

**2011**

**EXERCÍCIOS DE FIXAÇÃO  
SEGURANÇA DA INFORMAÇÃO**

**PROF. LÉO MATOS  
INFORMÁTICA PARA  
CONCURSOS**

**09/11/2011**

1) **(CESPE IPOJUCA 2010)** Entre os princípios básicos de segurança da informação, destacam-se a confidencialidade, a integridade e a disponibilidade.

2) **(CESPE IPOJUCA 2010)** Os programas de antivírus são indicados para fazer controle e eliminação de pragas virtuais. São exemplos típicos de pragas virtuais: spyware, worm, firewall e boot.

3) **(CESPE - CEHAP – PB 2009)** O firewall atua como barreira por meio de regras estabelecidas, mas não cumpre a função de controlar os acessos.

4) **(CESPE IPOJUCA 2010)** A criptografia é uma solução indicada para evitar que um arquivo seja decifrado, no caso de ele ser interceptado indevidamente, garantindo-se, assim, o sigilo das informações nele contidas.

5) **(CESPE - CEHAP – PB 2009)** Redes virtuais privadas são canais fechados utilizados, por exemplo, para tráfegar dados entre divisões de uma mesma empresa.

6) **(CESPE IPOJUCA 2010)** Phishing scam são e-mails não solicitados que tentam convencer o destinatário a acessar páginas fraudulentas na Internet com o objetivo de capturar informações, como senhas de contas bancárias e números de cartões de crédito.

7) **(CESPE – ANATEL 2009)** A disponibilidade e a integridade são itens que caracterizam a segurança da informação. A primeira representa a garantia de que usuários autorizados tenham acesso a informações e ativos associados quando necessário, e a segunda corresponde à garantia de que sistemas de informações sejam acessíveis apenas àqueles autorizados a acessá-los.

8) **(CESPE SEPLAG 2009)** Firewall e anti-spyware são nomes diferentes para software com os mesmos objetivos, ambos implementam o bloqueio a determinadas páginas web.

9) **(CESPE SEPLAG 2009)** A realização de cópias de segurança (backup) e armazenamento de arquivos em mídias e locais diferentes são procedimentos que contribuem para a disponibilidade da informação no ambiente computacional.

10) **(CESPE SEPLAG 2009)** A criptografia é um processo de segurança de dados que faz com que eles fiquem inacessíveis, sendo possível acessar o conteúdo apenas a partir de uma chave de criptografia equivalente.

11) **(CESPE SEPLAG 2009)** Hacker é um programa inteligente de computador que, após detectar falhas em um ambiente computacional, causa danos irreparáveis e a proliferação de outros programas maliciosos.

12) **(CESPE - CEHAP – PB 2009)** Programas de antivírus fazem varreduras no computador para procurar arquivos maliciosos disseminados pela transferência de arquivos.

13) **(CESPE - CEHAP – PB 2009)** Os programas de backup são usados para realizar cópias dos dados para que, em caso de defeito ou incidente, os dados possam ser recuperados posteriormente.

14) **(CESPE - CEHAP – PB 2009)** Assinatura digital é um conjunto de instruções matemáticas embasadas na criptografia que permite conferir autenticidade, confidencialidade e inviolabilidade a documentos digitais e transações comerciais efetuadas pela Internet.

15) **(CESPE - CEHAP – PB 2009)** Certificado digital é um arquivo eletrônico que contém dados referentes a uma pessoa ou instituição, que podem ser utilizados para comprovar sua identidade.

16) **(CESPE - CEHAP – PB 2009)** Secure Sockets Layer (SSL) constitui protocolo de segurança que prevê privacidade na comunicação realizada por meio da Internet.

17) **(CESPE SEPLAG 2009)** Apesar de firewalls serem ferramentas que podem ser utilizadas para a proteção de computadores contra ataques de hackers, eles não são suficientes para evitar a contaminação de computadores por vírus.

18) **(CESPE - BB 2008)** O Banco do Brasil (BB) disponibiliza ferramentas que proporcionam a você maior segurança para realizar suas operações financeiras pela Internet. Mas, para que essas ferramentas tenham real eficácia, você deve tomar alguns cuidados. Confira abaixo algumas regras para aumentar a sua segurança ao realizar transações financeiras pela Internet.

I CERTIFIQUE-SE de que está na área segura do portal BB, verifique a existência de um pequeno cadeado fechado na tela do programa de navegação. Note também que, no início do campo “endereço”, surgem as letras “https”.

II EVITE atalhos para acessar o sítio do BB, especialmente os obtidos em sítios de pesquisa. Digite sempre no campo “endereço”.

III EVITE abrir e-mail de origem desconhecida. EVITE também executar programas ou abrir arquivos anexados, sem verificá-los com antivírus atualizado. Eles podem conter vírus ou cavalos-de-troia, sem que os remetentes sequer saibam disso.

IV SOLICITE aos seus amigos que não enviem mensagens de e-mail de corrente (spam). Essas mensagens são muito utilizadas para propagar vírus e cavalo-de-troia.

V UTILIZE somente provedores com boa reputação no mercado e browsers e antivírus mais atualizados. A escolha de um provedor deve levar em conta também as políticas de segurança e a confiabilidade da empresa.

