresenta, de forma geral,
a) menor tempo de acesso e maior consumo de energia.
b) maior tempo de acesso e maior consumo de energia.
c) menor tempo de acesso e menor consumo de energia.
d) maior tempo de acesso e menor consumo de energia.

12 GABARITO

01 (AOCP|2020|PREFEITURA DE CARIACICA-ES|ASSISTENTE)

Resolução

WinRAR é um software que serve para compactar e descompactar dados, distribuído pela licença shareware. **GABARITO: LETRA B**.

02 (IBFC|2019|IDAM|ASSISTENTE TÉCNICO)

Resolução

Banco de dados ---> 2 software; memórias RAM e ROM ----> 1 hardware; placa-mãe ----> 1 hardware; editor de texto ---> 2 software.

Temos a sequência 1BC – 2AD. **GABARITO: LETRA D**

03 (FUMARC|2022|PC-MG|ANALISTA DA POLÍCIA CIVIL)

Resolução

Vamos lembrar do BIZU CAVERNOSO MATADOR: Executar (Liberdade 00) acesso para adaptar (Liberdade 01) fazer cópias (Liberdade 02) e melhorar o programa (Liberdade 03). Para tais ações é indispensável o acesso ao código fonte.

Logo, o item 3 é falso e todos os outros são verdadeiros e ficamos com a sequência de V, V, F, V. **GABARITO: LETRA D**

---

04 (AOCP|2018|ITEP-RN|AGENTE DE NECRÓPSIA)

Software é a parte lógica de um sistema computacional. Também pode ser chamado de programa, aplicação, aplicativo ou sistema. **GABARITO: LETRA C**

---

05 (FGV|2017|ALERJ|ESPECIALISTA LEGISLATIVO)

Resolução

A) ERRADO. Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para esse fim.

B) ERRADO. Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador.

C) CERTO. Conceito correto de BOT.

D) ERRADO. Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

E) ERRADO. Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

GABARITO: LETRA C.

---

06 (FCC|2016|PREFEITURA DE TERESINA-PI|AUDITOR FISCAL)

Resolução

A) **ERRADO.** Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

B) **ERRADO.** Rootkit é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

C) **ERRADO.** Keylogger é capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

D) **ERRADO.** Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

E) **CERTO.** Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

GABARITO: LETRA E.

---

07 (FCC|2017|TRE-SP|TÉCNICO JUDICIÁRIO)

Resolução

A) **ERRADO.** Trojan DoS é um tipo de trojan que instala ferramentas de negação de serviço e as utiliza para desferir ataques.

B) **ERRADO.** Screenlogger é similar ao keylogger, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o mouse e clicado, ou a região que circunda a posição onde o mouse é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.

C) **ERRADO.** Rootkit e um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.

D) ERRADO. Keylogger é um spyware capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um site específico de comercio eletrônico ou de Internet Banking.

F) CERTO. Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do worm, ou seja, é capaz de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados em computadores.

GABARITO: LETRA E.

---

08 (UFES|2019|UFES|JORNALISTA)

Resolução

A) ERRADO. Trojan é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

B) CERTO. Worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo, de computador para computador.

C) ERRADO. Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

D) ERRADO. Spyware é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros.

E) ERRADO. Backdoor é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim.

GABARITO: LETRA B.

---

09 (FUNCERN|2019|PREFEITURA DE APODI-RN|AGENTE COMUNITÁRIO)

Resolução

Worm são programas autorreplicantes, passando de um sistema para outro sem, necessariamente, utilizar um arquivo hospedeiro. Propaga-se automaticamente pelas redes, pode causar danos sem a ativação do usuário, diferentemente do vírus. **GABARITO: LETRA B.**

---

10 (FUNCERN|2019|PREFEITURA DE APODI-RN|AGENTE COMUNITÁRIO)

Resolução

A questão aborda conhecimentos sobre Malware, Spyware e Trojan. O malware Spyware é o responsável por espiar o usuário através das teclas pressionadas e pela visualização da tela do usuário, para conseguir acesso a senhas do usuário e aos seus hábitos de navegação. O malware Trojan se passa por um programa legítimo para enganar o usuário e softwares de antivírus, logo não avisa que executa um código malicioso. Os Malwares são os códigos maliciosos criados para prática ilegais, como sequestro de dados ou monitoramento da atividade do usuário. Desse modo, as alternativas II e III que estão corretas. **GABARITO: LETRA B.**

---

11 (CEBRASPE|2018|PF|ESCRIVÃO)

Resolução

Não é o mecanismo de infecção, mas sim o mecanismo de ativação. **ERRADO.**

---

12 (CEBRASPE|2013|PRF|POLICIAL RODOVIÁRIO FEDERAL)

Resolução

Os conceitos sobre vírus e worm foram invertidos. **ERRADO.**

---

13 (CEBRASPE|2022|PC-RO|AGENTE DE POLÍCIA)

