GRAN CONCURSOS

INFORMÁTICA

Princípios Básicos de Segurança da Informação

Livro Eletrônico

Presidente: Gabriel Granjeiro

Vice-Presidente: Rodrigo Calado

Diretor Pedagógico: Erico Teixeira

Diretora de Produção Educacional: Vivian Higashi

Gerência de Produção de Conteúdo: Magno Coimbra

Coordenadora Pedagógica: Élica Lopes

CÓDIGO:

230728234851

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

Na era digital em que vivemos, testemunhamos um crescimento exponencial na quantidade de dados que lidamos diariamente. Enfrentamos o desafio de gerenciar essas informações de modo a protegê-las e mantê-las em segurança, visto que o avanço tecnológico nos trouxe um volume imenso de informações digitais. É nesse contexto que a segurança da informação se torna uma preocupação fundamental.

Nesta aula, estudaremos um tópico muito importante dentro de Segurança da Informação: Princípios Básicos de Segurança da Informação.

Acredite, esse é um tema recorrente em editais de concursos. Tentarei te explicar de maneira leve e prática para que você gabarite todas as questões!

Estarei aqui do outro lado, mas 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!

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

A internet é uma ferramenta presente na vida de grande parte da população mundial. Por meio dela, podemos nos conectar a pessoas em qualquer lugar do mundo e esse é apenas um ponto das várias benesses as quais a internet pode nos proporcionar. Por meio da internet, podemos realizar serviços bancários, acessar notícias, estudar novas culturas e línguas, participar de cursos, palestras, aulas, fazer uma graduação, buscar pessoas desaparecidas, fazer compras de qualquer tipo, inclusive em outros países, utilizá-la como ferramenta de lazer ou trabalho, realizar agendamentos de serviços do governo. Enfim, a internet dispõe de inúmeras possibilidades para os usuários.

A tendência da utilização da internet é crescer cada vez mais. A sociedade moderna tem a internet como necessidade básica em seu dia a dia e isso impacta em maior produção de dados, mais informações inseridas na rede e maior preocupação de como essas informações serão protegidas e armazenadas.

Você já deve ter ouvido essa expressão: "Internet é terra sem lei". Venho lhe dizer que não funciona bem assim. Atualmente temos legislações para tentar minimizar os problemas causados por indivíduos que fazem o mau uso da internet, além de pequenas regras e boas práticas no ambiente digital.

Alguns exemplos dessas legislações:

Lei n. 13.709/2018 – Lei Geral de Proteção de Dados - Essa legislação regula a proteção dos dados pessoais buscando a proteção da privacidade e intimidade dos indivíduos.

Lei n. 12.965/2014 - Lei do Marco Civil da Internet – Essa Lei traz princípios, direitos e deveres para a utilização da internet no Brasil.

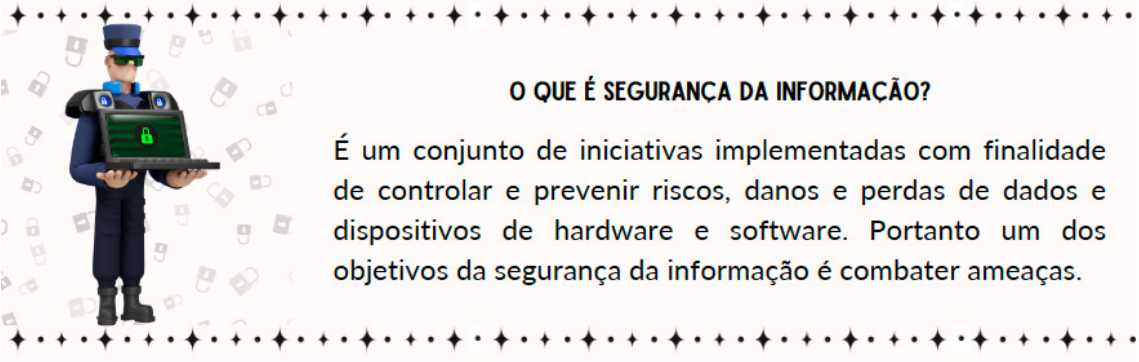
Lei n. 12.737/2012 - Carolina Dieckmann – Essa Lei tipifica crimes cibernéticos, com finalidade de minimizar as práticas ilegais no ambiente virtual.

Mas é aquele negócio: se tem Lei, infelizmente teve histórico. E por isso devemos nos preocupar e nos precaver quanto ao uso das redes.

Sei que parece meio óbvio, mas preciso te dizer: a internet NÃO é um ambiente seguro!!! Não estou fazendo terrorismo, mas existem muitos riscos que rondam as redes e vamos falar um pouco sobre isso.

A internet conecta o usuário em nível global e, da mesma forma que essa conexão pode trazer benefícios, também pode trazer vários riscos. É comum que o usuário seja exposto a conteúdos inapropriados, ofensivos, constrangedores os quais não buscou, além da conexão com outros usuários mal-intencionados, que utilizam as redes para cometer diversos crimes.

Nesse estudo vamos tratar sobre os princípios básicos de segurança da informação e como esse tópico é abordado em questões de concursos.



2. CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Não para por ai! Segundo a Norma ISO 27002, a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos.

A definição de segurança da informação engloba vários aspectos essenciais, como confidencialidade, integridade, responsabilidade, honestidade das pessoas, confiança e ética. Em suma, a segurança da informação é alcançada por meio de um conjunto abrangente de medidas que, quando aplicadas corretamente e revisadas regularmente, garantem a proteção dos dados.

Portanto, faz-se necessária a implementação de políticas e procedimentos de segurança, associados à tecnologia de proteção, como por exemplo criptografia e firewall que falaremos adiante, além da realização de treinamentos e conscientização dos usuários quanto ao uso da internet.

Aproveitando a deixa, vamos entrar no tópico central dessa aula, os princípios básicos de segurança da informação. Esses princípios são os pilares da segurança da informação e vamos analisar cada um deles.

3. PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Peço bastante atenção neste tópico, pois a incidência em provas de concurso é bem alta.

Nos editais, você também poderá encontrar esse tema com as seguintes nomenclaturas: requisitos básicos de segurança, propriedades básicas de segurança, pilares de segurança, isso vai de acordo com a criatividade do examinador. Todos eles dizem respeito ao tópico de conceitos básicos, portanto tratam da mesma coisa: os princípios básicos de segurança da informação.

Os princípios norteiam as políticas de segurança e podem ser aplicados tanto a recursos e ambientes computacionais quanto a ambientes não computacionais.

Quando estudamos sobre os princípios básicos, precisamos saber três aspectos que são constantemente abordados nas questões que envolvem esse assunto:

1) Quais são eles?
Basta decorar quais são os princípios, pois é exatamente o que é cobrado em algumas questões mais simples.

2) O que significam?
Aqui já é necessário conhecer a definição de cada um deles para poder responder, pois o examinador costuma trocar as definições entre eles.

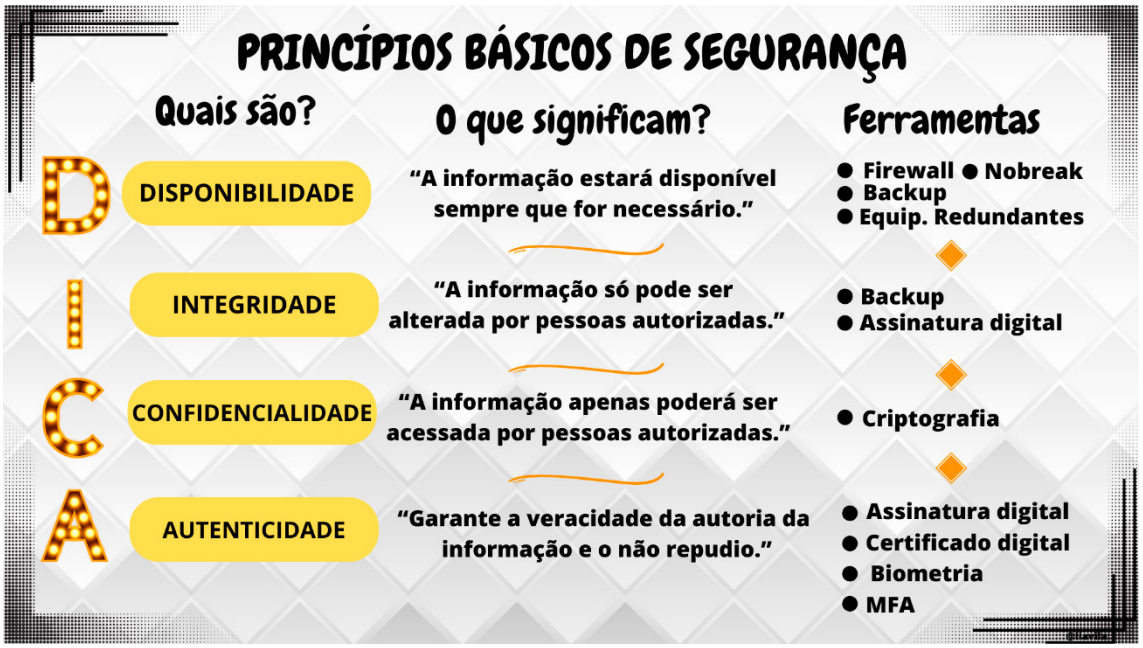
3) Quais as ferramentas que garantem tais princípios?
É preciso saber quais os recursos tecnológicos que estão envolvidos em cada um dos princípios básicos.

Então vamos responder todas essas perguntas de forma bem detalhada para que você internalize esses conceitos.

São princípios da segurança da informação:

- Disponibilidade;
- Integridade;
- Confidencialidade;
- Autenticidade.

Talvez esse seja o mapa mental mais importante dessa aula.

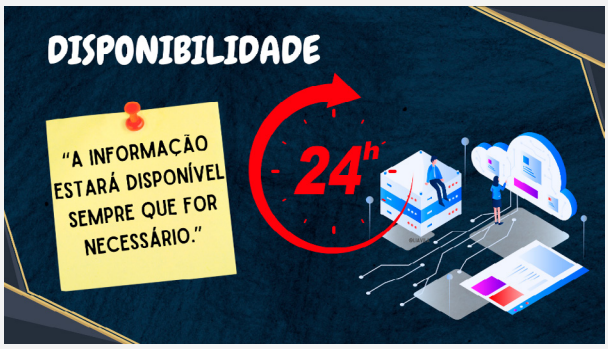


3.1. DISPONIBILIDADE

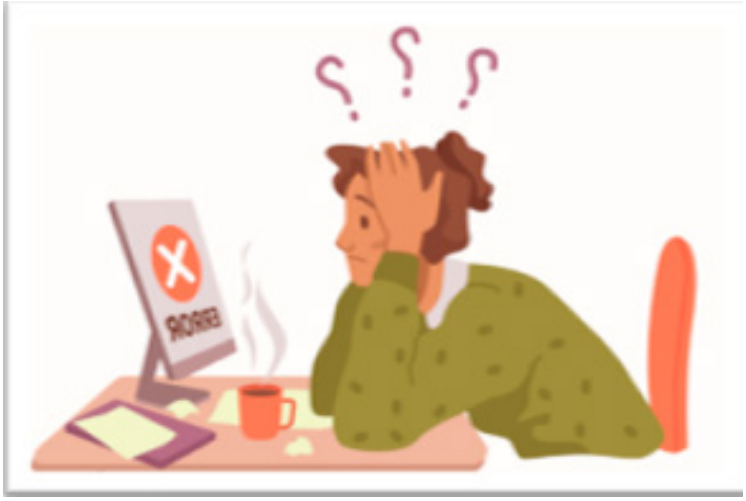
"Garante que a informação estará disponível sempre que for necessário".

Isso quer dizer que a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la. O hardware e o software devem estar em perfeito funcionamento para garantir a disponibilidade da informação.

De maneira bem simples, esse princípio está relacionado à garantia do acesso as informações e isso quer dizer que, independentemente de qualquer coisa, o usuário deve ter acesso às informações de forma contínua, sem interrupções.



Algumas situações podem violar o princípio da Disponibilidade e vou citar alguns exemplos com breves explicações para que você saiba identificar o problema e a possível solução.



ATAQUE DE NEGAÇÃO DE SERVIÇO (DOS)

Esse é um ataque que retira do ar um serviço, tornando-o inacessível ao usuário, consequentemente tornando o sistema e as informações indisponíveis.

Mecanismos de proteção contra ataques de negação de serviço e intrusão:

- **Firewall:** dispositivo que filtra tanto as conexões de entrada quanto as de saída de dados.
- **Sistema de Detecção de Invasão/Intrusão (IDS):** sistema de segurança que monitora o tráfego de rede em busca de padrões ou comportamentos anormais que possam identificar uma tentativa de invasão.
- **Sistema de Prevenção de Invasão (IPS):** sistema de segurança que complementa o IDS, tomando medidas ativas para bloquear e prevenir invasões em tempo real.

FALHAS DE INFRAESTRUTURA

Pode ser qualquer tipo de problema técnico relacionado ao hardware, que cause indisponibilidade de sistemas, aplicativos ou serviços.

Mecanismos de prevenção/proteção contra falhas de infraestrutura:

- **Equipamentos redundantes:** é o uso de equipamentos sobressalentes para substituir aquele que está em uso, em caso de falha.
- **Nobreak:** aparelho que armazena carga elétrica em baterias, capaz de fornecer energia elétrica por algum período quando a corrente elétrica alternada é interrompida.
- **Backup**: cópia de segurança dos dados.

Falhas de Segurança: as falhas de segurança podem ocorrer por meio de invasão de indivíduos mal-intencionados. Esse tipo de falha pode resultar na indisponibilidade dos sistemas afetados.
Mecanismos de prevenção/proteção contra falhas de Segurança:

- **Backup:** cópia de segurança dos dados.
- **Equipamentos redundantes**: é o uso de equipamentos sobressalentes para substituir aquele que está em uso, em caso de falha.

Desastres Naturais: São os eventos imprevisíveis que podem danificar a infraestrutura física e tecnológica, causando interrupções, perda ou indisponibilidade do sistema.

Mecanismos de prevenção contra desastres naturais:

- **Backup**: cópia de segurança dos dados.
- **Equipamentos redundantes:** é o uso de equipamentos sobressalentes para substituir aquele que está em uso, em caso de falha.

São várias as causas que podem violar a disponibilidade, mas também há diversas ferramentas que garantem a disponibilidade da informação, como já vimos anteriormente. Mas quero falar um pouco mais sobre essas ferramentas que garantem esse princípio, pois geralmente é isso que as questões de concursos exploram.

Portanto vou exemplificar as ferramentas que mais estão presentes nas provas:

- Nobreak;
- Firewall;
- Backup;
- Equipamentos Redundantes.

Nobreak: aparelho que armazena carga elétrica em baterias, capaz de fornecer energia elétrica por algum período quando a corrente elétrica alternada é interrompida.

Para que você consiga visualizar melhor, veja esse exemplo:

Fernando é um funcionário de uma empresa de marketing e precisa fazer um relatório de produção. Durante algumas semanas, ele coletou vários dados e salvou diariamente no computador do seu escritório. Dois dias antes da entrega desse relatório, houve uma queda de energia e tudo que Fernando havia produzido até aquela hora continuou lá, pois em seu escritório tinha um nobreak de energia que assegurou que ele não perdesse toda produção até o momento. Nesse caso, um hardware assegurou a disponibilidade. Mas digamos que, de alguma forma, o disco rígido do computador do Fernando parou de funcionar. Nesse caso,

Fernando utilizaria os backups para ter acesso às informações, utilizando, dessa forma, um software para garantir o princípio da disponibilidade

Firewall: dispositivo que filtra tanto as conexões de entrada quanto as de saída de dados.

Para que você consiga visualizar melhor, veja esse exemplo:

Camila utiliza um firewall configurado para controlar quais tipos de conexões de rede são permitidos em seu computador pessoal. O firewall atua como uma "barreira" filtrando o tráfego de entrada e saída de dados, conforme definido em configuração. Graças ao firewall Camila pode usufruir da rede com maior segurança, sabendo que o firewall é uma medida a mais de segurança para proteger suas informações e garantir a disponibilidade das informações.	

Backup: cópia de segurança dos dados.

