

**PREFEITURA MUNICIPAL DE CABEDELLO
SECRETARIA D EDUCAÇÃO – SEDUC**

PREPARA CABEDELLO

NOÇÕES BÁSICAS DE INFORMÁTICA

Aula 3: 13/03/2020

Professora: *Heloiza Helena T. Holmes*

(FAURGS/2017) 1. Qual protocolo de acesso ao correio eletrônico possui comandos que permitem a um usuário, através de sua ferramenta de correio eletrônico (agente de usuário), criar remotamente uma estrutura de pastas e subpastas em seu servidor de correio eletrônico para organizar suas mensagens?

- A) IMAP
- B) HTTP
- C) POP3
- D) SMTP
- E) SNMP

(CESPE /2018) 2. Em relação aos sistemas de gestão da segurança da informação, julgue o item a seguir. Uma política de segurança da informação deve ser apoiada em tópicos específicos que incluam a classificação e o tratamento da informação, a proteção e a privacidade da informação de identificação pessoal.

() Certo () Errado

(FGV/2018) 3. Um vírus de computador é um software malicioso que pode causar sérios danos ao sistema infectado. Sobre vírus de computador, assinale a afirmativa correta.

- A) Adwares são vírus pacíficos utilizados para examinar as informações alheias.
- B) Cavalos de Tróia são geralmente aplicativos simples que escondem funcionalidades maliciosas e alteram o sistema para permitir ataques posteriores.
- C) Backdoors são vírus que restringem o acesso ao sistema infectado e cobra um resgate para que o acesso possa ser restabelecido.
- D) Spywares são vírus de engenharia social que manipulam pessoas para conseguir informações confidenciais.
- E) Worms são arquivos nocivos que infectam um programa e necessita deste programa hospedeiro para se alastrar.

(CESPE/2018) 4. 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

(UECE/2018) 5. Atente ao que se diz a seguir sobre ataques cibernéticos por meio de vírus em dispositivos de memória flash (pendrives).

I. O meio mais seguro de proteger um documento digital é compactando-o como arquivo ZIP, uma vez que esse formato de arquivo é imune a ataques por malware.

II. O pendrive é um dos dispositivos mais suscetíveis a infecção por vírus mediante o uso indiscriminado em computadores corrompidos e/ou não devidamente protegidos.

III. Efetuar a formatação rápida em um pendrive infectado não garante a remoção completa de vírus porquanto alguns programas maliciosos alojam-se na MBR.

É correto o que se afirma em:

- A) I e II apenas.
- B) I e III apenas.
- C) II e III apenas.
- D) I, II e III.

(IDIB/2018) 6. Considerando que arquivos de computadores podem ser infectados por vírus ou serem portadores deles, marque a alternativa com o tipo de arquivo que NÃO pode ser infectado ou propagado por eles.

- A) .doc
- B) .docx
- C) .txt
- D) .xls

(CESPE/2015) 7. 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 backup 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.

(COPERVE/2016) 8. Indique a opção que contém somente ferramentas importantes para a proteção de um computador.

- A) Firewall, bridge, antispymware
- B) Antivírus, bridge, protector
- C) Antivírus, firewall, antispymware
- D) Antivírus, bridge, firewall
- E) Antivírus, firewall, protector

(SÃO FRANCISCO/2019) 9. É o nome dado a um software, cuja função é detectar ou impedir a ação de um cracker, de um spammer, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema. O mecanismo de segurança da informação do texto acima é:

- A. Integridade.
- B. Mecanismos de certificação.
- C. Controles físicos.
- D. Mecanismos de criptografia.
- E. Honeypo

(SÃO FRANCISCO/2019) 10. É um programa para você navegar na internet, lançado em 2 de setembro de 2008 e hoje é o navegador mais utilizado no mundo. Uma das vantagens dele é a velocidade de processamento das páginas. Nele já vem integrado proteção contra phishing e malware. O conceito acima é do Navegador:

- A. Internet Explorer.
- B. Google Chrome.
- C. Mozilla Firefox.
- D. Safari.
- E. Microsoft Edge.

(SÃO FRANCISCO/2019) 11. Segurança da Informação está relacionada com proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. O mecanismo de segurança da informação de Controles lógicos são:

- A. Barreiras que impedem ou limitam o acesso à informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a alteração não autorizada por elemento mal intencionado.
- B. São barreiras que limitam o contato ou acesso direto a informação ou a infra-estrutura (que garante a existência da informação) que a suporta.
- C. Um conjunto de dados criptografados, associados a um documento do qual são função, garantindo a integridade do documento associado, mas não a sua confidencialidade.
- D. Medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.
- E. Usado em funções de "Hashing" ou de checagem, consistindo na adição.

(VARZEA/2019) 12. Segurança da Informação envolve um conjunto de medidas necessárias por garantir que a confidencialidade, integridade e disponibilidade das informações de uma organização ou indivíduo de forma a preservar esta informação de acordo com necessidades específicas. Os princípios básicos da Segurança da Informação são:

- A. Disponibilidade, Integridade, Confidencialidade.
- B. Disponibilidade, Formalidade, Confidencialidade.
- C. Disponibilidade, Integridade, Formalidade.
- D. Formalidade, Integridade, Confidencialidade.
- E. Disponibilidade, Integridade, Igualdade.

(VARZEA/2019)13. É um Programa que se aloca como um arquivo no computador da vítima. Ele tem o intuito de roubar informações como passwords, logins e quaisquer dados, sigilosos, ou não, mantidos no micro da vítima. O Programa é:

- A. Worn.
- B. Hoaxe.
- C. Trojan Horse.
- D. Epywares.
- E. Keyloggers e hajackers.

(VARZEA/2019) 14. O armazenamento em Nuvem ou Cloud Storage é um modelo de armazenamento de arquivos online que permite que você mantenha seus dados sincronizados com todos os seus dispositivos, tais como tablets, smartphones, notebooks e Desktops. O armazenamento cloud pode ser feito em, EXCETO:

- A. Nuvens públicas.
- B. Nuvens comunitárias.
- C. Nuvens híbridas.
- D. Nuvens Simples.
- E. Nuvens privadas.