Resolução

Citou o conceito de resgate ou extorsão, já sabemos que a questão está falando sobre Ransomware, que é um tipo de malware que sequestra os dados e pede resgate para devolver. **GABARITO: LETRA D.**

---

14 (CEBRASPE|2021|PC-DF|ESCRIVÃO DE POLÍCIA)

Resolução

Worm não necessita que o usuário o acione, pois, por ser um programa completo, é autônomo. **ERRADO.**

---

15 (CEBRASPE|2021|PRF|POLICIAL RODOVIÁRIO FEDERAL)

Resolução

Temos mistura de assuntos sobre vírus e ransomware. Lembre-se que *ransom* é resgate em inglês e essa palavra precisa estar na questão. Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos, enquanto Ransomware é um tipo de código malicioso que torna inacessíveis os dados

armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário. **ERRADO**

---

16 (CEBRASPE|2018|PF|PERITO CRIMINAL FEDERAL)

Resolução

Os arquivos .docx e .xlsx são do programa Office e podem ser infectados com vírus de macro. Na sequência esses arquivos podem ser vetores de infecção, se existirem chamadas para a execução de ransonware (software malicioso que encripta dados e solicita pagamento de resgate para a liberação). O ransomware explorará vulnerabilidades nesse dispositivo que não recebeu as devidas atualizações de segurança. **CERTO**

---

17 (CEBRASPE|2018|PF|ESCRIVÃO DA POLÍCIA FEDERAL)

Resolução

O evento ou condição que determina quando a carga útil é ativada ou entregue, também conhecido como *bomba lógica* é conhecido como mecanismo de ativação. **ERRADO.**

---

18 (FAU|2017|PARANÁ COMUNICAÇÃO|TÉCNICO EM TI)

Resolução

(2 – Advance fee fraud) É um tipo de fraude na qual o golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.
(3 – Hoax) É uma mensagem que possui conteúdo alarmante ou falso e que, geralmente, tem como remetente, ou aponta como autora, alguma instituição, empresa importante ou órgão governamental.
(1 – Phishing) É um tipo de fraude por meio da qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social.
GABARITO: LETRA C

---

19 (FCC|2017|TRE-SP|ANALISTA JUDICIÁRIO-ANÁLISE DE SISTEMAS)

Phishing é uma fraude virtual que chega por e-mail na tentativa de convencer o usuário de que ele precisa preencher algo com seus dados ou clicar em um determinado link para baixar um arquivo, que na verdade é um vírus e, se for acessado, roubará todos os dados digitados. **GABARITO: LETRA C**

---

20 (IDECAN|2019)

Resolução

I - BIOS (Basic Input/ Output System) é um *software* pré-gravado pelo fabricante da placa-mãe na memória ROM (permanente). Quando um computador é ligado, é a BIOS que inicializa a máquina, verificando as memórias, discos rígidos e dispositivos de entrada e saída. Somente depois do "OK" da BIOS que o sistema operacional do computador é inicializado. Não é possível desinstalar o BIOS do computador, apenas atualizá-lo ou modificar as opções permitidas.

II - O touchpad de um notebook é considerado um dispositivo de **entrada**.

III - 1 Byte = 8 bits

GABARITO LETRA D

---

21 (IBGP|2021)

Resolução
Registradores = + rápida, + cara, - menor capacidade de armazenamento. **GABARITO LETRA C**

---

22 (IFSUL RIO-GRANDENSE|2019)

Resolução
Memória ROM armazena as informações da BIOS, que é responsável pela inicialização dos sistemas. **GABARITO LETRA C**

---

23 (IDECAN|2019)

Resolução
Blu-ray: Camada única 25GB e Camada dupla: 50GB. **GABARITO LETRA C**

---

24 (CETAP|2019)

Resolução
GABARITO LETRA D

25 (FCC|2019)

Resolução

USB-C possui encaixe simétrico sem polarização, podendo ser encaixado de qualquer um de seus lados. **GABARITO LETRA D**

26 (FCC|2019)

Resolução

Questões misturando HDs e SSD caem em todas as bancas e é preciso saber as diferenças entre os dois. SSD é mais silencioso do que o HD, é menos sensível a balanços, consome menos energia, é mais leve, usa memória flash, consegue trabalhar em ambientes mais quentes, realiza leituras e gravações de forma mais rápida, não trava o computador e não perde seu conteúdo quando a alimentação elétrica é cortada. Porém, possuem uma vida útil um pouco menor, pois as células de armazenamento dos dados são "gastas" à medida que esses são gravados ou regravados. **GABARITO LETRA B**

27 (CF-UFG|2019)

Resolução

GABARITO LETRA C

PROFISSÃO POLICIAL

CONCURSEIRO QUE PRETENDE SER
POLICIAL NÃO FAZ RATEIO