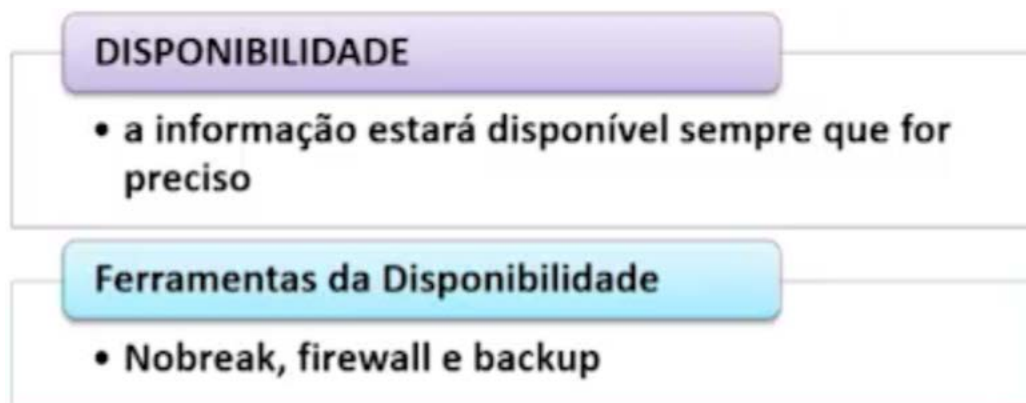


SEGURANÇA DA INFORMAÇÃO – PRINCÍPIOS BÁSICOS DE SEGURANÇA

Princípios Básicos de Segurança da Informação

Existem quatro princípios básicos de segurança da informação: Disponibilidade, Integridade, Confidencialidade e Autenticidade.

Princípio da Disponibilidade



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.

Ex.: Se o site do Submarino, que é uma grande empresa de venda de comércio eletrônico, é atacado e fica fora do ar por 24 horas, o prejuízo dessa empresa, por causa da indisponibilidade do sistema, será muito grande. Nesse caso, a Disponibilidade é um fator crítico para essa empresa.

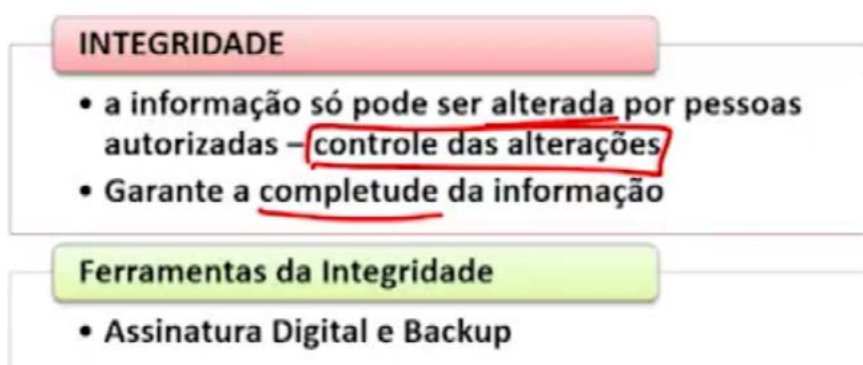
ANOTAÇÕES

Ferramentas do Princípio da Disponibilidade

As ferramentas que garantem o princípio da Disponibilidade são o **Nobreak**, o **Firewall** e o **Backup**.

- **Nobreak:** Dispositivo alimentado por baterias, capaz de fornecer energia elétrica a um sistema durante um determinado período, em situações de emergência, no caso de interrupção do fornecimento de energia da rede pública. Ou seja, o Nobreak impede que o sistema desligue e é uma ferramenta de Disponibilidade.
- **Firewall:** O Firewall é uma barreira de proteção contra ataques que visam tirar os serviços de funcionamento. Ele impede que ataques de intrusão e de negação de serviço sejam efetuados no ambiente.
- **Backup:** Quando uma informação é corrompida, ela se torna indisponível. O backup recupera essa informação, tornando-a disponível novamente.

Princípio da Integridade



De acordo com o Princípio da Integridade, a informação só pode ser alterada por pessoas autorizadas, ou seja, a Integridade garante o **controle das alterações**, impedindo que pessoas não autorizadas façam alterações indevidas na informação.

