AULA 06 - INFORMÁTICA - EXERCÍCIOS
PROFESSOR LUIS

85. (CESGRANRIO – 2016) Sistemas operacionais, como o Win- dows, trazem, em suas versões atuais, um programa no qual um dos objetivos é ajudar a impedir a invasão por harckers ou softwares mal-intencionados aos computadores dos usuários, podendo pôr em risco as informações neles contidas.
Esse tipo de programa consta, normalmente, nas políticas de proteção e segurança das empresas e é conhecido como
a) administrador
b) decodificador
c) firewall
d) host
e) script

86. (CESGRANRIO – 2011) Um computador recebe um progra- ma mal-intencionado, que pode prejudicar seus arquivos e sua segurança.
Qual a ferramenta adequada para descobrir e remover esse programa?
a) spam
b) firewall
c) adware
d) antivírus
e) spyware

87. (CESGRANRIO – 2011) Dentre as ferramentas que auxiliam a proteção de um computador, inclui-se o
a) HTTP.
b) driver do HD.
c) FTP.
d) RSS.
e) antivirus.

88. (CESGRANRIO – 2010) Entre os grandes problemas da atua- lidade relacionados à confidencialidade das informações um refere-se à prevenção da invasão dos computadores por pes- soas malintencionadas. A principal forma de evitar danos cau- sados por softwares espiões dos quais essas pessoas se utilizam para alcançarem seus objetivos é

a) utilizar apenas webmail para leitura das correspondências eletrônicas.
b) efetuar rotinas de backup semanais no disco rígido do computador.
c) compartilhar os principais documentos com pessoas idôneas.
d) possuir software antivírus e mantê-lo sempre atualizado.
e) navegar na internet sempre sob um pseudônimo.

89. (CESGRANRIO – 2010) Desde o surgimento das primeiras redes de computadores e, principalmente, após a difusão do uso da Internet para o desenvolvimento dos negócios corpora- tivos, a segurança da informação tornou-se uma preocupação constante dos gestores de tecnologia da informação. Dentre as diversas políticas de segurança implementadas, a manutenção de softwares antivírus atualizados é de grande importância, porque
a) permite o acesso às informações necessárias, mas evita instalações mal-intencionadas.
b) mapeia todo o tráfego de rede, permitindo o gerenciamento dos acessos e conteúdos.
c) fiscaliza o tráfego dos usuários na rede, permitindo sanções administrativas.
d) coordena o envio e recebimento de mensagens, otimizando os recursos de hardware.
e) monitora o conteúdo das informações, bloqueando o uso impróprio de dados confidenciais.

90. (CESGRANRIO – 2016) O responsável pela segurança da informação de uma empresa ministrou uma série de pales- tras sobre as diversas ameaças ao ambiente computacional da empresa, ressaltando pontos importantes a serem observados pelos usuários. Um desses usuários, revendo suas anotações, percebeu que se havia enganado no registro de um procedi- mento ou o instrutor tinha-se equivocado ao enunciá-lo. Qual é a suposta recomendação que está equivocada?
a) Conexões para pagamento de contas via Internet Banking devem ser finalizadas antes do fechamento do browser utilizado.
b) Documentos com informações muito sensíveis sobre os negócios da empresa, criados e editados no Microsoft Word 2010, devem, preferencialmente, ser criptografados antes de arquivados.
c) A infecção de um computador por vírus através de abertura de arquivos suspeitos anexados a e-mails é evitada com a instalação prévia de versões atualizadas de antivírus.
d) A autoexecução de mídias removíveis deve ser desabilitada.
e) O uso da navegação anônima é uma forma de proteção da privacidade quando a internet é acessada em computadores de terceiros.