Considerando as informações apresentadas no texto acima e na janela do Internet Explorer 7 (IE7) ilustrada, julgue os itens abaixo, sabendo que a janela do IE7 está sendo executada em um computador PC e usada para um acesso à Internet.

a) Em um acesso à Internet, caso seja verificado o uso do protocolo https, está garantido que as informações trafegam pela rede com certificado digital tanto do sítio acessado quanto do usuário que acessa tal sítio.

b) Entre os tipos de arquivos anexados que justificam a regra III, encontram-se os arquivos que contêm documentos Word.

c) No texto apresentado, seria correto se, na regra II, fosse igualmente informado que se evitassem atalhos para acessar o sítio do BB presentes em e-mails enviados por desconhecidos.

d) Os termos spam e cavalo-de-tróia, mencionados na regra IV, são sinônimos.

19)(CESPE BB 2007) Para que um computador esteja efetivamente protegido contra a ação de vírus de computador e contra ataques de hackers, é suficiente que haja, no computador, um programa antivírus que tenha sido atualizado há, no máximo, três meses, sendo desnecessário, atualmente, o uso de firewall no combate a ataques de hackers.

20)(CESPE - CEF 2006) Uma mensagem assinada digitalmente permite que os seus destinatários verifiquem a identidade de quem a envia, e a criptografia protege a mensagem contra leitura não autorizada.

21)(CESPE 2010 – TRE BA) Firewall é um recurso utilizado para a segurança tanto de estações de trabalho como de servidores ou de toda uma rede de comunicação de dados. Esse recurso possibilita o bloqueio de acessos indevidos a partir de regras preestabelecidas.

22)(CESPE 2010 – BASA 2009) Uma rede do tipo VPN (virtual private network) é fundamental para evitar que vírus ou programas maliciosos entrem nos computadores de determinada empresa, já que esse tipo de rede é configurado de modo a bloquear qualquer arquivo que não seja reconhecido pelo firewall nela instalado.

23)(CESPE 2008 – Min. Saúde) Um dos pilares básicos da segurança da informação é a confidencialidade, que visa a proteger a informação contra modificação sem permissão.

24)(CESPE 2008 – Min. Saúde) O controle de acesso, que é uma das formas de assegurar que somente pessoas autorizadas acessem determinada informação, pode ser feita através da utilização de dados biométricos.

25)(CESPE IBRAM SEPLAG 2009) Cavalo de troia é um programa executável que objetiva realizar a função maliciosa de se autorreplicar, ou seja, criar cópias.

26)(CESPE IBRAM SEPLAG 2009) Uma das pragas virtuais que constantemente vêm incomodando usuários da Internet é a técnica de phishing scan, que consiste em induzir os usuários por meio de páginas falsas a fornecer senhas ou outros dados pessoais.

27)(CESPE 2010 - BRB) Os worms são pouco ofensivos, pois referem-se ao envio automático de mensagens indesejadas de correio eletrônico a um grande número de destinatários, que não as solicitaram ou que tiveram seus endereços eletrônicos copiados de um sítio pirata.

28)(CESPE 2010 - BRB) Confidencialidade, um dos princípios básicos da segurança da informação, tem como característica garantir que uma informação não seja alterada durante o seu trânsito entre o emissor e o destinatário.

29)(CESPE 2008 PRF) Se o sistema de nomes de domínio (DNS) de uma rede de computadores for corrompido por meio de técnica denominada DNS cache poisoning, fazendo que esse sistema interprete incorretamente a URL (uniform resource locator) de determinado sítio, esse sistema pode estar sendo vítima de pharming.

30)(CESPE 2008 PRF) Quando enviado na forma de correio eletrônico para uma quantidade considerável de destinatários, um hoax pode ser considerado um tipo de spam, em que o spammer cria e distribui histórias falsas, algumas delas denominadas lendas urbanas.

31)(CESPE - CEHAP – PB 2009) Programa que a partir da execução em determinado computador vítima passa a monitorar informações digitadas e visualizadas e, em seguida, envia e-mail para o seu criador encaminhando informações capturadas denomina-se:

- a) cavalo de tróia.
- b) spyware.
- c) phishing scan.
- d) hijackers.

32)(CESPE - CEF 2010) A assinatura digital facilita a identificação de uma comunicação, pois baseia-se em criptografia simétrica de uma única chave.

33)(CESPE - CEF 2010) Quando um usuário com assinatura digital envia e-mail para um destinatário, a mensagem será assinada por uma chave pública do destinatário, para garantir que seja aberta apenas pelo destinatário.

34)(CESPE - CEF 2010) O destinatário de uma mensagem assinada utiliza a chave pública do remetente para garantir que essa mensagem tenha sido enviada pelo próprio remetente.

35)(CESPE CEF 2010) Acerca de certificação e assinatura digital, assinale a opção correta.