Para que você consiga visualizar melhor, veja esse exemplo:

Bruna está no último período da graduação e constantemente faz backups para assegurar que seu trabalho de conclusão de curso esteja seguro. Dessa forma, em caso de perda dos dados originais, Bruna poderá restaurar o arquivo rapidamente, garantindo a disponibilidade das informações contidas no backup.

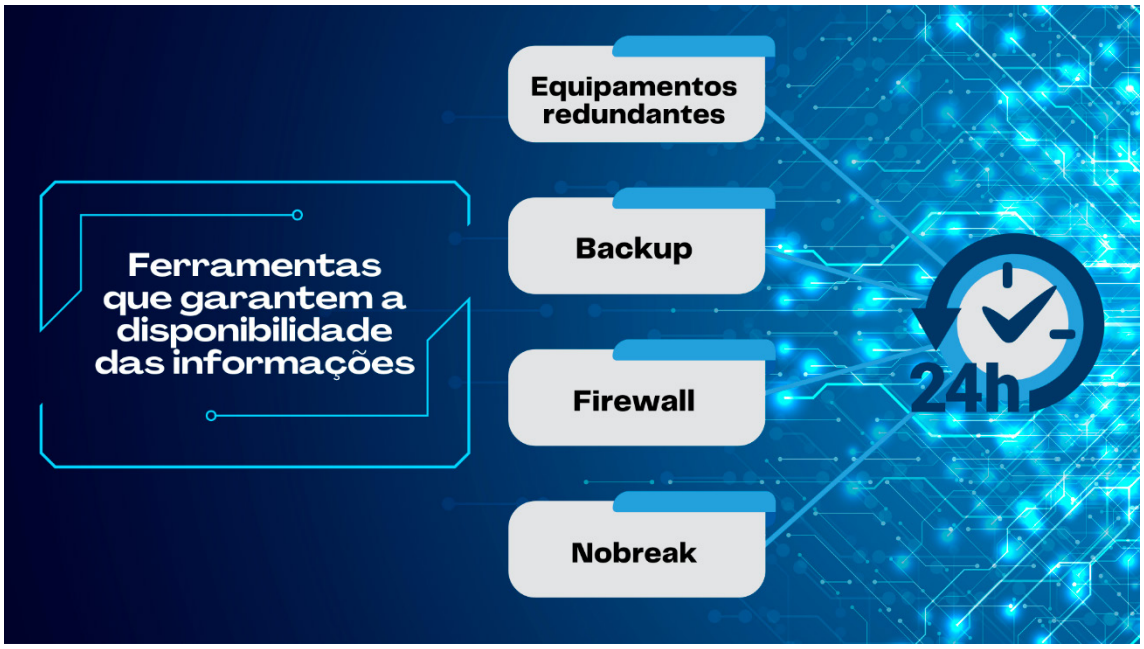
O Backup além de assegurar o princípio da disponibilidade, também assegura o princípio da integridade, que veremos em momento oportuno.

Equipamentos redundantes: é o uso de equipamentos sobressalentes para substituir aquele que está em uso, em caso de falha.

Para que você consiga visualizar melhor, veja esse exemplo:

	Uma empresa de marketing digital para garantir a disponibilidade contínua dos dados implementa um servidor sobressalente. Isso significa que a empresa disporá de dois servidores idênticos e operacionais. Dessa forma, se um servidor principal enfrentar alguma falha, o outro equipamento estará disponível, mantendo disponível todas as informações necessárias.

Veja esse mapa mental sobre as ferramentas que garantem o princípio da disponibilidade das informações.



3.2. INTEGRIDADE

"A informação só pode ser alterada por pessoas autorizadas".

Diariamente, grandes organizações, governo, setores de segurança, pessoas jurídicas ou físicas, entre outros, trocam informações, mas a grande preocupação é de fato saber

se aquela informação foi violada, se está completa ou se aqueles dados são os mesmos da mensagem original.

O princípio da integridade assegura que a informação não sofra qualquer alteração por usuário NÃO autorizado. Além de garantir entrega, recebimento ou armazenamento do conteúdo completo sem qualquer perda. Também garante a completude da informação, ou seja, garante que não se perca parte da informação ou que ela permaneça completa.

Qualquer evento ou ação que comprometa a integridade das informações podem violar o princípio da Integridade. Portanto, vou citar alguns exemplos com breves explicações para que você saiba identificar o problema.

Modificações não autorizadas: a adulteração NÃO autorizada de arquivos, registros, sistemas e banco de dados podem violar a Integridade.

Ataques de malware: ataques como vírus e trojan podem corromper a integridade dos dados, portanto violando o princípio da integridade.

Veja alguns exemplos de ferramentas que garantem a integridade da informação:

- Backup;
- Assinatura Digital.

Backup: é cópia de segurança dos dados.

Já vimos o exemplo do uso do backup na garantia da disponibilidade dos dados, agora veja esse exemplo do backup em relação à garantia da integridade dos dados.

Joana sofreu um ataque cibernético o qual acarretou perda parcial de seus dados, fazendo com que eles deixassem de ser íntegros. Diante desse cenário, Joana recorreu ao seu Backup para recuperar seus dados em sua integralidade, visto que o backup restaura os dados de maneira integral.

Assinatura digital: Ferramenta usada para autenticar a veracidade da autoria de uma informação. Ela garante a autenticidade, mas também é usada para garantir que a informação não sofra nenhuma alteração sem a devida permissão(Integridade). Quando um documento é assinado eletronicamente, se ele sofrer alteração, automaticamente essa assinatura será invalidada. Outra característica da assinatura digital é que ela pode ser utilizada tanto por pessoas físicas quanto por pessoas jurídicas.

Para que você consiga visualizar melhor, veja esse exemplo:

Daiana enviou um documento Word assinado digitalmente para seu chefe. No entanto, posteriormente, o chefe alterou alguns pontos do documento. Após a alteração, a integridade do documento foi comprometida, invalidando a assinatura digital de Dayana.

É como se fosse uma assinatura a próprio punho, que atesta sua identidade no documento, porém serve para assinar documentos digitais. Lembre-se: a assinatura digital possui validade jurídica.

3.3. CONFIDENCIALIDADE

"Garante que a informação apenas poderá ser acessada por pessoas autorizadas".

A confidencialidade é o princípio que visa garantir o sigilo das informações, impedindo que elas sejam acessadas por pessoas não autorizadas.

Algumas situações podem violar o princípio da Confidencialidade e vou citar alguns exemplos com breves explicações para que você saiba identificar o problema.

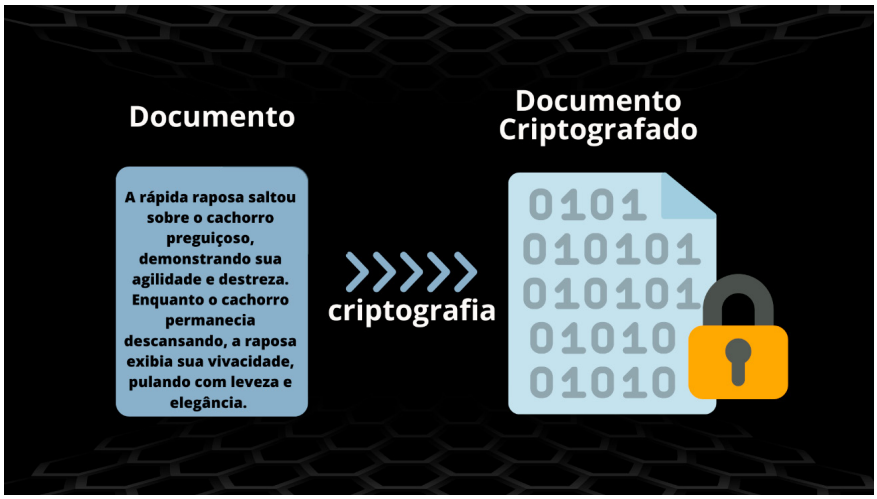
Spyware: tipo de software malicioso espião, que coleta dados confidenciais ou não, sem o conhecimento do usuário.

Sniffing: tipo de ataque que intercepta e monitora o tráfego de rede em busca de informações sensíveis (confidenciais).

O exemplo de ferramenta que garante a confidencialidade da informação:

- Criptografia;
- Certificado Digital.

Criptografia: De maneira bem simples. Criptografia é o mecanismo que transforma a informação original em algo ilegível, por meio de chaves ou códigos, de maneira que um agente sem autorização seja incapaz de compreender. Essa técnica envolve a conversão de informações inteligíveis em um texto cifrado (dados ilegíveis). O objetivo da criptografia é a proteção dos dados confidenciais, impedindo o acesso ou a compreensão da informação por pessoas não autorizadas.



Certificado digital: documento eletrônico que contém os dados pessoais do usuário, suas chaves públicas, dados da autoridade certificadora e data de validade. O certificado digital permite fazer criptografia de chave pública, portanto também garante a confidencialidade.

3.4. AUTENTICIDADE

Garante a veracidade da autoria da informação e, também, o não repudio".
Esse princípio busca garantir que o autor da informação é de fato quem diz ser.

Calma que vou explicar com um exemplo para que você compreenda melhor o que estou falando.

EXEMPLO

Um desembargador ao proferir uma sentença no processo judicial eletrônico (PJE) confirma a sua identidade por meio de sua assinatura digital, de forma a confirmar que foi ele quem proferiu a sentença, não havendo dúvidas em relação a sua identidade.

Algumas situações podem violar o princípio da Autenticidade e vou citar alguns exemplos com breves explicações para que você saiba identificar como isso pode ocorrer.

Ataque de Spoofing: é a situação em que o atacante intercepta a conexão do usuário passando-se como servidor perante o usuário e como usuário perante o servidor.

Golpe de Pharming e Phishing: golpes em que o atacante forja um site passando-se por uma instituição conhecida como um banco ou uma loja virtual.

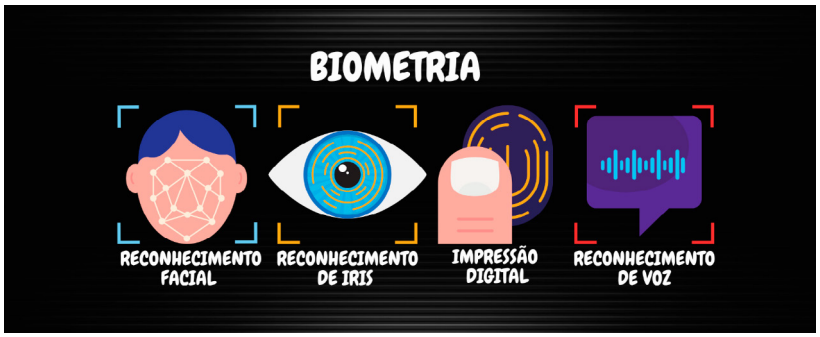
Veja os exemplos de ferramentas que garantem a autenticidade da informação:

- Certificado Digital;
- Assinatura Digital;
- Biometria.

Certificado digital: documento eletrônico que contém os dados pessoais do usuário, suas chaves públicas, dados da autoridade certificadora e data de validade.

Assinatura digital: Ferramenta usada para autenticar a veracidade da autoria de uma informação.

Biometria: mecanismo que analisa as características físicas, de forma a identificar o usuário.



Autenticação em Múltiplas Etapas (Multifactor Authentication): Esse é um método de autenticação que exige mais de uma etapa para verificação de identidade de uma pessoa.

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

Geralmente autenticação em múltiplo fatores envolve algo que o usuário conhece, como por exemplo uma senha, algo que o usuário possui, como por exemplo o seu smartphone e algo inerente ao usuário, como por exemplo sua impressão digital ou reconhecimento facial. Essas outras etapas servem para proteger o acesso em casos em que a senha do usuário é descoberta pelo atacante e 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 o acesso não autorizado.

E assim terminamos essa parte dos principais Princípios de Segurança da Informação. Esses princípios que estudamos são os que mais caem em questões de concursos. Quando você for responder as questões dessa aula, concordará com que estou falando.

Mas também veremos outros princípios e conceitos de segurança, os quais são secundários ou periféricos, sendo também importantes para consolidar esse tema.

Mas antes, vamos relembrar quais são os princípios básicos de segurança, por meio desse mnemônico, a famosa DICA:

Deixo para você um importantíssimo mapa mental para nosso estudo a seguir. Ele é importantíssimo, pois mapeia as ferramentas que garantem os princípios básicos. Perceba que uma mesma ferramenta pode garantir mais de um princípio básico:

4. PRINCÍPIOS SECUNDÁRIOS E OUTROS CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

Como dito, esses princípios são periféricos e não centrais, como os quatro anteriores que vimos agora há pouco. Vejamos quais são eles.

4.1. IRRETRATABILIDADE OU NÃO REPÚDIO

A irretratabilidade, também conhecida como "Não Repúdio", é a propriedade que garante que uma pessoa não pode negar ser a autora de uma transação ou informação, uma vez que foi autenticada para isso. Esse princípio visa garantir que uma pessoa autenticada não consiga negar a autoria de alguma informação ou transação em momento posterior.

Para que você consiga visualizar melhor, veja esse exemplo:

Luciana assinou com sua assinatura digital o procedimento de pregão eletrônico que possuía várias irregularidades e ilegalidades. Ao ser confrontada, alegou que não havia sido ela a responsável pelo procedimento, mas sim uma colega de trabalho. Nesta situação, não há como Luciana negar a autoria de seus atos, visto que todo procedimento fora assinado digitalmente.

Geralmente alguns alunos confundem irretratabilidade com autenticidade, por isso fiz um mapa mental para te auxiliar. Mas lembre-se: a autenticidade confirma a autoria, enquanto a irretratabilidade impede que a autoria seja negada.

4.2. IDENTIFICAÇÃO

"Permitir que uma entidade se identifique, ou seja, diga quem ela é".

A identificação consiste em um processo que visa permitir que uma entidade, e aqui entidade pode ser entendida como uma pessoa, uma empresa ou um programa de computador, se declare e forneça informações sobre sua identidade.

4.3. AUTENTICAÇÃO

"Verificar se a entidade e realmente quem ela diz ser."

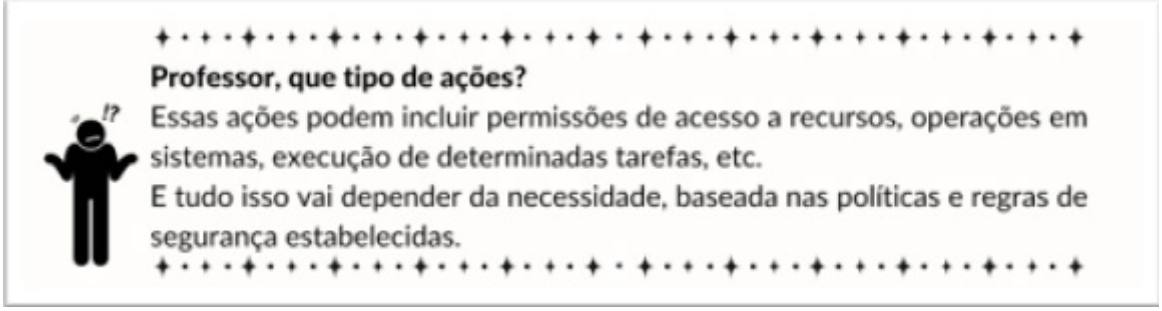
A autenticação consiste em um processo que visa confirmar a identidade de uma entidade (pessoa, empresa ou programa de computador). Para que seja possível a autenticação, faz-se necessário o uso de elementos ou informações que, geralmente, somente a entidade saiba.

São exemplos desses elementos: senhas, códigos, chaves de criptografia ou biometria.

4.4. AUTORIZAÇÃO

"Determinar as ações que a entidade pode executar."

A autorização está relacionada a atribuição de permissões e direitos a uma entidade (pessoa, empresa ou programa de computador) para realizar determinadas ações.



4.5. CONFIABILIDADE

A confiabilidade é um princípio secundário e está relacionado à capacidade de um sistema em manter a constância de serviços ao longo do tempo, sem interrupções ou falhas. Ou seja, ser capaz de cumprir o propósito para o qual foi criado, entregar aquilo que promete.

A confiabilidade visa assegurar que os sistemas, dispositivos e procedimentos sejam capazes de proteger as informações e garantir que elas estejam disponíveis sempre que precisar (disponibilidade), íntegras, ou seja, completas e inalteradas (integridade) e confidenciais quando necessário (confidencialidade).

