GRAN CONCURSOS

INFORMÁTICA

Segurança da Informação – Proteção

Livro Eletrônico

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerente de Produção Digital: Bárbara Guerra

CÓDIGO:
230811469289

MAURÍCIO FRANCESCHINI

Servidor público do TJDFT desde 1999, tendo atuado como supervisor de informática por 8 anos no órgão. Graduado em Ciência da Computação pela UnB, pós-graduado em Governança de TI pela UCB e mestrando pela UnB. É professor de Informática para concursos desde 2008 e ministra também algumas disciplinas da área de TI, com experiência em várias instituições renomadas.

GRAN CONCURSOS

SUMÁRIO

APRESENTAÇÃO

Seja bem-vindo(a) à nossa aula sobre Segurança da Informação – Mecanismos de Proteção Digital.

Estamos imersos no universo digital e está cada vez mais comum vivermos experiências tecnológicas. Diariamente, enfrentamos o desafio de gerenciar nossas informações de maneira a protegê-las e mantê-las em segurança. Nesse sentido, os mecanismos de proteção digital tornam-se essenciais à segurança da informação.

Nesta aula, abordaremos um tópico primordial dentro da Segurança da Informação: Mecanismos de Proteção Digital.

As bancas examinadoras gostam de explorar esse conteúdo nas questões de concursos; por isso, tentarei explicar de maneira leve e prática para que você gabarite todas as questões!

Estarei aqui do outro lado, junto com você nessa caminhada. Ao final desta aula, você estará preparado(a) para resolver questões de concursos sobre esse tema.

Desejo uma excelente aula!

SEGURANÇA DA INFORMAÇÃO – PROTEÇÃO

1. INTRODUÇÃO

A internet desempenha um papel significativo na vida de muitas pessoas ao redor do mundo. Ela nos permite estabelecer conexões com indivíduos em qualquer lugar do planeta, e isso é apenas uma das várias vantagens que oferece. Através da internet, temos acesso a uma variedade de benefícios, como serviços bancários, notícias, oportunidades de aprendizado sobre diferentes culturas e idiomas, participação em cursos, palestras e aulas, a possibilidade de obter um diploma universitário, buscar pessoas desaparecidas, realizar compras de todos os tipos, até mesmo em outros países, além de utilizá-la como ferramenta de entretenimento ou trabalho e agendar serviços governamentais. Em suma, a internet oferece inúmeras possibilidades para os usuários.

É evidente que o uso da internet está em constante crescimento. Na sociedade moderna, a internet tornou-se uma necessidade básica do dia a dia, o que resulta em uma maior produção de dados, no aumento da quantidade de informações inseridas na rede e em uma maior preocupação sobre como essas informações serão protegidas e armazenadas.

A conexão global proporcionada pela internet traz consigo benefícios, mas também expõe os usuários a conteúdos inapropriados, ofensivos e constrangedores que não foram solicitados. Além disso, há a ameaça de interação com outros usuários mal-intencionados que utilizam a internet para cometer diversos crimes.

Neste estudo, abordaremos os mecanismos de proteção digital e como esse tema é tratado em questões de concursos.

2. MECANISMOS DE PROTEÇÃO DIGITAL

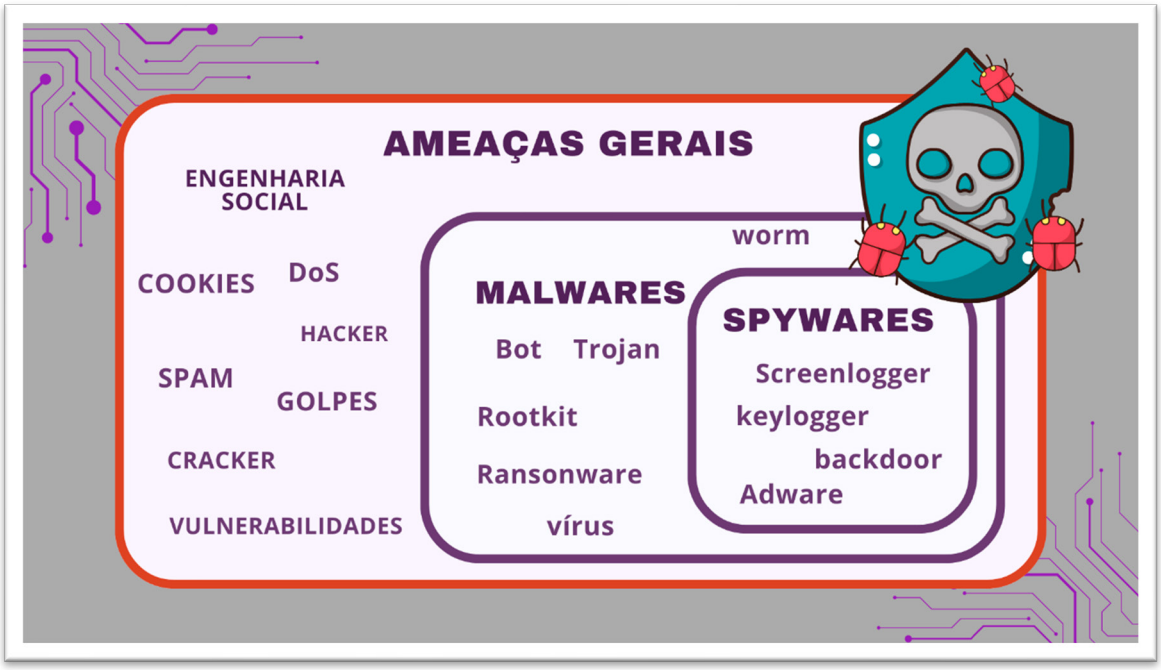
As ferramentas de proteção servem para evitar ou remediar os danos causados pelas ameaças digitais. Se o tópico de ameaças estiver descrito em seu edital, minha sugestão é que estude a aula de ameaças antes de estudar as ferramentas de proteção.

Mas, de qualquer forma, antes de entrarmos nas proteções propriamente ditas, quero diferenciar as ameaças das proteções, pois, em prova, é muito comum o examinador lançar questões que confundam ambas.

Ameaças x Proteções

Ameaças digitais são qualquer situação ou procedimento que coloca em risco a segurança e a integridade dos dados situados em algum meio digital.

Veja abaixo um mapa mental com alguns exemplos de ameaças digitais.



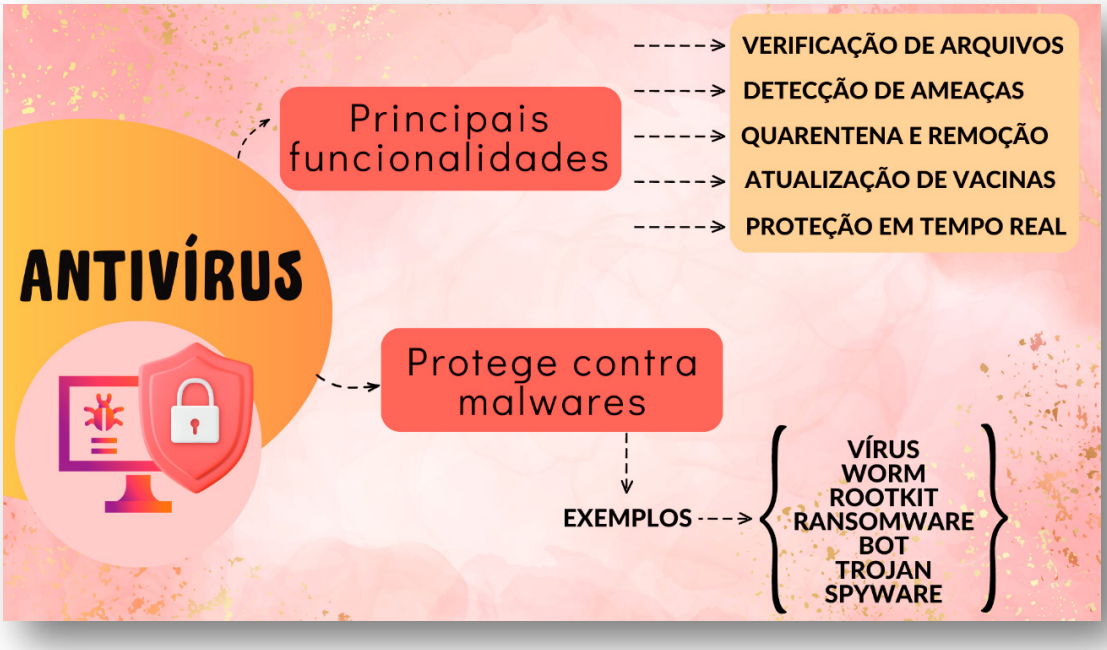
Proteção digital são os mecanismos e procedimentos criados para prevenir ou remediar os danos causados por ameaças digitais.

Veja abaixo um mapa mental com alguns exemplos de proteção digital.

Então, vamos estudar cada ferramenta de proteção digital.

2.1. ANTIVÍRUS

O antivírus é um software utilitário que identifica e elimina qualquer tipo de malware, como, por exemplo, worm, bot, trojan, vírus, rootkit, spyware e ransomware.



O antivírus é constituído por dois elementos básicos:

1º Um software console: mecanismo que executa a varredura;

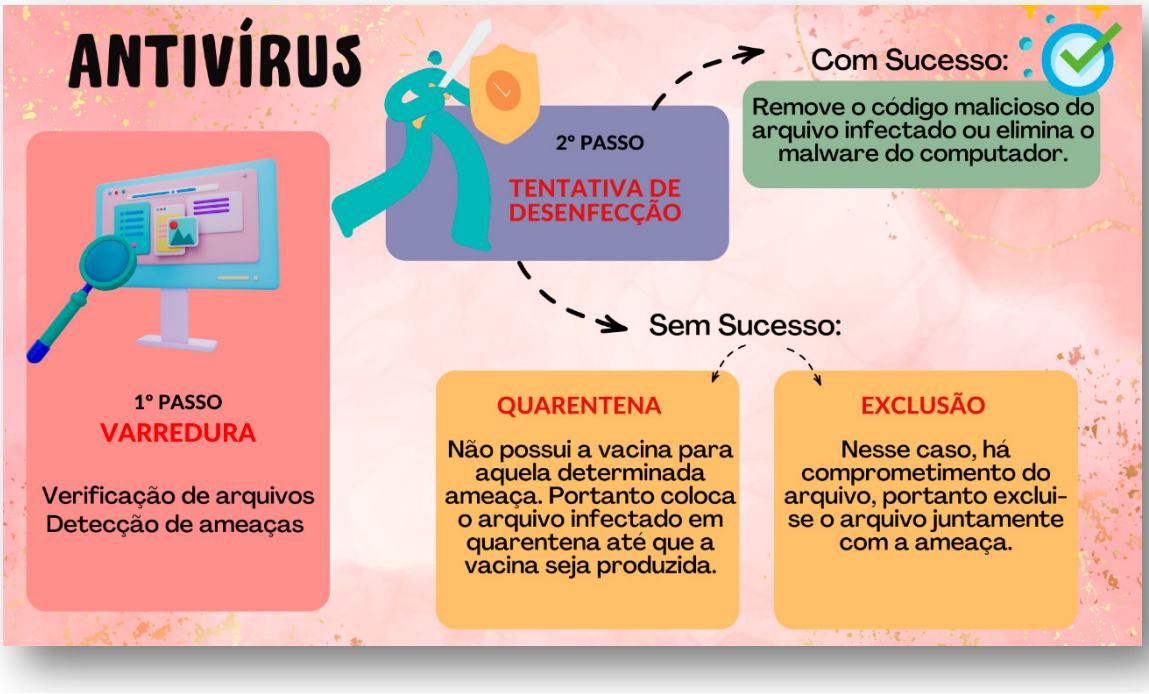
Varredura: é a forma como o antivírus busca malwares; portanto, o software procura um conjunto de características específicas capaz de identificar possíveis ameaças no computador.

2ª Vacinas: são as definições das ameaças (conjunto de padrões) que são atualizadas constantemente e identificam as características das ameaças na varredura.

O antivírus varre o local de armazenamento procurando as ameaças no CONTEÚDO do arquivo. Destaquei a palavra "conteúdo" porque, em provas de concursos, essa informação pode aparecer da seguinte forma equivocada: "O antivírus varre o local de armazenamento procurando as ameaças no NOME do arquivo." Fique atento!

Voltando à explicação, o antivírus varre o local de armazenamento procurando as ameaças no CONTEÚDO do arquivo. Caso encontre algum sinal de ameaça, isso significa que o arquivo pode estar infectado, sendo, portanto, necessário tomar algumas medidas para a limpeza ou remoção desses arquivos.

Veja a seguir como ocorre essa desinfecção:



Quarentena: é um recurso que impede que o arquivo seja executado, evitando que ele cause danos ao ambiente. Quando uma ameaça é detectada, o antivírus criptografa o arquivo suspeito e o move para uma área segura do disco.

Atualmente, o antivírus oferece proteção contra diversos tipos de ameaças, incluindo malwares que podem comprometer a segurança dos dados e do sistema. Portanto, caso uma questão afirme que o antivírus fornece proteção apenas contra vírus, essa afirmação está errada.

Existem diferenças entre os antivírus pagos e gratuitos, e a principal diferença está relacionada ao número de atualizações disponíveis. Os antivírus pagos geralmente oferecem um maior número de atualizações de vacinas em comparação com os antivírus gratuitos.

ATENÇÃO

Isso cai em prova!

Veja alguns exemplos de antivírus que mais aparecem em provas:

McAfee
Norton
Avast

AVG
Kaspersky

2.2. ANTISPYWARE

É uma ferramenta muito parecida com o antivírus, porém específica na busca por spywares, aqueles malwares espiões. Ou seja, suas vacinas contêm definições apenas de spywares, os quais serão procurados no local de armazenamento.

Veja algumas funcionalidades do antispyware:

Funcionalidades
Detecção de spyware
Varredura e remoção
Proteção em tempo real
Atualização das vacinas

2.3. ANTISPAM

É uma ferramenta importante utilizada nos aplicativos de e-mail. O antispam é responsável por verificar e filtrar, de forma automática, as mensagens indesejadas, conhecidas como spam.

O filtro antispam examina o conteúdo das mensagens, buscando características específicas ou padrões que identifiquem o spam, como links suspeitos e palavras-chave utilizadas em e-mails não solicitados. Quando o filtro identifica o spam, a mensagem é automaticamente transferida para a pasta “SPAM” ou outro nome, a depender do aplicativo de e-mail utilizado; por exemplo, no MS Outlook, essa pasta se chama “lixo eletrônico”. Geralmente, essas mensagens classificadas como spam ficam nessas pastas por trinta dias antes de serem automaticamente excluídas.

O filtro antispam vem integrado na maioria dos webmails e programas gerenciadores de e-mails. Ele permite separar os e-mails desejados dos indesejados (spams). Geralmente, os filtros passam por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai “aprendendo” a distinguir as mensagens.

Eles também utilizam varredura heurística para identificar e bloquear mensagens de spam. A varredura heurística é uma técnica que analisa o conteúdo e o comportamento das mensagens de e-mail para identificar características comuns de spam. Essa técnica permite

que os aplicativos antispam detectem e bloqueiem mensagens de spam novas e desconhecidas, que podem não ser capturadas pelos métodos tradicionais baseados em assinaturas.

Importante!!!
Todas as mensagens de e-mail passam pelo filtro antispam.

Veja abaixo um mapa mental sobre esse assunto.

2.4. IDS – INTRUSION DETECTION SYSTEM (SISTEMA DE DETECÇÃO DE INTRUSÃO)

Sistema de segurança que monitora o tráfego de rede em busca de padrões ou comportamentos anormais que possam identificar uma tentativa de invasão. Ele permite que a organização saiba se atividades anômalas ou maliciosas foram detectadas em seu ambiente computacional. Existem duas categorias de IDS: Network-based Intrusion Detection System (NIDS) e Host-based Intrusion Detection System (HIDS). O NIDS é projetado para detectar ameaças da rede (Network), enquanto o HIDS verifica ameaças no host, ou seja, na máquina do usuário ou em um servidor.

2.5. IPS – INTRUSION PREVENTION SYSTEM (SISTEMA DE PREVENÇÃO DE INTRUSÃO)

Sistema de segurança que complementa o IDS, tomando medidas ativas para bloquear e prevenir invasões em tempo real. Ele leva a detecção um passo adiante e desliga a rede antes que o acesso possa ser obtido ou para evitar o movimento adicional na rede. O IPS é geralmente colocado diretamente atrás do firewall.

O IDS se restringe a detectar tentativas de intrusão, registrá-las e enviá-las ao administrador da rede, enquanto o IPS opera "inline" na rede, adotando medidas adicionais para bloquear as intrusões em tempo real. Ou seja, enquanto o IDS é projetado para informar que algo está tentando entrar em seu sistema, o IPS atua tentando impedir o acesso, sendo uma ferramenta importante para garantir a segurança das redes de computadores e proteger dados sensíveis.

2.6. SENHAS FORTES

Outra forma de proteção contra várias ameaças de quebra de senha é o uso de senhas fortes. Uma senha é considerada forte quando é composta por 8 ou mais dígitos, combinados com letras maiúsculas, letras minúsculas, números e caracteres especiais. Quanto maior a senha, mais complexa é sua formação e mais difícil de ser descoberta. Assim, veja abaixo alguns critérios que devem ser observados para se criar senhas seguras:

- Letras minúsculas: 26 no alfabeto brasileiro.
- Letras maiúsculas: 26 letras no alfabeto brasileiro.
- Caracteres especiais: vamos considerar um conjunto com 10 caracteres especiais.
- Números: 10 dígitos numéricos (de 0 a 9).
- Não utilizar sequência repetida de caracteres, como 111aaa222.
- Não utilizar dados pessoais, como nome, sobrenome, número de CPF, data de nascimento etc.

Obs.: Lembre-se dessa composição acima! Ela já foi cobrada várias vezes em provas!

Portanto, o número total de combinações possíveis é calculado multiplicando o número de opções para cada tipo de caractere (26 + 26 + 10 + 10) ^ 8, o que resulta em 6,6 quatrilhões de combinações possíveis.

Isso parece impossível de ser quebrada, não é mesmo? Mas sabe quanto tempo leva para uma senha assim ser quebrada? Apenas 8 horas! Isso mesmo! Apenas 8 horas é o tempo necessário para uma senha de 8 dígitos, com letras maiúsculas, minúsculas, números e símbolos, ser quebrada! O que fazer, então? Aumentar o tamanho da senha.

Mesmo com essa aparente fragilidade, uma senha é considerada forte quando possui um tamanho mínimo de 8 dígitos; porém, o ideal é que tenha 14 dígitos. Veja abaixo o quadro

extraído da página Quanto Tempo para Descobrirem sua Senha? – IT Soluciona, o qual mostra o comparativo do tempo de quebra das combinações de senha. Particularmente, costumo usar uma senha bem forte, composta por 23 caracteres! Sim, dá para formar uma frase com ela kkkkkkkkk. E é exatamente assim que faço minhas senhas, compondo frases do tipo: ***V0uP@5s4R@G0ra***! Se você percebeu, isso é uma frase: Voupassaragora! Uma senha com 15 dígitos, que levaria 15 bilhões de anos para ser quebrada. Massa, né?

Nº DE CARACTERES	SOMENTE NÚMEROS	LETRAS MINÚSCULAS	LETRAS MINÚSCULAS E MAIÚSCULAS	MINÚSCULAS + MAIÚSCULAS + NÚMEROS	MINÚSCULAS + MAIÚSCULAS + NÚMEROS + SÍMBOLOS
4	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE
5	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE
6	IMEDIATAMENTE	IMEDIATAMENTE	IMEDIATAMENTE	1 SEGUNDO	5 SEGUNDOS
7	IMEDIATAMENTE	IMEDIATAMENTE	25 SEGUNDOS	1 MINUTO	6 MINUTOS
8	IMEDIATAMENTE	5 SEGUNDOS	22 MINUTOS	1 HORA	8 HORAS
9	IMEDIATAMENTE	2 MINUTOS	19 HORAS	3 DIAS	3 SEMANAS
10	IMEDIATAMENTE	58 MINUTOS	1 MÊS	7 MESES	5 ANOS
11	2 SEGUNDOS	1 DIA	5 ANOS	41 ANOS	400 ANOS
12	25 SEGUNDOS	3 SEMANAS	300 ANOS	2K ANOS	34K ANOS
13	4 MINUTOS	1 ANO	16K ANOS	100K ANOS	2M DE ANOS
14	41 MINUTOS	51 ANOS	800K ANOS	9M DE ANOS	200M DE ANOS
15	6 HORAS	1K ANOS	43M DE ANOS	600M DE ANOS	15 BI DE ANOS
16	2 DIAS	34K ANOS	2 BI DE ANOS	37 BI DE ANOS	1 TRI DE ANOS
17	4 SEMANAS	800K ANOS	100 BI DE ANOS	2 TRI DE ANOS	93 TRI DE ANOS
18	9 MESES	23M DE ANOS	100 TRI DE ANOS	100 TRI DE ANOS	7.10^{48} DE ANOS

Um último aspecto que pode tornar a senha forte é estabelecer prazos de expiração, por meio dos quais é necessário alterar a senha periodicamente. Isso aumenta a segurança, pois, caso algum sujeito mal-intencionado tenha conseguido obter aquela senha, ela terá sido alterada após um período. Combinado a isso, pode-se impedir que sejam utilizadas as duas últimas senhas, forçando a verdadeira alteração dela.

2.7. MFA – AUTENTICAÇÃO EM MÚLTIPLAS ETAPAS (MULTIFACTOR AUTHENTICATION)

Esse é um método de autenticação que exige mais de uma etapa para a verificação da identidade de uma pessoa.

Por exemplo, quando você utiliza apenas a senha para fazer login, significa que você usou um fator de segurança. Agora, quando você opta pela autenticação em múltiplas etapas, significa que você adiciona mais fatores de segurança à autenticação.

Geralmente, a autenticação em múltiplos fatores envolve algo que o usuário conhece, por exemplo, uma senha; algo que o usuário possui, por exemplo, o seu smartphone; e algo

inerente ao usuário, por exemplo, sua impressão digital ou reconhecimento facial. Essas etapas adicionais servem para proteger o acesso em casos em que a senha do usuário é descoberta pelo atacante e ele tenta acessar sua conta. Dessa forma, tais etapas asseguram que a pessoa que está acessando é realmente o usuário, pois há uma confirmação de sua identidade por um meio que somente o próprio usuário pode utilizar e confirmar.