- a) O uso da assinatura digital não garante que um arquivo tenha autenticidade no seu trâmite.
- b) A assinatura digital é uma ferramenta que garante o acesso a determinados ambientes eletrônicos por meio de biometria, com uso do dedo polegar.


c) A assinatura digital do remetente é utilizada para criptografar uma mensagem que será descriptografada pelo destinatário possuidor da respectiva chave pública.

d) A chave privada do remetente de uma mensagem eletrônica é utilizada para assinar a mensagem.

e) Para verificar se a mensagem foi de fato enviada por determinado indivíduo, o destinatário deve utilizar a chave privada do remetente.

36)(CESPE ANEEL 2010) Os vírus de macro que danificam documentos do Word podem ser eliminados com a instalação do aplicativo Visual Basic for Applications, do Windows.

37)(CESPE ANEEL 2010) Phishing é um tipo de ataque na Internet que tenta induzir, por meio de mensagens de e-mail ou sítios maliciosos, os usuários a informarem dados pessoais ou confidenciais.

38)(CESPE 2008 – BB) Por meio do botão , é possível que um usuário obtenha a denominada certificação digital, que, em aplicações bancárias, como a ilustrada na janela do IE7 permite conferir a autenticidade de um site.

39)(CESPE 2009 – UNIPAMPA) No Microsoft Word 2003 para se salvar o documento em edição em um arquivo com uma senha de segurança, é necessária a instalação de sistema de criptografia no computador em uso.

40)(CESPE 2009 – CEHAP PB) Spam é o envio de correio eletrônico solicitado pelo destinatário; é utilizado para distribuir propaganda, notícias e convites.

41)(CESPE 2009 – CEHAP PB) Os keyloggers são aplicativos destinados a capturar o que é digitado no teclado.

42)(CESPE 2009 – CEHAP PB) Os worms podem se propagar rapidamente para outros computadores por meio da Internet.

43)(CESPE 2009 – CEHAP PB) Com relação ao uso da criptografia na troca de informação pela Internet, julgue os seguintes itens.

I A criptografia de chave única (simétrica) utiliza uma mesma chave tanto para codificar quanto para decodificar mensagens.

II As criptografias de chave pública e chave privada (Assimétrica) utilizam duas chaves distintas, uma para codificar e outra para decodificar mensagens.

III É possível realizar transações seguras por meio da Internet, utilizando-se tanto métodos de criptografia de chave única (simétrica) quanto os de chave pública e chave privada (assimétrica), estabelecidas entre o navegador de um usuário e um sítio de Internet.

Assinale a opção correta.

a) Apenas os itens I e II estão certos.

b) Apenas os itens I e III estão certos.

c) Apenas os itens II e III estão certos.

d) Todos os itens estão certos.

44)(CESPE IBRAM SEPLAG 2009) O firewall é indicado para filtrar o acesso a determinado computador ou rede de computadores, por meio da atribuição de regras específicas que podem negar o acesso de usuários não autorizados, assim como de vírus e outras ameaças, ao ambiente computacional.

45)(CESPE 2010 AGU) Um arquivo criptografado fica protegido contra contaminação por vírus.

46)(CESPE 2010 AGU) A realização de um backup, ou cópia de segurança, consiste em copiar dados de um dispositivo de armazenamento para outro, de modo que esses dados possam ser restaurados em caso da perda dos dados originais provocada, por exemplo, por apagamento acidental ou corrupção de dados.

47)(CESPE 2010 AGU) A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, por isso, deve ser adequadamente protegida.

48)(CESPE 2010 CEF) Uma VPN é uma rede virtual privada utilizada como alternativa segura para usuários que não desejam utilizar a Internet.

49)(CESPE 2010 CEF) Uma mensagem digital somente pode ser assinada pelo destinatário da mesma.

50)(CESPE 2010 CEF) Para assinar uma mensagem digital, o remetente usa uma chave privada.

51)(CESPE 2010 CEF) Para assinar uma mensagem digital, o destinatário usa uma chave pública.

52)(CESPE 2010 CEF) Um certificado digital é pessoal, intransferível e não possui data de validade.

53)(CESPE 2010 UERN) A instalação de firewall só é permitida em um servidor de arquivos.

54)(CESPE 2010 UERN) Cavalo-de-troia é um programa que se instala a partir de um arquivo aparentemente inofensivo, sem conhecimento do usuário que o recebeu, e que pode oferecer acesso de outros usuários à máquina infectada.

55)(CESPE 2010 UERN) A disponibilidade da informação é a garantia de que a informação não será alterada durante o trânsito entre o emissor e o receptor, além da garantia de que ela estará disponível para uso nesse trânsito.

56)(CESPE 2010 UERN) A criptografia é uma das formas de garantir que a informação fique em uma área fora da rede, cujos dados somente são acessados, fisicamente, por pessoas Autorizadas.

57)(CESPE 2004 FUNCAB) Caso um servidor tenha instalado sistema antivírus, ele possui proteção contra ataques por vírus de computador e por hackers, constituindo, nos dias atuais, uma proteção infalível.

58)(CESPE 2009 SEPLAG/SEAPA/DF) Cavalos de troia (trojan) e worms são programas maliciosos, geralmente enviados por e-mail, que, instalados inadvertidamente pelo próprio usuário, causam impactos às vezes irreversíveis aos computadores e seus dados.