4.6. PRIMARIEDADE

Esse princípio está disponível na Lei de Acesso à Informação e está relacionado a qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

Exemplo de primariedade: dados fornecidos para um cadastro e armazenados em sua forma original, ou seja, sem passar por qualquer tipo de processamento.

4.7. LEGALIDADE NA SEGURANÇA DA INFORMAÇÃO

Esse princípio está relacionado a maneira que as informações são utilizadas, isso porque as informações devem ser utilizadas de acordo com as legislações aplicáveis ao tema, além dos regulamentos, licenças e contratos.

Como vimos no começo da aula, alguns exemplos de legislações sobre o tema, elas e todas as outras relacionadas ao tema devem ser respeitadas para que esse não seja violado.

Para você relembrar, alguns exemplos de legislações sobre o tema:

Lei n. 13.709/2018 – Lei Geral de Proteção de Dados - Essa legislação regula a proteção dos dados pessoais buscando a proteção da privacidade e intimidade dos indivíduos.

Lei n. 12.965/2014 - Lei do Marco Civil da Internet – Essa Lei traz princípios, direitos e deveres para a utilização da internet no Brasil.

Lei n. 12.737/2012 - Carolina Dieckmann – Essa Lei tipifica crimes cibernéticos, com finalidade de minimizar as práticas ilegais no ambiente virtual.

Terminamos nosso estudo sobre princípios básicos de segurança da informação.

Parabéns por sua perseverança e disciplina!

Eu espero ter atendido as suas expectativas e me coloco à disposição para responder qualquer dúvida, caso você tenha alguma, sobre esse tema.

Fórum de Dúvidas

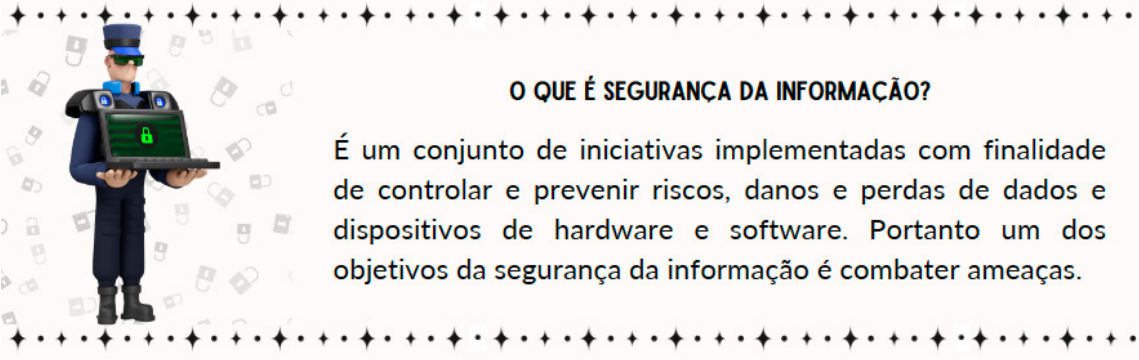
Excelente iniciativa em buscar esclarecer suas dúvidas! Caso tenha alguma questão sobre o conteúdo estudado, não hesite em postá-la no fórum de dúvidas. Farei de tudo para responder o mais rápido possível. Caso sua dúvida seja relacionada a alguma questão, seria ótimo se pudesse transcrevê-la para que eu possa ajudá-lo(a) de forma mais rápida e precisa. Estou à disposição para ajudar!

Se você gostou da aula, ficarei muito grato se puder avaliá-la. Lembre-se que notas de 4 e 5 são consideradas boas, enquanto notas de 1, 2 e 3 são consideradas ruins. É importante ressaltar que a avaliação diz respeito apenas ao conteúdo apresentado e didática do professor, não ao **seu** desempenho nem ao nível de dificuldade da aula. Não esqueça de deixar um comentário quando fizer sua avaliação, pois isso ajuda muito a entender sua nota. Caso você tenha alguma sugestão para melhorar o material, por favor, fique à vontade para compartilhar. Sua opinião é muito valiosa para mim.

Obrigado pela sua companhia nesse estudo teórico de conceitos básicos. Te vejo na resolução das questões, até logo!

RESUMO

Nesse estudo vamos tratar sobre os conceitos básicos de segurança da informação e como esse tópico é abordado em questões de concursos.



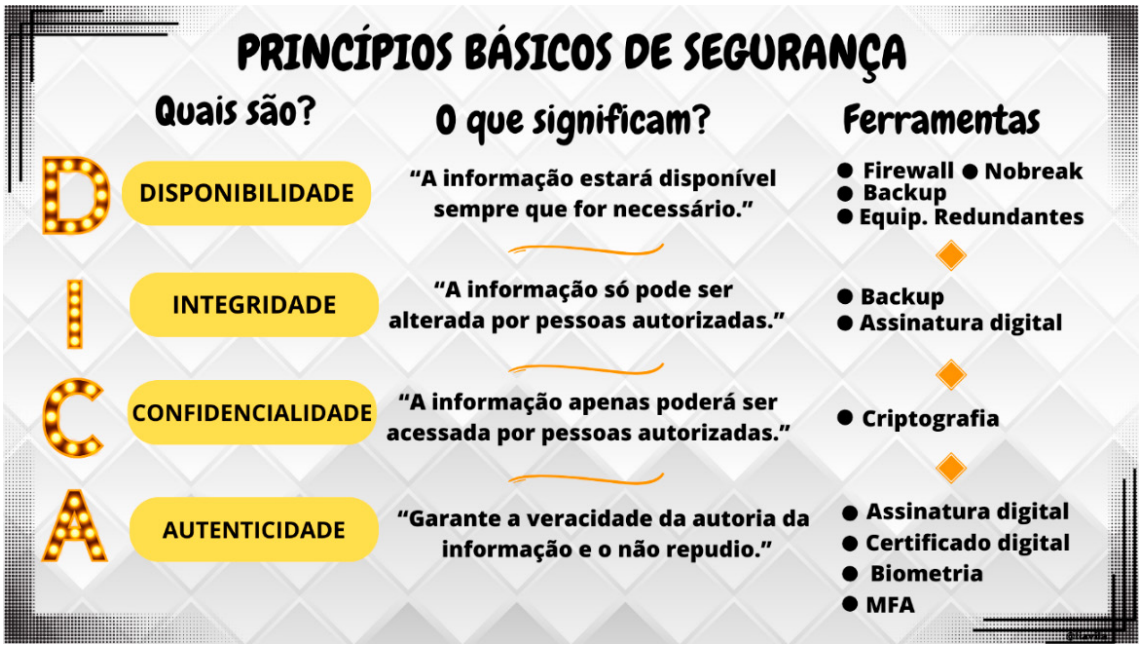
CONCEITO DE SEGURANÇA DA INFORMAÇÃO

PRINCÍPIOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

São princípios da segurança da informação:

- Disponibilidade;
- Integridade;
- Confidencialidade;
- Autenticidade.

Talvez esse seja o mapa mental mais importante dessa aula.

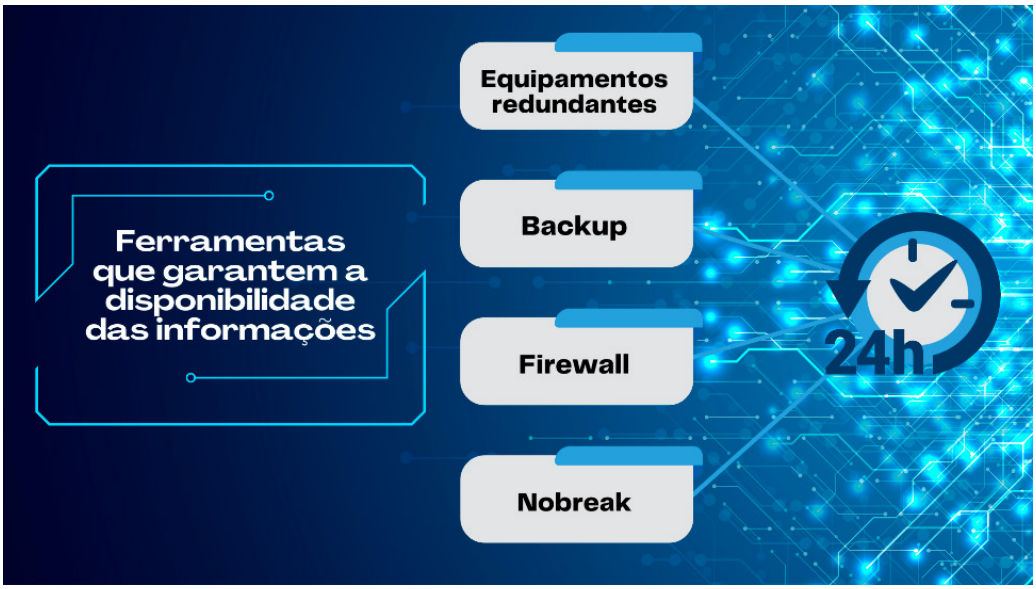


- **Disponibilidade:** A informação estará disponível sempre que for necessário.

Isso quer dizer que a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la. O hardware e o software devem estar em perfeito funcionamento para garantir a disponibilidade da informação.

Ferramentas que garantem a disponibilidade:

- Nobreak;
- Firewall;
- backup;
- equipamentos redundantes.



Veja esse mapa mental sobre as ferramentas que garantem o princípio da disponibilidade das informações.

- **Integridade:** A informação só pode ser alterada por pessoas autorizadas.

O princípio da integridade assegura que a informação não sofra qualquer alteração por usuário NÃO autorizado. Além de garantir entrega, recebimento ou armazenamento do conteúdo completo sem qualquer perda. Também garante a completude da informação, ou seja, garante que não se perca parte da informação ou que ela permaneça completa.

Veja alguns exemplos de ferramentas que garantem a integridade da informação:

- backup;
- assinatura digital.

- **Confidencialidade:** A informação apenas poderá ser acessada por pessoas autorizadas.

A confidencialidade é o princípio que visa garantir o sigilo das informações, impedindo que elas sejam acessadas por pessoas não autorizadas.

O exemplo de ferramenta que garante a confidencialidade da informação:

- Criptografia;
- Certificado digital.

Autenticidade: Garante a veracidade da autoria da informação e, também, o não repudio.

Esse princípio busca garantir que o autor da informação é de fato quem diz ser.
Veja os exemplos de ferramentas que garantem a autenticidade da informação:

- certificado digital;
- assinatura digital;
- biometria;
- Autenticação em Múltiplas Etapas (Multifactor Authentication).

E assim terminamos essa parte dos principais Princípios de Segurança da Informação.
Reveja esse importantíssimo mapa mental:

PRINCÍPIOS SECUNDÁRIOS E CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

- **Irretratabilidade ou Não Repúdio:** A irretratabilidade, também conhecida como "Não Repúdio", é a propriedade que garante que uma pessoa não pode negar ser a autora de uma transação ou informação, uma vez que foi autenticada para isso. Esse princípio visa garantir que uma pessoa autenticada não consiga negar a autoria de alguma informação ou transação em momento posterior.

- **Identificação:** permitir que uma entidade se identifique, ou seja, diga quem ela é.

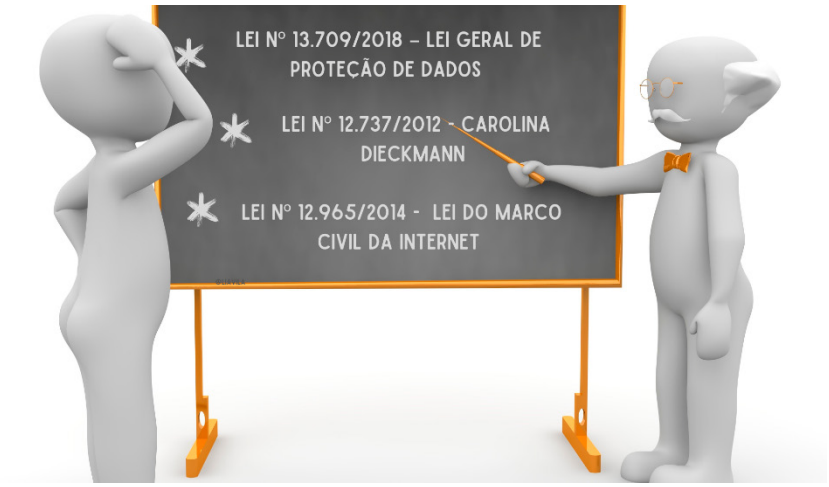
- **Autenticação:** verificar se a entidade e realmente quem ela diz ser.

A autenticação consiste em um processo que visa confirmar a identidade de uma entidade (pessoa, empresa ou programa de computador).

- **Autorização:** determinar as ações que a entidade pode executar.

A autorização está relacionada a atribuição de permissões e direitos a uma entidade (pessoa, empresa ou programa de computador) para realizar determinadas ações.

- **Confiabilidade:** A confiabilidade é um princípio secundário e está relacionado a capacidade de um sistema em manter a constância de serviços ao longo do tempo, sem interrupções ou falhas.
- **Primariedade:** Esse princípio está disponível na Lei de Acesso à Informação e está relacionado a qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.



- **Legalidade na Segurança da Informação:** Esse princípio está relacionado a maneira que as informações são utilizadas, isso porque as informações devem ser utilizadas de acordo com as legislações aplicáveis ao tema, além dos regulamentos, licenças e contratos.

Lei n. 13.709/2018 – Lei Geral de Proteção de Dados - Essa legislação regula a proteção dos dados pessoais buscando a proteção da privacidade e intimidade dos indivíduos.

Lei n. 12.965/2014 - Lei do Marco Civil da Internet – Essa Lei traz princípios, direitos e deveres para a utilização da internet no Brasil.

Lei n. 12.737/2012 - Carolina Dieckmann – Essa Lei tipifica crimes cibernéticos, com finalidade de minimizar as práticas ilegais no ambiente virtual.

Terminamos nosso resumo sobre conceitos básicos de segurança da informação.

Parabéns por sua resiliência e disciplina!

QUESTÕES DE CONCURSO

Agora que você conseguiu finalizar a parte teórica, vamos praticar a fundo tudo aquilo que foi visto, mas com muitas questões. Muito bem, foram selecionadas 50 questões de diferentes bancas muito conceituadas no mundo dos concursos. Todas as questões foram extraídas do nosso site Gran Questões, https://questoes.grancursosonline.com.br/, e possuem um identificador ou ID, por meio do qual é possível localizá-las pelo campo Pesquisar. Faça bom proveito dessa incrível ferramenta que a Assinatura Ilimitada oferece a você.

Primeiramente, trarei as questões para você resolvê-las. Logo após a bateria de questões, teremos o seu gabarito e, sem seguida, teremos cada uma delas comentadas com minha explicação, na qual procurei ser o mais minucioso possível para que não reste nenhuma dúvida e você nem precise voltar ao caderno de teoria. Mas se ainda assim você ficar com dúvida, não tem problema: é só me procurar no fórum de dúvidas que eu vou te responder o mais rápido possível.

Se quiser estar um pouco mais próximo de mim, venha para minha rede social no Instagram, ***@prof.mauriciofranceschini*** ou aponte a câmera do seu celular para o QR-Code abaixo. E se quiser fazer o meu curso completaço, você pode apontar para o outro QR-Code da direita, no qual você encontrará todas as matérias de Informática e Direito Digital, como LGPD, LAI, Marco Civil da Internet, SEI e tantas outras aulas. Te espero lá pra me dizer quantas questões deste caderno você gabaritou, ok?

Bom, sem mais delongas, mão na massa! Tenha um excelente desempenho!

001. (Q4323616/CPCON UEPB/PREFEITURA DE CONDADO/ELETRICISTA/2026) Um hospital foi alvo de um ataque cibernético que comprometeu seu sistema de prontuários eletrônicos de diferentes maneiras. Após a perícia técnica, foram identificados três impactos distintos:
I – Informações sigilosas de pacientes foram copiadas e divulgadas publicamente na internet;
II – Registros clínicos referentes a medicamentos administrados sofreram alterações não autorizadas, resultando em dosagens incorretas;
III – Profissionais de saúde devidamente credenciados ficaram impossibilitados de acessar os prontuários eletrônicos por aproximadamente 48 horas.
Considerando os princípios fundamentais de segurança da informação, a sequência CORRETA de violações configuradas por essas situações é:
a) Confidencialidade, Integridade e Disponibilidade.
b) Integridade, Confidencialidade e Autenticidade.
c) Disponibilidade, Integridade e Confidencialidade.
d) Autenticidade, Disponibilidade e Integridade.
e) Confidencialidade, Disponibilidade e Integridade.