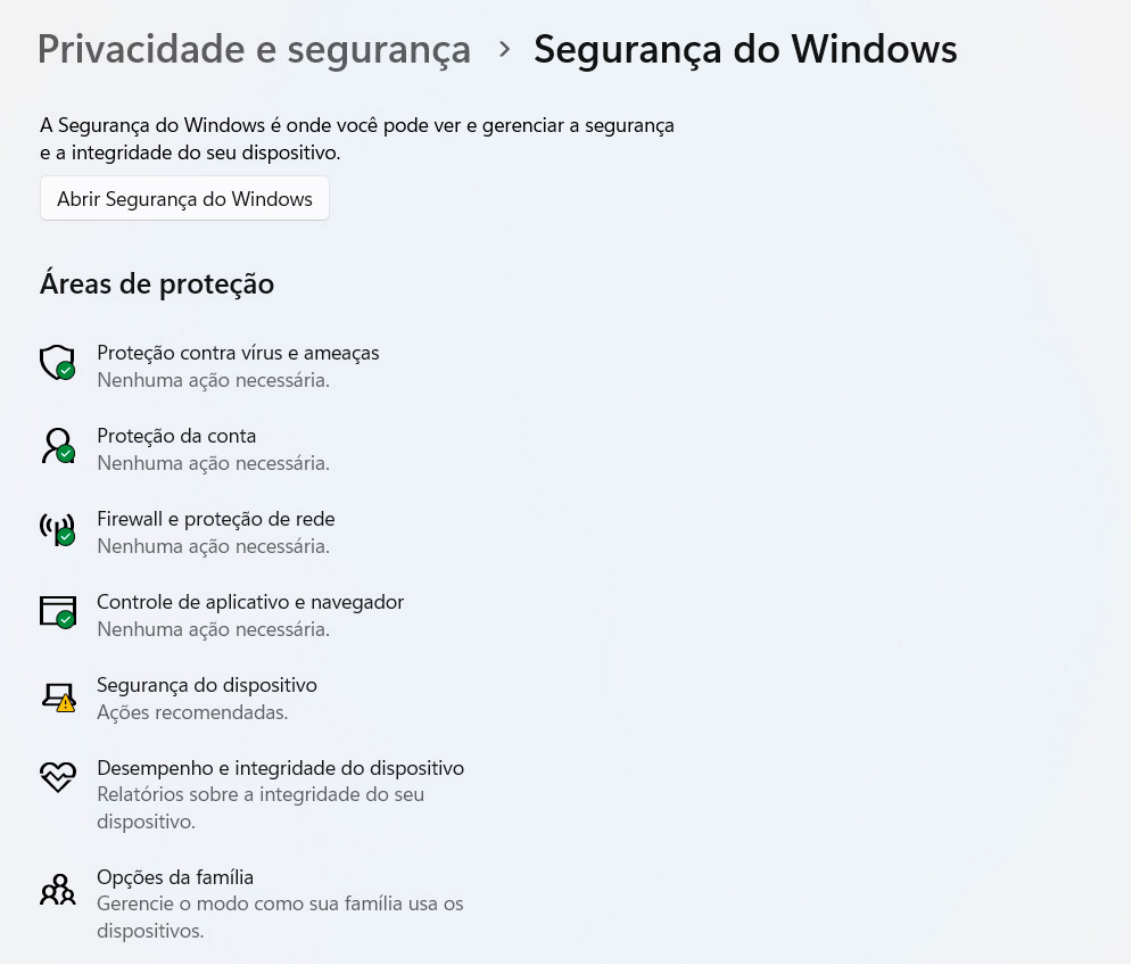
Essas etapas (fatores) são chamadas de camadas de segurança e auxiliam a aumentar a segurança do usuário, visto que o atacante precisa "quebrar" todos os fatores para obter acesso não autorizado.

Segundo a Cartilha de Segurança para Internet, em seu fascículo Verificação em Duas Etapas, existem alguns fatores que podem ser usados como etapas na autenticação, sendo eles:

- **Código de Verificação**: é um código individual criado pelo serviço e enviado de forma que apenas o usuário possa recebê-lo, por exemplo, por e-mail, chamada de voz ou mensagem de texto (SMS) para o telefone celular que o usuário cadastrou. Também pode ser gerado por um aplicativo autenticador instalado no dispositivo do usuário, que é o caso de João na questão.
- **Token gerador de senhas**: é um tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade.
- **Cartão de segurança**: é um cartão com diversos códigos numerados que são solicitados quando o usuário acessa a sua conta.
- **Dispositivo confiável**: é um computador ou dispositivo móvel que o usuário frequentemente usa para acessar suas contas.
- **Chave de recuperação**: é um número gerado pelo serviço quando o usuário ativa a verificação em duas etapas, permitindo que o usuário acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis.

2.8. SEGURANÇA DO WINDOWS

O sistema operacional Windows também oferece um conjunto de ferramentas de proteção nativas, ou seja, que já vêm integradas ao sistema. Veja abaixo! Pela sua imensa relevância em provas de concursos, gostaria de apresentar algumas de suas ferramentas a seguir:



Proteção contra vírus e ameaças: permite que o usuário verifique o computador em busca de ameaças e vírus, além de gerenciar as configurações de proteção em tempo real. Também é possível acessar as configurações de proteção contra ransomware e outras ameaças. No Windows, essa ferramenta se chama Microsoft Defender Antivírus. O Windows Defender é o antivírus nativo do Windows que oferece proteção abrangente, contínua e em tempo real contra diversas ameaças de software, incluindo vírus, malware e spyware, em várias frentes, como e-mails, aplicativos, na nuvem e na web. Antes do Windows 8, o Windows Defender funcionava exclusivamente como antispyware, mas, depois, foi aprimorado para se tornar um antivírus completo, capaz de combater diversas ameaças virtuais.

ATENÇÃO

O Windows Defender **não funciona** como ferramenta de criptografia de arquivos.

Firewall e proteção de rede: permite que o usuário gerencie as configurações do firewall do Windows e configure as opções de rede para manter o computador seguro. No Windows, essa opção se chama Windows Defender Firewall.

Controle de aplicativos e navegador: permite que o usuário gerencie as configurações de segurança do navegador e controle quais aplicativos podem ser executados no computador.

Segurança do dispositivo: permite que o usuário gerencie as configurações de segurança de seu dispositivo, incluindo a configuração de senhas e a criptografia de dados.

Além desses itens, há também alguns outros que não estão nesta seção das configurações, mas que considero bastante importantes. Dê uma olhada!

Central de Ações: é uma ferramenta de proteção que notifica o usuário sobre vulnerabilidades encontradas no sistema operacional Windows. Ou seja, essa é uma opção de segurança do Windows.

A partir do Windows 10, essa ferramenta recebeu mais funcionalidades, servindo quase como uma central de configurações básicas, disponibilizando vários botões de configuração, tais como redes, conexões a outros dispositivos, modo de tela e até o botão para todas as configurações do Windows.

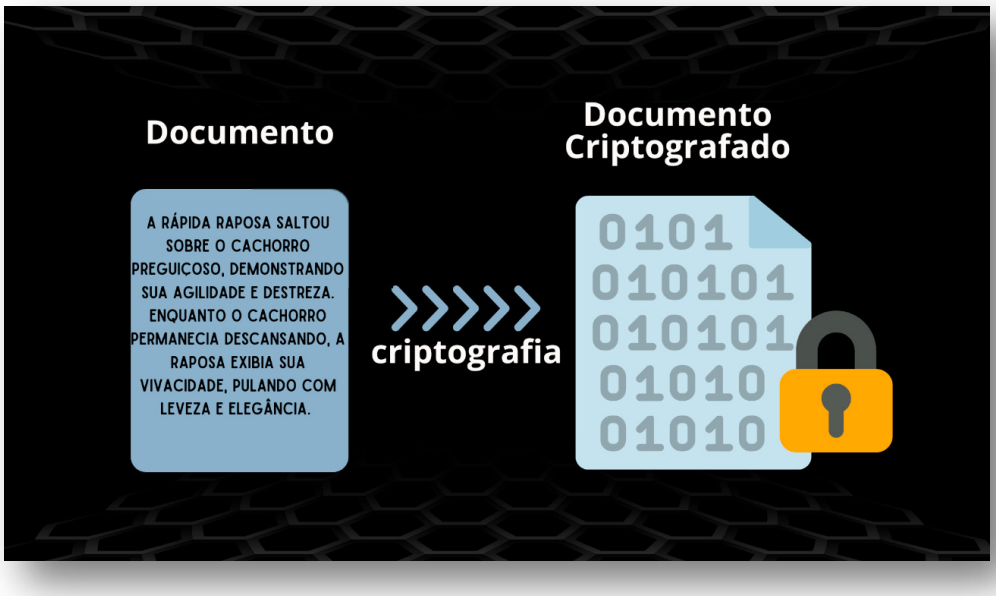
Não é o foco da nossa aula, mas, a título de curiosidade, a tecla de atalho para abrir a central de ações do Windows é **WIN+A.**

Windows Update: é uma ferramenta de atualizações automáticas do Windows. Sua principal função é identificar novos pacotes disponibilizados pela Microsoft, fazer download e instalar as correções e inovações para o sistema operacional.

A ação mais executada pelo Windows Update é a correção de vulnerabilidades, garantindo que o sistema operacional esteja sempre atualizado e, consequentemente, protegido contra possíveis ameaças.

2.9. CRIPTOGRAFIA

É a técnica de transformar a informação em algo ininteligível por meio do embaralhamento de seu conteúdo. Essa ferramenta é responsável por garantir o sigilo e a segurança das informações, podendo ser utilizada em ambientes tecnológicos ou não.

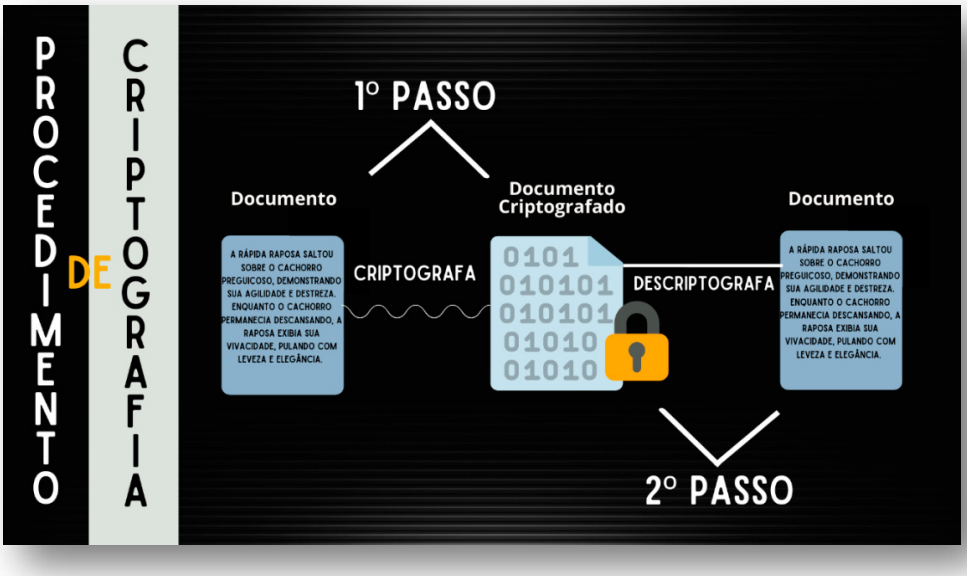


O processo de criptografia envolve duas etapas distintas:

1ª Etapa da criptografia – CRIPTOGRAFAR

Criptografar, ou seja, tornar a informação legível em ininteligível. Também podem ser usados os termos codificar, encriptar, cifrar etc. **2ª Etapa da criptografia – DESCRIPTOGRAFAR**

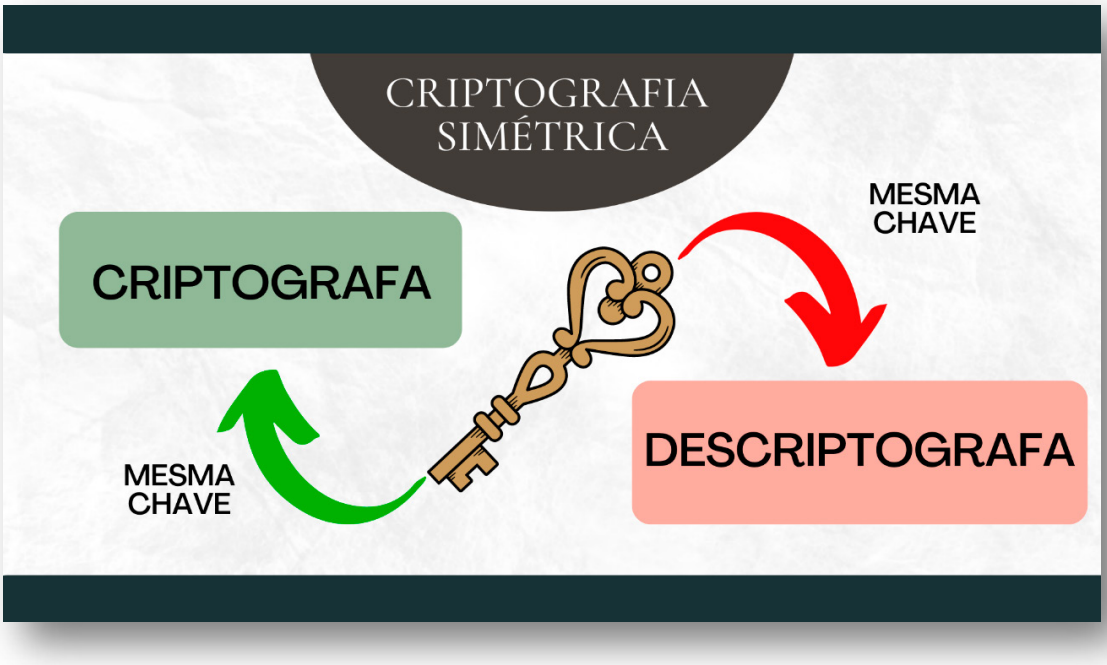
É o processo inverso, que pode ser chamado de descriptografar, decriptar, decodificar ou decifrar. Nesse processo, os dados criptografados são novamente transformados em sua forma original, tornando-os legíveis para os destinatários autorizados.



No contexto de criptografia, o termo "***chave***" é um elemento utilizado no processo de criptografar e descriptografar as informações. Vejamos os dois principais tipos de criptografia e como isso se aplica.

CRIPTOGRAFIA SIMÉTRICA/ CRIPTOGRAFIA DE CHAVE SECRETA OU CRIPTOGRAFIA DE CHAVE ÚNICA

Na criptografia simétrica, utiliza-se uma única chave para criptografar e descriptografar a informação. Essa chave pode ser uma senha ou um código e pode ser chamada de chave secreta ou chave de criptografia.



Considerando que será utilizada uma única chave para criptografar e descriptografar, essa chave deve ser mantida em sigilo para assegurar a confidencialidade dos dados. O remetente e o destinatário das informações precisam compartilhar a chave secreta previamente por meio de um canal de comunicação seguro.

Esse método de criptografia é encontrado em vários aplicativos que usamos no dia a dia, como o MS Word e o LibreOffice Writer, além do BitLocker, que é uma ferramenta nativa do Windows para criptografia de unidades de disco inteiras.

Vou utilizar um exemplo simples, mas visual, que ajudará a memorizar como a criptografia simétrica funciona.

EXEMPLO

Imagine especificamente a porta de entrada e saída da sua casa. Você tem uma única chave para entrar e sair. Ou seja, sua chave é a única que abre ou fecha sua casa; qualquer outra

chave que não seja a sua não abrirá a porta. Caso você queira que outra pessoa entre em sua casa, precisará entregar a chave a ela antes.

Da mesma maneira funciona a criptografia simétrica: a mesma chave para criptografar os dados será utilizada para descriptografá-los.

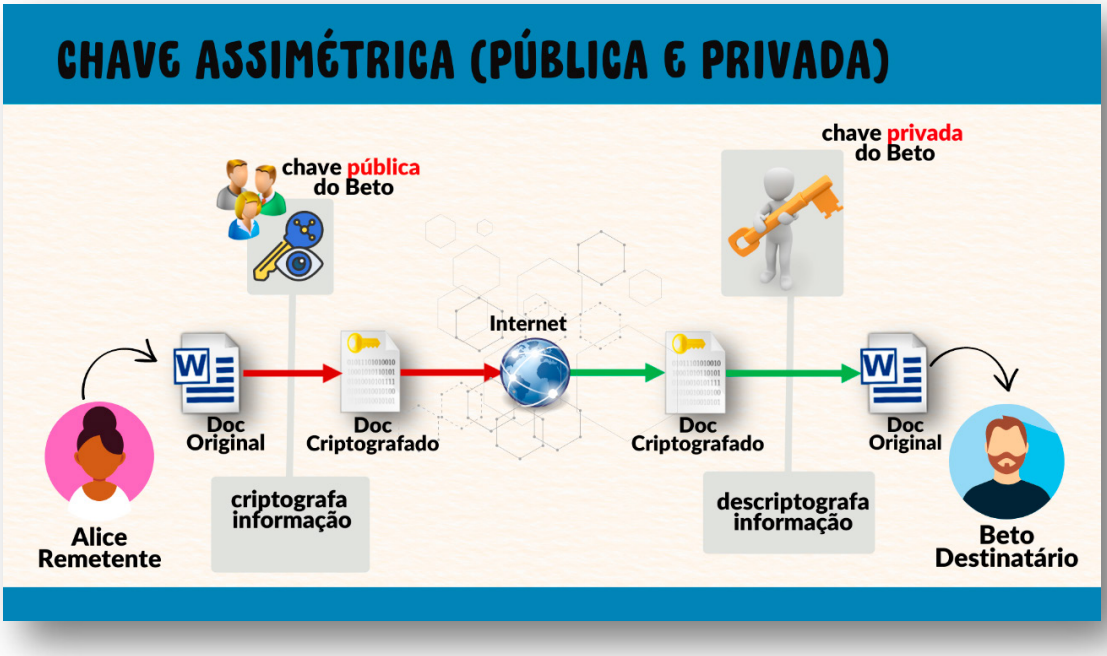
Lembre-se!

Criptografia simétrica usa **uma única** chave.

CRIPTOGRAFIA ASSIMÉTRICA/ CRIPTOGRAFIA DE CHAVE PÚBLICA

Na criptografia assimétrica, utilizam-se duas chaves, que formam um par: uma chave pública, usada para criptografar a informação, e a outra, uma chave privada, usada para descriptografar.

Tais chaves são códigos criados por uma autoridade certificadora e ficam armazenadas no certificado digital do usuário. Falarei sobre certificado digital e autoridade certificadora mais adiante. Muito utilizada no processo de envio de e-mail sigiloso, essa criptografia segue este esquema:



EXEMPLO

Alice, a remetente, está enviando uma mensagem criptografada para Beto, o destinatário. Assim, Beto compartilha com Alice sua chave pública, com a qual ela criptografa a mensagem e a envia para Beto de forma criptografada.

Por ser pública, tal chave pode ser compartilhada com qualquer pessoa, sem necessidade de um meio seguro para isso, pois, com ela, é possível apenas criptografar os dados.
Beto a recebe e a descriptografa com sua chave privada, conseguindo abrir a mensagem original. Esse método é encontrado em diversos softwares conhecidos, como o MS Outlook, software de correio eletrônico.

Lembre-se!

A criptografia assimétrica usa **duas** chaves, ambas do destinatário, sendo que a chave pública é a que criptografa e a chave privada é a que descriptografa.

Obs.: Somente o dono da chave privada pode abrir a mensagem criptografada; ninguém mais, nem mesmo a pessoa que a criptografou.

ALGORITMOS DE CRIPTOGRAFIA

Agora que você já visualizou e compreendeu o conteúdo de criptografia, vou repetir algumas informações explicadas de maneira mais técnica, desta vez.

Criptografia é a técnica que codifica os dados por meio de seu embaralhamento, impedindo que pessoas não autorizadas tenham acesso às informações contidas neles.

Para ser ativada, essa técnica necessita de uma chave ou código que inicia o algoritmo de embaralhamento. Existem algoritmos criptográficos que utilizam apenas uma chave, chamados de criptografia de **chave simétrica**, a qual deve ser mantida em sigilo e é conhecida como chave secreta ou privada.

Há também outros métodos criptográficos que utilizam duas chaves, chamados de criptografia de chaves públicas ou criptografia de **chave assimétrica**, pois utilizam uma chave pública, que pode ser compartilhada com qualquer pessoa e que é utilizada para cifrar os dados, e outra chave privada, também chamada de secreta, à qual somente o dono tem acesso para decifrar os dados, formando-se assim um par de chaves. As chaves públicas ficam contidas ou armazenadas em um certificado digital do proprietário dessas chaves.

DICA

Uma técnica para você memorizar é a seguinte: simétrica possui apenas um S, então usa apenas uma chave; assimétrica possui dois S's, então usa duas chaves.

Um aspecto importante que pode ser abordado em provas sobre criptografia são os algoritmos ou técnicas utilizadas tanto na criptografia simétrica quanto na assimétrica. Embora não seja necessário decorar todos eles, é útil concentrar-se nos algoritmos de criptografia assimétrica, que são menos numerosos, totalizando apenas quatro, apesar de existirem outros menos conhecidos. Dessa forma, se você estiver familiarizado com esses quatro algoritmos, será mais fácil identificá-los, caso apareçam na prova, diferenciando-os dos algoritmos simétricos.

Algoritmos de Criptografia Simétrica	Algoritmos de Criptografia Assimétrica
• **DES** – (**Data Encryption Standard**) algoritmo criptográfico simétrico selecionado como FIPS oficial (Federal Information Processing Standard) pelo governo dos EUA em 1976; ele realiza somente duas operações sobre sua entrada: deslocamento de bits e substituição de bits. • **IDEA** – (**International Data Encryption Algorithm**) é um algoritmo de criptografia simétrica que faz uso de chaves de 128 bits e que tem uma estrutura semelhante à do DES. • **3DES** – **Triple Data Encryption Standard** é um padrão de criptografia simétrica, baseado em outro algoritmo de criptografia simétrica, o DES. • **AES** – (**Advanced Encryption Standard**) padrão de criptografia avançada – é um algoritmo de chave simétrica que veio para substituir o padrão de criptografia de dados (DES). • **Blowfish** – criptografia simétrica com chaves de até 448 bits, a qual substituiu o IDEA. • **Twofish** – é uma chave simétrica que emprega a cifra de bloco de 128 bits, utilizando chaves de tamanhos variáveis, podendo ser de 128, 192 ou 256 bits. Ele realiza 16 interações durante a criptografia, sendo um algoritmo bastante veloz. • **RC2** – é uma cifra de bloco de chaves simétricas, projetada por Ronald Rivest em 1987. "RC" significa "Rivest Cipher" ou, em alternativa, "Ron's Code". RC2 é uma cifra de bloco de 64 bits com um tamanho de chave variável e usando 18 rodadas.	• **RSA** – (**Rivest-Shamir-Adleman**) – um dos algoritmos de criptografia assimétrica mais conhecidos, o qual usa uma chave pública que criptografa os dados e uma chave secreta que descriptografa. • **Diffie-Hellman** – permite que duas partes que não possuem conhecimento prévio uma da outra compartilhem uma chave secreta sob um canal de comunicação inseguro. Tal chave pode ser usada para encriptar mensagens posteriores usando um esquema de cifra de chave simétrica. • **ECC** – criptografia de curva elíptica é uma abordagem para a criptografia assimétrica que utiliza a estrutura algébrica de curvas elípticas sobre campos finitos. As chaves são menores se comparadas com outros algoritmos e proporcionam uma segurança similar. • **ElGamal** – utilizado para gerenciamento de chaves, o algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto.