59)(CESPE 2006 HUB) O uso de uma ferramenta *firewall* permite que sejam definidas restrições na troca de informações entre uma rede doméstica de computadores e a Internet.

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

61)(CESPE 2010 BRB) O uso de HTTPS (HTTP seguro) permite que as informações enviadas e recebidas em uma conexão na Internet estejam protegidas por meio de certificados digitais.

62)(CESPE MMA 2008) Antivírus, worms, spywares e crackers são programas que ajudam a identificar e combater ataques a computadores que não estão protegidos por firewalls.

63)(CESPE EMBASA 2009) Os cookies, também denominados cavalos de troia, são arquivos indesejáveis que se instalam no computador durante um acesso à Internet e coletam informações armazenadas na máquina para posterior envio a destinatário não autorizado.

64)(CESPE 2010 SEDU ES) Vírus é um programa que pode se reproduzir anexando seu código a um outro programa, da mesma forma que os vírus biológicos se reproduzem.

65)(CESPE 2010 SEDU ES) Spywares são programas que agem na rede, checando pacotes de dados, na tentativa de encontrar informações confidenciais como senhas de acesso e nome de usuário.

66)(CESPE 2004 IEMA ES) Atualmente, muitos usuários fazem uso de programas antivírus e de sistemas denominados *firewalls*. Esses programas podem ser ferramentas úteis para diminuir a probabilidade de infecção dos computadores por vírus de computador ou de invasão do sistema pelos *hackers*.

67)(CESPE 2008 SERPRO) Um usuário pode fazer um acesso seguro à intranet do SERPRO usando a tecnologia VPN, que cria um túnel virtual com o computador do usuário, usando criptografia.

68)(CESPE 2005 ANS / MS) Ataques de um computador por cavalo-de-troia consistem em exemplos de

ataque de *phishing*, acarretando o tipo de roubo de informações ali descrito.

69. (FGV 2009 – SEFAZ/RJ) No Brasil, a NBR ISO17799 constitui um padrão de recomendações para práticas na gestão de Segurança da Informação. De acordo com o estabelecido nesse padrão, três termos assumem papel de importância capital: confidencialidade, integridade e disponibilidade. Nesse contexto, a confidencialidade tem por objetivo:

- a) salvaguardar a exatidão e a inteireza das informações e métodos de processamento.
- b) salvaguardar os dados gravados no backup por meio de software que utilize assinatura digital.
- c) permitir que os usuários tenham acesso aos arquivos de backup e aos métodos de criptografia empregados.
- d) permitir que os usuários autorizados tenham acesso às informações e aos ativos associados, quando necessário.
- e) garantir que as informações sejam acessíveis apenas para aqueles que estejam autorizados a acessá-las.

70. (ESAF 2007 – SEFAZ CE – Auditor Fiscal) Nos sistemas de Segurança da Informação, existe um método que \_\_\_\_\_ . Este método visa garantir a integridade da informação. Escolha a opção que preenche corretamente a lacuna acima.

- a) valida a autoria da mensagem
- b) verifica se uma mensagem em trânsito foi alterada
- c) verifica se uma mensagem em trânsito foi lida por pessoas não autorizadas
- d) cria um backup diferencial da mensagem a ser transmitida
- e) passa um antivírus na mensagem a ser transmitida

71. (ESAF 2006 – MTE Auditor Fiscal) A assinatura digital é o processo de manter mensagens e dados em segurança, permitindo e assegurando a confidencialidade. Quando utilizam apenas chaves privadas, as assinaturas digitais são usadas para fornecer serviços de integridade de dados, autenticação e não repúdio.

72. (CESPE ABIN 2010) No Internet Explorer, ao acessar uma página por meio do protocolo seguro HTTP, que utiliza o algoritmo de criptografia SSL (secure socket layer), o usuário é informado pelo navegador, mediante a exibição de um ícone contendo um cadeado, de que a conexão é segura.

73. (FCC 2009 – TJ PI – Analista Judiciário) Evitar a abertura de mensagens eletrônicas não solicitadas, provenientes de instituições bancárias ou empresas, que possam induzir o acesso a páginas fraudulentas na Internet, com vistas a roubar senhas e outras informações pessoais valiosas registradas no computador.

A recomendação acima é para evitar um tipo de fraude conhecida por

- a) chat.

- b) cracker.
- c) spam.
- d) hacker.
- e) phishing scam.

**74. (FCC 2009 – TJ PI – Téc. Judiciário)** Evite a Propagação de Hoaxes. A precaução mencionada acima tem por motivo a ciência de que frequentemente:

- a) ocorre a execução de programas antivírus não certificados.
- b) são executados arquivos anexados em sites maliciosos.
- c) existe falta de controle sobre arquivos lidos nos sites.
- d) ocorrem boatos espalhados para fins maliciosos ou para desinformação via e-mail.
- e) não são instalados programas antivírus

**75. (FGV 2006 – SEFAZ/MS)** No contexto da criptografia, um método emprega um tipo de chave, em que o emissor e o receptor fazem uso da mesma chave, usada tanto na codificação como na decodificação da informação. Esse método é conhecido por:

- a) assinatura digital.
- b) assinatura cifrada.
- c) chave simétrica.
- d) chave primária.
- e) chave assimétrica.