002. (Q4313834/IBADE/PC ES/INVESTIGADOR DE POLÍCIA/2026) No contexto da segurança da informação, a tríade CIA (Confidencialidade, Integridade, Disponibilidade) é um modelo fundamental. Qual a relação entre a não repudiação e a autenticidade dentro deste modelo, e como a criptografia de chave pública contribui para ambos?
a) Não repudiação e autenticidade são sinônimos; criptografia de chave pública garante apenas confidencialidade.
b) Não repudiação é um subconjunto da disponibilidade; criptografia de chave pública assegura a integridade dos dados.
c) Autenticidade é irrelevante para não repudiação; criptografia de chave pública é usada para controle de acesso.
d) Autenticidade garante a identidade do remetente, e não repudiação impede que o remetente negue o envio; criptografia de chave pública, através de assinaturas digitais, provê ambos
e) Ambos são conceitos externos à tríade CIA; criptografia de chave pública é apenas para confidencialidade.

003. (Q4284589/FUNDATEC/PC RS/ESCRIVÃO DE POLÍCIA CONHECIMENTO ESPECÍFICOS/2026) Na cadeia de custódia de evidências digitais, os algoritmos de hash, como MD5, SHA-1 e SHA-256, podem ser utilizados para garantir a _____ dos dados, permitindo detectar se houve qualquer alteração no conteúdo original entre a fase de coleta e a fase de análise. Assinale a alternativa que preenche corretamente a lacuna do trecho acima.
a) integridade
b) disponibilidade
c) confidencialidade
d) irretratabilidade
e) conformidade

004. (9Q4011458/FURB/PREFEITURA DE BIGUAÇU/MÉDICO CARDIOLOGISTA/2025) Uma empresa exige que cada ordem de compra eletrônica seja assinada digitalmente, garantindo que o signatário não possa, posteriormente, negar que enviou o documento. Sobre esse procedimento de controle, assinale a alternativa que apresenta o princípio fundamental de segurança da informação que ele aborda:
a) Disponibilidade.
b) Não repúdio.
c) Integridade.
d) Autenticidade.
e) Confidencialidade.

005. (Q3650678/SELECON/PREFEITURA DE SINOP/TÉCNICO DE MULTIMEIOS DIDÁTICOS/2025) Segurança da informação é definida como a proteção de informações importantes contra acesso não autorizado, divulgação, uso, alteração ou interrupção, com o objetivo de assegurar que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados e permaneçam confidenciais. Entre os pilares da segurança da informação, um deles relaciona-se com a veracidade da informação durante todo o seu ciclo de vida, sendo seu princípio básico que as informações permanecem imutáveis quando estão em repouso ou durante sua transmissão, significando garantir que todas as informações contidas nos bancos de dados da empresa sejam completas e precisas. Esse pilar da segurança da informação é denominado:
a) confidencialidade
b) confiabilidade
c) autenticidade
d) integridade

006. (Q3872798/CPCON UEPB/PREFEITURA DE POMBAL/RECEPCIONISTA/2025) Existiu uma época em que as informações eram armazenadas, unicamente, em papel e, por isso, o controle, a segurança e a privacidade das informações eram mais simples. Com o advento da tecnologia tornou-se necessário mais investimentos e estruturas lógicas e robustas de segurança.Em relação as boas práticas em segurança da informação, analise as proposições a seguir:
I – A segurança da informação tem como objetivo proporcionar e garantir os seguintes princípios: integridade, confidencialidade e disponibilidade das informações.
II – A confidencialidade é a limitação de acesso às informações.
III – A integridade consiste na inconsistência das informações.
IV – A disponibilidade está relacionada à proteção de que a informação estará assegurada de forma tempestiva.
É CORRETO o que se afirma em:
a) II e III apenas.
b) IV apenas.
c) I, II, III e IV.
d) III apenas.
e) I, II e IV apenas.

007. (Q4292138/IBAM/CÂMARA PARAÍBA DO SUL/TÉCNICO ADMINISTRATIVO/2025) A segurança da informação está relacionada a uma série de boas práticas focadas especialmente em garantir a proteção dos dados de instituição, a mitigação dos riscos e a adequação às leis vigentes. A segurança da informação baseia-se em pilares, sendo dois deles descritos a seguir.

I – Está diretamente relacionado ao sigilo dos dados, sendo que seu princípio básico estabelece que as informações serão "tratadas" apenas pelas pessoas para as quais o acesso foi fornecido.
II – Está diretamente relacionado à veracidade da informação durante todo o seu ciclo de vida, sendo que seu princípio básico estabelece que as informações permanecem imutáveis quando estão em repouso ou durante sua transmissão.
Esses pilares são conhecidos, respectivamente, como:
a) autenticidade e confidencialidade
b) confidencialidade e integridade
c) confiabilidade e autenticidade
d) integridade e confiabilidade

008. (Q3807880/UNESC/PREFEITURA/MÉDICO/2025) Podemos pensar nelas como os pilares que sustentam a proteção dos nossos dados e sistemas. Marque a alternativa CORRETA que corresponde as principais propriedades da segurança da informação, frequentemente referidas como o "tríade CID".
a) Confidencialidade, a Integridade e a Disponibilidade.
b) Transmissão, Armazenamento e Processamento.
c) Vulnerabilidade, Ameaças e Organização.
d) Autenticidade, Não Repúdio e Responsabilidade.
e) Tecnologias, Políticas e procedimentos e Conscientização.

009. (Q3717252/SELECON/HEMOMINAS/TÉCNICO EM INFORMÁTICA/2025) Ao adotar a ISO 27002, as organizações se comprometem com um conjunto de boas práticas, com base em três critérios que constituem os pilares fundamentais dessa norma. O primeiro visa a prevenir o acesso não autorizado às informações, já o segundo assegura que os dados não sejam alterados de maneira inadequada, mantendo sua precisão e confiabilidade, e para finalizar, o terceiro garante que as informações estejam acessíveis sempre que necessário.
Esses três pilares são conhecidos, respectivamente, como:
a) disponibilidade, autenticidade e confidencialidade
b) confidencialidade, integridade e disponibilidade
c) autenticidade, confiabilidade e irretratabilidade
d) confiabilidade, irretratabilidade e autenticidade

010. (Q3960666/CEV/UECE/PC CE/INVESTIGADOR DE POLÍCIA/2025) Uma organização precisa implementar a criptografia de dados para proteger suas informações durante a transmissão pela rede. Em relação aos princípios de Segurança da Informação, essa medida visa especificamente garantir o princípio de

a) disponibilidade dos dados.
b) auditoria dos acessos.
c) integridade referencial.
d) confidencialidade das informações.
e) recuperação de desastres.

011. (Q4245307/IGEDUC/PREFEITURA DE SÃO JOSÉ DO SERIDÓ/TÉCNICO DE LABORATÓRIO/ÁREA: ANÁLISES CLÍNICAS/2025) A segurança da informação é um conjunto de práticas, políticas e tecnologias voltadas à proteção de dados e sistemas contra acessos indevidos, perdas e modificações não autorizadas. Com o avanço das comunicações digitais, esses princípios tornaram-se indispensáveis para a confiabilidade das transações eletrônicas e a integridade das informações armazenadas em rede. Com os conhecimentos destes fundamentos, analise as afirmativas a seguir:
I – O pilar da confidencialidade busca garantir que apenas pessoas autorizadas tenham acesso às informações, evitando a exposição de dados sensíveis.
II – O princípio da integridade está relacionado à verificação de que a informação permanece completa, sem alterações indevidas, durante o armazenamento ou a transmissão.
III – A disponibilidade assegura que os dados e sistemas estejam acessíveis sempre que necessários, mas não tem relação com a continuidade das operações de uma organização.
IV – O conceito de autenticidade refere-se à comprovação de que o emissor e o receptor da informação são realmente quem afirmam ser, prevenindo fraudes e falsificações digitais.
Assinale a alternativa correta:
a) Apenas as afirmativas I, II e III são verdadeiras.
b) Apenas as afirmativas I, II e IV são verdadeiras.
c) As afirmativas I, II, III e IV são verdadeiras.
d) Apenas as afirmativas II, III e IV são verdadeiras.

012. (Q4233666/FUNDATEC/IGP/PERITO CRIMINAL/ÁREA GEOLOGIA/2025) Sobre os princípios da segurança da informação, analise as assertivas abaixo:
I – A autenticidade garante que a informação deve ser protegida de acordo com o grau de sigilo aplicado ao seu conteúdo.
II – A integridade garante que a informação deve ser mantida da mesma forma, na mesma condição em que foi disponibilizada por seu proprietário.
III – A conformidade garante que a informação gerada ou adquirida por um indivíduo ou instituição deve estar acessível e operacional para usuários autorizados sempre que necessário.

Quais estão corretas?
a) Apenas I.
b) Apenas II.
c) Apenas I e II.
d) Apenas II e III.
e) I, II e III.

013. (Q4034610/VUNESP/CÂMARA DE MARÍLIA/AUXILIAR DE INFORMÁTICA/2025) Um auxiliar de informática, que não tem acesso ao sistema de contabilidade, mas tem acesso ao banco de dados, recebeu um pedido de um analista da contabilidade para executar um SQL para alterar registros em um banco de dados desse sistema, alterando assim seus valores. O auxiliar de informática sabe que isso não deve ser feito, porque viola um dos 3 pilares fundamentais da segurança da informação. Trata-se de
a) Confidencialidade.
b) Disponibilidade.
c) Monitoramento.
d) Integridade.
e) Acesso.

014. (Q4157649/IBAM/PREFEITURA DE ARRAIAL DO CABO/SECRETÁRIO ESCOLAR/2025) No que se refere à segurança da informação, de equipamentos, de sistemas, em redes, na internet e na nuvem, com a evolução tecnológica, os riscos aumentam e exigem uma gestão de proteção cada vez mais eficaz. A base de defesa dos sistemas e infraestrutura das corporações são os pilares da segurança da informação, que atuam por meio de políticas, senhas, softwares de criptografia, dentre outros processos necessários a essa gestão de riscos. Um desses pilares é responsável por manter as características originais dos dados, assim como foram configuradas em sua criação, destacando que a informação não pode ser alterada sem autorização. Já outro pilar se caracteriza por proteger a informação dos acessos não autorizados, estabelecendo a privacidade para os dados da empresa, evitando situações de ataques cibernéticos ou espionagem. Em consequência, a base desse segundo pilar é controlar o acesso por autenticação de senha, podendo ser também por verificação biométrica, além da criptografia, que vem gerando resultados favoráveis nessa função. Esses dois pilares são conhecidos, respectivamente, como:
a) irretratabilidade e integridade
b) integridade e confidencialidade
c) autenticidade e irretratabilidade
d) confidencialidade e autenticidade

015. (Q4102629/IDECAN/PREFEITURA DE PATOS/FISCAL DE OBRAS E URBANISMO/2025) Durante o desenvolvimento de uma política de segurança para uma organização, um analista de TI identificou a necessidade de proteger os dados contra acessos não autorizados, garantir que as informações não sejam alteradas indevidamente e que estejam disponíveis sempre que necessário. Além disso, buscou implementar ferramentas de defesa contra malwares e ataques. Com base nesse cenário e nos princípios da Segurança da Informação, identifique o item correto.

a) A confidencialidade garante que os dados estejam sempre disponíveis, mesmo após falhas ou ataques.

b) A integridade está relacionada ao uso de firewalls para evitar o acesso físico a servidores de rede.

c) A assinatura digital é um recurso usado apenas para criptografar arquivos sigilosos em backups.

d) A disponibilidade pode ser comprometida por ataques de negação de serviço (DoS), dificultando o acesso aos sistemas.

e) O antivírus é uma ferramenta eficaz apenas contra ataques baseados em rede e não detecta arquivos maliciosos locais.

016. (Q3930308/INSTITUTO CONSULPAM/CONAB/ANALISTA/ÁREA PSICOLOGIA/2025) Os pilares da segurança da informação protegem dados contra ameaças e asseguram a confiabilidade das informações em um mundo digital cada vez mais vulnerável. Dessa forma, analise as sentenças a seguir:

Quando um usuário tenta fazer uma transação bancária e o sistema encontra-se fora do ar, observa-se o comprometimento da disponibilidade.

PORQUE

O pilar da disponibilidade trata da oferta do acesso à informação quando esta é necessária para o usuário.

Acerca dessas sentenças, assinale a alternativa CORRETA.

a) As duas sentenças são verdadeiras, mas a segunda não é uma justificativa correta da primeira.

b) A primeira sentença é verdadeira, e a segunda, falsa.

c) As duas sentenças são verdadeiras, e a segunda é uma justificativa correta da primeira.

d) A primeira sentença é falsa, e a segunda, verdadeira.

017. (Q3997483/FUNDATEC/IF SERTÃO/ADMINISTRADOR/2025) A definição de segurança de computadores do NIST (National Institute of Standards and Technology – Manual NIST SP 800 – 12 Rev. 1) estabelece que o objetivo principal da segurança em sistemas computacionais é

proteger os recursos de informação (hardware, software, firmware, dados e comunicações), garantindo um conjunto de propriedades fundamentais. Considerando essa definição, são objetivos centrais da segurança de computadores:
I – Confidencialidade de dados: garantir que informações privadas e confidenciais não sejam acessíveis por indivíduos ou sistemas não autorizados.
II – Privacidade: assegurar que os indivíduos tenham controle sobre como seus dados pessoais são criptografados, roteados e compartilhados com terceiros.
III – Integridade de dados: garantir que informações e programas sejam modificados somente de forma autorizada e conforme especificado.
IV – Disponibilidade: garantir que os serviços, sistemas e informações estejam acessíveis aos usuários autorizados quando necessário.
Quais estão corretos?
a) Apenas I e III.
b) Apenas II e IV.
c) Apenas I, II e III.
d) Apenas I, III e IV.
e) I, II, III e IV.

018. (Q4250158/IBAM/PREFEITURA DE ARAPIRACA/ASSISTENTE ADMINISTRATIVO EDUCACIONAL/2025) Segurança da informação é definida como a proteção contra acesso não autorizado, divulgação, uso, alteração ou interrupção, tendo por finalidade assegurar que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados, permaneçam confidenciais e mantenham sua integridade. É um conceito que possui pilares como fundamentos, dos quais um deles tem por finalidade garantir que os usuários possam acessar as informações a que estão autorizados a acessar quando precisarem. Esse pilar é denominado:
a) integridade
b) autenticidade
c) disponibilidade
d) irretratabilidade

019. (Q4225810/UNOCHAPECÓ/PREFEITURA DE GUATAMBU/TÉCNICO EM INFORMÁTICA/2025) Esse pilar da segurança de Informação assegura que as informações permaneçam completas e inalteradas durante o armazenamento, o processamento e a transmissão, protegendo contra modificações acidentais ou maliciosas. Marque a alternativa CORRETA que corresponde ao pilar descrito.

a) Disponibilidade.
b) Confidencialidade.
c) Autenticidade.
d) Integridade.

020. (Q3388049/INSTITUTO ÁGATA/PREFEITURA DE ANAJÁS/ASSISTENTE/ÁREA: DIGITAÇÃO DE DADOS/2024) No contexto da segurança da informação, a confidencialidade tem como objetivo garantir
a) que nenhuma pessoa tenha acesso ao arquivo cifrado.
b) a autenticidade da informação, ou seja, dar a certeza da autoria da informação enviada para o destinatário.
c) que somente pessoas autorizadas tenham acesso ao conteúdo do dado cifrado. No contexto simétrico, entende-se como pessoa autorizada aquela que possui a chave secreta.
d) a autenticidade da informação, ou seja, dar a certeza de autoria da informação cifrada.
e) que somente pessoas autorizadas tenham acesso ao arquivo cifrado. No contexto simétrico, entende-se como pessoa autorizada aquela que possui a chave pública.