2.10. ASSINATURA DIGITAL

Assinatura digital é a ferramenta utilizada para autenticar a veracidade da autoria de uma informação; portanto, garante a autenticidade. Além disso, a assinatura digital pode ser utilizada para garantir que a informação não sofra nenhuma alteração sem a devida permissão; ou seja, ela também garante a integridade dos dados.

Quando um documento é assinado eletronicamente, a assinatura torna-se inválida se houver qualquer alteração no conteúdo. Vários aplicativos usam a assinatura digital, tais como MS Word, LibreOffice Writer e MS Outlook.

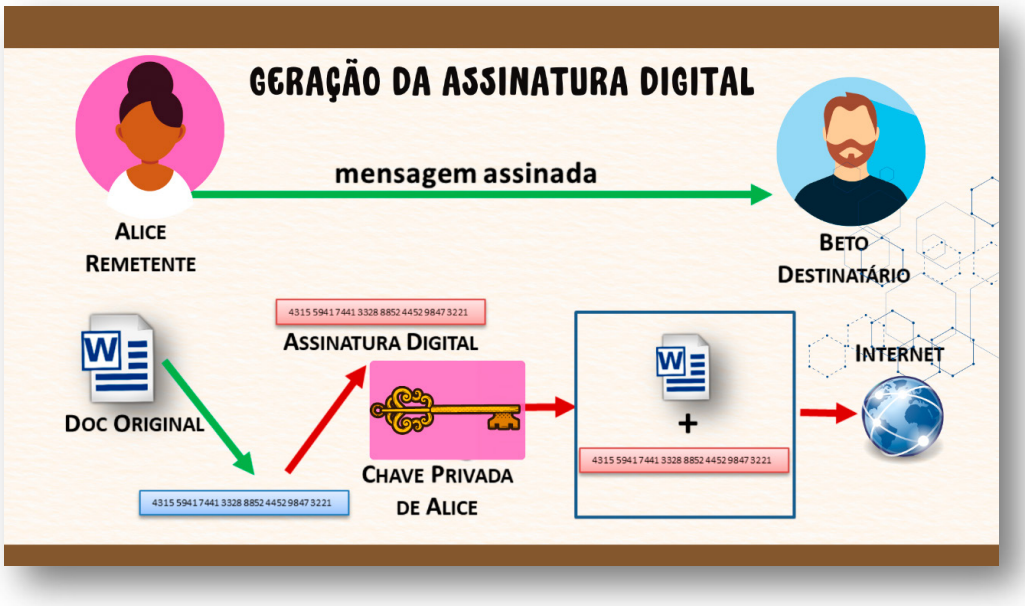
A assinatura digital possui dois passos:

1º passo da assinatura digital: **a geração da assinatura.**

A geração da assinatura ocorre quando o documento é assinado, ou seja, quando a assinatura é feita. Nesse momento, o aplicativo extrai um resumo, chamado também de hash (esse nome já foi utilizado várias vezes em provas), e, depois, criptografa esse hash

com a chave privada do autor da informação. Então, tanto o documento quanto a assinatura e a chave de quem assinou o documento são enviados para o destinatário.

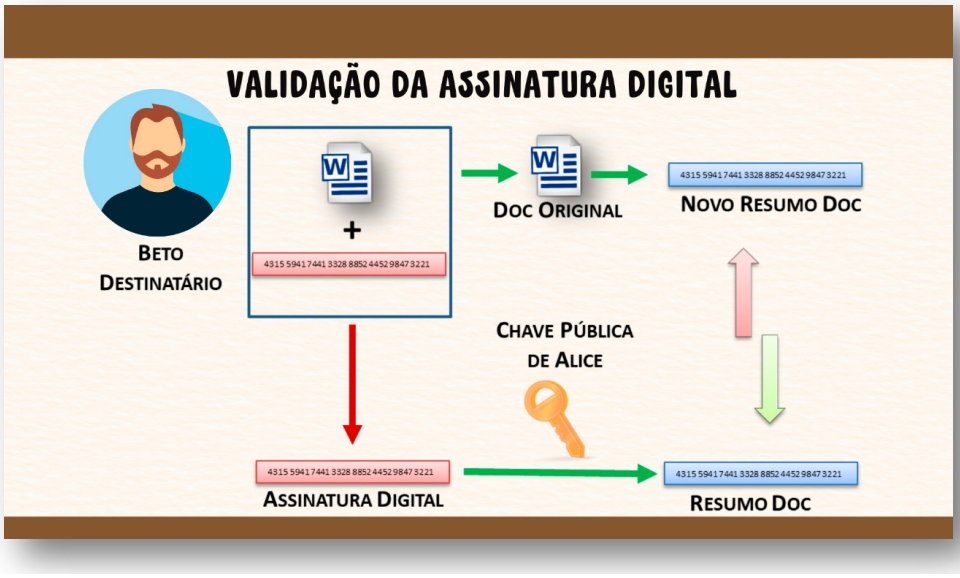
Veja como isso funciona na ilustração a seguir:



2º passo da assinatura digital: verificação ou validação da assinatura

Na verificação da assinatura, o destinatário recebe o documento, a assinatura e a chave pública enviados pelo remetente. Assim, o aplicativo do destinatário usa a chave pública e verifica se o documento foi alterado ou se foi assinado por outra pessoa que não seja o remetente, acusando quando isso acontece.

Veja a seguir como essa verificação ocorre:



ATENÇÃO

A assinatura digital utiliza as chaves do remetente, sendo a chave privada responsável por criptografar apenas o resumo ou hash do documento, e não o documento inteiro. Enquanto isso, a chave pública é utilizada na etapa de verificação.

Obs.: Assinatura digital não é a mesma coisa que assinatura digitalizada, como a que você tem na carteira de habilitação (CNH), nem aquela assinatura do corpo das mensagens de e-mail. Essa distinção é importante, pois a assinatura digital funciona como uma camada extra de proteção, enquanto a assinatura digitalizada não oferece os mesmos benefícios.

2.11. CERTIFICADO DIGITAL

É um documento eletrônico que identifica o usuário com seus dados pessoais, seja pessoa física ou jurídica. Também é nele que ficam guardadas as chaves criptográficas pública e privada. Ele é certificado.

O certificado digital é emitido por uma autoridade certificadora, a qual é uma instituição delegada pela Infraestrutura de Chaves Públicas (ICP) para desempenhar tal papel. Várias instituições conhecidas atuam como autoridades certificadoras, tais como SERPRO, Caixa Econômica Federal, SERASA, CertiSign, entre várias outras.

Na ICP, há também as autoridades de registro, que apenas recebem as solicitações dos usuários quando estes desejam adquirir um certificado. O interessante é que a mesma instituição pode exercer os dois papéis, ou seja, pode ser tanto autoridade certificadora quanto autoridade de registro.

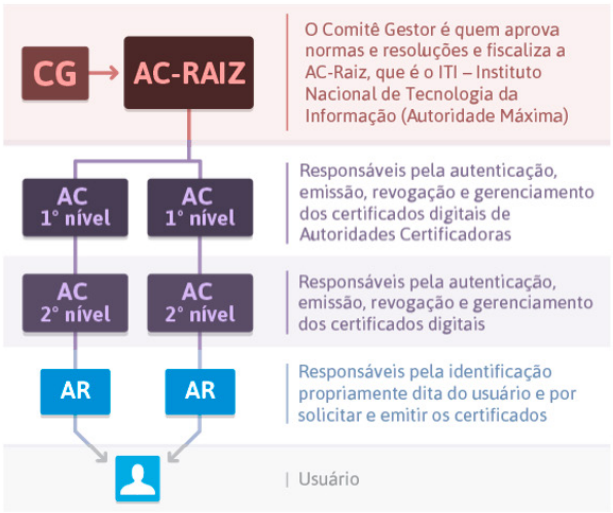
Em geral, os certificados digitais são compostos por alguns dados básicos, como:

- versão e número de série do certificado;
- dados que identificam a Autoridade Certificadora que emitiu o certificado;
- dados que identificam o dono do certificado (para quem ele foi emitido);
- chave pública do dono do certificado;
- validade do certificado (data de emissão e data de validade);
- assinatura digital da Autoridade Certificadora emissora e dados para verificação da assinatura.

Por fim, existe ainda a autoridade certificadora raiz, a qual está no topo da pirâmide, responsável por gerir toda a ICP. O certificado digital é usado tanto na criptografia assimétrica quanto na assinatura digital.

Veja essa estrutura geral da ICP-Brasil, extraída do seu próprio site ICP-Brasil – Instituto Nacional de Tecnologia da Informação (www.gov.br).

É a estrutura hierárquica organizacional que cuida da certificação digital no Brasil



2.12. BACKUP

O tópico de backup, apesar de ser um mecanismo de segurança da informação, nesta aula será tratado apenas como um resumo, pois o assunto de backup é bem extenso, sendo necessária uma aula à parte para tratar todo o conteúdo de backup.

Geralmente, os editais cobram esse tópico como "procedimentos de Backup" e temos uma aula específica sobre isso. De qualquer maneira, deixo aqui um pequeno resumo sobre backup.

Backup é uma cópia de segurança. Você também encontrará o nome "becape", aportuguesado, em suas provas, e não está errado; é apenas um costume de algumas bancas. Não é uma simples cópia, como copiar uma pasta do seu computador e colar em um pen drive. O backup é realizado por uma ferramenta específica, tal como a ferramenta de backup do Windows, a qual verifica os arquivos copiados, faz o versionamento dos arquivos, marca os que já foram copiados etc.

Há duas ações relacionadas ao backup: cópia e restauração. A cópia é quando o backup é realizado, copiando os dados. A restauração é quando os arquivos copiados do backup são restaurados, seja devido à perda dos dados originais ou por qualquer outro motivo.

O backup, geralmente, produz uma cópia compactada dos arquivos para economizar espaço de armazenamento. Além dessas características mencionadas, é preciso também conhecer os tipos de backup que existem.

São quatro tipos principais que vamos estudar, sendo que os dois primeiros realizam a cópia completa dos dados originais e os dois últimos copiam os dados parcialmente.

- **Backup normal**: também chamado de global, total ou completo, ele copia todos os arquivos marcados para backup, mesmo aqueles que já foram copiados anteriormente e que não sofreram alterações. Após copiar os arquivos originais, ele os identifica como copiados.
- **Backup de cópia**: ele é igual ao normal, porém não identifica os arquivos copiados. É um tipo de backup tempestivo, ou seja, usado emergencialmente para evitar uma perda em caso de manutenção no sistema. Ele é invisível à rotina normal de backup, pois não identifica os arquivos copiados.
- **Backup incremental**: é um backup parcial que copia apenas os arquivos novos ou alterados desde o último backup normal ou incremental. O seu objetivo é economizar espaço, copiando apenas aquilo que está diferente dos dados originais. O backup incremental identifica os arquivos originais que sofreram backup.
- **Backup diferencial**: é igual ao incremental, porém não identifica os arquivos.

RESUMO

Vamos revisar rapidamente todos os ataques vistos em nossa aula para relembrarmos cada um deles e irmos para a prova afiadíssimos, ok?

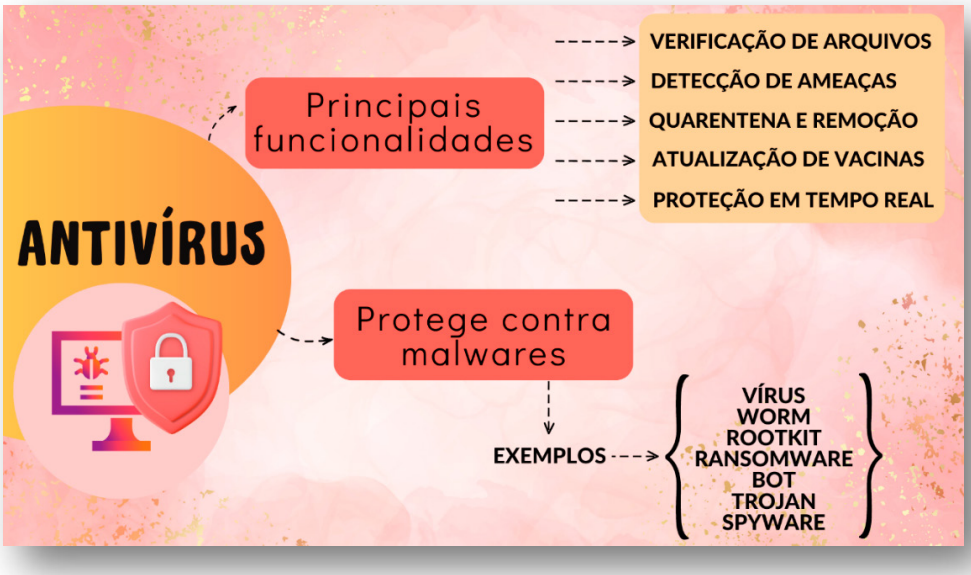
Proteção digital são os mecanismos e procedimentos criados para prevenir ou remediar os danos causados por ameaças digitais.

Veja abaixo um mapa mental com alguns exemplos de proteção digital.

Então, vamos estudar cada ferramenta de proteção digital.

Antivírus

O antivírus é um software utilitário que identifica e elimina qualquer tipo de malware, como, por exemplo, worm, bot, trojan, vírus, rootkit, spyware e ransomware.



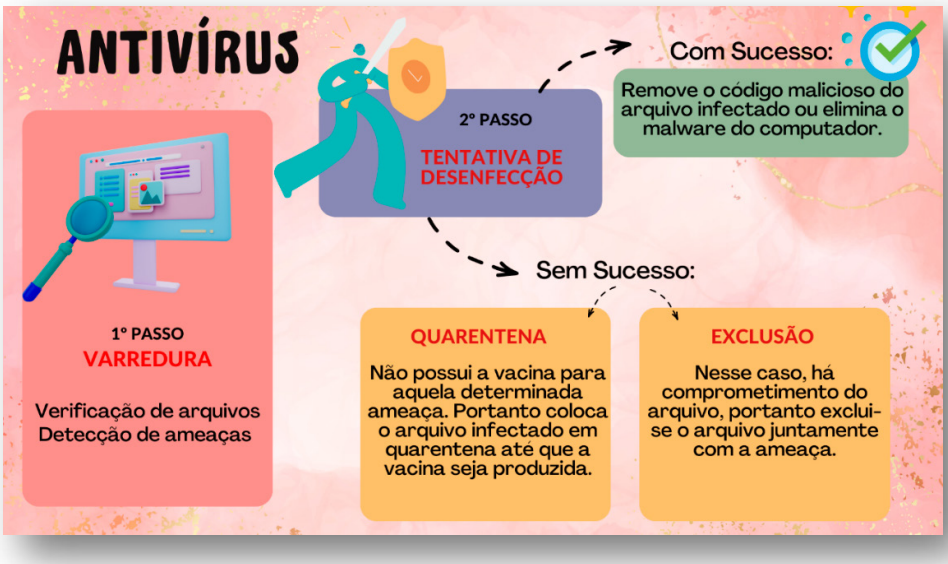
O antivírus é constituído por dois elementos básicos:

1º Um software console: mecanismo que executa a varredura;

Varredura: é a forma que o antivírus utiliza para buscar malwares; portanto, o software busca um conjunto de características específicas capaz de identificar possíveis ameaças no computador.

2ª Vacinas: são as definições das ameaças (conjunto de padrões) que são atualizadas constantemente e identificam as características das ameaças na varredura.

Veja abaixo como o antivírus atua, seus passos etc.



Quarentena: é um recurso que impede que o arquivo seja executado, evitando que ele cause danos ao ambiente. Quando uma ameaça é detectada, o antivírus criptografa o arquivo suspeito e o move para uma área segura do disco.

Veja alguns exemplos de antivírus que mais aparecem em provas:

McAfee
Norton
Avast
AVG
Kaspersky

Antispyware

É uma ferramenta muito parecida com o antivírus, porém é específica na busca por spywares, aqueles malwares espiões. Ou seja, suas definições contêm apenas informações sobre spywares, os quais serão procurados no local de armazenamento.

Veja algumas funcionalidades do antispyware:

Funcionalidades
Detecção de spyware
Varredura e remoção
Proteção em tempo real
Atualização das vacinas

Antispam

É uma ferramenta importante utilizada nos aplicativos de e-mail. O antispam é responsável por verificar e filtrar, de forma automática, as mensagens indesejadas, conhecidas como spam.

O filtro antispam examina o conteúdo das mensagens, buscando características específicas ou padrões que identifiquem o spam, como, por exemplo, links suspeitos e palavras-chave utilizadas em e-mails não solicitados. Quando o filtro identifica o spam, a mensagem é automaticamente transferida para a pasta "SPAM" ou outro nome, a depender do aplicativo de e-mail utilizado; por exemplo, no MS Outlook, essa pasta se chama "lixo eletrônico". Geralmente, essas mensagens classificadas como spam ficam nessas pastas por trinta dias antes de serem automaticamente excluídas.

O filtro antispam vem integrado na maioria dos webmails e programas gerenciadores de e-mails. Ele permite separar os e-mails desejados dos indesejados (spams). Geralmente, os

filtros passam por um período inicial de treinamento, no qual o usuário seleciona manualmente as mensagens consideradas spam e, com base nas classificações, o filtro vai "aprendendo" a distinguir as mensagens.

Eles também utilizam varredura heurística para identificar e bloquear mensagens de spam. A varredura heurística é uma técnica que analisa o conteúdo e o comportamento das mensagens de e-mail para identificar características comuns de spam. Essa técnica permite que os aplicativos antispam detectem e bloqueiem mensagens de spam novas e desconhecidas, que podem não ser capturadas pelos métodos tradicionais baseados em assinaturas.

ATENÇÃO

Todas as mensagens de e-mail passam pelo filtro antispam.

Veja abaixo um mapa mental sobre esse assunto.

Segurança do Windows

O sistema operacional Windows também oferece um conjunto de ferramentas de proteção nativas, ou seja, que já vêm integradas ao sistema. Veja abaixo! Pela sua imensa relevância em provas de concursos, gostaria de apresentar algumas de suas ferramentas a seguir:

Proteção contra vírus e ameaças: permite que o usuário verifique o computador em busca de ameaças e vírus, além de gerenciar as configurações de proteção em tempo real. Também é possível acessar as configurações de proteção contra ransomware e outras ameaças. No Windows, essa ferramenta se chama Microsoft Defender Antivírus.

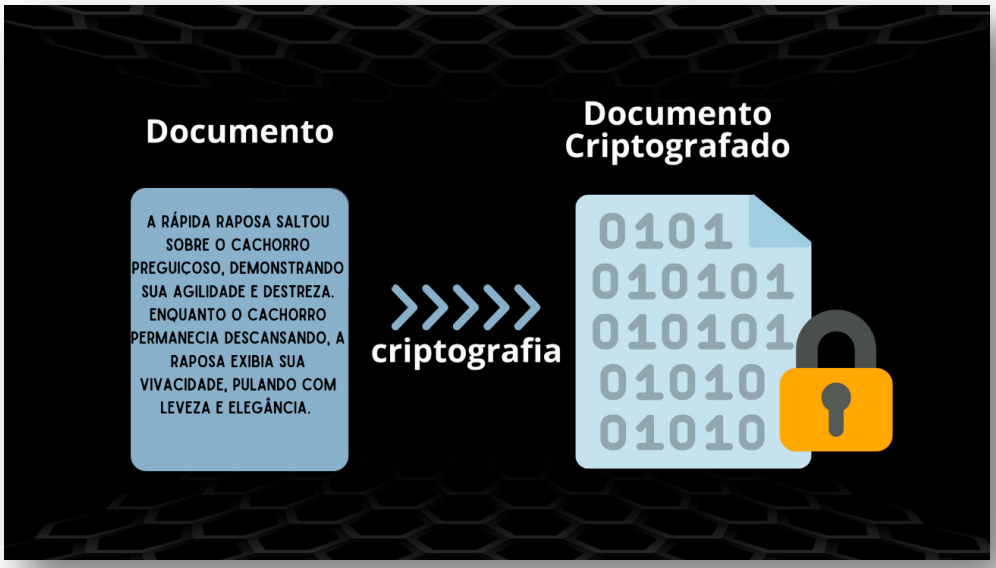
Firewall e proteção de rede: permite que o usuário gerencie as configurações do firewall do Windows e configure as opções de rede para manter o computador seguro. No Windows, essa opção se chama Windows Defender Firewall.

Controle de aplicativos e navegador: permite que o usuário gerencie as configurações de segurança do navegador e controle quais aplicativos podem ser executados no computador.

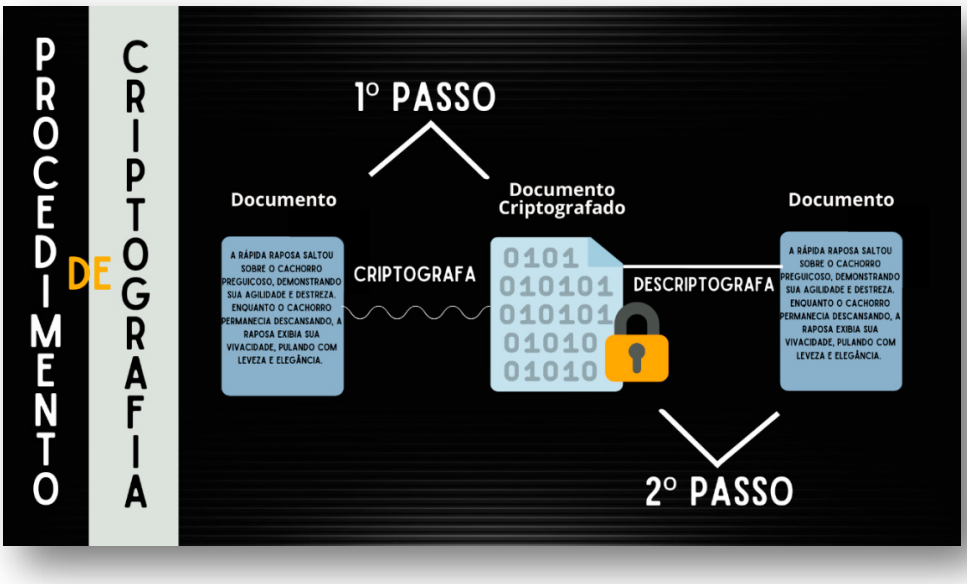
Segurança do dispositivo: permite que o usuário gerencie as configurações de segurança de seu dispositivo, incluindo a configuração de senhas e a criptografia de dados.