**76. (CESPE 2010 – TRT/RN)** No governo e nas empresas privadas, ter segurança da informação significa ter-se implementado uma série de soluções estritamente tecnológicas que garantem total proteção das informações, como um firewall robusto que filtre todo o tráfego de entrada e saída da rede, um bom software antivírus em todas as máquinas e, finalmente, senhas de acesso a qualquer sistema.

**77. (ESAF 2005 – Auditor da Receita)** Analise as seguintes afirmações relacionadas à segurança e uso da Internet:

I. Engenharia Social é um termo que designa a prática de obtenção de informações por intermédio da exploração de relações humanas de confiança, ou outros métodos que enganem usuários e administradores de rede.

II. *Port Scan* é a prática de varredura de um servidor ou dispositivo de rede para se obter todos os serviços TCP e UDP habilitados.

III. *Backdoor* são sistemas simuladores de servidores que se destinam a enganar um invasor, deixando-o pensar que está invadindo a rede de uma empresa.

IV. *Honey Pot* é um programa implantado secretamente em um computador com o objetivo de obter informações e dados armazenados, interferir com a operação ou obter controle total do sistema.

Indique a opção que contenha todas as afirmações verdadeiras.

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

**78. (CESGRANRIO 2009 – FUNASA Bibliotecário)** A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, aplicando-se tanto às informações corporativas quanto às pessoais. Abaixo, são apresentadas algumas propriedades básicas que, atualmente, orientam a análise, o planejamento e a implementação da segurança para um determinado grupo de informações que se deseja proteger. Relacione as propriedades apresentadas na coluna da esquerda com as respectivas descrições, na coluna da direita.

#### Propriedade

- I - Confidencialidade
- II - Disponibilidade
- III - Integridade

#### Descrição

(Q) Propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

(R) Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação.

Estão corretas as associações:

- a) I - Q; II - R
- b) I - Q; III - R
- c) I - R; II - Q
- d) II - Q; III - R
- e) II - R; III - Q

**79. (ESAF 2006 – MTE Auditor Fiscal)** Um algoritmo de criptografia simétrica requer que uma chave secreta seja usada na criptografia e uma chave pública diferente e complementar da secreta, utilizada no processo anterior, seja utilizada na decriptografia. Devido à sua baixa velocidade, a criptografia simétrica é usada quando o emissor de uma mensagem precisa criptografar pequenas quantidades de dados. A criptografia simétrica também é chamada criptografia de chave pública.

**80. (FCC 2006 – MPE PE - Analista Ministerial)** Permissão dada a um *Cracker* para controlar o micro infectado, por uma porta aberta inadvertidamente pelo usuário. Normalmente é um programa que vem embutido em um arquivo recebido por e-mail ou *baixado* da rede. Ao executar o arquivo, o usuário libera uma função que abre

uma porta para que o autor do programa passe a controlar o computador de modo completo ou restrito. Esta invasão, do tipo *backdoor*, por sua forma disfarçada de entrega, é frequentemente associada a um tipo de *malware* conhecido por

- a) *trojan horse*.
- b) *hoax*.
- c) *stealth*.
- d) *boot*.
- e) *adware*.

**81. (MOVENS 2009 – ADEPARÁ )** Os antivírus são programas que procuram detectar e eliminar os vírus de computador. Acerca dos conceitos de vírus de computador, prevenção e tratamento, assinale a opção correta.

(A) O firewall é um recurso do antivírus que permite a detecção de programas maliciosos em arquivos anexados aos e-mails.

(B) Vírus de Macro são vírus que afetam os arquivos de inicialização dos discos. São tipicamente encontrados em arquivos de registros do Windows ou em arquivos de inicialização do sistema.

(C) Cavalos-de-tróia ou trojans são malwares, que basicamente, permitem acesso remoto ao computador após a infecção. Os cavalos-de-tróia podem ter outras funcionalidades, como captura de dados do usuário e execução de funções não autorizadas no sistema.

(D) A abertura de arquivos executáveis de origem desconhecida, que tenham sido recebidos em mensagens de correio eletrônico, não apresenta risco de contaminação do computador por vírus.

**82. (FCC 2006 – INSS Perito Médico)** Dadas as seguintes declarações:

- I. Programas que se replicam e se espalham de um computador a outro, atacando outros programas, áreas ou arquivos em disco.
- II. Programas que se propagam em uma rede sem necessariamente modificar programas nas máquinas de destino.
- III. Programas que parecem ter uma função inofensiva, porém, têm outras funções sub-reptícias.

Os itens I, II e III correspondem, respectivamente, a ameaças programadas do tipo:

- a) cavalo de tróia, vírus e *worms*.
- b) *worms*, vírus e cavalo de tróia.
- c) *worms*, cavalo de tróia e vírus.
- d) vírus, *worms* e cavalo de tróia
- e) vírus, cavalo de tróia e *worms*.

**83. (FESAG 2006 – TRE ES)** Um dos recursos para o acesso seguro a rede de sua organização através de redes públicas é utilizar conexões do tipo:

- a) direta.
- b) rede local.
- c) rede virtual privada (VPN).
- d) dial-up.