93. (CESGRANRIO – 2012) As informações em mídia digital de empresas que, entre outras atividades, possuem acesso à inter- net em suas intranets, são alvos constantes de ataques por meio de pragas eletrônicas.
Dentre as atividades que podem ser agentes facilitadores des- ses ataques, inclui-se a(o)
a) abertura de anexos de e-mails enviados por desconhecidos
b) execução programada de softwares de antivírus
c) limitação de acesso a sites fornecedores de downloads
d) bloqueio de programas P2P(peer-to-peer)
e) uso de proxy servers

94. (CESGRANRIO – 2010) Os mecanismos implementados por software, usados para restringir o acesso e o uso do sistema operacional, de redes, de programas utilitários e aplicativos, constituem um processo de segurança
a) digital.
b) física.
c) lógica.
d) restrita.
e) simples.

96. (CESGRANRIO – 2010) Com o desenvolvimento de novas tecnologias, tornaram-se possíveis de serem executadas com segurança na Internet transações como movimentações ban- cárias e compras de diversos produtos. A segurança na Internet é auditada por diversas empresas especializadas, e um usuário comum pode identificar se está navegando em um site seguro, verificando se está
a) presente na página exibida pelo navegador o ícone de um cadeado.
b) presente no final do endereço do site, no navegador, a extensão ".seg".
c) criptografada no formulário de navegação a senha que foi digitada para acesso.
d) selecionada no navegador, em suas configurações de segu- rança, a opção navegar off-line.
e) instalado no equipamento de navegação fornecido pelo fabricante um pacote de segurança.

97. (CESGRANRIO – 2010) A maior parte dos problemas que ocorrem em relação à segurança da informação é gerada por pessoas que tentam obter algum tipo de benefício ou causar prejuízos às organizações. Para garantir a segurança adequa- da em uma organização, as seguintes medidas de segurança devem ser aplicadas, EXCETO
a) avaliar os riscos à segurança.
b) implementar controles de segurança.
c) rever a política de segurança de forma constante.
d) manter uma tabela atualizada com todas as senhas da organização.
e) monitorar e manter a eficácia dos controles de segurança

98. (CESGRANRIO – 2018) Uma empresa tem uma intranet forte- mente protegida, porém deseja dar aos seus funcionários uma forma de estabelecer uma conexão segura do computador de sua casa à intranet da empresa, estando ligado na internet. Isso dará ao funcionário a impressão de que está dentro da intranet da própria empresa
Para isso, deve estabelecer um(a.)
a) Captcha
b) DNS
c) Firewall
d) LAN
e) VPN

99. (CESGRANRIO – 2016) Para que um usuário acesse a intranet, implantada corretamente, de uma universidade, a partir de seu computador pessoal em sua residência, o setor de TI da universidade deve possibilitar o acesso via
a) DHCP
b) LAN
c) VPN
d) FTP
e) HTTP

73. (CESGRANRIO – 2011) Um adware, em sua concepção origi- nal, é um
a) software projetado para ajudar a exibir propagandas e/ou sites não desejados no computador.
b) software projetado para ajudar o browser a inibir pop--ups no computador.
c) programa destrutivo que se duplica sozinho.
d) programa utilizado para capturar senhas.
e) vírus que se instala no computador para apagar arquivos do disco rígido.

70. (CESGRANRIO – 2013) Há características importantes que distinguem os códigos maliciosos denominados worm daque- les denominados trojan.
Uma dessas características é a
a) autorreplicação automática pela rede
b) instalação por execução de arquivo infectado
c) contaminação através de redes sociais
d) contaminação por compartilhamento de arquivos
e) instalação por execução explícita do código malicioso

9. (CESGRANRIO – 2014) Um dos recursos presentes no Windo- ws, desde a versão xp, é o Windows Firewall.
Esse recurso tem o objetivo de
a) aumentar a segurança do sistema.
b) melhorar o desempenho do sistema.
c) tornar o sistema mais acessível e prático.
d) melhorar a comunicação dos usuários com a Microsoft.
e) facilitar o uso do sistema por pessoas com necessidades especiais