Criptografia

É a técnica de transformar a informação em algo ininteligível por meio do embaralhamento de seu conteúdo. Essa ferramenta garante o sigilo e a segurança das informações, podendo ser utilizada em ambientes tecnológicos ou não.



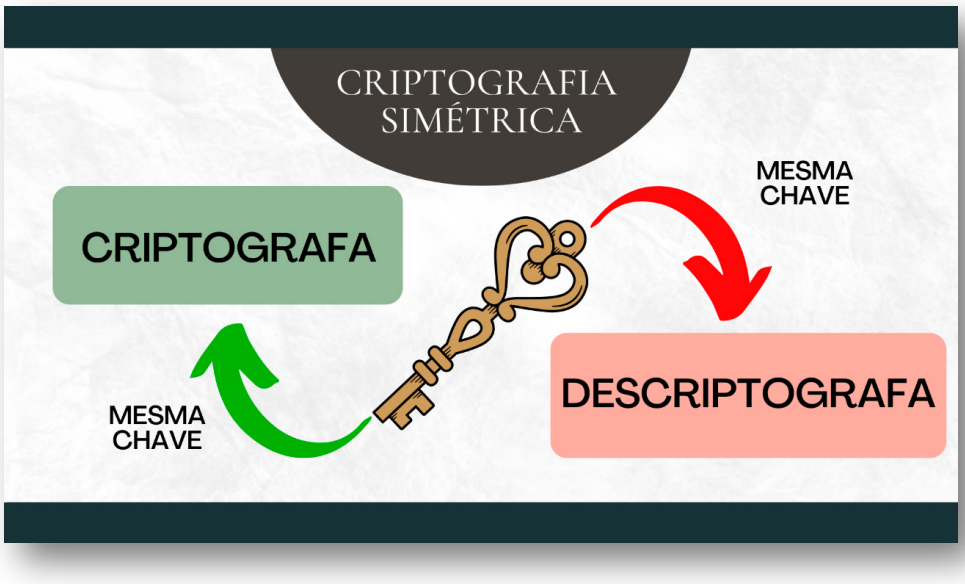
O processo de criptografia envolve duas etapas distintas; veja na imagem a seguir:



Vejamos os dois principais tipos de criptografia e como se aplicam.

Criptografia Simétrica: **Criptografia de Chave Secreta ou Criptografia de Chave Única**

Na criptografia simétrica, utiliza-se uma única chave para criptografar e descriptografar a informação.

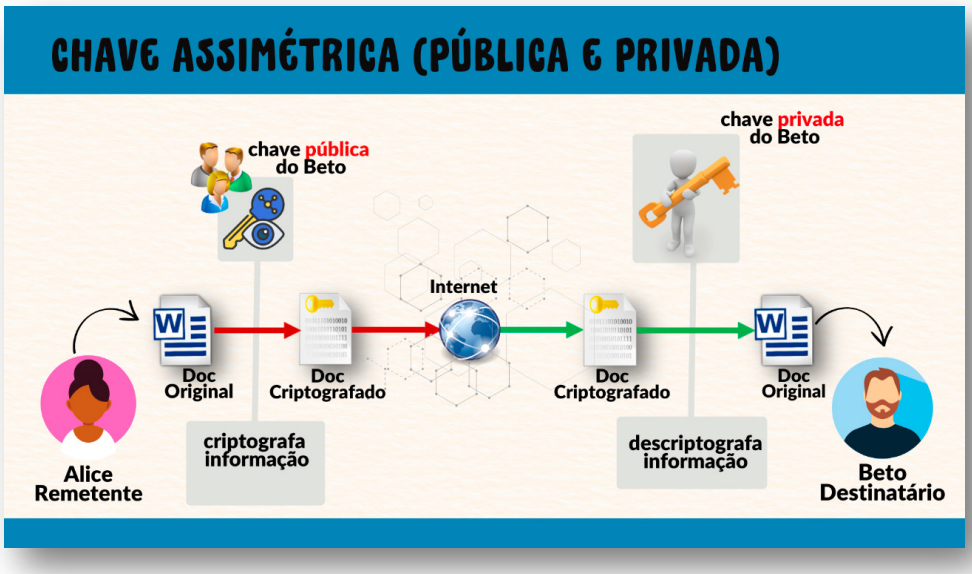


Considerando que será utilizada uma única chave para criptografar e descriptografar, essa chave deve ser mantida em sigilo para assegurar a confidencialidade dos dados. O remetente e o destinatário das informações precisam compartilhar a chave secreta previamente por meio de um canal de comunicação seguro.

Obs.: Criptografia Simétrica usa **uma única** chave.

Criptografia Assimétrica / Criptografia de Chave Pública

Na criptografia assimétrica, utilizam-se duas chaves que formam um par: uma chave pública, usada para criptografar a informação, e uma chave privada, usada para descriptografar.



ATENÇÃO

A criptografia assimétrica usa **duas** chaves, ambas do destinatário, sendo que a chave pública é a que criptografa e a chave privada é a que descriptografa.

Obs.: Somente o dono da chave privada pode abrir a mensagem criptografada; ninguém mais, nem mesmo a pessoa que a criptografou.

Algoritmos de Criptografia

Um aspecto importante que pode ser abordado em provas sobre criptografia são os algoritmos ou técnicas utilizados tanto na criptografia simétrica quanto na assimétrica.

Algoritmos de Criptografia Simétrica	Algoritmos de Criptografia Assimétrica
• **DES – (Data Encryption Standard)** • **IDEA – (International Data Encryption Algorithm)** • **3DES – Triple Data Encryption Standard** • **AES – (Advanced Encryption Standard)** • **Blowfish** • **Twofish** • **RC2**	• **RSA – (Rivest-Shamir-Adleman)** • **Diffie-Hellman** • **ECC** • **ElGamal**

Assinatura Digital

Assinatura digital é a ferramenta utilizada para autenticar a veracidade da autoria de uma informação; portanto, garante a autenticidade. Além disso, a assinatura digital pode

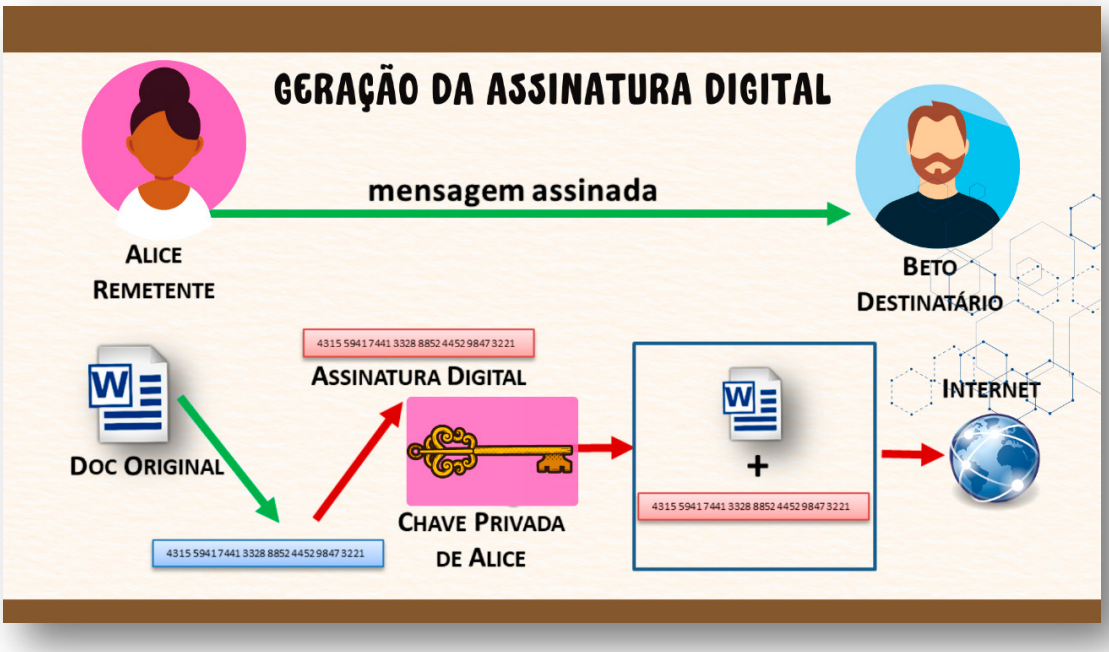
ser utilizada para assegurar que a informação não sofra nenhuma alteração sem a devida permissão; ou seja, ela também garante a integridade dos dados.

A assinatura digital possui dois passos:

1º passo da assinatura digital: **a geração da assinatura.**

A geração da assinatura ocorre quando o documento é assinado, ou seja, quando a assinatura é feita. Nesse momento, o aplicativo extrai um resumo, chamado também de hash (esse nome já foi utilizado várias vezes em provas), e, depois, criptografa esse hash com a chave privada do autor da informação. Assim, tanto o documento quanto a assinatura e a chave de quem assinou o documento são enviados para o destinatário.

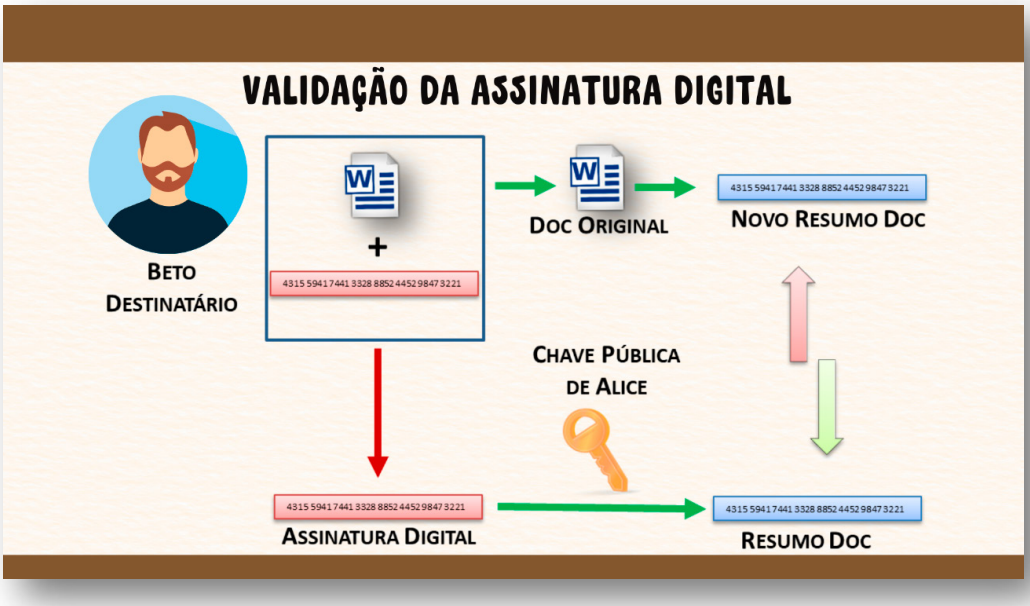
Veja como isso funciona na ilustração a seguir:



2º passo da assinatura digital: verificação ou validação da assinatura

Na verificação da assinatura, o destinatário recebe o documento, a assinatura e a chave pública enviados pelo remetente. Assim, o aplicativo do destinatário utiliza a chave pública e verifica se o documento foi alterado ou se foi assinado por outra pessoa que não seja o remetente, acusando quando isso acontece.

Veja a seguir como essa verificação ocorre:



ATENÇÃO

A assinatura digital utiliza as chaves do remetente, sendo a chave privada responsável por criptografar apenas o resumo ou hash do documento, e não o documento inteiro. Enquanto isso, a chave pública é utilizada na etapa de verificação.

Certificado Digital

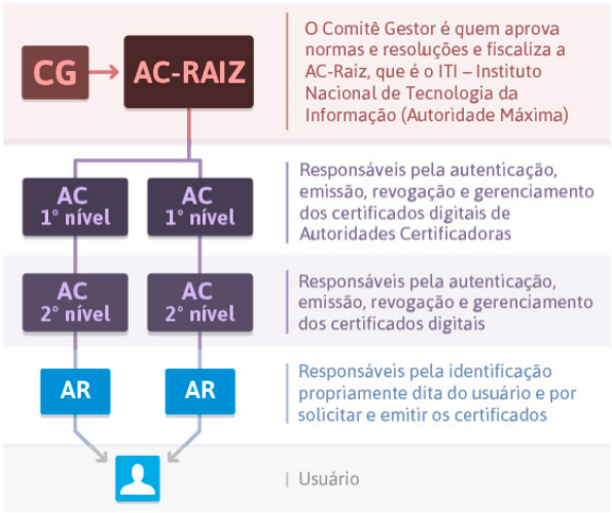
É um documento eletrônico que identifica o usuário com seus dados pessoais, seja pessoa física ou jurídica. Também é nele que ficam guardadas as chaves criptográficas pública e privada.

O certificado digital é emitido por uma autoridade certificadora, a qual é uma instituição delegada pela Infraestrutura de Chaves Públicas (ICP) para desempenhar tal papel. Várias instituições conhecidas atuam como autoridades certificadoras, tais como SERPRO, Caixa Econômica Federal, SERASA, CertiSign, entre várias outras.

Em geral, os certificados digitais são compostos por alguns dados básicos; veja abaixo:

Veja a estrutura geral da ICP-Brasil, extraída do seu próprio site, ICP-Brasil – Instituto Nacional de Tecnologia da Informação (www.gov.br).

É a estrutura hierárquica organizacional que cuida da certificação digital no Brasil



Backup

Deixo aqui um pequeno resumo sobre backup.

Há duas ações relacionadas ao backup: cópia e restauração. A cópia é quando o backup é realizado, copiando os dados. A restauração é quando os arquivos copiados do backup são restaurados, seja devido à perda dos dados originais ou por qualquer outro motivo.

São quatro tipos principais que vamos estudar, sendo que os dois primeiros realizam a cópia completa dos dados originais e os dois últimos copiam os dados parcialmente.

- **Backup normal**: também chamado de global, total ou completo, ele copia todos os arquivos marcados para backup, mesmo aqueles que já foram copiados anteriormente e que não sofreram alterações. Após copiar os arquivos originais, ele os identifica como copiados.
- **Backup de cópia**: ele é igual ao normal, porém não identifica os arquivos copiados. É um tipo de backup tempestivo, ou seja, usado emergencialmente para evitar uma perda em caso de se fazer uma manutenção no sistema. Ele é invisível à rotina normal de backup, pois não identifica os arquivos copiados.
- **Backup incremental**: é um backup parcial que copia apenas os arquivos novos ou alterados desde o último backup normal ou incremental. O seu objetivo é economizar espaço, copiando apenas aquilo que está diferente dos dados originais. O backup incremental identifica os arquivos originais que sofreram backup.
- **Backup diferencial**: é igual ao incremental, porém não identifica os arquivos copiados.

IDS – Intrusion Detection System (Sistema de Detecção de Intrusão)

Sistema de segurança que monitora o tráfego de rede em busca de padrões ou comportamentos anormais que possam indicar uma tentativa de invasão. Ele permite que a organização saiba se atividades anômalas ou maliciosas foram detectadas em seu ambiente computacional. Existem duas categorias de IDS: Network-based Intrusion Detection System (NIDS) e Host-based Intrusion Detection System (HIDS). O NIDS é projetado para detectar ameaças da rede (Network), enquanto o HIDS verifica ameaças no host, ou seja, na máquina do usuário ou em um servidor.

IPS – Intrusion Prevention System (Sistema de Prevenção de Intrusão)

Sistema de segurança que complementa o IDS, tomando medidas ativas para bloquear e prevenir invasões em tempo real. Ele leva a detecção um passo adiante e desliga a rede antes que o acesso possa ser obtido ou para evitar o movimento adicional na rede. O IPS é geralmente colocado diretamente atrás do firewall.

O IDS se restringe a detectar tentativas de intrusão, registrá-las e enviá-las ao administrador da rede, enquanto o IPS opera "inline" na rede, adotando medidas adicionais para bloquear as intrusões em tempo real. Ou seja, enquanto o IDS é projetado para informar que algo está tentando entrar em seu sistema, o IPS atua tentando impedir o acesso, sendo uma ferramenta importante para garantir a segurança das redes de computadores e proteger dados sensíveis.

Senhas fortes

Outra forma de proteção contra várias ameaças de quebra de senha é o uso de senhas fortes. Uma senha é considerada forte quando é composta por 8 ou mais dígitos, combinados

com letras maiúsculas, letras minúsculas, números e caracteres especiais. Quanto maior a senha, mais complexa é sua formação e mais difícil de ser descoberta. Assim, veja abaixo alguns critérios que devem ser observados para se criar senhas seguras:

- Letras minúsculas: 26 no alfabeto brasileiro.
- Letras maiúsculas: 26 letras no alfabeto brasileiro.
- Caracteres especiais: vamos considerar um conjunto com 10 caracteres especiais.
- Números: 10 dígitos numéricos (de 0 a 9).
- Não utilizar sequência repetida de caracteres, como 111aaa222.
- Não utilizar dados pessoais, como nome, sobrenome, número de CPF, data de nascimento etc.

Obs.: Lembre-se dessa composição acima! Ela já foi cobrada várias vezes em provas!

Um último aspecto que pode tornar a senha forte é estabelecer prazos de expiração, por meio dos quais é necessário alterar a senha periodicamente. Isso aumenta a segurança, pois, caso algum sujeito mal-intencionado tenha conseguido obter aquela senha, ela terá sido alterada após um período. Combinado a isso, pode-se impedir que sejam utilizadas as duas últimas senhas, forçando a verdadeira alteração dela.

MFA – Autenticação em Múltiplas Etapas (Multi-Factor Authentication)

Esse é um método de autenticação que exige mais de uma etapa para a verificação da identidade de uma pessoa.

Geralmente, a autenticação em múltiplos fatores envolve algo que o usuário conhece, por exemplo, uma senha; algo que o usuário possui, por exemplo, o seu smartphone; e algo inerente ao usuário, por exemplo, sua impressão digital ou reconhecimento facial. Essas etapas servem para proteger o acesso em casos em que a senha do usuário é descoberta pelo atacante e ele tenta acessar sua conta. Dessa forma, tais etapas asseguram que a pessoa que está acessando é realmente o usuário, pois há uma confirmação de sua identidade por um meio que somente o próprio usuário pode utilizar e confirmar.

Essas etapas (fatores) são chamadas de camadas de segurança e auxiliam a aumentar a segurança do usuário, visto que o atacante precisa "quebrar" todos os fatores para obter acesso não autorizado.

Segundo a Cartilha de Segurança para Internet, em seu fascículo Verificação em Duas Etapas, existem alguns fatores que podem ser usados como etapas na autenticação, sendo eles:

- **Código de Verificação**: é um código individual criado pelo serviço e enviado de forma que apenas o usuário possa recebê-lo, por exemplo, por e-mail, chamada de voz ou mensagem de texto (SMS) para o telefone celular que o usuário cadastrou. Também pode ser gerado por um aplicativo autenticador instalado no dispositivo do usuário, que é o caso de João na questão.
- **Token gerador de senhas**: é um tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade.
- **Cartão de segurança**: é um cartão com diversos códigos numerados que são solicitados quando o usuário acessa a sua conta.
- **Dispositivo confiável**: é um computador ou dispositivo móvel que o usuário frequentemente usa para acessar suas contas.
- **Chave de recuperação**: é um número gerado pelo serviço quando o usuário ativa a verificação em duas etapas, permitindo que o usuário acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis.

Agora que vimos a parte teórica, vamos treinar tudo o que aprendemos por meio de questões de concursos aplicadas anteriormente, todas comentadas por mim mesmo.

QUESTÕES DE CONCURSO

001. (Q4296855/INSTITUTO AOCP/SEJUSP MG/POLICIAL PENAL/2026) Durante uma vistoria de rotina em um dos computadores administrativos de uma unidade prisional, o policial penal percebe que o sistema apresenta lentidão, redirecionamentos automáticos ao acessar a intranet e janelas estranhas surgindo sem comando do usuário. O antivírus indica que a proteção em tempo real foi desativada sem autorização. O servidor responsável informa que, dias antes, recebeu um e-mail com o título "Atualização urgente do sistema de vigilância", contendo um arquivo compactado, que ele abriu acreditando ser um comunicado interno. Considerando as boas práticas de segurança digital e o uso adequado dos softwares utilitários, qual medida deve ser adotada para solucionar o problema identificado e prevenir novos incidentes semelhantes?
a) Reativar o firewall do sistema e compactar novamente o arquivo suspeito para posterior envio ao suporte técnico, evitando sua exclusão imediata.
b) Instalar um novo reprodutor de mídia, substituindo codecs corrompidos que possam estar causando lentidão e falhas no acesso à intranet.
c) Realizar uma varredura completa com um antivírus atualizado, eliminar os arquivos contaminados e restaurar a proteção automática, reforçando orientações sobre anexos compactados.
d) Reencaminhar o e-mail recebido para os demais servidores, incluindo um alerta de possível ameaça, a fim de confirmar se o problema ocorreu em outros setores.

002. (Q4419438/FEPESE/PREFEITURA DE CAXAMBU DO SUL/ASSISTENTE ADMINISTRATIVO/2026) Considerando as atividades de organização e atualização de arquivos e fichários previstas para o cargo, analise o cenário de gestão de arquivos digitais em um ambiente de rede municipal. Para garantir a integridade e a disponibilidade dos documentos públicos eletrônicos em caso de falha técnica no hardware do computador local, o procedimento técnico essencial é:
a) A exclusão de arquivos temporários da lixeira.
b) A compactação de todos os arquivos em pastas com senha no próprio computador local.
c) A realização periódica de cópias de segurança, armazenadas em local distinto da origem, como servidores de rede ou serviços de nuvem.
d) A desfragmentação semanal do disco rígido local.
e) A atualização constante dos softwares de edição de texto e planilhas utilizados para criar os documentos.