**84. (ESAF 2004 – MPU Técnico Jud.)** O Denial of Service (DoS) é um ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Há muitas variantes, como os ataques distribuídos de negação de serviço (DDoS) que paralisam vários sites ao mesmo tempo.

**85. (CESPE 2011 – TRT/RN)** A disponibilidade é um conceito muito importante na segurança da informação, e refere-se à garantia de que a informação em um ambiente eletrônico ou físico deve estar ao dispor de seus usuários autorizados, no momento em que eles precisem fazer uso dela.

**86. (CESPE 2011 – TRE/ES)** Para se abrirem arquivos anexados a mensagens recebidas por correio eletrônico, sem correr o risco de contaminar o computador em uso, é necessário habilitar o firewall do Windows.

**87. (CESPE 2011 – PGR/RR)** Caso se deseje mais segurança do que a convencional, o uso do HTTPS no servidor webmail é indicado para conferir confidencialidade aos dados trafegados.

**88. (CESPE DETRAN/ES)** Um *firewall*, em um computador, é um *software* que, corretamente configurado, verifica as informações provenientes da Internet e evita que o computador seja infectado com vírus transmitidos por meio de *email*.

**89. (CESGRANRIO 2009 – DECEA)** Considere o contexto no qual não existe falha de segurança na proteção da(s) chave(s) privada(s) e pública(s). Dentro deste contexto, se Marcelo escreve um e-mail para José e o assina digitalmente, José pode ter certeza de que

- a) Marcelo foi quem enviou a mensagem para José.
- b) receberá a mensagem, mesmo se seu servidor de email deixar de existir.
- c) receberá a mensagem, mesmo que Marcelo não consiga enviá-la.
- d) somente quem possui a chave privada de Marcelo pode ter acesso à mensagem.
- e) somente ele próprio pode ter acesso à mensagem que Marcelo enviou.



**90. (FCC 2010 – TCE/SP)** Mensagem não solicitada e mascarada sob comunicação de alguma instituição conhecida e que pode induzir o internauta ao acesso a páginas fraudulentas, projetadas para o furto de dados pessoais ou financeiros do usuário. Trata-se especificamente de:

- a) keylogger.
- b) scanning.
- c) botnet.
- d) phishing.
- e) rootkit.

**91. (ESAF 2006 – ENAP)** Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que Autenticação é o processo

- a) que rastreia as atividades dos usuários ao gravar tipos selecionados de eventos no *log* de segurança de um servidor ou de uma estação de trabalho.
- b) iniciado para impedir que usuários acessem um serviço de rede, como um servidor Web ou um servidor de arquivos.
- c) que disponibiliza a lista de programas do menu Iniciar para todos os usuários do Windows que fazem *logon* no computador.
- d) de transmissão de mensagens que permite que um aplicativo distribuído possa acessar serviços disponíveis em vários computadores em uma rede.
- e) utilizado para verificar se uma entidade ou objeto é quem ou o que afirma ser.

**92. (ESAF 2005 Auditor Fiscal da Receita)** O *SYN flooding* é um ataque do tipo DoS, que consiste em explorar mecanismos de conexões TCP, prejudicando as conexões de usuários legítimos.

**93. (FCC BB 2006 – Escriturário)** Os arquivos de dados de editores de texto e de planilhas eletrônicas podem ser contaminados normalmente por programas do tipo vírus

- (A) parasitas.
- (B) camuflados.
- (C) polimórficos.
- (D) de *boot*.
- (E) de macro.

**94. (FUNIVERSA PCDF 2009)** No que se refere à segurança da informação, julgue os itens que se seguem e assinale a alternativa correta.

I *Spam* é o termo usado para se referir aos *e-mails* solicitados, que geralmente são enviados para um grande número de pessoas.

II Vírus é um programa ou parte de um programa de computador que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

III Criptografia é uma ferramenta que pode ser usada para manter informações confidenciais e garantir sua integridade e autenticidade. Os métodos criptográficos podem ser subdivididos em três grandes categorias, de acordo com o tipo de chave utilizada: criptografia de chave única, criptografia de chave pública e criptografia de chave privada.

IV Antivírus são programas projetados para detectar e eliminar vírus de computador. Existem no mercado excelentes antivírus: o que dificulta o acesso a estes programas é o fato de que, hoje, todos são pagos.

- (A) Todos os itens estão errados.
- (B) Há apenas um item certo.
- (C) Há apenas dois itens certos.
- (D) Há apenas três itens certos.
- (E) Todos os itens estão certos.

**95. (ESAF 2006 – Ministério do Trabalho)** O *Ping da Morte* (*Ping of Death*) é um recurso utilizado na Internet por pessoas mal intencionadas, que consiste:

- a. no envio de pacotes TCP/IP de tamanho inválidos para servidores, levando-os ao travamento ou ao impedimento de trabalho.
- b. na impossibilidade de identificação do número de IP de máquina conectada à rede. Desta forma, muitos dos serviços de segurança disponíveis deixam de funcionar, incluindo os "rastreamentos" que permitem a identificação de segurança das fontes de origem de ataques.
- c. em instalar em um computador conectado a uma rede um programa cliente que permite a um programa servidor utilizar esta máquina sem restrições.
- d. no mecanismo de "abertura" de portas e acha-se atualmente incorporado em diversos ataques de vírus.
- e. na captura e alteração de "pacotes" TCP/IP transmitidos pelas redes.