021. (Q3301560/FUNDATEC/SIMAE/CONTADOR/2024) Em matéria de Segurança da Informação, a garantia da identidade de uma pessoa, seja ela física ou jurídica ou de um servidor (computador) com quem se estabelece uma transação, é chamada de:
a) Confiabilidade.
b) Disponibilidade.
c) Integridade.
d) Confidencialidade.
e) Autenticidade.

022. (Q3194371/CESPE/CEBRASPE/MPE TO/TÉCNICO MINISTERIAL/ÁREA: TÉCNICO EM TELECOMUNICAÇÕES/2024) Acerca da segurança da informação, julgue os seguintes itens.
Uma rede de comunicação atende ao requisito de disponibilidade quando é capaz de garantir que os dados trafegados só sejam acessíveis pelas partes autorizadas, seja para impressão, exibição ou outras formas de divulgação, que incluem a simples revelação da existência de um objeto qualquer.

023. (Q3076445/QUADRIX/CRT SP/ADVOGADO/2023) Quanto aos procedimentos de segurança da informação, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup, julgue os itens de 36 a 40.
Na organização, uma ação que representa uma violação da segurança da informação é o fato de o funcionário ou o colaborador divulgar publicamente informações confidenciais da organização.

024. (Q2685030/Quadrix/CRO/Técnico em Informática/2023) ulgue o item, relativos aos conceitos de proteção e segurança da informação.
A definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

025. (Q2695994/CESGRANRIO/BANRISUL/ESCRITURÁRIO/2023) Os serviços de segurança de uma empresa são implementados por mecanismos de segurança e visam a satisfazer os requisitos da política de segurança dessa empresa. Para aprimorar o serviço de segurança que controla o acesso aos sistemas de informação, o controle de autenticação em uma etapa de verificação está sendo substituído pelo controle de autenticação em mais de uma etapa de verificação.
Esse controle em mais de uma etapa de verificação é conhecido como autenticação
a) complexa
b) resistente
c) qualificada
d) estendida
e) multifator

026. (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.

027. (Q2829853/UFRRJ/UFRRJ/AUDITOR/2023) Com relação aos princípios de segurança da informação, aspectos como confidencialidade, integridade, disponibilidade, legalidade e a autenticidade são considerados pilares.
Sobre estes princípios, é correto afirmar que a
a) autenticidade garante que a informação foi produzida em conformidade com a lei.
b) confidencialidade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.
c) legalidade garante que os dados tenham completeza e estejam disponíveis permanentemente para acesso quando desejados.
d) disponibilidade está relacionada à privacidade e ao sigilo das informações, de modo a garantir o acesso apenas para pessoas autorizadas.
e) integridade garante a completude e exatidão das informações, de modo que sejam preservadas, precisas e confiáveis durante todos os seus ciclos de vida.

028. (Q2685030/QUADRIX/CRO/TÉCNICO EM INFORMÁTICA/2023) Julgue os itens relativos aos conceitos de proteção e segurança da informação.
A definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

029. (Q2706726/FUNDEP/PREFEITURA DE BARRA LONGA/ASSISTENTE SOCIAL/CRAS/2023) Conforme o cert.br, para permitir que possam ser aplicados na internet cuidados similares aos do dia a dia, é necessário que os serviços disponibilizados e as comunicações realizadas pela internet garantam alguns requisitos básicos de segurança, como
a) autenticação, identificação e repúdio.
b) confidencialidade, identificação e repúdio.
c) autenticação, confidencialidade e identificação.
d) autenticação, confidencialidade e repúdio.

030. (Q2682336/MS CONCURSOS/PREFEITURA DE PATROCÍNIO/PSICÓLOGO/2023) De acordo com o Princípio da Disponibilidade, a informação estará disponível sempre que for preciso. Esse aspecto é de suma importância, principalmente, para sistemas que não podem ter falhas na disponibilidade, pois essas falhas comprometem o serviço. Assinale a alternativa que não garante o Princípio da Disponibilidade:
a) Nobreak.
b) Firewall.
c) Backup.
d) Assinatura Digital.

031. (Q2685028/QUADRIX/CRO/TÉCNICO EM INFORMÁTICA/2023) Julgue os itens, relativos aos conceitos de proteção e segurança da informação.
Aplicativos específicos, que ajudam a limpar o registro do computador, podem ser usados com o objetivo de proteger o computador de programas estranhos.

032. (Q2414224/FGV/TJDFT/ANALISTA JUDICIÁRIO/ÁREA SUPORTE EM TECNOLOGIA DA INFORMAÇÃO/2022) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele. Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

a) confidencialidade;
b) autenticidade;
c) integridade;
d) disponibilidade;
e) irretratabilidade.

033. (Q2354044/LEGALLE CONCURSOS/BADESUL DESENVOLVIMENTO/AGÊNCIA DE FOMENTO DO RIO GRANDE DO SUL/TÉCNICO EM DESENVOLVIMENTO/ÁREA: ANALISTA DE SISTEMAS/SEGURANÇA DA INFORMAÇÃO/2022) Sobre segurança da informação, é um princípio que garante que alguém não pode negar algo. Tipicamente, esse princípio se refere à habilidade em assegurar que uma parte de um contrato, ou de uma comunicação, não pode negar a autenticidade de sua assinatura em um documento ou o envio de uma mensagem que originou. Trata-se de qual princípio?
a) Confidencialidade.
b) Integridade.
c) Legalidade.
d) Não repúdio.
e) Autenticidade.

034. (Q2586985/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA: QUALITY ASSURANCE E ANALISTAS DE TESTE/2022) Acerca de confiabilidade, integridade e disponibilidade em segurança da informação, julgue os itens subsequentes.
Ataque de DoS, política de backup não implementada e falha nos discos violam a disponibilidade.

035. (Q2451925/INSTITUTO ACCESS/PREFEITURA DE OURO BRANCO/PSICÓLOGO/2022) No que diz respeito à segurança da informação, um termo técnico está diretamente associado à cópia de segurança dos arquivos, tarefa que pode ser feita por meio de uma mídia física, em CDs/DVDs HDs ou pendrives, mas também pela Internet, por serviços específicos, como armazenamento na nuvem, por exemplo. A ideia é garantir a integridade dos dados e que os documentos importantes possam ser recuperados, mesmo quando há algum problema de hardware, no sistema ou se a máquina (PC ou celular, por exemplo) for roubada.-
Esse termo técnico é conhecido como
a) deadlock.
b) swap.
c) backup.
d) firewall.

036. (Q2464459/UNIFAP/UNIFAP/TÉCNICO EM ASSUNTOS EDUCACIONAIS/2022) No que concerne à segurança da informação, temos os quatro princípios básicos: disponibilidade, integridade, confidencialidade e autenticidade. Assim, quando desejamos garantir a autenticidade em um sistema de informação, podemos usar vários mecanismos, sendo um deles:
a) Biometria
b) Certificado Digital
c) Redundância
d) Backup
e) Encapsulamento

037. (Q2390540/QUADRIX/CRMV SP/TÉCNICO EM INFORMÁTICA/2022) Com relação aos conceitos de proteção e segurança, julgue o item.
A propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, um órgão, uma entidade ou um sistema recebe o nome de autenticidade.

038. (Q2488932/IBADE/CRC RO/ASSISTENTE ADMINISTRATIVO/2022) Sobre o Princípio da Integridade, é correto afirmar que:
a) a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la.
b) garante o sigilo da informação, impedindo que ela seja acessada por pessoas não autorizadas.
c) impossibilita o emissor negar a autoria de determinada mensagem ou transação.
d) assegura que a informação não sofra qualquer alteração por usuário não autorizado. Além de garantir entrega, recebimento ou armazenamento do conteúdo completo sem qualquer perda.
e) garante que o autor da informação é realmente quem ele diz que é.

039. (Q2586438/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA SUPORTE A PLATAFORMA MAINFRAME/2022) Com relação à segurança da informação, julgue o item seguinte.
A integridade da informação, um dos pilares da segurança da informação, visa garantir que a informação esteja disponível a seus usuários, aos quais é conferido o acesso.

040. (Q2269851/CESPE/CEBRASPE/TELEBRAS/ESPECIALISTA EM GESTÃO DE TELECOMUNICAÇÕES/ÁREA ENGENHEIRO DE REDES/2022) Com relação a criptografia e segurança de servidores e sistemas operacionais, julgue o item subsequente.
Irretratabilidade é o mecanismo de segurança que prova que a mensagem foi enviada pela origem especificada e que foi recebida pelo destino especificado.

041. (Q2431465/INAZ do Pará/SAMAE São Bento do Sul/Operador de Máquinas/2022/ADAPTADA) "Para implementar a Segurança da Informação nos seus processos, a empresa deve ter em mente cinco pilares responsáveis por sustentar as políticas, estratégias e práticas de proteção de dados e informações. Um desses pilares trata de garantir que os dados estejam disponíveis apenas para as pessoas autorizadas. Uma das maneiras de garantir o cumprimento desse pilar é a inclusão de controles de acessos (por meio de biometria e liveness, por exemplo), senhas fortes ou criptografia". (IdBlog).
O pilar a que se refere o texto acima é o da
a) integridade.
b) autenticidade.
c) confidencialidade.
d) irretratabilidade.
e) disponibilidade.

042. (Q2404203/IFPA/IFPA/PROFESSOR DE ENSINO BÁSICO, TÉCNICO E TECNOLÓGICO/ÁREA: INFORMÁTICA/2022) Para manter uma comunicação em rede de forma segura, existem algumas propriedades desejáveis. Dado o seguinte cenário, a Pessoa X deseja enviar uma mensagem sigilosa para a Pessoa Y.
Qual propriedade, relacionada à segurança de rede, garante que apenas a Pessoa Y conseguirá entender o conteúdo da mensagem enviada pela Pessoa X?
a) Não repúdio
b) Integridade de Mensagem
c) Segurança Operacional
d) Autenticação do Ponto Final
e) Confidencialidade

043. (Q2586983/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA: QUALITY ASSURANCE E ANALISTAS DE TESTE/2022) Acerca de confiabilidade, integridade e disponibilidade em segurança da informação, julgue os itens subsequentes.
Um gestor que, por acidente, apague um arquivo de inicialização de um serviço web ou insira valores incorretos em uma aplicação de cobrança de um cliente comprometerá a integridade.

044. (Q2341094/OBJETIVA CONCURSOS/PREFEITURA DE SETE LAGOAS/TÉCNICO DE LABORATÓRIO/2022) De acordo com a Cartilha de Segurança para Internet, assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:A assinatura digital permite comprovar a _____ e o(a) _____ de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que não foi alterada.

a) autenticidade | integridade
b) autorização | disponibilidade
c) integridade | autenticidade
d) confidencialidade | não repúdio

045. (Q2509477/CESPE/CEBRASPE/APEX BRASIL/ANALISTA/ÁREA: AUDITORIA INTERNA/2022) O princípio básico voltado à segurança da informação que permite ao usuário recuperar uma informação em sua forma original é a
a) confidencialidade.
b) autenticidade.
c) disponibilidade.
d) integralidade.

046. (Q2484020/RHEMA/CÂMARA DE SEARA/ADVOGADO/2022) Para todas as questões de informática básica tenha por base o software de distribuição atual, na versão Português Brasil, salvo em caso de citação específica de versão ou distribuição no enunciado da questão: Tendo por base os pilares da segurança da informação, temos um total de cinco itens, envolvendo a confidencialidade e a irretratabilidade. Avalie os itens dispostos a seguir e indique aquele que representa uma opção inadequada em relação a estes pilares.
a) Integridade.
b) Disponibilidade.
c) Autenticidade.
d) Sustentabilidade.

047. (Q2284135/AMEOSC/CÂMARA DE BANDEIRANTE/AUXILIAR LEGISLATIVO/2022) Diante de uma enorme troca de informações entre os computadores com as mais variadas informações e principalmente pela vulnerabilidade oferecida pelos sistemas, tornou-se necessário o desenvolvimento de um conjunto de princípios, técnicas, protocolos, normas e regras que visassem garantir um melhor nível de confiabilidade. Dessa forma, tomando por base a segurança da informação, analise o conceito de um dos princípios e assinale a alternativa CORRETA: "Atua para que um indivíduo ou entidade não negue a autoria de uma ação específica (criar ou assinar um arquivo/documento, por exemplo)".
Esse conceito trata do princípio da:
a) Disponibilidade.
b) Autenticidade.
c) Integridade.
d) Irretratabilidade.

048. (Q2366187/UFPE/UFPE/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/ÁREA: SISTEMAS/2022) Um dos objetivos principais da Segurança da Informação é o de assegurar acesso à informação sempre que desejado.
Estamos falando do princípio da
a) Redundância.
b) Privacidade.
c) Disponibilidade.
d) Autenticidade.
e) Acessibilidade.

049. (Q2586333/CESPE/CEBRASPE/BANRISUL/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/ÁREA: DESENVOLVIMENTO/2022) Considerando que uma empresa tenha disponibilizado um website na Internet com as informações cadastrais de clientes e as de pagamentos com cartão de crédito de produtos vendidos, julgue os itens a seguir, com base nos conceitos de confiabilidade, integridade e disponibilidade, bem como nos mecanismos de segurança da informação.
Caso um funcionário da empresa altere maliciosamente os dados informados pelos clientes e armazenados pela organização, essa alteração necessariamente caracteriza uma violação da disponibilidade.

050. (Q2419862/FUNDATEC/PREFEITURA DE SÃO JOSÉ DOS AUSENTES/TÉCNICO EM INFORMÁTICA/2022) Assinale a alternativa que apresenta somente pilares que norteiam a segurança da informação.
a) Integridade e confiança.
b) Comunicabilidade e disponibilidade.
c) Sistemas e pessoas.
d) Autenticidade e confidencialidade.
e) Dados e informações.

GABARITO

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

GABARITO COMENTADO

001. (Q4323616/CPCON UEPB/PREFEITURA DE CONDADO/ELETRICISTA/2026) Um hospital foi alvo de um ataque cibernético que comprometeu seu sistema de prontuários eletrônicos de diferentes maneiras. Após a perícia técnica, foram identificados três impactos distintos:
I – Informações sigilosas de pacientes foram copiadas e divulgadas publicamente na internet;
II – Registros clínicos referentes a medicamentos administrados sofreram alterações não autorizadas, resultando em dosagens incorretas;
III – Profissionais de saúde devidamente credenciados ficaram impossibilitados de acessar os prontuários eletrônicos por aproximadamente 48 horas.
Considerando os princípios fundamentais de segurança da informação, a sequência CORRETA de violações configuradas por essas situações é:
a) Confidencialidade, Integridade e Disponibilidade.
b) Integridade, Confidencialidade e Autenticidade.
c) Disponibilidade, Integridade e Confidencialidade.
d) Autenticidade, Disponibilidade e Integridade.
e) Confidencialidade, Disponibilidade e Integridade.

Vejamos como os incidentes se relacionam com os princípios básicos de segurança da informação:
I – Informações sigilosas de pacientes foram copiadas e divulgadas publicamente na internet – esse incidente expõe a informação a pessoas não autorizadas, especialmente por se tratar de dados de saúde de pacientes, o que, na LGPD, são considerados dados sensíveis. Isso viola o princípio da confidencialidade.
II – Registros clínicos referentes a medicamentos administrados sofreram alterações não autorizadas, resultando em dosagens incorretas – esse incidente viola o princípio da integridade, pois ocorre a alteração de dados por pessoas não autorizadas.
III – Profissionais de saúde devidamente credenciados ficaram impossibilitados de acessar os prontuários eletrônicos por aproximadamente 48 horas – esse incidente viola o princípio da disponibilidade, pois os profissionais ficaram impossibilitados de ter acesso à informação, ou seja, ela se tornou indisponível a esses usuários.
Letra a.

---

002. (Q4313834/IBADE/PC ES/INVESTIGADOR DE POLÍCIA/2026) No contexto da segurança da informação, a tríade CIA (Confidencialidade, Integridade, Disponibilidade) é um modelo

fundamental. Qual a relação entre a não repudiação e a autenticidade dentro deste modelo, e como a criptografia de chave pública contribui para ambos?
a) Não repudiação e autenticidade são sinônimos; criptografia de chave pública garante apenas confidencialidade.
b) Não repudiação é um subconjunto da disponibilidade; criptografia de chave pública assegura a integridade dos dados.
c) Autenticidade é irrelevante para não repudiação; criptografia de chave pública é usada para controle de acesso.
d) Autenticidade garante a identidade do remetente, e não repudiação impede que o remetente negue o envio; criptografia de chave pública, através de assinaturas digitais, provê ambos
e) Ambos são conceitos externos à tríade CIA; criptografia de chave pública é apenas para confidencialidade.