003. (Q4308321/CESGRANRIO/CEF/ENGENHEIRO CIVIL/2026) Os mecanismos de segurança são utilizados para implementar serviços de segurança. Um mecanismo pode operar por

conta própria ou em conjunto com outros para fornecer um serviço específico. Um dos principais mecanismos de segurança usa algoritmos matemáticos para transformar os dados em um código secreto e, subsequentemente, permite a recuperação dos dados através de um algoritmo e um ou mais segredos. Esse mecanismo de segurança é o de
a) assinatura digital
b) cifragem de dados simétrica
c) resumo de mensagem
d) certificação de chave pública
e) certificação de carimbo de tempo

004. (Q4340423/FCC/MPE AP/TÉCNICO MINISTERIAL/ÁREA APOIO ADMINISTRATIVO/2026) Em um ambiente corporativo de um Ministério Público Estadual, na qual são tratadas informações sensíveis e sigilosas, a adoção de procedimentos de segurança digital é fundamental para proteger a instituição contra ameaças cibernéticas. Entre essas ameaças, destacam-se os vírus, worms, malware, phishing e outras pragas virtuais, as quais podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados. Considerando as melhores práticas de segurança digital para a proteção de sistemas institucionais contra ameaças virtuais, um procedimento de prevenção eficaz e recomendado é
a) realizar backups completos dos dados sensíveis uma vez por ano, armazenando-os no mesmo servidor principal para agilizar a recuperação em caso de incidente.
b) configurar o navegador para armazenar automaticamente senhas de acesso a sistemas internos, facilitando o login rápido dos usuários e reduzindo a perda de tempo com digitação repetitiva.
c) implementar a verificação em duas etapas (2FA) para acessos a sistemas de email e redes internas, exigindo uma segunda forma de autenticação além da senha.
d) criar uma política de senhas que obrigue o uso de sequências numéricas simples, como datas de aniversário, para facilitar a memorização pelo usuário e evitar o registro em papéis.
e) permitir o acesso a links suspeitos contidos em e-mails, desde que o usuário utilize o computador em modo visitante, garantindo assim o isolamento de qualquer ameaça potencial.

005. (Q3934686/IDECAN/SEE/PB/PROFESSOR DE EDUCAÇÃO BÁSICA/ÁREA QUÍMICA/2025) Os aplicativos de segurança digital desempenham papéis distintos e complementares na proteção de sistemas contra ameaças cibernéticas. A escolha e a configuração adequada desses programas são essenciais para garantir a integridade e a confidencialidade das informações. Assim, marque a alternativa que descreve corretamente uma função de aplicativo de segurança digital.

a) Antivírus são eficazes contra todos os tipos de ameaças, incluindo ataques de negação de serviço (DDoS), pois monitoram o tráfego de rede em tempo real.
b) Firewalls detectam e removem malwares armazenados no disco rígido ao escanear periodicamente os arquivos do sistema.
c) Anti-spywares são projetados especificamente para detectar e remover softwares que coletam informações do usuário sem consentimento.
d) Programas anti-malware atuam apenas na prevenção de ameaças, sem capacidade de detectar arquivos já infectados.
e) Antivírus modernos não necessitam de atualizações constantes, pois utilizam algoritmos genéricos que detectam todas as novas ameaças automaticamente.

006. (Q3963632/QUADRIX/CONRERP SP/PR/ASSISTENTE ADMINISTRATIVO/2025) Vírus e malwares são problemas para a segurança de informação. Com base nessa informação, assinale a opção que apresenta a melhor combinação de ferramentas para proteção contra pragas virtuais, como vírus e Worms.
a) apenas um antivírus atualizado
b) firewall e proxy corporativo
c) antivírus, antispyware e firewall habilitados
d) backup semanal dos arquivos
e) reinstalação periódica do sistema operacional

007. (Q4144511/INSTITUTO AOCP/UENF/TÉCNICO – ÁREA: ASSISTENTE ADMINISTRATIVO/2025) A segurança na internet é fundamental para proteger dados sensíveis contra acessos não autorizados, fraudes e ataques cibernéticos. Dentre as diversas técnicas utilizadas, existe uma que transforma os dados em um formato ilegível para quem não possui a chave correta, garantindo a confidencialidade das informações durante o armazenamento ou a transmissão. Essa técnica de segurança digital é denominada
a) criptografia.
b) firewall.
c) antivírus.
d) phishing.
e) backup.

008. (Q3965754/FCC/TRT 2/ANALISTA JUDICIÁRIO – ÁREA: ADMINISTRATIVA/2025) A servidora Ana trabalha na vara cível de um tribunal e frequentemente acessa sistemas judiciais, manipula documentos sigilosos e recebe e-mails com arquivos anexos. Recentemente, percebeu lentidão no computador e janelas pop-up incomuns. Para evitar riscos à integridade

e confidencialidade das informações tratadas, Ana decide adotar boas práticas de segurança digital com base na ação correta e segura no contexto da administração pública, que é:
a) abrir os arquivos no e-mail institucional, pois isso garante que estão livres de vírus.
b) desativar temporariamente o antivírus para permitir a abertura de anexos recebidos por e-mail institucional, confiando que se trata de documentos judiciais.
c) manter o antivírus e o firewall ativados, evitar abrir anexos suspeitos e acionar a equipe de TI ao notar comportamentos anormais no sistema.
d) instalar softwares baixados de sites alternativos, desde que usados por colegas de trabalho a fim de agilizar o acesso aos documentos.
e) compartilhar senhas com colegas de equipe, desde que o objetivo seja facilitar o trabalho conjunto em processos urgentes.

009. (Q3845339/VUNESP/PREFEITURA MUNICIPAL/PROFESSOR DE EDUCAÇÃO BÁSICA/ÁREA: MATEMÁTICA/2025) Observe as afirmações numeradas a seguir:
I – Detecta, previne e remove software malicioso, como vírus, worms e trojans.
II – Controla o tráfego de entrada e saída de uma rede analisando pacotes de dados.
III – Coleta dados do computador e do usuário sem o seu consentimento.
Assinale a alternativa que correlaciona corretamente afirmações e seus respectivos conceitos.
a) I – Antivírus; II – Firewall.
b) I – Spyware; III – Antivírus.
c) I – Antivírus; II – Spyware.
d) II – Firewall; III – Antispyware.
e) II – Antivírus; III – Firewall.

010. (Q3810664/QUADRIX/CRMV TO/ASSISTENTE ADMINISTRATIVO/2025) Uma prática recomendada para que se identifiquem ou se evitem tentativas de phishing na Internet é
a) fornecer informações pessoais após verificar apenas a logomarca ou a identidade visual presente nas mensagens recebidas por e-mail.
b) confirmar imediatamente dados bancários clicando em links recebidos em e-mails com alertas sobre bloqueio ou problemas na conta.
c) utilizar regularmente programas antivírus atualizados e verificar cuidadosamente o endereço (URL) do site antes de inserir informações confidenciais.
d) informar dados pessoais ao receber ligações telefônicas de números desconhecidos que solicitam confirmação urgente, para se evitar o bloqueio de serviços.
e) responder diretamente aos e-mails suspeitos para solicitar esclarecimentos antes de enviar qualquer informação pessoal solicitada.

011. (Q3730271/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR/ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.
Sabendo-se que uma AC funciona como um terceiro confiável, se um documento for assinado digitalmente por um certificado digital de uma AC, esse tipo de identidade virtual permitirá a identificação segura e inequívoca do autor de uma mensagem.

012. (Q3822769/INSTITUTO AOCP/MPE RS/ANALISTA/ÁREA: DIREITO/2025) A segurança da informação abrange um conjunto de práticas e políticas voltadas para a proteção dos sistemas de informação contra ameaças digitais, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados. Nesse contexto, assinale a alternativa que apresenta uma ferramenta cuja principal função é a proteção contra vírus e malwares.
a) Avast.
b) Zoom.
c) Spotify.
d) AutoCAD.
e) Slack.

013. (Q3757826/CESPE/CEBRASPE/IBAMA/ANALISTA AMBIENTAL/ÁREA: PROTEÇÃO, LICENCIAMENTO, MONITORAMENTO E QUALIDADE AMBIENTAL/2025) Julgue os itens seguintes, considerando a arquitetura e os aspectos operacionais do MS Windows, bem como os aspectos funcionais de aplicativos de segurança da informação.
Suponha que certo aplicativo de segurança móvel utilize análise de comportamento para detecção de atividades suspeitas. Nesse caso, se um usuário realizar ações legítimas, mas incomuns, como acessar dados corporativos em um horário atípico e de um local diferente, o aplicativo sempre classificará essas ações como ameaças.

014. (Q3938169/IADES/CRMV PI/TÉCNICO ADMINISTRATIVO/2025) Muitos aplicativos e serviços on-line, para aumentar a segurança, exigem um segundo passo de verificação além da senha, geralmente por meio de um código enviado a um dispositivo móvel. Essa camada adicional de segurança é um exemplo de
a) autenticação de dois fatores.
b) backup na nuvem.
c) criptografia de ponta a ponta.
d) software de antivírus.
e) conexão por VPN.

015. (Q4233546/FUNDATEC/IGP/TÉCNICO EM ENFERMAGEM/2025) O processo de criar uma cópia de segurança de dados, com o objetivo de permitir a recuperação desses dados caso ocorra perda, dano, falha de hardware, ataque cibernético ou exclusão acidental é conhecido como:
a) Criptografia.
b) Restore.
c) Backup.
d) Storage.
e) Antivírus.

016. (Q3730268/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR – ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.
No âmbito de uma AC confiável, a assinatura digital possui autenticidade, integridade, confiabilidade e o não repúdio.

017. (Q4136409/FUNCERN/IFPE/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/2025) João está preocupado em perder seus arquivos importantes no computador. Para garantir a segurança dos seus dados, João deve
a) armazenar os arquivos e confiar que estarão sempre seguros sem a necessidade de cópias de segurança.
b) salvar arquivos importantes somente na pasta “Documentos”, pois isso garante a recuperação em caso de falha do sistema operacional.
c) ativar o antivírus, pois essa ação é suficiente para manter todos os arquivos preservados, e evitar a realização de backups.
d) efetuar cópias de segurança periódicas em dispositivos externos ou em serviços de nuvem.
e) guardar uma cópia de segurança na mesma partição, em diretórios distintos, pois garante o backup do arquivo.

018. (Q4206387/IDECAN/CBM DF/ASPIRANTE COMPLEMENTAR/ÁREA: DIREITO/2025) Um técnico em informática configura um computador conectado à internet em uma repartição pública e ativa um aplicativo que controla quais programas podem enviar ou receber dados pela rede, bloqueando conexões não autorizadas. O tipo de ferramenta utilizada nessa situação é conhecido como:
a) Antivírus.
b) Firewall.

c) Antispyware.
d) Antispam.

019. (Q4258419/IDECAN/CBM DF/BOMBEIRO MILITAR GERAL DE CONDUTOR E OPERADOR DE VIATURAS/2025) Um usuário percebe que seu navegador exibe anúncios constantes e redireciona para páginas desconhecidas ao digitar endereços. Esses sintomas indicam a presença de um programa que coleta seus dados de navegação sem permissão. O tipo de ferramenta necessária para remover essa ameaça é:
a) Firewall.
b) Navegador.
c) Antispyware.
d) Compactador.

020. (Q3941666/INSTITUTO AOCP/PREFEITURA DE SÃO LUÍS/PROFESSOR ANOS INICIAIS (1º AO 5º ANO DO ENSINO FUNDAMENTAL)/2025) Você, como professor da rede pública municipal de ensino de São Luís (MA), está ministrando uma aula sobre segurança digital para os alunos do ensino fundamental. Durante a explicação, você apresenta uma situação hipotética em que um estudante, ao acessar informações confidenciais de um projeto escolar, encontra esses dados em um formato ilegível, o que impede que terceiros não autorizados acessem essas informações. Ao explicar como garantir que os dados permaneçam protegidos e confidenciais, você deve esclarecer que a técnica responsável por essa proteção é a(o)
a) autenticação.
b) antivírus.
c) criptografiaa.
d) firewall.
e) phishing.

021. (Q3730265/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR/ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.
Assinatura digitalizada e assinatura digital, para fins de integridade, possuem as mesmas propriedades de integridade quanto à verificação de documentos eletrônicos.

022. (Q3476108/QUADRIX/CREF 9/AUXILIAR ADMINISTRATIVO/2024) Backups, autenticação multifator e firewalls são recursos de produção de um datacenter necessários para garantir a segurança e a capacidade de recuperação de incidentes e desastres. Com base nessa informação, assinale a alternativa correta.

a) A implementação de firewalls na rede não ajuda a bloquear tráfego malicioso nem prevenir contra ataques à rede.
b) O uso de autenticação multifator (MFA) reduz significativamente a segurança do acesso aos sistemas, pois complica o acesso para os usuários que tendem a fragilizar esse recurso.
c) Os backups regulares protegem contra falhas humanas no desenvolvimento de software.
d) Os backups periódicos de segurança devem ser guardados junto aos computadores para serem rapidamente utilizados em caso de necessidade.
e) A criptografia de dados é essencial para proteger informações sensíveis contra acessos não autorizados.

023. (Q3610032/IDECAN/PREFEITURA DE JOÃO PESSOA/AGENTE DE COMBATE ÀS ENDEMIAS/2024) Assinale a alternativa que apresenta um procedimento de segurança usado para proteger dados durante a transmissão através de redes inseguras.
a) Autenticação baseada em certificados.
b) Criptografia de ponta a ponta.
c) Hashing de senhas.
d) Uso de sítios com HTTP.
e) Criptografia de dados em repouso.

024. (Q3204082/IBADE/PREFEITURA DE VILA VELHA/AGENTE COMUNITÁRIO DE SAÚDE/2024) Leia o trecho e preencha a lacuna abaixo corretamente."_____ são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da sua conexão com a Internet. Eles representam uma primeira linha de defesa porque podem impedir que um programa ou invasor mal-intencionado obtenha acesso à sua rede e informações antes que qualquer dano potencial seja causado.
a) Nobreaks
b) Backups
c) Biometrias
d) Firewalls
e) Certificados digitais

025. (Q3151774/FGV/PREFEITURA DE CARAGUATATUBA/ANALISTA AMBIENTAL/2024) Um backup diferencial de um conjunto de arquivos copia para o meio de backup:
a) todos os arquivos que tenham uma extensão específica.
b) todos os arquivos maiores que um determinado tamanho.
c) todos os arquivos diferentes de um formato previamente especificado.
d) todos os arquivos criados ou alterados depois do último backup completo ou total.
e) todos os arquivos presentes no disco em questão que não estejam já marcados para cópia.

026. (Q3131253/CESPE/CEBRASPE/PREFEITURA DE CAMAÇARI/FISCAL/ÁREA: USO DO SOLO E MEIO AMBIENTE/2024) No que se refere aos procedimentos becape, identificação e manipulação de arquivos, assinale a opção correta.
a) Um arquivo é movido para a lixeira quando é recortado.
b) A ação de recortar arquivo cria uma cópia de becape do arquivo.
c) Arquivos de becape possuem extensão do tipo PDF.
d) Os arquivos excluídos podem ser restaurados da lixeira.
e) O sistema Windows não possui ferramenta nativa de becape.

027. (Q3380344/FGV/TCE PA/AUDITOR DE CONTROLE EXTERNO/ÁREA: ADMINISTRATIVA/ESPECIALIDADE: ENGENHARIA TELECOMUNICAÇÕES/2024) Os firewalls desempenham um papel fundamental na proteção dos dados sigilosos que trafegam na rede corporativa de um órgão público. Há diversos tipos, como firewall filtro de pacotes, firewall em estado de conexão e firewall em nível de aplicação. O firewall filtro de pacotes
a) permite detectar diversas ameaças à rede, por exemplo: spam, phishing e spyware.
b) permite distinguir entre os diferentes tipos de tráfego HTTP
c) mapeia todos os pacotes que entram e saem da rede interna, relacionando-os às conexões TCP/IP ativas.
d) inspeciona apenas os endereços IP e as portas TCP/UDP dos pacotes que entram e saem de uma rede interna, descartando aqueles que não atendem aos critérios estabelecidos pelo administrador de rede.
e) torna possível o envio de tráfego encriptado, garantindo assim a confidencialidade das informações e a privacidade dos dados.

028. (Q2703675/CESPE/CEBRASPE/POLC AL/PERITO ODONTOLEGISTA/2023) No que se refere a sistemas operacionais, pacotes office, navegadores e redes de computadores, julgue os itens que se seguem.
Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

029. (Q2700563/CESPE/CEBRASPE/POLC AL/PAPILOSCOPISTA/2023) No que se refere a sistemas operacionais, pacotes office, navegadores e redes de computadores, julgue os itens que se seguem.
Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de

invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

030. (Q2810389/IDCAP/IASES/AGENTE SOCIOEDUCATIVO/2023) São considerados programas antivírus, EXCETO:
a) Avast.
b) McAfee.
c) Kaspersky.
d) MySQL.
e) AVG.

031. (Q2674995/IADES/SEAGRI/DF/ANALISTA DE DESENVOLVIMENTO AGROPECUÁRIA/ÁREA ADMINISTRADOR/2023) Aplicativos de segurança conhecidos como antivírus monitoram o sistema para detectar arquivos maliciosos. Quando uma ameaça é detectada, o antivírus criptografa o arquivo suspeito e move-o para uma área segura do disco.
Esse tratamento denomina-se
a) varredura.
b) backup.
c) quarentena.
d) restauração.
e) desfragmentação.

032. (Q2832899/IBADE/PREFEITURA DE TARAUACÁ/TÉCNICO EM ENFERMAGEM/2023) Assinale a alternativa que corresponda a um exemplo de antivírus.
a) McAfee
b) SublimeText
c) CodeBlocks
d) MySQL
e) IBM Informix

033. (Q2823504/CESGRANRIO/BB/ESCRITURÁRIO/ÁREA: AGENTE COMERCIAL/2023) O Windows 10 possui um esquema de segurança nativo que fornece vários tipos de proteção contra ameaças ao sistema.
A ferramenta antivírus, integrada ao Windows 10, que ajuda a proteger o computador do usuário contra vírus, ransomware e outros malwares é a
a) Microsoft Defender Antivirus
b) Microsoft Defender Protection
c) Microsoft Malware Alert

d) Microsoft Malware Protection
e) Microsoft Antivirus Protection

034. (Q2805117/SELECON/PREFEITURA DE NOVA MUTUM/INSTRUTOR DE INFORMÁTICA/2023) Uma empresa de comércio eletrônico pretende utilizar um mecanismo de criptografia para gerenciar a comunicação de seus clientes com as suas lojas instaladas em sites. Esse mecanismo vai utilizar uma mesma chave criptografada tanto para codificar como para decodificar informações, sendo usada, principalmente, para garantir a confidencialidade dos dados. Esse tipo de chave de criptografia é denominado de chave:
a) hash
b) virtual
c) simétrica
d) assimétrica

035. (Q2866764/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA TECNOLOGIA DA INFORMAÇÃO/2023) No que diz respeito aos conceitos de proteção e de segurança da informação, julgue os itens.
A criptografia assimétrica, a qual utiliza um par de chaves, é uma das técnicas utilizadas para que os dados sejam criptografados de forma segura.

036. (Q2817646/INSTITUTO CONSULPLAN/FEPAM/TÉCNICO EM ADMINISTRAÇÃO/2023) As ferramentas para segurança da informação são o conjunto de software, hardware e técnicas que têm como principal objetivo combater os ataques. A técnica utilizada para cifrar uma informação, tornando-a incompreensível, exceto para o destinatário e o transmissor que sabem como decifrá-la é:
a) Proxy.
b) Firewall.
c) Antivírus.
d) Criptografia.
e) Sistema de Detecção de Intrusos (IDS).

037. (Q2734022/FUNDEP/PREFEITURA DE LAVRAS/PROFESSOR/ÁREA: GEOGRAFIA/2023) A técnica que transforma, por meio de chaves ou códigos, informação inteligível em algo que um agente externo seja incapaz de compreender é chamada de
a) senha.
b) autenticação em duas etapas.
c) criptografia.
d) token.

038. (Q2824611/MS CONCURSOS/PREFEITURA DE TURVELÂNDIA/PROFESSOR/ÁREA: MATEMÁTICA/2023) Considere a afirmativa: "A criptografia apresenta práticas ou processos para tornar segura a comunicação entre partes. Um dos métodos conhecidos é a utilização de uma chave para encriptar o conteúdo de uma mensagem em uma informação cifrada e decriptar a mensagem cifrada com essa mesma chave para obter o dado original.". Sobre a utilização de técnicas de criptografia para Certificados Digitais e Assinaturas Digitais, a alternativa que apresenta corretamente o conceito da afirmativa é:
a) A afirmativa corresponde à Criptografia Simétrica, que pode reforçar a confidencialidade de dados, mas como a mesma chave é usada para encriptar e decriptar a informação, a técnica por si só não garante a Irretratabilidade no caso do uso como Certificado Digital.
b) A afirmativa corresponde a uma função de Hash, muito utilizada em Certificados Digitais para cifrar mensagens confidenciais e garantir a Integridade dos dados, uma vez que é necessário conhecer a chave para acessar seu conteúdo.
c) A afirmativa corresponde à Criptografia Assimétrica, medida de segurança utilizada em Certificados Digitais para garantir que a assinatura de um documento corresponde corretamente à pessoa que o assinou, pois apenas as partes interessadas conhecem a chave utilizada para cifrar o conteúdo da mensagem.
d) A afirmativa corresponde ao processo utilizado em Certificados Digitais, em que uma empresa reconhecida e confiável vincula a chave utilizada para criptografar a Assinatura Digital a seu titular.

039. (Q2920394/SELECON/CREA RJ/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2023) A utilização de um certificado digital, emitido por uma autoridade certificadora, para gerar uma assinatura digital em um documento, tem como uma de suas característica:
a) utilizar a chave pública de quem assina
b) garantir a confidencialidade desse documento
c) proteger o documento contra falhas de hardware
d) autenticar o conteúdo no momento da assinatura
e) estabelecer uma conexão segura entre origem e destino

040. (Q2687175/FUNDAÇÃO CEFETMINAS/PREFEITURA DE CONTAGEM/AGENTE FAZENDÁRIO/2023) Certificados digitais podem ser utilizados na troca de informação entre pessoas na internet.
São dados que compõem um certificado digital, EXCETO o(a)
a) número de série do certificado.
b) código de integridade do software de criptografia.
c) identificação da pessoa que é dona do certificado.

d) identificação da autoridade certificadora emissora do certificado.
e) assinatura digital da autoridade certificadora emissora do certificado.