O princípio da integridade também garante a **completude da informação**, para que não haja perda de partes da informação.

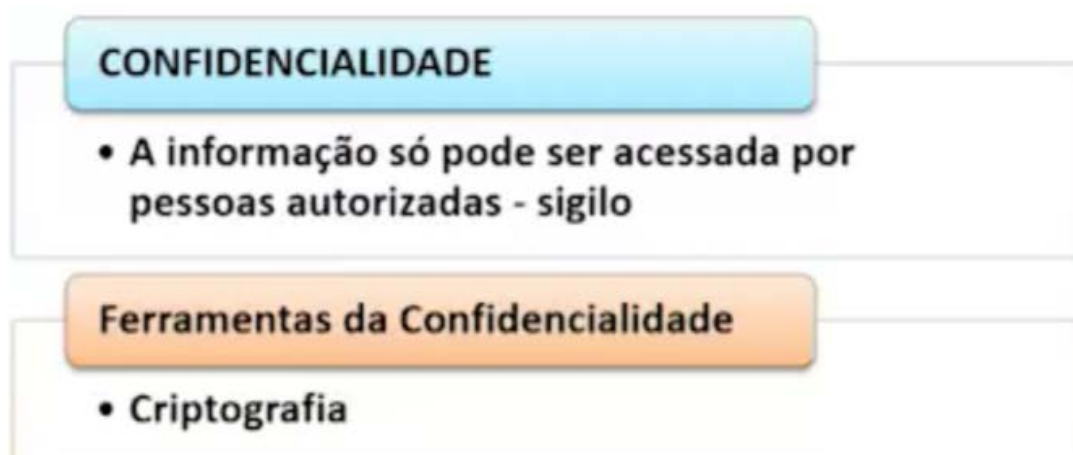
ANOTAÇÕES

Ferramentas do Princípio da Integridade

As ferramentas que garantem o Princípio da Integridade são a **Assinatura Digital** e o **Backup**.

- **Assinatura Digital:** Quando o usuário assina digitalmente um documento, qualquer alteração que for feita no documento violará essa assinatura. Portanto, se houver alteração em um documento assinado digitalmente ou eletronicamente, ele precisará ser assinado novamente, pois a assinatura anterior foi violada. A assinatura garante o controle das alterações.
- **Backup:** A completude faz parte do backup. Quando parte da informação se corrompe e o usuário restaura o backup, a totalidade da informação é recuperada, tornando-se íntegra novamente.

Princípio da Confidencialidade



Segundo o Princípio da Confidencialidade, a informação pode ser acessada apenas por pessoas autorizadas – isso significa o sigilo da informação. Portanto, a confidencialidade garante o sigilo da informação e impede que pessoas não autorizadas tenham acesso ao conteúdo.

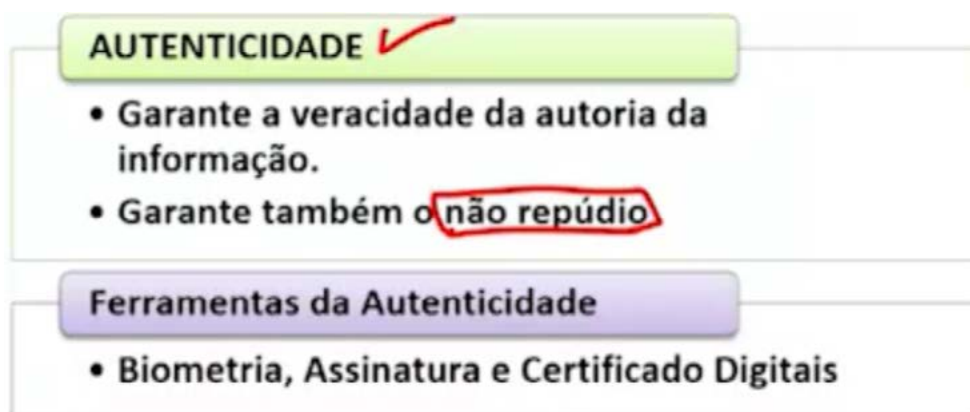
ANOTAÇÕES

Ferramenta do Princípio da Confidencialidade

A ferramenta que garante o princípio da Confidencialidade é a **Criptografia**.