A não repudiação ou não repúdio, que é sinônimo de irretratabilidade, é uma consequência da autenticidade. Pois, uma vez que a autenticidade garante a veracidade de autoria da informação, torna-se impossível negá-la, o que é exatamente a irretratabilidade, ou seja, a impossibilidade de um usuário negar a sua autoria de uma informação.
Letra d.

---

003. (Q4284589/FUNDATEC/PC RS/ESCRIVÃO DE POLÍCIA CONHECIMENTO ESPECÍFICOS/2026) Na cadeia de custódia de evidências digitais, os algoritmos de hash, como MD5, SHA-1 e SHA-256, podem ser utilizados para garantir a _____ dos dados, permitindo detectar se houve qualquer alteração no conteúdo original entre a fase de coleta e a fase de análise. Assinale a alternativa que preenche corretamente a lacuna do trecho acima.
a) integridade
b) disponibilidade
c) confidencialidade
d) irretratabilidade
e) conformidade

A integridade é a garantia de que a informação não será alterada sem a devida permissão. Uma vez que tais algoritmos permitem detectar se houve qualquer alteração no conteúdo original entre a fase de coleta e a fase de análise, isso significa que é a integridade que está sendo garantida no uso deles.
Letra a.

---

004. (9Q4011458/FURB/PREFEITURA DE BIGUAÇU/MÉDICO CARDIOLOGISTA/2025) Uma empresa exige que cada ordem de compra eletrônica seja assinada digitalmente, garantindo que o signatário não possa, posteriormente, negar que enviou o documento. Sobre esse procedimento de controle, assinale a alternativa que apresenta o princípio fundamental de segurança da informação que ele aborda:

a) Disponibilidade.
b) Não repúdio.
c) Integridade.
d) Autenticidade.
e) Confidencialidade.

O não repúdio ou irretratabilidade é a garantia de que o signatário não possa, posteriormente, negar que enviou o documento. Lembre-se que a irretratabilidade pode ser não apenas do envio, mas também do recebimento, ou seja, ela pode garantir que o destinatário não possa negar que recebeu a mensagem.

Letra b.

---

005. (Q3650678/SELECON/PREFEITURA DE SINOP/TÉCNICO DE MULTIMEIOS DIDÁTICOS/2025) Segurança da informação é definida como a proteção de informações importantes contra acesso não autorizado, divulgação, uso, alteração ou interrupção, com o objetivo de assegurar que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados e permaneçam confidenciais. Entre os pilares da segurança da informação, um deles relaciona-se com a veracidade da informação durante todo o seu ciclo de vida, sendo seu princípio básico que as informações permanecem imutáveis quando estão em repouso ou durante sua transmissão, significando garantir que todas as informações contidas nos bancos de dados da empresa sejam completas e precisas. Esse pilar da segurança da informação é denominado:

a) confidencialidade
b) confiabilidade
c) autenticidade
d) integridade

Muito cuidado, pois o enunciado fala da "veracidade da informação durante todo o seu ciclo de vida", isso não está relacionado à autenticidade, pois não foi mencionada a autoria aqui, mas sim o seu conteúdo. Em seguida, temos a confirmação de que se trata da integridade,

pois afirma que “as informações permanecem imutáveis quando estão em repouso ou durante sua transmissão, significando garantir que todas as informações contidas nos bancos de dados da empresa sejam completas e precisas”.

Letra d.

---

006. (Q3872798/CPCON UEPB/PREFEITURA DE POMBAL/RECEPCIONISTA/2025) Existiu uma época em que as informações eram armazenadas, unicamente, em papel e, por isso, o controle, a segurança e a privacidade das informações eram mais simples. Com o advento da tecnologia tornou-se necessário mais investimentos e estruturas lógicas e robustas de segurança.Em relação as boas práticas em segurança da informação, analise as proposições a seguir:

I – A segurança da informação tem como objetivo proporcionar e garantir os seguintes princípios: integridade, confidencialidade e disponibilidade das informações.

II – A confidencialidade é a limitação de acesso às informações.

III – A integridade consiste na inconsistência das informações.

IV – A disponibilidade está relacionada à proteção de que a informação estará assegurada de forma tempestiva.

É CORRETO o que se afirma em:

a) II e III apenas.

b) IV apenas.

c) I, II, III e IV.

d) III apenas.

e) I, II e IV apenas.

Vejamos cada uma das assertivas

I – Certa. Embora não sejam os únicos princípios de segurança da informação, esses são princípios muito importantes: integridade, confidencialidade e disponibilidade das informações.

II – Certa. A confidencialidade impõe restrição de acesso às informações, permitindo que apenas pessoas autorizadas as acessem.

III – Errada. A integridade consiste na CONSISTÊNCIA das informações, garantindo sua completude e o controle de suas alterações, realizadas somente por pessoas autorizadas.

IV – Certa. A disponibilidade vai garantir que a informação esteja disponível sempre que preciso, ou seja, tempestivamente, a todo o momento.

Letra e.

---

007. (Q4292138/IBAM/CÂMARA PARAÍBA DO SUL/TÉCNICO ADMINISTRATIVO/2025) A segurança da informação está relacionada a uma série de boas práticas focadas especialmente em garantir a proteção dos dados de instituição, a mitigação dos riscos e a adequação às leis vigentes. A segurança da informação baseia-se em pilares, sendo dois deles descritos a seguir.
I – Está diretamente relacionado ao sigilo dos dados, sendo que seu princípio básico estabelece que as informações serão "tratadas" apenas pelas pessoas para as quais o acesso foi fornecido.
II – Está diretamente relacionado à veracidade da informação durante todo o seu ciclo de vida, sendo que seu princípio básico estabelece que as informações permanecem imutáveis quando estão em repouso ou durante sua transmissão.
Esses pilares são conhecidos, respectivamente, como:
a) autenticidade e confidencialidade
b) confidencialidade e integridade
c) confiabilidade e autenticidade
d) integridade e confiabilidade

- **Confidencialidade:** garante o sigilo dos dados, ou seja, as informações acessadas apenas pelas pessoas para as quais o acesso foi fornecido.
- **Integridade:** garante a veracidade da informação durante todo o seu ciclo de vida, preservando a imutabilidade das informações, incluída sua completude e o controle das alterações.

Letra b.

---

008. (Q3807880/UNESC/PREFEITURA/MÉDICO/2025) Podemos pensar nelas como os pilares que sustentam a proteção dos nossos dados e sistemas. Marque a alternativa CORRETA que corresponde as principais propriedades da segurança da informação, frequentemente referidas como o "tríade CID".
a) Confidencialidade, a Integridade e a Disponibilidade.
b) Transmissão, Armazenamento e Processamento.
c) Vulnerabilidade, Ameaças e Organização.
d) Autenticidade, Não Repúdio e Responsabilidade.
e) Tecnologias, Políticas e procedimentos e Conscientização.

Eu costumo ensinar os quatro princípios, formando a DICA (disponibilidade, integridade, confidencialidade, autenticidade). Essa questão enfatizou apenas a confidencialidade, a

integridade e a disponibilidade. Isso não significa que a autenticidade não seja um princípio, mas apenas que não houve ênfase nela pelo examinador.

Letra a.

---

009. (Q3717252/SELECON/HEMOMINAS/TÉCNICO EM INFORMÁTICA/2025) Ao adotar a ISO 27002, as organizações se comprometem com um conjunto de boas práticas, com base em três critérios que constituem os pilares fundamentais dessa norma. O primeiro visa a prevenir o acesso não autorizado às informações, já o segundo assegura que os dados não sejam alterados de maneira inadequada, mantendo sua precisão e confiabilidade, e para finalizar, o terceiro garante que as informações estejam acessíveis sempre que necessário. Esses três pilares são conhecidos, respectivamente, como:

a) disponibilidade, autenticidade e confidencialidade
b) confidencialidade, integridade e disponibilidade
c) autenticidade, confiabilidade e irretratabilidade
d) confiabilidade, irretratabilidade e autenticidade

Essa foi uma questão bem completa, abordando não apenas o nome do princípio, mas seu significado, sendo que explorou três deles.

- **Confidencialidade:** visa a prevenir o acesso não autorizado às informações, ou seja, garante que apenas pessoas autorizadas acessem as informações.
- **Integridade:** assegura que os dados não sejam alterados de maneira inadequada, mantendo sua precisão e confiabilidade, ou seja, garante que apenas pessoas autorizadas realizem alterações nas informações.
- **Disponibilidade:** garante que as informações estejam acessíveis sempre que necessário.

Letra b.

---

010. (Q3960666/CEV/UECE/PC CE/INVESTIGADOR DE POLÍCIA/2025) Uma organização precisa implementar a criptografia de dados para proteger suas informações durante a transmissão pela rede. Em relação aos princípios de Segurança da Informação, essa medida visa especificamente garantir o princípio de

a) disponibilidade dos dados.
b) auditoria dos acessos.
c) integridade referencial.
d) confidencialidade das informações.
e) recuperação de desastres.

Essa questão foi além, relacionando a ferramenta ao princípio de segurança, da forma como vimos em nossa aula. Dessa maneira, aprendemos que a criptografia é a ferramenta que garante a confidencialidade da informação, visto que ela se torna inacessível às pessoas não autorizadas, as quais não terão condições de decifrar os dados criptografados.

Letra d.

---

011. (Q4245307/IGEDUC/PREFEITURA DE SÃO JOSÉ DO SERIDÓ/TÉCNICO DE LABORATÓRIO/ÁREA: ANÁLISES CLÍNICAS/2025) A segurança da informação é um conjunto de práticas, políticas e tecnologias voltadas à proteção de dados e sistemas contra acessos indevidos, perdas e modificações não autorizadas. Com o avanço das comunicações digitais, esses princípios tornaram-se indispensáveis para a confiabilidade das transações eletrônicas e a integridade das informações armazenadas em rede. Com os conhecimentos destes fundamentos, analise as afirmativas a seguir:

I – O pilar da confidencialidade busca garantir que apenas pessoas autorizadas tenham acesso às informações, evitando a exposição de dados sensíveis.

II – O princípio da integridade está relacionado à verificação de que a informação permanece completa, sem alterações indevidas, durante o armazenamento ou a transmissão.

III – A disponibilidade assegura que os dados e sistemas estejam acessíveis sempre que necessários, mas não tem relação com a continuidade das operações de uma organização.

IV – O conceito de autenticidade refere-se à comprovação de que o emissor e o receptor da informação são realmente quem afirmam ser, prevenindo fraudes e falsificações digitais.

Assinale a alternativa correta:

a) Apenas as afirmativas I, II e III são verdadeiras.

b) Apenas as afirmativas I, II e IV são verdadeiras.

c) As afirmativas I, II, III e IV são verdadeiras.

d) Apenas as afirmativas II, III e IV são verdadeiras.

Vamos analisar cada uma das assertivas

I – Certa. A confidencialidade garante que somente pessoas autorizadas tenham acesso às informações, isso evita a exposição de dados sensíveis.

II – Certa. A integridade garante a completude e inteireza da informação, impedindo alterações indevidas, durante o armazenamento ou a transmissão.

III – Errada. Apenas o final da assertiva ficou incorreta, pois a disponibilidade tem, sim, relação com a continuidade das operações de uma organização.

IV – Certa. A autenticidade garante que o emissor e o receptor da informação são realmente quem afirmam ser, prevenindo fraudes e falsificações digitais, especialmente ataques, como Spoofing ou M.I.T.M (Man In The Middle ou Home no Meio).

Letra b.

---

012. (Q4233666/FUNDATEC/IGP/PERITO CRIMINAL/ÁREA GEOLOGIA/2025) Sobre os princípios da segurança da informação, analise as assertivas abaixo:

I – A autenticidade garante que a informação deve ser protegida de acordo com o grau de sigilo aplicado ao seu conteúdo.

II – A integridade garante que a informação deve ser mantida da mesma forma, na mesma condição em que foi disponibilizada por seu proprietário.

III – A conformidade garante que a informação gerada ou adquirida por um indivíduo ou instituição deve estar acessível e operacional para usuários autorizados sempre que necessário.

Quais estão corretas?

a) Apenas I.

b) Apenas II.

c) Apenas I e II.

d) Apenas II e III.

e) I, II e III.

Vejamos cada uma das assertivas

I – Errada. É a confidencialidade que garante que a informação deve ser protegida de acordo com o grau de sigilo aplicado ao seu conteúdo.

II – Certa. A integridade garante que a informação não pode ser alterada, permanecendo na mesma condição em que foi disponibilizada por seu proprietário.

III – Errada. É a disponibilidade que garante que a informação gerada ou adquirida por um indivíduo ou instituição deve estar acessível e operacional para usuários autorizados sempre que necessário.

Letra b.

---

013. (Q4034610/VUNESP/CÂMARA DE MARÍLIA/AUXILIAR DE INFORMÁTICA/2025) Um auxiliar de informática, que não tem acesso ao sistema de contabilidade, mas tem acesso ao banco de dados, recebeu um pedido de um analista da contabilidade para executar um SQL para alterar registros em um banco de dados desse sistema, alterando assim seus valores. O auxiliar de informática sabe que isso não deve ser feito, porque viola um dos 3 pilares fundamentais da segurança da informação. Trata-se de

a) Confidencialidade.
b) Disponibilidade.
c) Monitoramento.
d) Integridade.
e) Acesso.

Na situação descrita no enunciado da questão, houve uma alteração indevida de registros de um banco de dados, visto que seu acesso e alteração devem ser feitos apenas por pessoas autorizadas a acessar o sistema institucional de contabilidade. O auxiliar de informática, por ser da área de TI, tem acesso ao banco de dados, mas não tem relação com o setor de contabilidade, nem permissão de acesso via sistema de contabilidade. Portanto, tal acesso que lhe foi solicitado é indevido e viola o princípio da integridade, pelo fato de realizar alterações não autorizadas.
Letra d.

---

014. (Q4157649/IBAM/PREFEITURA DE ARRAIAL DO CABO/SECRETÁRIO ESCOLAR/2025) No que se refere à segurança da informação, de equipamentos, de sistemas, em redes, na internet e na nuvem, com a evolução tecnológica, os riscos aumentam e exigem uma gestão de proteção cada vez mais eficaz. A base de defesa dos sistemas e infraestrutura das corporações são os pilares da segurança da informação, que atuam por meio de políticas, senhas, softwares de criptografia, dentre outros processos necessários a essa gestão de riscos. Um desses pilares é responsável por manter as características originais dos dados, assim como foram configuradas em sua criação, destacando que a informação não pode ser alterada sem autorização. Já outro pilar se caracteriza por proteger a informação dos acessos não autorizados, estabelecendo a privacidade para os dados da empresa, evitando situações de ataques cibernéticos ou espionagem. Em consequência, a base desse segundo pilar é controlar o acesso por autenticação de senha, podendo ser também por verificação biométrica, além da criptografia, que vem gerando resultados favoráveis nessa função. Esses dois pilares são conhecidos, respectivamente, como:
a) irretratabilidade e integridade
b) integridade e confidencialidade
c) autenticidade e irretratabilidade
d) confidencialidade e autenticidade

- **Integridade:** mantém as características originais dos dados, assim como foram configuradas em sua criação, destacando que a informação não pode ser alterada sem autorização.

- **Confidencialidade:** protege a informação dos acessos não autorizados, estabelecendo a privacidade para os dados da empresa, evitando situações de ataques cibernéticos ou espionagem.

Letra b.

---

015. (Q4102629/IDECAN/PREFEITURA DE PATOS/FISCAL DE OBRAS E URBANISMO/2025) Durante o desenvolvimento de uma política de segurança para uma organização, um analista de TI identificou a necessidade de proteger os dados contra acessos não autorizados, garantir que as informações não sejam alteradas indevidamente e que estejam disponíveis sempre que necessário. Além disso, buscou implementar ferramentas de defesa contra malwares e ataques. Com base nesse cenário e nos princípios da Segurança da Informação, identifique o item correto.

a) A confidencialidade garante que os dados estejam sempre disponíveis, mesmo após falhas ou ataques.

b) A integridade está relacionada ao uso de firewalls para evitar o acesso físico a servidores de rede.

c) A assinatura digital é um recurso usado apenas para criptografar arquivos sigilosos em backups.

d) A disponibilidade pode ser comprometida por ataques de negação de serviço (DoS), dificultando o acesso aos sistemas.

e) O antivírus é uma ferramenta eficaz apenas contra ataques baseados em rede e não detecta arquivos maliciosos locais.