041. (Q2823632/CESGRANRIO/BB/ESCRITURÁRIO/ÁREA: AGENTE COMERCIAL/2023) O mecanismo de segurança é um método ou processo que pode ser utilizado por um sistema para implementar um serviço de segurança. Para verificar a autenticidade ou a autoria de um documento com relação ao seu signatário, deve-se validar a(o)
a) envelope digital
b) assinatura digital
c) criptograma simétrico
d) chave simétrica
e) algoritmo simétrico

042. (Q2719827/SELECON/PREVILUCAS/ADVOGADO/2023) Uma característica essencial de uma assinatura digital em uma determinada mensagem ou arquivo (por exemplo, um documento em PDF) é:
a) confidencialidade da mensagem
b) garantia de disponibilidade e acesso à mensagem
c) controle de acesso à mensagem
d) autenticação da origem e integridade da mensagem

043. (Q2695313/COPEVE/UFAL/FUNDEPES/IFAL/ASSISTENTE EM ADMINISTRAÇÃO/2023) Em algumas organizações comerciais ou até mesmo em certos países, o acesso a determinados sites ou tipos de conteúdo são bloqueados. Os motivos por trás dos bloqueios são diversos, desde o local onde estão publicados (sites), como o fato de tais endereços ou serviços serem considerados inseguros ou suspeitos. Qual ferramenta poderia ser utilizada para realizar as ações de bloqueio, descritas anteriormente?
a) Spam
b) Cookies
c) Firewall
d) Antivírus
e) Anti Spyware

044. (Q2708555/IBFC/PREFEITURA DE CUIABÁ/ESPECIALISTA EM SAÚDE/ÁREA: QUÍMICO/2023) Quanto às características dos programas Antivírus e ao Firewall, analise as afirmativas a seguir e dê valores Verdadeiro (V) ou Falso (F).

( ) O firewall é um sistema de segurança de rede de computadores que limita o tráfego de entrada e/ou saída dentro de uma rede.
( ) Se numa instalação já tiver um firewall será desnecessário instalar adicionalmente um programa Antivírus, em termos de segurança de dados.
( ) A concepção de um firewall atual pode-se considerar tecnicamente como sendo a terceira geração evolutiva dos antigos programas Antivírus.

Assinale a alternativa que apresenta a sequência correta de cima para baixo.
a) V – F – F
b) V – V – F
c) F – V – V
d) F – F – V

045. (Q2937944/FGV/DPE RS/TÉCNICO APOIO ESPECIALIZADO/ÁREA: SUPORTE DE TI/2023) Amanda enviou uma mensagem à Virgínia que deve efetuar a verificação de assinatura feita por Amanda para o pacote. O processo de verificação de assinatura digital a ser executado por Virgínia consiste em alguns passos, nos quais ela deve decifrar a:
a) assinatura digital, com a chave pública de Amanda contida no certificado digital, obtendo o sumário da mensagem gerado e cifrado por Amanda na assinatura;
b) assinatura digital, com a chave pública de Virgínia contida no certificado digital, obtendo o código digital gerado e cifrado pela Autoridade Certificadora;
c) criptografia, com a chave privada de Virgínia contida no código digital gerado e cifrado por Amanda, para a emissão do certificado;
d) assinatura digital, com a chave privada de Amanda contida no resumo criptográfico gerado e cifrado por Virgínia, quando da aquisição do certificado;
e) criptografia, com a chave pública de Virgínia a qual foi enviada por broadcast a todos os usuários da rede.

046. (Q2931181/OBJETIVA CONCURSOS/PREFEITURA DE NOVO ITACOLOMI/PROFESSOR DE EDUCAÇÃO FÍSICA/2023) Para maximizar a segurança do usuário, é fundamental que, ao criar uma senha nova, alguns cuidados sejam tomados. Assinalar a alternativa que NÃO representa um comportamento adequado ou seguro na hora de elaborar uma nova senha:
a) Utilizar caracteres aleatórios.
b) Misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas.
c) Evitar senhas parecidas com senhas que você já utiliza.
d) Utilizar a mesma senha para o máximo de coisas que puder.

047. (Q2818790/OBJETIVA CONCURSOS/CÂMARA DE SÃO JOÃO DO MANHUAÇU/TESOUREIRO/2023) A respeito das boas práticas ao criar senhas de acesso a sites da internet, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

( ) Ao criar uma senha na internet, não é recomendado utilizar dados pessoais, como nome e sobrenome.
( ) Utilizar senhas com números sequenciais do teclado, como 123456, facilita a identificação da senha por terceiros.
( ) A variação entre números, letras maiúsculas e minúsculas e caracteres especiais não aumenta a segurança da senha.

a) C – C – E.
b) E – E – C.
c) C – E – E.
d) E – C – C.

048. (Q2684985/QUADRIX/CRO/AGENTE FISCAL/2023) A respeito dos procedimentos de segurança da informação e backup, julgue os itens.
Para adicionar maior proteção ao processo de autenticação de usuários, o uso de autenticação multifator (MFA) é indicado, porque adiciona duas ou mais camadas diferentes de verificação adicionais, como uso de aplicativos de autenticação, tokens físicos, reconhecimento facial e biometria.

049. (Q2866762/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA TECNOLOGIA DA INFORMAÇÃO/2023) No que diz respeito aos conceitos de proteção e de segurança da informação, julgue os itens.
A autenticação em duas etapas, ou em dois fatores, como é comumente chamada, é considerada uma medida ineficaz para o aumento da segurança do computador e para a proteção das contas on-line, já que sua finalidade é, especificamente, o bloqueio dos pacotes duvidosos que trafegam pela Internet.

050. (Q2851272/FGV/PGM/TÉCNICO EM PROCURADORIA/2023) Julia usa senhas fortes em suas contas digitais, mas quer elevar o seu nível de segurança. Para isso, consultou o técnico de informática Matheus que a orientou a adicionar uma segunda camada de proteção no acesso às suas contas. Assim, mesmo que o atacante descubra sua senha, ele precisará de outras informações para invadir sua conta. Matheus completou dizendo: “Escolha o método

que considerar mais prático e seguro, como: usar um aplicativo de celular para gerar códigos de verificação; ou receber códigos por mensagem de texto ou voz.” A proteção sugerida por Matheus é o(a):

a) Antispam;

b) Firewall pessoal;

c) Certificado digital;

d) Gerenciador de senha;

e) Verificação em duas etapas.

GABARITO

1. c
2. c
3. b
4. c
5. c
6. c
7. a
8. c
9. a
10. c
11. C
12. a
13. E
14. a
15. c
16. C
17. d
18. b
19. c
20. c
21. E
22. e
23. b
24. d
25. d
26. d
27. d
28. E
29. E
30. d
31. c
32. a
33. a
34. c
35. C
36. d
37. c
38. a
39. d
40. b
41. b
42. d
43. c
44. a
45. a
46. d
47. a
48. C
49. E
50. e

GABARITO COMENTADO

001. (Q4296855/INSTITUTO AOCP/SEJUSP MG/POLICIAL PENAL/2026) Durante uma vistoria de rotina em um dos computadores administrativos de uma unidade prisional, o policial penal percebe que o sistema apresenta lentidão, redirecionamentos automáticos ao acessar a intranet e janelas estranhas surgindo sem comando do usuário. O antivírus indica que a proteção em tempo real foi desativada sem autorização. O servidor responsável informa que, dias antes, recebeu um e-mail com o título "Atualização urgente do sistema de vigilância", contendo um arquivo compactado, que ele abriu acreditando ser um comunicado interno. Considerando as boas práticas de segurança digital e o uso adequado dos softwares utilitários, qual medida deve ser adotada para solucionar o problema identificado e prevenir novos incidentes semelhantes?

a) Reativar o firewall do sistema e compactar novamente o arquivo suspeito para posterior envio ao suporte técnico, evitando sua exclusão imediata.

b) Instalar um novo reprodutor de mídia, substituindo codecs corrompidos que possam estar causando lentidão e falhas no acesso à intranet.

c) Realizar uma varredura completa com um antivírus atualizado, eliminar os arquivos contaminados e restaurar a proteção automática, reforçando orientações sobre anexos compactados.

d) Reencaminhar o e-mail recebido para os demais servidores, incluindo um alerta de possível ameaça, a fim de confirmar se o problema ocorreu em outros setores.

Esse foi um golpe do tipo scareware, no qual o golpista utiliza uma situação alarmante e assustadora para colocar o usuário em uma condição de urgência e, consequentemente, instalar a ameaça em sua máquina. Pelo comportamento apresentado, identifica-se que houve ações de algum vírus, visto que está abrindo janelas indevidamente, redirecionamentos e inativação do próprio antivírus. Diante dessa situação, a melhor ação a ser realizada é executar uma varredura completa da memória e dos discos de armazenamento por meio do antivírus. Porém, é necessário também orientar os usuários para que não abram arquivos anexos suspeitos.

Letra c.

---

002. (Q4419438/FEPESE/PREFEITURA DE CAXAMBU DO SUL/ASSISTENTE ADMINISTRATIVO/2026) Considerando as atividades de organização e atualização de arquivos e fichários previstas para o cargo, analise o cenário de gestão de arquivos digitais em um ambiente de rede municipal.

Para garantir a integridade e a disponibilidade dos documentos públicos eletrônicos em caso de falha técnica no hardware do computador local, o procedimento técnico essencial é:
a) A exclusão de arquivos temporários da lixeira.
b) A compactação de todos os arquivos em pastas com senha no próprio computador local.
c) A realização periódica de cópias de segurança, armazenadas em local distinto da origem, como servidores de rede ou serviços de nuvem.
d) A desfragmentação semanal do disco rígido local.
e) A atualização constante dos softwares de edição de texto e planilhas utilizados para criar os documentos.

O foco da questão é a integridade e a disponibilidade dos arquivos, sendo que o backup é uma ferramenta que atende a ambos os requisitos de segurança. O backup garante a integridade, na medida em que a corrupção de arquivos viola tal princípio, e a restauração de cópias de segurança traz os dados à sua condição original de integridade. Por outro lado, o backup também garante a disponibilidade, pois, uma vez corrompidos os dados, eles se tornam, consequentemente, indisponíveis; porém, a restauração do backup traz de volta os dados para que sejam acessados novamente.
Letra c.

---

003. (Q4308321/CESGRANRIO/CEF/ENGENHEIRO CIVIL/2026) Os mecanismos de segurança são utilizados para implementar serviços de segurança. Um mecanismo pode operar por conta própria ou em conjunto com outros para fornecer um serviço específico. Um dos principais mecanismos de segurança usa algoritmos matemáticos para transformar os dados em um código secreto e, subsequentemente, permite a recuperação dos dados através de um algoritmo e um ou mais segredos. Esse mecanismo de segurança é o de
a) assinatura digital
b) cifragem de dados simétrica
c) resumo de mensagem
d) certificação de chave pública
e) certificação de carimbo de tempo

Veja a utilidade de cada uma das ferramentas da questão.
a) Errada. **Assinatura Digital**: garante a autenticidade, a integridade e o não repúdio de um documento eletrônico através de criptografia assimétrica.
b) Certa. **Cifragem de Dados Simétrica**: codifica a informação utilizando uma única chave secreta para garantir a confidencialidade durante o armazenamento ou transmissão.

c) Errada. **Resumo de Mensagem** (**Hash**): transforma um volume de dados em uma sequência fixa de caracteres para verificar se o conteúdo original foi alterado.
d) Errada. **Certificação de Chave Pública**: vincula a identidade de uma entidade a uma chave criptográfica por meio de um certificado emitido por uma autoridade confiável.
e) Errada. **Certificação de Carimbo de Tempo**: prova legalmente que um documento ou assinatura digital existia em uma data e hora específicas.
Letra b.

---

004. (Q4340423/FCC/MPE AP/TÉCNICO MINISTERIAL/ÁREA APOIO ADMINISTRATIVO/2026) Em um ambiente corporativo de um Ministério Público Estadual, na qual são tratadas informações sensíveis e sigilosas, a adoção de procedimentos de segurança digital é fundamental para proteger a instituição contra ameaças cibernéticas. Entre essas ameaças, destacam-se os vírus, worms, malware, phishing e outras pragas virtuais, as quais podem comprometer a integridade, a confidencialidade e a disponibilidade dos dados. Considerando as melhores práticas de segurança digital para a proteção de sistemas institucionais contra ameaças virtuais, um procedimento de prevenção eficaz e recomendado é
a) realizar backups completos dos dados sensíveis uma vez por ano, armazenando-os no mesmo servidor principal para agilizar a recuperação em caso de incidente.
b) configurar o navegador para armazenar automaticamente senhas de acesso a sistemas internos, facilitando o login rápido dos usuários e reduzindo a perda de tempo com digitação repetitiva.
c) implementar a verificação em duas etapas (2FA) para acessos a sistemas de email e redes internas, exigindo uma segunda forma de autenticação além da senha.
d) criar uma política de senhas que obrigue o uso de sequências numéricas simples, como datas de aniversário, para facilitar a memorização pelo usuário e evitar o registro em papéis.
e) permitir o acesso a links suspeitos contidos em e-mails, desde que o usuário utilize o computador em modo visitante, garantindo assim o isolamento de qualquer ameaça potencial.

Nesta questão, é interessante sabermos por que as demais alternativas estão incorretas. Vejamos:
a) Errada. Realizar backups completos dos dados sensíveis apenas uma vez por ano constitui um período muito grande de dados sem cópias de segurança. Além disso, armazená-los no mesmo servidor principal, embora possa agilizar a recuperação em caso de incidente, causa um grande risco em caso de o servidor sofrer alguma danificação.
b) Errada. Em um ambiente corporativo, armazenar automaticamente as senhas no navegador pode expor tais dados sigilosos a outros usuários, em caso de computador compartilhado.

c) Certa. A implementação da 2FA fortalece o processo de autenticação, pelo fato de as senhas poderem sofrer vazamento, e uma outra forma de verificar a identidade do usuário se torna uma camada extra de proteção.
d) Errada. O uso de sequências numéricas simples, como datas de aniversário, acarreta vulnerabilidade, visto ser uma forma não segura de senhas, pois cria senhas fracas.
e) Errada. O modo visitante não proporciona proteção na navegação contra o acesso a links suspeitos.
Letra c.

---

005. (Q3934686/IDECAN/SEE/PB/PROFESSOR DE EDUCAÇÃO BÁSICA/ÁREA QUÍMICA/2025) Os aplicativos de segurança digital desempenham papéis distintos e complementares na proteção de sistemas contra ameaças cibernéticas. A escolha e a configuração adequada desses programas são essenciais para garantir a integridade e a confidencialidade das informações. Assim, marque a alternativa que descreve corretamente uma função de aplicativo de segurança digital.
a) Antivírus são eficazes contra todos os tipos de ameaças, incluindo ataques de negação de serviço (DDoS), pois monitoram o tráfego de rede em tempo real.
b) Firewalls detectam e removem malwares armazenados no disco rígido ao escanear periodicamente os arquivos do sistema.
c) Anti-spywares são projetados especificamente para detectar e remover softwares que coletam informações do usuário sem consentimento.
d) Programas anti-malware atuam apenas na prevenção de ameaças, sem capacidade de detectar arquivos já infectados.
e) Antivírus modernos não necessitam de atualizações constantes, pois utilizam algoritmos genéricos que detectam todas as novas ameaças automaticamente.

Vejamos cada uma das ferramentas de proteção.
a) Errada. Antivírus são eficazes contra muitos, mas não todos os tipos de ameaças. Ataques de negação de serviço (DDoS) são evitados por meio de firewall e não de antivírus, pois os firewalls monitoram o tráfego de rede em tempo real.
b) Errada. São os antivírus/antimalwares que detectam e removem malwares armazenados no disco rígido ao escanear periodicamente os arquivos do sistema, não os firewalls.
c) Certa. De fato, os anti-spywares são focados na detecção e remoção de softwares que coletam informações do usuário sem consentimento.

d) Errada. Programas anti-malware atuam tanto na prevenção de ameaças quanto na detecção e remoção de arquivos já infectados.
e) Errada. Todos os antivírus necessitam de atualizações constantes, pois é a assinatura ou "vacina" que os torna aptos a detectar as ameaças nos demais arquivos e programas.
Letra c.

---

006. (Q3963632/QUADRIX/CONRERP SP/PR/ASSISTENTE ADMINISTRATIVO/2025) Vírus e malwares são problemas para a segurança de informação. Com base nessa informação, assinale a opção que apresenta a melhor combinação de ferramentas para proteção contra pragas virtuais, como vírus e Worms.
a) apenas um antivírus atualizado
b) firewall e proxy corporativo
c) antivírus, antispyware e firewall habilitados
d) backup semanal dos arquivos
e) reinstalação periódica do sistema operacional

A combinação das três ferramentas aumenta a proteção do ambiente cibernético, impedindo infecções dos mais variados tipos de software malicioso, detectando e removendo-os, bem como evitando a intrusão indesejada por meio de firewalls.
Letra c.

---

007. (Q4144511/INSTITUTO AOCP/UENF/TÉCNICO – ÁREA: ASSISTENTE ADMINISTRATIVO/2025) A segurança na internet é fundamental para proteger dados sensíveis contra acessos não autorizados, fraudes e ataques cibernéticos. Dentre as diversas técnicas utilizadas, existe uma que transforma os dados em um formato ilegível para quem não possui a chave correta, garantindo a confidencialidade das informações durante o armazenamento ou a transmissão. Essa técnica de segurança digital é denominada
a) criptografia.
b) firewall.
c) antivírus.
d) phishing.
e) backup.

A criptografia é a ferramenta de proteção que garante o princípio da confidencialidade das informações, pois torna os dados ininteligíveis ou inacessíveis.
Letra a.

---

008. (Q3965754/FCC/TRT 2/ANALISTA JUDICIÁRIO – ÁREA: ADMINISTRATIVA/2025) A servidora Ana trabalha na vara cível de um tribunal e frequentemente acessa sistemas judiciais, manipula documentos sigilosos e recebe e-mails com arquivos anexos. Recentemente, percebeu lentidão no computador e janelas pop-up incomuns. Para evitar riscos à integridade e confidencialidade das informações tratadas, Ana decide adotar boas práticas de segurança digital com base na ação correta e segura no contexto da administração pública, que é:
a) abrir os arquivos no e-mail institucional, pois isso garante que estão livres de vírus.
b) desativar temporariamente o antivírus para permitir a abertura de anexos recebidos por e-mail institucional, confiando que se trata de documentos judiciais.
c) manter o antivírus e o firewall ativados, evitar abrir anexos suspeitos e acionar a equipe de TI ao notar comportamentos anormais no sistema.
d) instalar softwares baixados de sites alternativos, desde que usados por colegas de trabalho a fim de agilizar o acesso aos documentos.
e) compartilhar senhas com colegas de equipe, desde que o objetivo seja facilitar o trabalho conjunto em processos urgentes.

Vejamos as alternativas que apresentam ações incorretas e aquela que é a correta, bem como seus motivos.
a) Errada. Abrir os arquivos no e-mail institucional é uma vulnerabilidade, pois tais arquivos não estão livres de vírus.
b) Errada. Desativar temporariamente o antivírus causa vulnerabilidade, pois os arquivos anexos recebidos por e-mail institucional podem estar infectados por vírus ou outros tipos de malware.
c) Certa. Manter o antivírus e o firewall ativados, evitar abrir anexos suspeitos e acionar a equipe de TI ao notar comportamentos anormais no sistema são medidas de segurança, cada uma delas.
d) Errada. Instalar softwares baixados de sites alternativos é uma ação de vulnerabilidade, pois tais sites podem oferecer softwares infectados para download.
e) Errada. O compartilhamento de senhas com colegas de equipe as expõe de forma a serem usadas indevidamente.
Letra c.

---

009. (Q3845339/VUNESP/PREFEITURA MUNICIPAL/PROFESSOR DE EDUCAÇÃO BÁSICA/ÁREA: MATEMÁTICA/2025) Observe as afirmações numeradas a seguir:
I – Detecta, previne e remove software malicioso, como vírus, worms e trojans.
II – Controla o tráfego de entrada e saída de uma rede analisando pacotes de dados.

III – Coleta dados do computador e do usuário sem o seu consentimento.
Assinale a alternativa que correlaciona corretamente afirmações e seus respectivos conceitos.
a) I – Antivírus; II – Firewall.
b) I – Spyware; III – Antivírus.
c) I – Antivírus; II – Spyware.
d) II – Firewall; III – Antispyware.
e) II – Antivírus; III – Firewall.

I – Antivírus: detecta, previne e remove software malicioso, como vírus, worms e trojans.
II – Firewall: controla o tráfego de entrada e saída de uma rede, analisando pacotes de dados.
III – Spyware: coleta dados do computador e do usuário sem o seu consentimento.
Letra a.

---

010. (Q3810664/QUADRIX/CRMV TO/ASSISTENTE ADMINISTRATIVO/2025) Uma prática recomendada para que se identifiquem ou se evitem tentativas de phishing na Internet é
a) fornecer informações pessoais após verificar apenas a logomarca ou a identidade visual presente nas mensagens recebidas por e-mail.
b) confirmar imediatamente dados bancários clicando em links recebidos em e-mails com alertas sobre bloqueio ou problemas na conta.
c) utilizar regularmente programas antivírus atualizados e verificar cuidadosamente o endereço (URL) do site antes de inserir informações confidenciais.
d) informar dados pessoais ao receber ligações telefônicas de números desconhecidos que solicitam confirmação urgente, para se evitar o bloqueio de serviços.
e) responder diretamente aos e-mails suspeitos para solicitar esclarecimentos antes de enviar qualquer informação pessoal solicitada.

O phishing é um golpe que utiliza o e-mail, geralmente imitando uma instituição conhecida, contendo um link que direciona para uma página fraudulenta ou um download de arquivo infectado com spyware. Para evitar essas ameaças, é preciso verificar o URL do site antes de inserir informações confidenciais. No caso de ser um link para download, o uso de antivírus é importante para evitar a infecção.
Letra c.

---

011. (Q3730271/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR/ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação

digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.
Sabendo-se que uma AC funciona como um terceiro confiável, se um documento for assinado digitalmente por um certificado digital de uma AC, esse tipo de identidade virtual permitirá a identificação segura e inequívoca do autor de uma mensagem.

AC é a Autoridade Certificadora, a qual emite os certificados digitais, sendo o "terceiro confiável". Tais certificados digitais permitem assegurar a autenticidade do documento, ou seja, garantem a veracidade da autoria do documento de forma inquestionável e inconfundível.
Certo.

---

012. (Q3822769/INSTITUTO AOCP/MPE RS/ANALISTA/ÁREA: DIREITO/2025) A segurança da informação abrange um conjunto de práticas e políticas voltadas para a proteção dos sistemas de informação contra ameaças digitais, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados. Nesse contexto, assinale a alternativa que apresenta uma ferramenta cuja principal função é a proteção contra vírus e malwares.
a) Avast.
b) Zoom.
c) Spotify.
d) AutoCAD.
e) Slack.