**96. (CESPE 2008 – Min. Saúde)** O controle de acesso, que é uma das formas de assegurar que somente pessoas autorizadas acessem determinada informação, pode ser feita através da utilização de dados biométricos.

**97. (CESPE 2011 – IFB)** Os ataques de negação de serviços são feitos por meio de abuso da ingenuidade ou confiança do usuário.

**98. (CESPE 2011 – FUB)** Se o acesso à Internet ocorrer por meio de um servidor proxy, é possível que seja necessária uma autenticação por parte do usuário, que deve fornecer nome e senha de acesso.

**99. (CESPE 2010 BRB)** Um worm se aloja no servidor de e-mail e infecta automaticamente o computador do usuário



sempre que este realiza uma conexão ao serviço de correio eletrônico.

**100. (CESPE 2010 BRB)** Firewall, mecanismo que auxilia na proteção de um computador, permite ou impede que pacotes IP, TCP e UDP possam entrar ou sair da interface de rede do computador

**101. (CESPE 2011 TRT 21ª)** A disponibilidade é um conceito muito importante na segurança da informação, e refere-se à garantia de que a informação em um ambiente eletrônico ou físico deve estar ao dispor de seus usuários autorizados, no momento em que eles precisem fazer uso dela.

**102. (CESPE 2011 TRT 21ª)** O acesso a um endereço de um sítio na Internet que se inicie com https é feito por meio de uma conexão segura. Nesse contexto, a informação trafega em um canal seguro, usando uma rede cuja segurança não é garantida

**103. (FCC 2011 TER/AP)** Em relação aos tipos de backup, é correto afirmar que o Backup Incremental

- a) é uma cópia extraída diariamente, contendo todos os incrementos que ocorreram no sistema operacional.
- b) é uma cópia de segurança que incrementa todas as inclusões e alterações de programas e configurações.
- c) é a cópia de segurança na qual são copiados somente os arquivos alterados depois do último backup.
- d) copia todos os arquivos do sistema operacional, assinalando aqueles que foram alterados.
- e) é programado para ser executado sempre que houver alteração nos dados armazenados.

**104. (FGV 2011 SEFAZ RJ AUDITOR FISCAL)** Segurança da Informação é um tema que se reveste atualmente de alta importância para os negócios. Um de seus aspectos mais relevantes está associado à capacidade do sistema de permitir que alguns usuários acessem determinadas informações e paralelamente impede que outros, não autorizados, a vejam. O aspecto abordado é denominado

- a) Integridade.
- b) Privacidade.
- c) Confidencialidade.
- d) Vulnerabilidade.
- e) Disponibilidade.

**105. (CESPE CNPQ 2011)** A fim de se preservar a integridade, a confidencialidade e a autenticidade das informações corporativas, é necessário que os empregados e os contratados do órgão sejam treinados, de forma que se conscientizem da importância da segurança da informação e se familiarizem com os procedimentos adequados na ocorrência de incidentes de segurança.

**106. (CESPE TJ/SE 2011)** Tecnologias como a biometria por meio do reconhecimento de digitais de dedos das mãos ou o reconhecimento da íris ocular são exemplos de aplicações que permitem exclusivamente garantir a integridade de informações.

**107. (CESPE TJ/SE 2011)** O conceito de confidencialidade refere-se a disponibilizar informações em ambientes digitais apenas a pessoas para as quais elas foram destinadas, garantindo-se, assim, o sigilo da comunicação ou a exclusividade de sua divulgação apenas aos usuários autorizados.

**108. (FCC 2011 BANCO DO BRASIL)** Ativado quando o disco rígido é ligado e o sistema operacional é carregado; é um dos primeiros tipos de vírus conhecido e que infecta a partição de inicialização do sistema operacional. Trata-se de

- a) vírus de boot.
- b) cavalo de Troia.
- c) verme.
- d) vírus de macro.
- e) spam.

**109. (CONSULPLAN 2011 MUNICÍPIO DE LONDRINA/PR)** “Segurança da informação é a proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou organização. O conceito de Segurança da Informática ou Segurança de Computadores está intimamente relacionado ao de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si.” Os principais atributos que orientam a análise, o planejamento e a implementação da segurança para um grupo de informações que se deseja proteger são:

- A) Confidencialidade, Integridade, Disponibilidade.
- B) Confidencialidade, Persistência, Disponibilidade.
- C) Consistência, Integridade, Disponibilidade.
- D) Confidencialidade, Integridade, Durabilidade.
- E) Confiabilidade, Integridade, Disponibilidade.