Vamos corrigir cada uma das alternativas

a) Errada. A DISPONIBILIDADE garante que os dados estejam sempre disponíveis, mesmo após falhas ou ataques.

b) Errada. A CONFIDENCIALIDADE está relacionada ao uso de firewalls para evitar o acesso físico a servidores de rede.

c) Errada. A assinatura digital é um recurso usado para assinar documentos digitais e criptografar arquivos sigilosos em backups.

d) Certa. Ataques de negação de serviço (DoS), tornam os recursos de informação indisponíveis, dificultando o acesso aos sistemas. Isso viola a Disponibilidade.

e) Errada. O antivírus é uma ferramenta eficaz tanto contra ataques baseados em rede e como para detectar arquivos maliciosos locais.

Letra d.

---

016. (Q3930308/INSTITUTO CONSULPAM/CONAB/ANALISTA/ÁREA PSICOLOGIA/2025) Os pilares da segurança da informação protegem dados contra ameaças e asseguram a confiabilidade das informações em um mundo digital cada vez mais vulnerável. Dessa forma, analise as sentenças a seguir:

Quando um usuário tenta fazer uma transação bancária e o sistema encontra-se fora do ar, observa-se o comprometimento da disponibilidade.

PORQUE

O pilar da disponibilidade trata da oferta do acesso à informação quando esta é necessária para o usuário.

Acerca dessas sentenças, assinale a alternativa CORRETA.

a) As duas sentenças são verdadeiras, mas a segunda não é uma justificativa correta da primeira.

b) A primeira sentença é verdadeira, e a segunda, falsa.

c) As duas sentenças são verdadeiras, e a segunda é uma justificativa correta da primeira.

d) A primeira sentença é falsa, e a segunda, verdadeira.

Esse tipo de questão é muito interessante, pois não se baseia em decoreba, mas exige o raciocínio do aluno. A primeira assertiva retrata a indisponibilidade do sistema bancário, violando a disponibilidade. A segunda assertiva explica e justifica a disponibilidade, a qual é a garantia de que a informação está acessível sempre que necessário.

Letra c.

---

017. (Q3997483/FUNDATEC/IF SERTÃO/ADMINISTRADOR/2025) A definição de segurança de computadores do NIST (National Institute of Standards and Technology – Manual NIST SP 800 – 12 Rev. 1) estabelece que o objetivo principal da segurança em sistemas computacionais é proteger os recursos de informação (hardware, software, firmware, dados e comunicações), garantindo um conjunto de propriedades fundamentais. Considerando essa definição, são objetivos centrais da segurança de computadores:

I – Confidencialidade de dados: garantir que informações privadas e confidenciais não sejam acessíveis por indivíduos ou sistemas não autorizados.

II – Privacidade: assegurar que os indivíduos tenham controle sobre como seus dados pessoais são criptografados, roteados e compartilhados com terceiros.

III – Integridade de dados: garantir que informações e programas sejam modificados somente de forma autorizada e conforme especificado.

IV – Disponibilidade: garantir que os serviços, sistemas e informações estejam acessíveis aos usuários autorizados quando necessário.

Quais estão corretos?
a) Apenas I e III.
b) Apenas II e IV.
c) Apenas I, II e III.
d) Apenas I, III e IV.
e) I, II, III e IV.

Vejamos cada uma das assertivas
I – Certa. A confidencialidade de dados garante que informações privadas e confidenciais não sejam acessíveis por indivíduos ou sistemas não autorizados. Ou seja, é a forma negativa de dizer que apenas pessoas autorizadas podem acessar as informações privadas.
II – Errada. A privacidade assegura que o titular dos dados tem controle sobre o consentimento relacionado ao tratamento dos dados para finalidades específicas, não sobre aspectos técnicos de criptografia e roteamento.
III – Certa. A integridade de dados garante que informações e programas sejam modificados somente de forma autorizada e conforme especificado.
IV – Certa. A disponibilidade garante que os serviços, sistemas e informações estejam acessíveis aos usuários autorizados quando necessário.
Letra d.

---

018. (Q4250158/IBAM/PREFEITURA DE ARAPIRACA/ASSISTENTE ADMINISTRATIVO EDUCACIONAL/2025) Segurança da informação é definida como a proteção contra acesso não autorizado, divulgação, uso, alteração ou interrupção, tendo por finalidade assegurar que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados, permaneçam confidenciais e mantenham sua integridade. É um conceito que possui pilares como fundamentos, dos quais um deles tem por finalidade garantir que os usuários possam acessar as informações a que estão autorizados a acessar quando precisarem. Esse pilar é denominado:
a) integridade
b) autenticidade
c) disponibilidade
d) irretratabilidade

A disponibilidade tem garante que os usuários tenham acesso às informações a que estão autorizados a acessar quando precisarem.
Letra c.

---

019. (Q4225810/UNOCHAPECÓ/PREFEITURA DE GUATAMBU/TÉCNICO EM INFORMÁTICA/2025) Esse pilar da segurança de Informação assegura que as informações permaneçam completas e inalteradas durante o armazenamento, o processamento e a transmissão, protegendo contra modificações acidentais ou maliciosas. Marque a alternativa CORRETA que corresponde ao pilar descrito.

a) Disponibilidade.
b) Confidencialidade.
c) Autenticidade.
d) Integridade.

A integridade garante a completude e imutabilidade da informação durante o armazenamento, o processamento e a transmissão, protegendo contra modificações acidentais ou maliciosas.

Letra d.

---

020. (Q3388049/INSTITUTO ÁGATA/PREFEITURA DE ANAJÁS/ASSISTENTE/ÁREA: DIGITAÇÃO DE DADOS/2024) No contexto da segurança da informação, a confidencialidade tem como objetivo garantir

a) que nenhuma pessoa tenha acesso ao arquivo cifrado.
b) a autenticidade da informação, ou seja, dar a certeza da autoria da informação enviada para o destinatário.
c) que somente pessoas autorizadas tenham acesso ao conteúdo do dado cifrado. No contexto simétrico, entende-se como pessoa autorizada aquela que possui a chave secreta.
d) a autenticidade da informação, ou seja, dar a certeza de autoria da informação cifrada.
e) que somente pessoas autorizadas tenham acesso ao arquivo cifrado. No contexto simétrico, entende-se como pessoa autorizada aquela que possui a chave pública.

Vejamos cada uma das alternativas

a) Errada. A confidencialidade não impede que a pessoa tenha acesso ao arquivo cifrado, mas sim que não consiga acessar a informação que nele está armazenada, justamente pelo fato de estar codificada.
b) Errada. A confidencialidade não garante a autenticidade da informação, mas sim seu sigilo.
c) Certa. A confidencialidade garante que somente pessoas autorizadas tenham acesso ao conteúdo do dado cifrado. No contexto simétrico, o qual utiliza uma mesma chave para cifrar e decifrar a informação, entende-se como pessoa autorizada aquela que possui a chave secreta.
d) Errada. A confidencialidade não garante a autenticidade da informação.
e) Errada. Na criptografia assimétrica, pessoa autorizada é aquela que possui a chave privada.

Letra c.

---

021. (Q3301560/FUNDATEC/SIMAE/CONTADOR/2024) Em matéria de Segurança da Informação, a garantia da identidade de uma pessoa, seja ela física ou jurídica ou de um servidor (computador) com quem se estabelece uma transação, é chamada de:

a) Confiabilidade.

b) Disponibilidade.

c) Integridade.

d) Confidencialidade.

e) Autenticidade.

A autenticidade é a garantia da identidade de uma pessoa, seja ela física ou jurídica ou de um servidor (computador) com quem se estabelece uma transação.

Letra e.

---

022. (Q3194371/CESPE/CEBRASPE/MPE TO/TÉCNICO MINISTERIAL/ÁREA: TÉCNICO EM TELECOMUNICAÇÕES/2024) Acerca da segurança da informação, julgue os seguintes itens.

Uma rede de comunicação atende ao requisito de disponibilidade quando é capaz de garantir que os dados trafegados só sejam acessíveis pelas partes autorizadas, seja para impressão, exibição ou outras formas de divulgação, que incluem a simples revelação da existência de um objeto qualquer.

A questão definiu o atributo de confidencialidade, quando diz que “os dados trafegados só sejam acessíveis pelas partes autorizadas”.

Errado.

---

023. (Q3076445/QUADRIX/CRT SP/ADVOGADO/2023) Quanto aos procedimentos de segurança da informação, às noções de vírus, worms e pragas virtuais e aos procedimentos de backup, julgue os itens de 36 a 40.

Na organização, uma ação que representa uma violação da segurança da informação é o fato de o funcionário ou o colaborador divulgar publicamente informações confidenciais da organização.

Essa violação diz respeito ao princípio da confidencialidade. Esse princípio garante que apenas pessoas autorizadas podem ter acesso à informação.

Certo.

---

024. (Q2685030/Quadrix/CRO/Técnico em Informática/2023) ulgue o item, relativos aos conceitos de proteção e segurança da informação.
A definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

Embora essa questão cite alguns dos princípios básicos de segurança da informação, ela não focava exclusivamente neles, mas sim no conceito mais geral do assunto. Sendo assim, ela está correta quando faz menção à confidencialidade e à integridade.
Certo.

---

025. (Q2695994/CESGRANRIO/BANRISUL/ESCRITURÁRIO/2023) Os serviços de segurança de uma empresa são implementados por mecanismos de segurança e visam a satisfazer os requisitos da política de segurança dessa empresa. Para aprimorar o serviço de segurança que controla o acesso aos sistemas de informação, o controle de autenticação em uma etapa de verificação está sendo substituído pelo controle de autenticação em mais de uma etapa de verificação.
Esse controle em mais de uma etapa de verificação é conhecido como autenticação
a) complexa
b) resistente
c) qualificada
d) estendida
e) multifator

Autenticação em Múltiplas Etapas (Multifactor Authentication) é um método de autenticação que exige mais de uma etapa para verificação de identidade de uma pessoa. Isso significa que, além da senha de autenticação, o usuário precisa fornecer uma segunda comprovação, como um código gerado por um outro meio de confirmação, geralmente um que apenas o próprio usuário tenha acesso, como um código enviado por SMS para o seu celular ou um código enviado por e-mail.
Letra e.

---

026. (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.

Vejamos a justificativa de cada uma das alternativas.
De maneira bem simples. Criptografia é o mecanismo que transforma a informação original em algo ilegível, por meio de chaves ou códigos, de maneira que um agente sem autorização seja incapaz de compreender. Essa técnica envolve a conversão de informações inteligíveis em um texto cifrado (dados ilegíveis). O objetivo da criptografia é a proteção dos dados confidenciais, impedindo o acesso ou a compreensão da informação por pessoas não autorizadas.
Letra c.

---

027. (Q2829853/UFRRJ/UFRRJ/AUDITOR/2023) Com relação aos princípios de segurança da informação, aspectos como confidencialidade, integridade, disponibilidade, legalidade e a autenticidade são considerados pilares.
Sobre estes princípios, é correto afirmar que a
a) autenticidade garante que a informação foi produzida em conformidade com a lei.
b) confidencialidade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.
c) legalidade garante que os dados tenham completeza e estejam disponíveis permanentemente para acesso quando desejados.
d) disponibilidade está relacionada à privacidade e ao sigilo das informações, de modo a garantir o acesso apenas para pessoas autorizadas.
e) integridade garante a completude e exatidão das informações, de modo que sejam preservadas, precisas e confiáveis durante todos os seus ciclos de vida.

Vejamos a justificativa de cada uma das alternativas.
a) Errada. A Legalidade garante que a informação foi produzida em conformidade com a lei.
b) Errada. A integridade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.
c) Errada. A integridade garante que os dados tenham completeza e a disponibilidade garante o acesso apenas para pessoas autorizadas.
d) Errada. A confidencialidade está relacionada à privacidade e ao sigilo das informações, de modo a garantir o acesso apenas para pessoas autorizadas.
Letra e.

---

028. (Q2685030/QUADRIX/CRO/TÉCNICO EM INFORMÁTICA/2023) Julgue os itens relativos aos conceitos de proteção e segurança da informação.

A definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

Vejamos a justificativa de cada uma das alternativas.

A segurança da Informação será obtida por meio de um conjunto de medidas abrangentes que, se aplicados de forma correta e revisados sempre que necessário, vão assegurar a proteção dos dados. A definição de segurança da informação abarca a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

Certo.

---

029. (Q2706726/FUNDEP/PREFEITURA DE BARRA LONGA/ASSISTENTE SOCIAL/CRAS/2023) Conforme o cert.br, para permitir que possam ser aplicados na internet cuidados similares aos do dia a dia, é necessário que os serviços disponibilizados e as comunicações realizadas pela internet garantam alguns requisitos básicos de segurança, como

a) autenticação, identificação e repúdio.

b) confidencialidade, identificação e repúdio.

c) autenticação, confidencialidade e identificação.

d) autenticação, confidencialidade e repúdio.

Como vimos, a autenticação também é princípio secundário, pois é o ato de comprovar a veracidade da autoria da informação, ou seja, é a execução da autenticidade. A confidencialidade também é um princípio de segurança que garante que a informação só pode ser acessada por pessoas autorizadas. A identificação, também um princípio periférico de segurança, garante que o usuário ou entidade se identifique, fornecendo suas credenciais.

Letra c.

---

030. (Q2682336/MS CONCURSOS/PREFEITURA DE PATROCÍNIO/PSICÓLOGO/2023) De acordo com o Princípio da Disponibilidade, a informação estará disponível sempre que for preciso. Esse aspecto é de suma importância, principalmente, para sistemas que não podem ter falhas na disponibilidade, pois essas falhas comprometem o serviço. Assinale a alternativa que não garante o Princípio da Disponibilidade:

a) Nobreak.
b) Firewall.
c) Backup.
d) Assinatura Digital.

Nobreak, firewall e backup são ferramentas que visam garantir a disponibilidade das informações. Assinatura digital visa garantir a autenticidade e integridade das informações.
Letra d.

---

031. (Q2685028/QUADRIX/CRO/TÉCNICO EM INFORMÁTICA/2023) Julgue os itens, relativos aos conceitos de proteção e segurança da informação.
Aplicativos específicos, que ajudam a limpar o registro do computador, podem ser usados com o objetivo de proteger o computador de programas estranhos.

Alguns programas maliciosos buscam informações de navegação do usuário, tais como logins e senhas utilizados ao acessar alguns sites. Tais dados ficam registrados no histórico de navegação e em cookies. Nesse sentido, fazer sempre a limpeza de tais registros evita que programas maliciosos tentem acessá-los.
Certo.

---

032. (Q2414224/FGV/TJDFT/ANALISTA JUDICIÁRIO/ÁREA SUPORTE EM TECNOLOGIA DA INFORMAÇÃO/2022) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele. Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:
a) confidencialidade;
b) autenticidade;
c) integridade;
d) disponibilidade;
e) irretratabilidade.

Vejamos a justificativa de cada uma das alternativas.

a) Errada. A confidencialidade está relacionada à privacidade e ao sigilo das informações, de modo a garantir o acesso apenas para pessoas autorizadas.

b) Errada. A autenticidade tem por objetivo assegurar que a informação é proveniente do executor indicado

c) Errada. A integridade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.

d) Errada. Disponibilidade diz que a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la.

e) Certa. A irretratabilidade, também conhecida como "Não Repúdio", é a propriedade que garante que uma pessoa não pode negar ser a autora de uma transação ou informação, uma vez que foi autenticada para isso. Esse princípio visa garantir que uma pessoa autenticada não consiga negar a autoria de alguma informação ou transação em momento posterior.

Letra e.