Veja o significado de cada aplicativo.
a) Certa. **Avast**: software de segurança focado na proteção contra malwares, vírus e ameaças cibernéticas em tempo real.
b) Errada. **Zoom**: plataforma de videoconferência e comunicação unificada para reuniões remotas, webinars e chats colaborativos.
c) Errada. **Spotify**: serviço de streaming que oferece acesso instantâneo a um vasto catálogo de músicas, podcasts e vídeos digitais.
d) Errada. **AutoCAD**: software de projeto auxiliado por computador (CAD) utilizado para a criação precisa de desenhos técnicos em 2D e 3D.
e) Errada. **Slack**: ferramenta de comunicação corporativa baseada em canais que centraliza mensagens, arquivos e integração de fluxos de trabalho.
Letra a.

---

013. (Q3757826/CESPE/CEBRASPE/IBAMA/ANALISTA AMBIENTAL/ÁREA: PROTEÇÃO, LICENCIAMENTO, MONITORAMENTO E QUALIDADE AMBIENTAL/2025) Julgue os itens seguintes, considerando a arquitetura e os aspectos operacionais do MS Windows, bem como os aspectos funcionais de aplicativos de segurança da informação.
Suponha que certo aplicativo de segurança móvel utilize análise de comportamento para detecção de atividades suspeitas. Nesse caso, se um usuário realizar ações legítimas, mas incomuns, como acessar dados corporativos em um horário atípico e de um local diferente, o aplicativo sempre classificará essas ações como ameaças.

Aqui, a palavra "sempre" tornou a questão falsa. De fato, tal comportamento suspeito pode acionar um alerta quando combinado com outros atributos, como acesso a partir de um dispositivo móvel que não seja o do usuário ou ainda em um horário incomum ao expediente, como às 3h da manhã, juntamente com várias tentativasde autenticação malsucedidas.
Errado.

---

014. (Q3938169/IADES/CRMV PI/TÉCNICO ADMINISTRATIVO/2025) Muitos aplicativos e serviços on-line, para aumentar a segurança, exigem um segundo passo de verificação além da senha, geralmente por meio de um código enviado a um dispositivo móvel. Essa camada adicional de segurança é um exemplo de
a) autenticação de dois fatores.
b) backup na nuvem.
c) criptografia de ponta a ponta.
d) software de antivírus.
e) conexão por VPN.

A autenticação em dois fatores (2FA), ou também MFA (Multifator de Autenticação), aplica uma camada adicional ao processo de autenticação para validar a identidade do usuário. Tal procedimento exige o envio de um código de confirmação a partir de um meio que somente o titular do login tenha acesso, como um aplicativo autenticador (ex.: MS Authenticator, Google Authenticator); uma chave física de acesso que possui um PIN cadastrado pelo titular, a qual exige seu toque físico para prosseguir na autenticação; ou um código de acesso enviado por e-mail ou por SMS.
Letra a.

---

015. (Q4233546/FUNDATEC/IGP/TÉCNICO EM ENFERMAGEM/2025) O processo de criar uma cópia de segurança de dados, com o objetivo de permitir a recuperação desses dados caso ocorra perda, dano, falha de hardware, ataque cibernético ou exclusão acidental é conhecido como:

a) Criptografia.
b) Restore.
c) Backup.
d) Storage.
e) Antivírus.

Essa foi uma questão bem fácil, não foi mesmo? Vejamos as definições das demais ferramentas elencadas nas alternativas.

a) Errada. **Criptografia**: técnica que utiliza algoritmos para transformar dados em um formato ilegível, garantindo que apenas pessoas autorizadas acessem a informação.

b) Errada. **Restore**: processo de recuperação e retorno dos dados salvos em uma cópia de segurança para o seu estado original ou funcional.

c) Certa. **Backup**: criação de uma cópia de segurança dos dados para permitir a recuperação em caso de perda, falha ou corrupção do sistema.

d) Errada. **Storage**: dispositivo ou infraestrutura tecnológica dedicada ao armazenamento e organização de grandes volumes de dados digitais.

e) Errada. **Antivírus**: programa desenvolvido para detectar, prevenir e remover softwares maliciosos que possam comprometer a segurança do dispositivo.

Letra c.

---

016. (Q3730268/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR – ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.

No âmbito de uma AC confiável, a assinatura digital possui autenticidade, integridade, confiabilidade e o não repúdio.

Quando se fala “no âmbito de uma AC confiável”, significa que estamos falando de assinaturas digitais com certificados digitais ICP-Brasil, o mais alto nível de segurança de assinaturas eletrônicas. Ela oferece autenticidade, pois permite validar a veracidade da autoria de uma informação. Oferece também integridade, pois permite identificar alterações não autorizadas no documento após sua assinatura. Oferece “confiabilidade”, não “confidencialidade”;

atenção! Aqui, confiabilidade é a característica de a ferramenta entregar aquilo que ela se propõe, ou seja, ela é realmente capaz de oferecer a autenticidade e a integridade. Por fim, ela oferece não repúdio ou irretratabilidade, que é a impossibilidade da negação da autoria da informação, isto é, o titular da informação não pode negar que foi seu autor após ter realizado a autenticação.

Certo.

---

017. (Q4136409/FUNCERN/IFPE/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/2025) João está preocupado em perder seus arquivos importantes no computador. Para garantir a segurança dos seus dados, João deve

a) armazenar os arquivos e confiar que estarão sempre seguros sem a necessidade de cópias de segurança.

b) salvar arquivos importantes somente na pasta "Documentos", pois isso garante a recuperação em caso de falha do sistema operacional.

c) ativar o antivírus, pois essa ação é suficiente para manter todos os arquivos preservados, e evitar a realização de backups.

d) efetuar cópias de segurança periódicas em dispositivos externos ou em serviços de nuvem.

e) guardar uma cópia de segurança na mesma partição, em diretórios distintos, pois garante o backup do arquivo.

A questão pede que você identifique qual das alternativas é um procedimento que garante a segurança dos dados contra a perda de arquivos. Vamos analisar cada uma das alternativas.

a) Errada. Não garante a segurança, pois armazenar os arquivos sem cópias de segurança é um grande risco em caso de perda ou corrupção dos arquivos, podendo haver a possibilidade de perda total e completa.

b) Errada. Não garante a segurança, pois salvar arquivos importantes somente na pasta "Documentos" do sistema operacional não garante a recuperação em caso de falha do sistema operacional. É preciso realizar cópias de segurança ou sincronizar essa pasta com o armazenamento em nuvem da própria Microsoft, o OneDrive, ou de outro provedor.

c) Errada. Não garante a segurança, pois apenas ativar o antivírus não é suficiente para manter todos os arquivos preservados, sem a realização de backups. Como vimos, caso ocorra corrupção dos arquivos, eles poderão ser perdidos definitivamente.

d) Certa. Essa ação garante a segurança, pois efetuar cópias de segurança periódicas em dispositivos externos ou em serviços de nuvem permite sua recuperação em caso de perda

de tais arquivos. Embora não seja totalmente suficiente para garantir a proteção total, para o objetivo de evitar a perda de arquivos, ela é suficiente.
e) Errada. Não garante a segurança, pois guardar uma cópia de segurança na mesma partição, porém em diretórios distintos, não garante o backup do arquivo, visto que, em caso de pane no sistema operacional que exija formatação do disco, tais arquivos serão excluídos. O ideal é que tais arquivos sejam armazenados em uma outra unidade de disco distinta do sistema operacional.
Letra d.

---

018. (Q4206387/IDECAN/CBM DF/ASPIRANTE COMPLEMENTAR/ÁREA: DIREITO/2025) Um técnico em informática configura um computador conectado à internet em uma repartição pública e ativa um aplicativo que controla quais programas podem enviar ou receber dados pela rede, bloqueando conexões não autorizadas. O tipo de ferramenta utilizada nessa situação é conhecido como:
a) Antivírus.
b) Firewall.
c) Antispyware.
d) Antispam.

Veja uma rápida descrição de cada uma das ferramentas.
a) Errada. **Antivírus**: software de proteção que detecta, bloqueia e remove programas maliciosos que tentam infectar ou danificar o sistema.
b) Certa. **Firewall**: mecanismo de segurança que pode combinar software e hardware, que monitora e filtra o tráfego de rede para impedir acessos não autorizados entre diferentes zonas de confiança.
c) Errada. **Antispyware**: software de proteção especializado em identificar e eliminar softwares espiões que coletam informações do usuário sem o seu consentimento.
d) Errada. **Antispam**: filtro de software que identifica e desvia mensagens eletrônicas indesejadas ou maliciosas enviadas em massa para a caixa de entrada.
Letra b.

---

019. (Q4258419/IDECAN/CBM DF/BOMBEIRO MILITAR GERAL DE CONDUTOR E OPERADOR DE VIATURAS/2025) Um usuário percebe que seu navegador exibe anúncios constantes e redireciona para páginas desconhecidas ao digitar endereços. Esses sintomas indicam a presença de um programa que coleta seus dados de navegação sem permissão. O tipo de ferramenta necessária para remover essa ameaça é:

a) Firewall.
b) Navegador.
c) Antispyware.
d) Compactador.

A descrição da ameaça indica um spyware, programa espião que se instala no computador do usuário e coleta suas informações sem o seu conhecimento ou consentimento. Para esse tipo de ameaça, é necessário um antispyware.
Letra c.

---

020. (Q3941666/INSTITUTO AOCP/PREFEITURA DE SÃO LUÍS/PROFESSOR ANOS INICIAIS (1º AO 5º ANO DO ENSINO FUNDAMENTAL)/2025) Você, como professor da rede pública municipal de ensino de São Luís (MA), está ministrando uma aula sobre segurança digital para os alunos do ensino fundamental. Durante a explicação, você apresenta uma situação hipotética em que um estudante, ao acessar informações confidenciais de um projeto escolar, encontra esses dados em um formato ilegível, o que impede que terceiros não autorizados acessem essas informações. Ao explicar como garantir que os dados permaneçam protegidos e confidenciais, você deve esclarecer que a técnica responsável por essa proteção é a(o)
a) autenticação.
b) antivírus.
c) criptografiaa.
d) firewall.
e) phishing.

a) Errada. **Autenticação**: processo de verificação da identidade de um usuário, sistema ou dispositivo para garantir que ele é quem afirma ser.
b) Errada. **Antivírus**: software que monitora, detecta e elimina códigos maliciosos para proteger a integridade dos sistemas e arquivos.
c) Certa. **Criptografia**: essa é nossa resposta. É o conjunto de técnicas que codifica a informação para que apenas o destinatário autorizado consiga decifrá-la e acessá-la.
d) Errada. **Firewall**: barreira de segurança que controla o tráfego de dados em uma rede, permitindo ou bloqueando comunicações com base em regras definidas.
e) Errada. **Phishing**: golpe que usa técnica de engenharia social, utilizando mensagens enganosas para induzir pessoas a revelarem dados confidenciais ou instalarem softwares nocivos.
Letra c.

---

021. (Q3730265/CESPE/CEBRASPE/EMBRAPA/PESQUISADOR/ÁREA: CIÊNCIAS EXATAS E DA TERRA: RASTREABILIDADE E CERTIFICAÇÃO DIGITAL/2025) Acerca de protocolos de certificação digital e assinaturas digitais, julgue os itens seguintes. Nesse sentido, considere que a sigla AC, sempre que empregada, se refere a autoridade certificadora.
Assinatura digitalizada e assinatura digital, para fins de integridade, possuem as mesmas propriedades de integridade quanto à verificação de documentos eletrônicos.

Veja a diferença entre as duas ferramentas.

- **Assinatura Digital**: É um processo eletrônico que utiliza criptografia assimétrica e certificados digitais para garantir a autenticidade, a integridade e o não repúdio de um documento.
- **Assinatura Digitalizada**: É apenas a reprodução gráfica (como uma foto ou scan) de uma assinatura feita à mão, não possuindo garantias tecnológicas de que o conteúdo do documento não foi alterado.

Errado.

---

022. (Q3476108/QUADRIX/CREF 9/AUXILIAR ADMINISTRATIVO/2024) Backups, autenticação multifator e firewalls são recursos de produção de um datacenter necessários para garantir a segurança e a capacidade de recuperação de incidentes e desastres. Com base nessa informação, assinale a alternativa correta.
a) A implementação de firewalls na rede não ajuda a bloquear tráfego malicioso nem prevenir contra ataques à rede.
b) O uso de autenticação multifator (MFA) reduz significativamente a segurança do acesso aos sistemas, pois complica o acesso para os usuários que tendem a fragilizar esse recurso.
c) Os backups regulares protegem contra falhas humanas no desenvolvimento de software.
d) Os backups periódicos de segurança devem ser guardados junto aos computadores para serem rapidamente utilizados em caso de necessidade.
e) A criptografia de dados é essencial para proteger informações sensíveis contra acessos não autorizados.

Veja abaixo a justificativa das alternativas da questão.
a) Errada. A implementação de firewalls na rede foi projetada justamente para ajudar a bloquear tráfego malicioso e prevenir ataques externos à rede.
b) Errada. O uso de autenticação multifator (MFA) aumenta a segurança do acesso aos sistemas, adicionando uma camada extra de proteção ao processo de autenticação.

c) Errada. Os backups regulares visam proteger contra a corrupção de dados em arquivos e bases de dados, não no desenvolvimento de sistemas e aplicações. A ferramenta que auxilia nesse sentido seria um software de versionamento, o qual permite recuperar versões anteriores dos arquivos em caso de erros no código-fonte.
d) Errada. Os backups periódicos de segurança devem ser guardados em dispositivos e locais diferentes de onde os dados de produção se encontram, visando à proteção física em caso de incidentes catastróficos, como incêndios, desabamentos, terremotos etc.
e) Certa. A criptografia de dados é essencial para proteger informações sensíveis contra acessos não autorizados, o que garante a confidencialidade da informação, uma vez que ela se torna inacessível por estar indecifrável.
Letra e.

---

023. (Q3610032/IDECAN/PREFEITURA DE JOÃO PESSOA/AGENTE DE COMBATE ÀS ENDEMIAS/2024) Assinale a alternativa que apresenta um procedimento de segurança usado para proteger dados durante a transmissão através de redes inseguras.
a) Autenticação baseada em certificados.
b) Criptografia de ponta a ponta.
c) Hashing de senhas.
d) Uso de sítios com HTTP.
e) Criptografia de dados em repouso.

Veja a justificativa de cada uma das alternativas.
a) Errada. A autenticação baseada em certificados não impede ataques de interceptação, os quais permitem a captura dos pacotes de dados transmitidos ao longo da conexão em redes inseguras, ou seja, redes que não exigem autenticação e não oferecem criptografia dos dados.
b) Certa. A criptografia de ponta a ponta é o que torna a conexão segura quando ela é estabelecida sobre uma rede insegura, pois todos os dados trafegados na conexão estão protegidos, desde os acessados via navegadores, como também os transmitidos por outras aplicações desktop.
c) Errada. O hashing de senhas protege a senha quando ela é fornecida durante uma conexão ou quando armazenada em uma base de dados. Porém, tal recurso não protege a conexão em si, apenas a própria senha.
d) Errada. O uso de sítios com HTTP não protege a conexão, pois tal protocolo não possui criptografia. A solução alternativa seria o HTTPS, o qual oferece criptografia com o uso de certificado digital do site.
e) Errada. A criptografia de dados em repouso significa a codificação dos dados armazenados, o que não protege as conexões, as quais lidam com dados em movimento.
Letra b.

---

024. (Q3204082/IBADE/PREFEITURA DE VILA VELHA/AGENTE COMUNITÁRIO DE SAÚDE/2024) Leia o trecho e preencha a lacuna abaixo corretamente."_____ são programas de software ou dispositivos de hardware que filtram e examinam as informações provenientes da sua conexão com a Internet. Eles representam uma primeira linha de defesa porque podem impedir que um programa ou invasor mal-intencionado obtenha acesso à sua rede e informações antes que qualquer dano potencial seja causado.

a) Nobreaks
b) Backups
c) Biometrias
d) Firewalls
e) Certificados digitais

Veja o significado de cada alternativa.

a) Errada. **Nobreaks**: dispositivos que fornecem energia ininterrupta e proteção contra oscilações na rede elétrica, permitindo o funcionamento de aparelhos durante quedas de luz.

b) Errada. **Backups**: cópias de segurança de arquivos e sistemas armazenadas em locais distintos para permitir a recuperação de dados em caso de perda ou falha.

c) Errada. **Biometrias**: métodos de identificação baseados em características físicas ou comportamentais únicas, como impressões digitais ou reconhecimento facial.

d) Certa. **Firewalls**: barreiras de segurança que controlam o fluxo de dados entre redes, bloqueando tráfegos maliciosos ou acessos não autorizados, podendo ser apenas software ou uma combinação de software e hardware.

e) Errada. **Certificados digitais**: documentos eletrônicos que funcionam como uma identidade virtual, permitindo assinar documentos e realizar transações online com validade jurídica, além de criptografar a informação com base em chaves públicas.

Letra d.

---

025. (Q3151774/FGV/PREFEITURA DE CARAGUATATUBA/ANALISTA AMBIENTAL/2024) Um backup diferencial de um conjunto de arquivos copia para o meio de backup:

a) todos os arquivos que tenham uma extensão específica.
b) todos os arquivos maiores que um determinado tamanho.
c) todos os arquivos diferentes de um formato previamente especificado.
d) todos os arquivos criados ou alterados depois do último backup completo ou total.
e) todos os arquivos presentes no disco em questão que não estejam já marcados para cópia.

O backup diferencial é um método de cópia de segurança que armazena apenas os arquivos que foram alterados ou criados desde o último backup completo. Uma de suas características é que ele não identifica os arquivos copiados, os quais serão novamente copiados em uma nova execução posterior.

Letra d.

---

026. (Q3131253/CESPE/CEBRASPE/PREFEITURA DE CAMAÇARI/FISCAL/ÁREA: USO DO SOLO E MEIO AMBIENTE/2024) No que se refere aos procedimentos becape, identificação e manipulação de arquivos, assinale a opção correta.

a) Um arquivo é movido para a lixeira quando é recortado.

b) A ação de recortar arquivo cria uma cópia de becape do arquivo.

c) Arquivos de becape possuem extensão do tipo PDF.

d) Os arquivos excluídos podem ser restaurados da lixeira.

e) O sistema Windows não possui ferramenta nativa de becape.

Veja o significado de cada alternativa.

a) Errada. Um arquivo é movido para a Lixeira quando é excluído.

b) Errada. A ação de recortar um arquivo o copia para a área de transferência, de onde ele poderá ser posteriormente colado em outro local de destino.

c) Errada. Arquivos de backup do Windows podem possuir as extensões.bkf,.vhdx ou.vhd. Os arquivos.pdf são aqueles que podem ser abertos pelo aplicativo Adobe Reader, os quais preservam o conteúdo e a formatação do documento, permitindo sua visualização original, independentemente do sistema operacional ou do aplicativo visualizador utilizados.

d) Certa. No Windows, os arquivos excluídos são enviados à Lixeira e podem ser restaurados, recuperando-os ao seu local original anterior à exclusão.

e) Errada. O sistema Windows possui ferramenta nativa de backup integrada à nuvem OneDrive, da Microsoft. Tal backup protege não apenas os arquivos configurados para cópia, como também as configurações do sistema.

Letra d.

---

027. (Q3380344/FGV/TCE PA/AUDITOR DE CONTROLE EXTERNO/ÁREA: ADMINISTRATIVA/ ESPECIALIDADE: ENGENHARIA TELECOMUNICAÇÕES/2024) Os firewalls desempenham um papel fundamental na proteção dos dados sigilosos que trafegam na rede corporativa de um órgão público. Há diversos tipos, como firewall filtro de pacotes, firewall em estado de conexão e firewall em nível de aplicação. O firewall filtro de pacotes

a) permite detectar diversas ameaças à rede, por exemplo: spam, phishing e spyware.
b) permite distinguir entre os diferentes tipos de tráfego HTTP
c) mapeia todos os pacotes que entram e saem da rede interna, relacionando-os às conexões TCP/IP ativas.
d) inspeciona apenas os endereços IP e as portas TCP/UDP dos pacotes que entram e saem de uma rede interna, descartando aqueles que não atendem aos critérios estabelecidos pelo administrador de rede.
e) torna possível o envio de tráfego encriptado, garantindo assim a confidencialidade das informações e a privacidade dos dados.

Veja a diferença entre os três tipos de firewalls.
Firewall de Filtro de Pacotes (**Stateless**): É a forma mais básica, que analisa cada pacote de dados individualmente com base em um conjunto de regras predefinidas (como endereço IP de origem/destino e porta TCP/UDP). Ele não guarda memória de pacotes anteriores, decidindo se permite ou bloqueia a passagem de forma isolada, sem entender o contexto da comunicação.
Firewall de Estado de Conexão (**Stateful Inspection**): Diferente do filtro de pacotes, este monitora o estado das conexões ativas. Ele mantém uma tabela de estados para saber se um pacote faz parte de uma sessão legítima já estabelecida (como uma navegação web em curso), oferecendo maior segurança ao impedir que pacotes maliciosos entrem sem que tenham sido solicitados internamente.
Firewall de Nível de Aplicação (**Proxy Gateway**): É o mais avançado e seguro, pois atua na camada mais alta do modelo OSI. Ele analisa o conteúdo real dos dados (como o corpo de um e-mail ou comandos HTTP) e não apenas os cabeçalhos. Funciona como um intermediário(proxy), interceptando a comunicação para filtrar comandos específicos de aplicativos e impedir ataques que exploram vulnerabilidades de softwares. Cuidado, pois não é a mesma coisa que um proxy de rede, mas sim uma função de firewall que o proxy de rede pode exercer.
Letra d.

---

028. (Q2703675/CESPE/CEBRASPE/POLC AL/PERITO ODONTOLEGISTA/2023) No que se refere a sistemas operacionais, pacotes office, navegadores e redes de computadores, julgue os itens que se seguem.
Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

Segundo a Cartilha de Segurança da Informação, o antivírus é um tipo de ferramenta antimalware desenvolvida para **detectar**, **anular e eliminar** de um computador vírus e outros tipos de códigos maliciosos. Pode incluir também a funcionalidade de firewall pessoal. Portanto, o enunciado da questão está errado por extrapolar as funcionalidades do antivírus.
Errado.