**110. (FCC 2011 TRT 4ª)** É uma forma de fraude eletrônica, caracterizada por tentativas de roubo de identidade. Ocorre de várias maneiras, principalmente por e-mail, mensagem instantânea, SMS, dentre outros, e, geralmente, começa com uma mensagem de e-mail semelhante a um aviso oficial de uma fonte confiável, como um banco, uma empresa de cartão de crédito ou um site de comércio eletrônico. Trata-se de

- a) Hijackers.
- b) Phishing.
- c) Trojans.
- d) Wabbit.
- e) Exploits.

**111. (CESGRANRIO 2011 - PETROBRAS)** O objetivo do firewall é:

- a) possibilitar a conexão com a Internet.
- b) configurar uma rede privada.
- c) visualizar diversos tipos de arquivos.
- d) permitir a edição de imagens.
- e) realizar a segurança de redes privadas.

**112. (CESGRANRIO 2010 - BACEN)** O Certificado Digital é um arquivo eletrônico que contém os dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Dentre as principais informações encontradas em um Certificado Digital, referentes ao usuário, citam-se:

- (A) códigos de acesso ao sistema.
- (B) informações biométricas para leitura ótica.
- (C) número de série e período de validade do certificado.
- (D) dados de identificação pessoal: RG, CPF ou CNPJ.
- (E) dados de localização: endereço e Cep.

**113. (FCC 2011 TER/TO)** Arquivos de dados produzidos por suite de aplicativos para escritório, por ex. Microsoft Office, costumam ser alvo predileto de contaminação por:

- a) trojans.
- b) worms.
- c) hijackers
- d) vírus de boot.
- e) vírus de macro.

**114. (CESPE 2011 - PREVIC)** Entre os atributos de segurança da informação, incluem-se a confidencialidade, a integridade, a disponibilidade e a autenticidade. A integridade consiste na propriedade que limita o acesso à informação somente às pessoas ou entidades autorizadas pelo proprietário da informação.

**115. (CESGRANRIO 2011 – SEPLAG/BA)** Criar cópias de si mesmo de um computador para outro de forma automática, com capacidade de se replicar em grande volume, é característica de uma praga eletrônica Denominada:

- (A) Trojan Horse
- (B) Opteron
- (C) Freeware
- (D) Shareware
- (E) Worm

**116. (FUNIVERSA 2010 – Sesi)** Assinale a alternativa que apresenta um endereço de acesso à Internet (URL) seguro.

- (A) <http://www.homebanking.com.br>
- (B) <tls://prouni.mec.gov.br>
- (C) <https://prouni.mec.gov.br>

- (D) <ftp://www.mec.gov.br>
- (E) <ssl://www.homebanking.com.br>

**117. (FUNIVERSA 2006 APEX BRASIL)** Atualmente, a segurança da informação na Internet pode ser auxiliada pelo recurso de certificação digital. A que conceito refere-se a seguinte definição? "A garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital."

- a) Confidencialidade.
- b) Integridade.
- c) Autenticação.
- d) Não repúdio.
- e) Autoria.

**118. (FCC 2011 TRF 1ª REGIÃO TÉCNICO JUDICIÁRIO)** O golpe de Pharming é um ataque que consiste em

- (A) corromper o DNS, fazendo com que a URL de um site passe a apontar para um servidor diferente do original.
- (B) alterar as tabelas de roteamento para que o roteador desvie os pacotes para um falso servidor.
- (C) impedir que o servidor DNS converta o endereço em um número IP e assim congestionar a rede.
- (D) instalar um programa cliente no servidor de destino para capturar senhas e endereços de sites.
- (E) travar um servidor de páginas através do envio de pacotes IP inválidos.

**119. (CESPE 2012 AL/CE)** Worms são programas que se espalham em uma rede, criam cópias funcionais de si mesmo e infectam outros computadores.

**120. (CESPE 2012 AL/CE)** O adware, tipo de firewall que implementa segurança de acesso às redes de computadores que fazem parte da Internet, evita que essas redes sejam invadidas indevidamente.

Faça todas as questões e depois confira o gabarito verificando qual foi o seu erro! Bom estudo! Abraços

Professor **Léo Matos**

#### **GABARITO**

1) C	2) E
3) E	4) C
5) C	6) C
7) E	8) E
9) C	10) C
11) E	12) C

13) C	14) E
15) C	16) C
17) C	18) E   C   C   E
19) E	20) C
21) C	22) E
23) E	24) C
25) E	26) C
27) E	28) E
29) C	30) C
31) B	32) E
33) E	34) C
35) D	36) E
37) C	38) C
39) E	40) E
41) C	42) C
43) D	44) C
45) E	46) C
47) C	48) E
49) E	50) C
51) E	52) E
53) E	54) C
55) E	56) E
57) E	58) C
59) C	60) E
61) C	62) E
63) E	64) C
65) C	66) C
67) C	68) E
69) E	70) B
71) E	72) E
73) E	74) D
75) C	76) E
77) A	78) B
79) E	80) A
81) C	82) D
83) C	84) C
85) C	86) E
87) C	88) E
89) A	90) D
91) E	92) C
93) E	94) B
95) A	96) C
97) E	98) C
99) E	100) C
101) C	102) C
103) C	104) C
105) C	106) E
107) C	108) A
109) A	110) B
111) E	112) C
113) E	114) E
115) E	116) C
117) D	118) A
119) C	120)