---

033. (Q2354044/LEGALLE CONCURSOS/BADESUL DESENVOLVIMENTO/AGÊNCIA DE FOMENTO DO RIO GRANDE DO SUL/TÉCNICO EM DESENVOLVIMENTO/ÁREA: ANALISTA DE SISTEMAS/SEGURANÇA DA INFORMAÇÃO/2022) Sobre segurança da informação, é um princípio que garante que alguém não pode negar algo. Tipicamente, esse princípio se refere à habilidade em assegurar que uma parte de um contrato, ou de uma comunicação, não pode negar a autenticidade de sua assinatura em um documento ou o envio de uma mensagem que originou. Trata-se de qual princípio?

a) Confidencialidade.

b) Integridade.

c) Legalidade.

d) Não repúdio.

e) Autenticidade.

O não repúdio também é considerado um princípio básico de segurança da informação, embora seja um subproduto da Autenticidade. Pois, segundo a autenticidade, ao garantir a veracidade da autoria da informação, consequentemente, garante-se também a impossibilidade de se negar a autoria de uma assinatura em documentos e mensagens eletrônicas.

Letra d.

---

034. (Q2586985/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA: QUALITY ASSURANCE E ANALISTAS DE TESTE/2022) Acerca de confiabilidade, integridade e disponibilidade em segurança da informação, julgue os itens subsequentes.

Ataque de DoS, política de backup não implementada e falha nos discos violam a disponibilidade.

Disponibilidade diz que a informação estará disponível sempre que for necessário. Isso quer dizer que a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la. O hardware e o software devem estar em perfeito funcionamento para garantir a disponibilidade da informação. Portanto um ataque de DoS, uma política de backup não implementada ou falha nos discos podem violar o princípio da disponibilidade.

Certo.

---

035. (Q2451925/INSTITUTO ACCESS/PREFEITURA DE OURO BRANCO/PSICÓLOGO/2022) No que diz respeito à segurança da informação, um termo técnico está diretamente associado à cópia de segurança dos arquivos, tarefa que pode ser feita por meio de uma mídia física, em CDs/DVDs HDs ou pendrives, mas também pela Internet, por serviços específicos, como armazenamento na nuvem, por exemplo. A ideia é garantir a integridade dos dados e que os documentos importantes possam ser recuperados, mesmo quando há algum problema de hardware, no sistema ou se a máquina (PC ou celular, por exemplo) for roubada.

Esse termo técnico é conhecido como

a) deadlock.

b) swap.

c) backup.

d) firewall.

O Backup é uma cópia de segurança e uma ferramenta que assegura a disponibilidade e a integridade.

Letra c.

---

036. (Q2464459/UNIFAP/UNIFAP/TÉCNICO EM ASSUNTOS EDUCACIONAIS/2022) No que concerne à segurança da informação, temos os quatro princípios básicos: disponibilidade, integridade, confidencialidade e autenticidade. Assim, quando desejamos garantir a autenticidade em um sistema de informação, podemos usar vários mecanismos, sendo um deles:

a) Biometria
b) Certificado Digital
c) Redundância
d) Backup
e) Encapsulamento

Certificado digital: autenticidade, integridade e confidencialidade
Revisando as ferramentas que garante os princípios básicos:

- Criptografia: confidencialidade
- Assinatura digital: autenticidade e integridade
- Backup: disponibilidade e integridade
- Firewall: disponibilidade
- Nobreak: disponibilidade
- Biometria: autenticidade

Letra b.

---

037. (Q2390540/QUADRIX/CRMV SP/TÉCNICO EM INFORMÁTICA/2022) Com relação aos conceitos de proteção e segurança, julgue o item.
A propriedade de que a informação foi produzida, modificada ou descartada por uma determinada pessoa física, um órgão, uma entidade ou um sistema recebe o nome de autenticidade.

Muitas vezes associamos a autenticidade apenas ao dono que produziu a informação. No entanto, outras ações realizadas sobre as informações também podem ter a autoria confirmada e garantida, como é o caso da modificação e do descarte. Muitas vezes precisamos verificar a veracidade de autoria de tais ações também, sendo aí onde entra a autenticidade.
Certo.

---

038. (Q2488932/IBADE/CRC RO/ASSISTENTE ADMINISTRATIVO/2022) Sobre o Princípio da Integridade, é correto afirmar que:
a) a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la.
b) garante o sigilo da informação, impedindo que ela seja acessada por pessoas não autorizadas.
c) impossibilita o emissor negar a autoria de determinada mensagem ou transação.

d) assegura que a informação não sofra qualquer alteração por usuário não autorizado. Além de garantir entrega, recebimento ou armazenamento do conteúdo completo sem qualquer perda.
e) garante que o autor da informação é realmente quem ele diz que é.

Vejamos a justificativa de cada uma das alternativas.
a) Errada. Disponibilidade diz que a informação deverá estar disponível sempre que um usuário autorizado queira acessá-la.
b) Errada. Confidencialidade garante o sigilo da informação, impedindo que ela seja acessada por pessoas não autorizadas.
c) Errada. irretratabilidade impossibilita o emissor negar a autoria de determinada mensagem ou transação.
e) Errada. Autenticidade garante que o autor da informação é realmente quem ele diz que é.
Letra d.

---

039. (Q2586438/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA SUPORTE A PLATAFORMA MAINFRAME/2022) Com relação à segurança da informação, julgue o item seguinte.
A integridade da informação, um dos pilares da segurança da informação, visa garantir que a informação esteja disponível a seus usuários, aos quais é conferido o acesso.

Na verdade, essa é a definição de disponibilidade, um dos pilares da segurança da informação, a qual visa garantir que a informação esteja disponível a seus usuários, aos quais é conferido o acesso. A integridade é outro princípio, porém garante que a informação só pode ser alterada por pessoas autorizadas, além de garantir a completude da informação.
Errado.

---

040. (Q2269851/CESPE/CEBRASPE/TELEBRAS/ESPECIALISTA EM GESTÃO DE TELECOMUNICAÇÕES/ÁREA ENGENHEIRO DE REDES/2022) Com relação a criptografia e segurança de servidores e sistemas operacionais, julgue o item subsequente.
Irretratabilidade é o mecanismo de segurança que prova que a mensagem foi enviada pela origem especificada e que foi recebida pelo destino especificado.

A irretratabilidade, também conhecida como "Não Repúdio", é a propriedade que garante que uma pessoa não pode negar ser a autora de uma transação ou informação, uma vez

que foi autenticada para isso. Esse princípio visa garantir que uma pessoa autenticada não consiga negar a autoria de alguma informação ou transação em momento posterior. Irretratabilidade (não repúdio), segundo William Stallings, em seu livro Criptografia e Segurança de Redes, Princípios e Práticas (2016, p. 13), há duas definições irretratabilidade que se complementam:

- Irretratabilidade de origem: essa é a mais conhecida, adotada por todas as bancas, a qual é prova de que a mensagem foi enviada pela parte especificada;
- Irretratabilidade de destino: prova de que a mensagem foi recebida pela parte especificada. Essa é uma definição pouco adotada pelas bancas. No entanto, a CESPE/CEBRASPE adota essa definição, conforme gabarito desta questão.

Certo.

---

041. (Q2431465/INAZ do Pará/SAMAE São Bento do Sul/Operador de Máquinas/2022/ADAPTADA) "Para implementar a Segurança da Informação nos seus processos, a empresa deve ter em mente cinco pilares responsáveis por sustentar as políticas, estratégias e práticas de proteção de dados e informações. Um desses pilares trata de garantir que os dados estejam disponíveis apenas para as pessoas autorizadas. Uma das maneiras de garantir o cumprimento desse pilar é a inclusão de controles de acessos (por meio de biometria e liveness, por exemplo), senhas fortes ou criptografia". (IdBlog).

O pilar a que se refere o texto acima é o da

a) integridade.

b) autenticidade.

c) confidencialidade.

d) irretratabilidade.

e) disponibilidade.

Vejamos a justificativa de cada uma das alternativas.

a) Errada. A integridade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.

b) Errada. A autenticidade tem por objetivo assegurar que a informação é proveniente do executor indicado

d) Errada. A Irretratabilidade é o mecanismo de segurança que prova que a mensagem foi enviada pela origem especificada e que foi recebida pelo destino especificado.

e) Errada. A disponibilidade visa a utilização de mecanismos que tornem/mantenha as informações disponíveis

Letra c.

---

042. (Q2404203/IFPA/IFPA/PROFESSOR DE ENSINO BÁSICO, TÉCNICO E TECNOLÓGICO/ÁREA: INFORMÁTICA/2022) Para manter uma comunicação em rede de forma segura, existem algumas propriedades desejáveis. Dado o seguinte cenário, a Pessoa X deseja enviar uma mensagem sigilosa para a Pessoa Y.
Qual propriedade, relacionada à segurança de rede, garante que apenas a Pessoa Y conseguirá entender o conteúdo da mensagem enviada pela Pessoa X?
a) Não repúdio
b) Integridade de Mensagem
c) Segurança Operacional
d) Autenticação do Ponto Final
e) Confidencialidade

A confidencialidade é o princípio que visa garantir o sigilo das informações, impedindo que elas sejam acessadas por pessoas não autorizadas.
Letra e.

---

043. (Q2586983/CESPE/CEBRASPE/BANRISUL/TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO/ÁREA: QUALITY ASSURANCE E ANALISTAS DE TESTE/2022) Acerca de confiabilidade, integridade e disponibilidade em segurança da informação, julgue os itens subsequentes.
Um gestor que, por acidente, apague um arquivo de inicialização de um serviço web ou insira valores incorretos em uma aplicação de cobrança de um cliente comprometerá a integridade.

A integridade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas
Certo.

---

044. (Q2341094/OBJETIVA CONCURSOS/PREFEITURA DE SETE LAGOAS/TÉCNICO DE LABORATÓRIO/2022) De acordo com a Cartilha de Segurança para Internet, assinalar a alternativa que preenche as lacunas abaixo CORRETAMENTE:A assinatura digital permite comprovar a _____ e o(a) _____ de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que não foi alterada.
a) autenticidade | integridade
b) autorização | disponibilidade
c) integridade | autenticidade
d) confidencialidade | não repúdio

Para revisão das ferramentas:

- Criptografia: confidencialidade
- Assinatura digital: autenticidade e integridade
- Backup: disponibilidade e integridade
- Firewall: disponibilidade
- Nobreak: disponibilidade
- Biometria: autenticidade
- Certificado digital: autenticidade, integridade e confidencialidade

Letra a.

---

045. (Q2509477/CESPE/CEBRASPE/APEX BRASIL/ANALISTA/ÁREA: AUDITORIA INTERNA/2022) O princípio básico voltado à segurança da informação que permite ao usuário recuperar uma informação em sua forma original é a

a) confidencialidade.

b) autenticidade.

c) disponibilidade.

d) integralidade.

Vejamos a justificativa de cada uma das alternativas.

a) Errada. A confidencialidade é o princípio que visa garantir o sigilo das informações, impedindo que elas sejam acessadas por pessoas não autorizadas.

b) Errada. A autenticidade tem por objetivo assegurar que a informação é proveniente do executor indicado

c) Errada. A disponibilidade visa a utilização de mecanismos que tornem/mantenha as informações disponíveis

Letra d.

---

046. (Q2484020/RHEMA/CÂMARA DE SEARA/ADVOGADO/2022) Para todas as questões de informática básica tenha por base o software de distribuição atual, na versão Português Brasil, salvo em caso de citação específica de versão ou distribuição no enunciado da questão: Tendo por base os pilares da segurança da informação, temos um total de cinco itens, envolvendo a confidencialidade e a irretratabilidade. Avalie os itens dispostos a seguir e indique aquele que representa uma opção inadequada em relação a estes pilares.

a) Integridade.
b) Disponibilidade.
c) Autenticidade.
d) Sustentabilidade.

Nessa questão o examinador quer saber se você sabe quais são os princípios básicos de segurança da informação, mas usou a nomenclatura "pilares da segurança da informação". Portanto, integridade, disponibilidade e autenticidade são princípios. Sustentabilidade não é um princípio de segurança da informação.
Letra d.

---

047. (Q2284135/AMEOSC/CÂMARA DE BANDEIRANTE/AUXILIAR LEGISLATIVO/2022) Diante de uma enorme troca de informações entre os computadores com as mais variadas informações e principalmente pela vulnerabilidade oferecida pelos sistemas, tornou-se necessário o desenvolvimento de um conjunto de princípios, técnicas, protocolos, normas e regras que visassem garantir um melhor nível de confiabilidade. Dessa forma, tomando por base a segurança da informação, analise o conceito de um dos princípios e assinale a alternativa CORRETA: "Atua para que um indivíduo ou entidade não negue a autoria de uma ação específica (criar ou assinar um arquivo/documento, por exemplo)".
Esse conceito trata do princípio da:
a) Disponibilidade.
b) Autenticidade.
c) Integridade.
d) Irretratabilidade.

Vejamos a justificativa de cada uma das alternativas.
a) Errada. A disponibilidade visa a utilização de mecanismos que tornem/mantenha as informações disponíveis
b) Errada. A autenticidade tem por objetivo assegurar que a informação é proveniente do executor indicado
c) Errada. A integridade garante que os dados sejam legítimos, assegurando que não sofram alterações por pessoas não autorizadas.
Letra d.

---

048. (Q2366187/UFPE/UFPE/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/ÁREA: SISTEMAS/2022) Um dos objetivos principais da Segurança da Informação é o de assegurar acesso à informação sempre que desejado.

Estamos falando do princípio da
a) Redundância.
b) Privacidade.
c) Disponibilidade.
d) Autenticidade.
e) Acessibilidade.

Vejamos a justificativa de cada uma das alternativas.
a) Errada. Redundância não é um princípio da segurança da informação, embora seja usada para garantir o princípio da disponibilidade.
b) Errada. Privacidade não é um princípio da segurança da informação.
d) Errada. A autenticidade tem por objetivo assegurar que a informação é proveniente do executor indicado.
e) Errada. Acessibilidade não é um princípio da segurança da informação.
Letra c.

---

049. (Q2586333/CESPE/CEBRASPE/BANRISUL/TÉCNICO DE TECNOLOGIA DA INFORMAÇÃO/ÁREA: DESENVOLVIMENTO/2022) Considerando que uma empresa tenha disponibilizado um website na Internet com as informações cadastrais de clientes e as de pagamentos com cartão de crédito de produtos vendidos, julgue os itens a seguir, com base nos conceitos de confiabilidade, integridade e disponibilidade, bem como nos mecanismos de segurança da informação.
Caso um funcionário da empresa altere maliciosamente os dados informados pelos clientes e armazenados pela organização, essa alteração necessariamente caracteriza uma violação da disponibilidade.

Essa alteração caracteriza uma violação à integridade dos dados.
Errado.

---

050. (Q2419862/FUNDATEC/PREFEITURA DE SÃO JOSÉ DOS AUSENTES/TÉCNICO EM INFORMÁTICA/2022) Assinale a alternativa que apresenta somente pilares que norteiam a segurança da informação.
a) Integridade e confiança.
b) Comunicabilidade e disponibilidade.

c) Sistemas e pessoas.
d) Autenticidade e confidencialidade.
e) Dados e informações.

Nessa questão o examinador fala sobre pilares que norteiam a segurança da informação, esses pilares são os princípios estudados na nossa aula.
a) Errada. Integridade é um princípio de segurança da informação, confiança não.
b) Errada. Comunicabilidade não é um princípio de segurança da informação, disponibilidade é.
c) Errada. Nem sistemas nem pessoas são princípios de segurança da informação.
e) Errada. Dados e informações não são princípios de segurança da informação.
Letra d.

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 pra mim o quanto você gostou dela e quantas questões você gabaritou, beleza? Eu lerei sua avaliação assim que você a fizer, pois eu 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:

@PROF.MAURICIOFRANCESCHINI

INFORMÁTICA PARA CONCURSOS
CURSO COMPLETO
Professor: Maurício Franceschini
(CÓDIGO: 149083)

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 parado antes de terminar todas as questões! Você é uma pessoa vencedora, campeã mesmo!

Estou muito orgulhoso de você!!!!

REFERÊNCIA

CERT.br/Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet – Versão 4.0 (cert.br)

Segurança da Informação: conceito, função e como proteger dados sigilosos (docusign.com.br)

Segurança da Informação (ufpel.edu.br)

CGI.br/Publicações

L12527 (planalto.gov.br)

Abra

caminhos

crie

futuros

gran.com.br