---

029. (Q2700563/CESPE/CEBRASPE/POLC AL/PAPILOSCOPISTA/2023) No que se refere a sistemas operacionais, pacotes office, navegadores e redes de computadores, julgue os itens que se seguem.
Um antivírus, quando bem configurado, permite, entre outras ações: bloquear o envio para terceiros de informações coletadas por invasores e malwares; bloquear as tentativas de invasão e de exploração de vulnerabilidades do computador; e identificar as origens dessas tentativas, evitando que o malware seja capaz de se propagar na rede.

Segundo a Cartilha de Segurança da Informação, o antivírus é um tipo de ferramenta antimalware desenvolvido para **detectar**, **anular e eliminar** de um computador vírus e outros tipos de códigos maliciosos. Pode incluir também a funcionalidade de firewall pessoal. Portanto, o enunciado da questão está errado por extrapolar as funcionalidades do antivírus.
Errado.

---

030. (Q2810389/IDCAP/IASES/AGENTE SOCIOEDUCATIVO/2023) São considerados programas antivírus, EXCETO:
a) Avast.
b) McAfee.
c) Kaspersky.
d) MySQL.
e) AVG.

MySQL é um gerenciador de banco de dados e não um exemplo de antivírus.
Letra d.

---

031. (Q2674995/IADES/SEAGRI/DF/ANALISTA DE DESENVOLVIMENTO AGROPECUÁRIA/ÁREA ADMINISTRADOR/2023) Aplicativos de segurança conhecidos como antivírus monitoram o

sistema para detectar arquivos maliciosos. Quando uma ameaça é detectada, o antivírus criptografa o arquivo suspeito e move-o para uma área segura do disco.
Esse tratamento denomina-se
a) varredura.
b) backup.
c) quarentena.
d) restauração.
e) desfragmentação.

a) Errada. Varredura é o mecanismo de busca e detecção de ameaças.
b) Errada. Backup é uma cópia de segurança.
c) Certa. Quarentena é um recurso que impede que o arquivo seja executado, evitando que ele cause danos ao ambiente. Quando uma ameaça é detectada, o antivírus criptografa o arquivo suspeito e move-o para uma área segura do disco.
d) Errada. Restauração extrapola as funcionalidades do antivírus.
e) Errada. Desfragmentação extrapola as funcionalidades do antivírus.
Letra c.

---

032. (Q2832899/IBADE/PREFEITURA DE TARAUACÁ/TÉCNICO EM ENFERMAGEM/2023)
Assinale a alternativa que corresponda a um exemplo de antivírus.
a) McAfee
b) SublimeText
c) CodeBlocks
d) MySQL
e) IBM Informix

a) Certa. McAfee é um exemplo de antivírus.
b) Errada. Sublime Text é um editor de código-fonte.
c) Errada. Code::Blocks é um ambiente de desenvolvimento.
d) Errada. MySQL é um sistema de gerenciamento de banco de dados.
e) Errada. IBM Informix é um sistema de gerenciamento de banco de dados.
Letra a.

---

033. (Q2823504/CESGRANRIO/BB/ESCRITURÁRIO/ÁREA: AGENTE COMERCIAL/2023) O Windows 10 possui um esquema de segurança nativo que fornece vários tipos de proteção contra ameaças ao sistema.
A ferramenta antivírus, integrada ao Windows 10, que ajuda a proteger o computador do usuário contra vírus, ransomware e outros malwares é a
a) Microsoft Defender Antivirus
b) Microsoft Defender Protection
c) Microsoft Malware Alert
d) Microsoft Malware Protection
e) Microsoft Antivirus Protection

a) Certa. Microsoft Defender Antivirus – ou também pode ser chamado de Windows Defender.
b) Errada. Microsoft Defender Protection – não existe esse aplicativo.
c) Errada. Microsoft Malware Alert – não existe esse aplicativo.
d) Errada. Microsoft Malware Protection – não existe esse aplicativo.
e) Errada. Microsoft Antivirus Protection – não existe esse aplicativo.
Letra a.

---

034. (Q2805117/SELECON/PREFEITURA DE NOVA MUTUM/INSTRUTOR DE INFORMÁTICA/2023) Uma empresa de comércio eletrônico pretende utilizar um mecanismo de criptografia para gerenciar a comunicação de seus clientes com as suas lojas instaladas em sites. Esse mecanismo vai utilizar uma mesma chave criptografada tanto para codificar como para decodificar informações, sendo usada, principalmente, para garantir a confidencialidade dos dados. Esse tipo de chave de criptografia é denominado de chave:
a) hash
b) virtual
c) simétrica
d) assimétrica

Simétrica – tipo de criptografia que utiliza a mesma chave para codificar e decodificar.
Assimétrica – tipo de criptografia que utiliza duas chaves: uma chave pública para criptografar e uma chave privada para descriptografar.
Letra c.

---

035. (Q2866764/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA TECNOLOGIA DA INFORMAÇÃO/2023) No que diz respeito aos conceitos de proteção e de segurança da informação, julgue os itens.
A criptografia assimétrica, a qual utiliza um par de chaves, é uma das técnicas utilizadas para que os dados sejam criptografados de forma segura.

A criptografia assimétrica usa **duas** chaves, ambas do destinatário, sendo que a chave pública é a que criptografa e a chave privada é a que descriptografa. Somente o dono da chave privada pode abrir a mensagem criptografada; ninguém mais, nem mesmo a pessoa que a criptografou.
Certo.

---

036. (Q2817646/INSTITUTO CONSULPLAN/FEPAM/TÉCNICO EM ADMINISTRAÇÃO/2023) As ferramentas para segurança da informação são o conjunto de software, hardware e técnicas que têm como principal objetivo combater os ataques. A técnica utilizada para cifrar uma informação, tornando-a incompreensível, exceto para o destinatário e o transmissor que sabem como decifrá-la é:
a) Proxy.
b) Firewall.
c) Antivírus.
d) Criptografia.
e) Sistema de Detecção de Intrusos (IDS).

Antivírus – É um software utilitário que identifica e elimina qualquer tipo de malware, como, por exemplo, worm, bot, trojan, vírus, rootkit, spyware e ransomware.
Criptografia – É a técnica de transformar a informação em algo ininteligível por meio do embaralhamento. Essa ferramenta é responsável por garantir o sigilo e a segurança das informações, podendo ser utilizada em ambientes tecnológicos ou não.
Letra d.

---

037. (Q2734022/FUNDEP/PREFEITURA DE LAVRAS/PROFESSOR/ÁREA: GEOGRAFIA/2023) A técnica que transforma, por meio de chaves ou códigos, informação inteligível em algo que um agente externo seja incapaz de compreender é chamada de
a) senha.
b) autenticação em duas etapas.
c) criptografia.
d) token.

a) Errada. Senha – são caracteres utilizados para realizar a autenticação do usuário em um sistema.
b) Errada. Autenticação em duas etapas – camada extra de proteção na autenticação do usuário.
c) Certa. Criptografia – é a técnica de transformar a informação em algo ininteligível por meio do embaralhamento. Essa ferramenta é responsável por garantir o sigilo e a segurança das informações, podendo ser utilizada em ambientes tecnológicos ou não.
Letra c.

---

038. (Q2824611/MS CONCURSOS/PREFEITURA DE TURVELÂNDIA/PROFESSOR/ÁREA: MATEMÁTICA/2023) Considere a afirmativa: "A criptografia apresenta práticas ou processos para tornar segura a comunicação entre partes. Um dos métodos conhecidos é a utilização de uma chave para encriptar o conteúdo de uma mensagem em uma informação cifrada e decriptar a mensagem cifrada com essa mesma chave para obter o dado original.". Sobre a utilização de técnicas de criptografia para Certificados Digitais e Assinaturas Digitais, a alternativa que apresenta corretamente o conceito da afirmativa é:
a) A afirmativa corresponde à Criptografia Simétrica, que pode reforçar a confidencialidade de dados, mas como a mesma chave é usada para encriptar e decriptar a informação, a técnica por si só não garante a Irretratabilidade no caso do uso como Certificado Digital.
b) A afirmativa corresponde a uma função de Hash, muito utilizada em Certificados Digitais para cifrar mensagens confidenciais e garantir a Integridade dos dados, uma vez que é necessário conhecer a chave para acessar seu conteúdo.
c) A afirmativa corresponde à Criptografia Assimétrica, medida de segurança utilizada em Certificados Digitais para garantir que a assinatura de um documento corresponde corretamente à pessoa que o assinou, pois apenas as partes interessadas conhecem a chave utilizada para cifrar o conteúdo da mensagem.
d) A afirmativa corresponde ao processo utilizado em Certificados Digitais, em que uma empresa reconhecida e confiável vincula a chave utilizada para criptografar a Assinatura Digital a seu titular.

a) Certa. Gabarito da questão. Na criptografia simétrica, utiliza-se uma única chave para criptografar e descriptografar a informação. Essa chave pode ser uma senha ou um código e pode ser chamada de chave secreta ou chave de criptografia.
b) Errada. Não se trata do uso da função Hash, a qual é usada na assinatura digital para identificar o documento e garantir a sua integridade.
c) Errada. A criptografia assimétrica usa **DUAS** chaves, ambas do destinatário, sendo que a chave pública é a que criptografa e a chave privada é a que descriptografa. Somente o

dono da chave privada pode abrir a mensagem criptografada; ninguém mais, nem mesmo a pessoa que a criptografou.
d) Errada. Essa alternativa retrata a assinatura digital da autoridade certificadora no certificado digital, que tem por função autenticar a autoria daquele documento de identidade eletrônica.
Letra a.

---

039. (Q2920394/SELECON/CREA RJ/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO/2023) A utilização de um certificado digital, emitido por uma autoridade certificadora, para gerar uma assinatura digital em um documento, tem como uma de suas característica:
a) utilizar a chave pública de quem assina
b) garantir a confidencialidade desse documento
c) proteger o documento contra falhas de hardware
d) autenticar o conteúdo no momento da assinatura
e) estabelecer uma conexão segura entre origem e destino

a) Errada. A assinatura digital utiliza a chave privada de quem assina.
b) Errada. A assinatura digital não garante a confidencialidade de documentos assinados.
c) Errada. A assinatura digital não protege o documento contra falhas de hardware. Para isso, é necessário o uso de backup.
d) Certa. A assinatura digital é utilizada para autenticar o conteúdo do documento no momento da assinatura, garantindo a veracidade de sua autoria.
e) Errada. A assinatura digital não estabelece uma conexão segura entre origem e destino. Isso é função de protocolos como SSL, SSH e VPN.
Letra d.

---

040. (Q2687175/FUNDAÇÃO CEFETMINAS/PREFEITURA DE CONTAGEM/AGENTE FAZENDÁRIO/2023) Certificados digitais podem ser utilizados na troca de informação entre pessoas na internet.
São dados que compõem um certificado digital, EXCETO o(a)
a) número de série do certificado.
b) código de integridade do software de criptografia.
c) identificação da pessoa que é dona do certificado.
d) identificação da autoridade certificadora emissora do certificado.
e) assinatura digital da autoridade certificadora emissora do certificado.

O certificado digital não armazena o código de integridade do software de criptografia, algo que não faz sentido. Já o número de série do certificado serve para identificá-lo unicamente. A identificação da pessoa que é dona do certificado serve para que sua autoria em documentos eletrônicos seja autenticada. A identificação da autoridade certificadora emissora do certificado serve para verificar se ele foi emitido por uma fonte confiável. A assinatura digital da autoridade certificadora emissora do certificado serve para autenticar o próprio certificado digital, atribuindo validade jurídica a essa identidade eletrônica.

Letra b.

---

041. (Q2823632/CESGRANRIO/BB/ESCRITURÁRIO/ÁREA: AGENTE COMERCIAL/2023) O mecanismo de segurança é um método ou processo que pode ser utilizado por um sistema para implementar um serviço de segurança. Para verificar a autenticidade ou a autoria de um documento com relação ao seu signatário, deve-se validar a(o)

a) envelope digital

b) assinatura digital

c) criptograma simétrico

d) chave simétrica

e) algoritmo simétrico

a) Errada. O envelope digital é um contêiner seguro de dados digitais que protege uma mensagem eletrônica por meio de autenticação de dados e criptografia. Ele é utilizado nas comunicações eletrônicas, como e-mails, mensagens instantâneas como WhatsApp e Telegram, bem como na transferência de arquivos.

b) Certa. A assinatura digital é um mecanismo de segurança que atua como um método ou processo que pode ser utilizado por um sistema para implementar um serviço de segurança. É utilizada para verificar a autenticidade ou a autoria de um documento em relação ao seu signatário.

c) Errada. Criptograma e criptografia simétrica não são a mesma coisa. Ela não serve para verificar a autenticidade ou autoria do documento em relação ao seu assinante.

d) Errada. A chave simétrica é a chave utilizada na criptografia simétrica, ou seja, a única chave envolvida no mecanismo, a qual é responsável por criptografar e descriptografar os dados.

e) Errada. Algoritmo simétrico é o mesmo que criptografia simétrica, pois é o código utilizado para realizar a criptografia simétrica.

Letra b.

---

042. (Q2719827/SELECON/PREVILUCAS/ADVOGADO/2023) Uma característica essencial de uma assinatura digital em uma determinada mensagem ou arquivo (por exemplo, um documento em PDF) é:

a) confidencialidade da mensagem

b) garantia de disponibilidade e acesso à mensagem

c) controle de acesso à mensagem

d) autenticação da origem e integridade da mensagem

a) Errada. Quem garante a confidencialidade da mensagem é a criptografia.

b) Errada. Quem garante a disponibilidade e o acesso à mensagem são mecanismos como backup, nobreak e firewall.

c) Errada. Quem garante o controle de acesso à mensagem é a autenticação e a criptografia.

d) Certa. Pois a assinatura digital garante a autenticação da origem e a integridade da mensagem.

Letra d.

---

043. (Q2695313/COPEVE/UFAL/FUNDEPES/IFAL/ASSISTENTE EM ADMINISTRAÇÃO/2023) Em algumas organizações comerciais ou até mesmo em certos países, o acesso a determinados sites ou tipos de conteúdo são bloqueados. Os motivos por trás dos bloqueios são diversos, desde o local onde estão publicados (sites), como o fato de tais endereços ou serviços serem considerados inseguros ou suspeitos. Qual ferramenta poderia ser utilizada para realizar as ações de bloqueio, descritas anteriormente?

a) Spam

b) Cookies

c) Firewall

d) Antivírus

e) Anti Spyware

a) Errada. O Spam é uma mensagem não solicitada enviada em massa; ou seja, ela é uma ameaça e não uma proteção.

b) Errada. Os Cookies são arquivos de texto salvos pelo site no computador do usuário, os quais guardam informações sobre os dados de navegação dos usuários.

c) Certa. Firewall é a ferramenta utilizada para realizar as ações de bloqueio descritas no enunciado da questão.

d) Errada. O Antivírus é uma solução que visa eliminar softwares maliciosos que infectam os arquivos ou a estação de trabalho dos usuários, não sendo o bloqueio de conexões a sua função.
e) Errada. Antispyware é um software de proteção voltado exclusivamente para proteger contra spywares, buscando-os e eliminando-os.
Letra c.

---

044. (Q2708555/IBFC/PREFEITURA DE CUIABÁ/ESPECIALISTA EM SAÚDE/ÁREA: QUÍMICO/2023) Quanto às características dos programas Antivírus e ao Firewall, analise as afirmativas a seguir e dê valores Verdadeiro (V) ou Falso (F).

( ) O firewall é um sistema de segurança de rede de computadores que limita o tráfego de entrada e/ou saída dentro de uma rede.
( ) Se numa instalação já tiver um firewall será desnecessário instalar adicionalmente um programa Antivírus, em termos de segurança de dados.
( ) A concepção de um firewall atual pode-se considerar tecnicamente como sendo a terceira geração evolutiva dos antigos programas Antivírus.

Assinale a alternativa que apresenta a sequência correta de cima para baixo.
a) V – F – F
b) V – V – F
c) F – V – V
d) F – F – V

- O firewall é um sistema de segurança de rede de computadores que limita o tráfego de entrada e/ou saída dentro de uma rede.
- A instalação de um firewall não dispensa a instalação adicional de um programa antivírus, visto que são proteções de naturezas distintas.
- Os firewalls atuais não são considerados tecnicamente como sendo a terceira geração evolutiva dos antigos programas antivírus, pois atuam em funções totalmente distintas, embora alguns antivírus embutam funções típicas de um firewall, mas não o contrário.

Letra a.

---

045. (Q2937944/FGV/DPE RS/TÉCNICO APOIO ESPECIALIZADO/ÁREA: SUPORTE DE TI/2023) Amanda enviou uma mensagem à Virgínia que deve efetuar a verificação de assinatura feita por Amanda para o pacote. O processo de verificação de assinatura digital a ser executado por Virgínia consiste em alguns passos, nos quais ela deve decifrar a:

a) assinatura digital, com a chave pública de Amanda contida no certificado digital, obtendo o sumário da mensagem gerado e cifrado por Amanda na assinatura;
b) assinatura digital, com a chave pública de Virgínia contida no certificado digital, obtendo o código digital gerado e cifrado pela Autoridade Certificadora;
c) criptografia, com a chave privada de Virgínia contida no código digital gerado e cifrado por Amanda, para a emissão do certificado;
d) assinatura digital, com a chave privada de Amanda contida no resumo criptográfico gerado e cifrado por Virgínia, quando da aquisição do certificado;
e) criptografia, com a chave pública de Virgínia a qual foi enviada por broadcast a todos os usuários da rede.

O processo de verificação ou validação da assinatura consiste em decifrar ou descriptografar a assinatura digital, com a chave pública de Amanda contida no certificado digital, obtendo o sumário da mensagem gerado e cifrado por Amanda na assinatura.
Letra a.

---

046. (Q2931181/OBJETIVA CONCURSOS/PREFEITURA DE NOVO ITACOLOMI/PROFESSOR DE EDUCAÇÃO FÍSICA/2023) Para maximizar a segurança do usuário, é fundamental que, ao criar uma senha nova, alguns cuidados sejam tomados. Assinalar a alternativa que NÃO representa um comportamento adequado ou seguro na hora de elaborar uma nova senha:
a) Utilizar caracteres aleatórios.
b) Misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas.
c) Evitar senhas parecidas com senhas que você já utiliza.
d) Utilizar a mesma senha para o máximo de coisas que puder.

Ao utilizar a mesma senha em vários serviços, há o risco de que, se sua senha for descoberta, todos os serviços poderão ser acessados com ela. É necessário utilizar uma senha muito forte, porém distinta para cada serviço, pois isso aumenta as chances de sua senha não ser descoberta.
Letra d.

---

047. (Q2818790/OBJETIVA CONCURSOS/CÂMARA DE SÃO JOÃO DO MANHUAÇU/TESOUREIRO/2023) A respeito das boas práticas ao criar senhas de acesso a sites da internet, marcar C para as afirmativas Certas, E para as Erradas e, após, assinalar a alternativa que apresenta a sequência CORRETA:

( ) Ao criar uma senha na internet, não é recomendado utilizar dados pessoais, como nome e sobrenome.
( ) Utilizar senhas com números sequenciais do teclado, como 123456, facilita a identificação da senha por terceiros.
( ) A variação entre números, letras maiúsculas e minúsculas e caracteres especiais não aumenta a segurança da senha.

a) C – C – E.
b) E – E – C.
c) C – E – E.
d) E – C – C.

A última afirmativa está incorreta, pois a variação entre números, letras maiúsculas e minúsculas e caracteres especiais aumenta aindamais a segurança da senha.
Letra a.

---

048. (Q2684985/QUADRIX/CRO/AGENTE FISCAL/2023) A respeito dos procedimentos de segurança da informação e backup, julgue os itens.
Para adicionar maior proteção ao processo de autenticação de usuários, o uso de autenticação multifator (MFA) é indicado, porque adiciona duas ou mais camadas diferentes de verificação adicionais, como uso de aplicativos de autenticação, tokens físicos, reconhecimento facial e biometria.

Exatamente! Com o MFA, não basta apenas o atacante descobrir a senha do usuário, pois será necessário confirmar sua identidade por outro meio seguro de autenticação, o qual, geralmente, somente o usuário tem acesso.
Certo.

---

049. (Q2866762/QUADRIX/CRECI PR/PROFISSIONAL DE SUPORTE TÉCNICO/ÁREA TECNOLOGIA DA INFORMAÇÃO/2023) No que diz respeito aos conceitos de proteção e de segurança da informação, julgue os itens.
A autenticação em duas etapas, ou em dois fatores, como é comumente chamada, é considerada uma medida ineficaz para o aumento da segurança do computador e para a proteção das contas on-line, já que sua finalidade é, especificamente, o bloqueio dos pacotes duvidosos que trafegam pela Internet.

Errado, pois é uma medida altamente eficaz para proteger a forma de autenticação em sistemas e plataformas digitais. Além disso, não é finalidade o bloqueio de pacotes, pois isso é função do firewall.

Errado.

---

050. (Q2851272/FGV/PGM/TÉCNICO EM PROCURADORIA/2023) Julia usa senhas fortes em suas contas digitais, mas quer elevar o seu nível de segurança. Para isso, consultou o técnico de informática Matheus que a orientou a adicionar uma segunda camada de proteção no acesso às suas contas. Assim, mesmo que o atacante descubra sua senha, ele precisará de outras informações para invadir sua conta. Matheus completou dizendo: "Escolha o método que considerar mais prático e seguro, como: usar um aplicativo de celular para gerar códigos de verificação; ou receber códigos por mensagem de texto ou voz." A proteção sugerida por Matheus é o(a):

a) Antispam;
b) Firewall pessoal;
c) Certificado digital;
d) Gerenciador de senha;
e) Verificação em duas etapas.

Verificação em duas etapas ou autenticação em múltiplos fatores (MFA) é a técnica que adiciona uma segunda camada de proteção no acesso às contas online por meio da necessidade de confirmação da autenticação por outro meio seguro.

Letra e.

Chegamos, assim, ao fim dessa maratona de questões! Espero que você tenha gabaritado todas elas. Ah! Faz o seguinte agora: vai lá nas avaliações dessa aula, diz para mim o quanto você gostou dela e quantas questões você gabaritou, beleza? Eu lerei sua avaliação assim que você a fizer, pois leio todos os comentários das avaliações dos meus alunos!

Se você quiser fazer parte da minha rede social, aponte sua câmera para o QR Code da esquerda e siga-me:

E se quiser acessar meu curso completo de informática para concursos, aponte sua câmera para o QR Code da direita.

Parabéns por ter chegado até aqui! Parabéns por não ter desistido e por ter terminado todas as questões! Você é uma pessoa vencedora, uma verdadeira campeã!

Estou muito orgulhoso de você!

Abra

caminhos

crie

futuros

gran.com.br