- **Criptografia:** É uma técnica que embaralha a informação por meio de algoritmos de criptografia, e faz com que a informação se transforme em algo ininteligível.

Princípio da Autenticidade



O Princípio da Autenticidade garante a veracidade da autoria da informação, porém, não garante a veracidade do conteúdo da informação. A autenticidade garante a veracidade do autor, de quem de fato produziu aquela informação, não importando se o conteúdo é verdadeiro ou falso.

- **Não Repúdio:** A Autenticidade garante também um subproduto, que é o Não Repúdio. O Não Repúdio está contido na autenticidade e significa que o autor da informação não tem como recusar que ele é o verdadeiro autor. Ou seja, o Não Repúdio é a incapacidade da negação da autoria da informação.

Ferramentas do Princípio da Autenticidade

As ferramentas que garantem o Princípio da Autenticidade são a **Biometria**, a **Assinatura Digital** e os **Certificados Digitais**.

- **Biometria:** A Biometria é uma ferramenta que verifica algumas características físicas da pessoa para certificar que aquela característica identifica a pessoa unicamente. A Biometria é muito utilizada nos bancos.
- **Assinatura Digital:** A assinatura digital identifica unicamente o autor da informação, garantindo a autenticidade.
- **Certificados Digitais:** Os certificados Digitais garantem a autenticidade da autoria dos sites. **Ex.:** Quando um usuário acessa um site de comércio eletrônico, geralmente há um cadeado no canto da tela, que mostra o certificado digital do site, afirmando que aquele site de fato pertence àquela empresa.



IMPORTANTE!

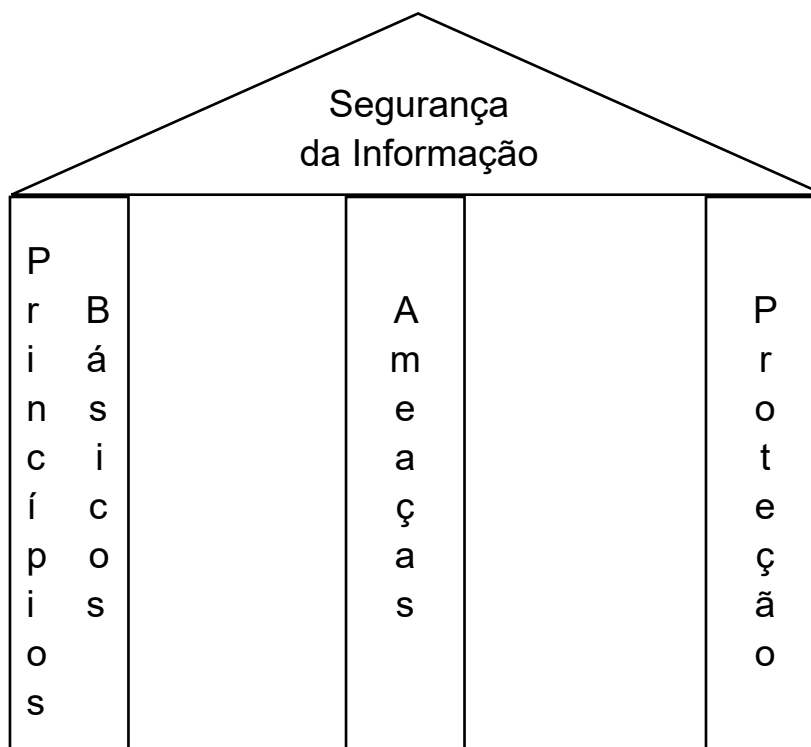
As iniciais dos princípios básicos de Segurança da Informação formam a palavra **DICA** – é importante memorizar essa palavra para lembrar, com mais facilidade, na hora de resolver as questões de provas.



ANOTAÇÕES

Pilares da Segurança da Informação

Os Princípios Básicos, as Ameaças e as Ferramentas de Proteção são os três pilares da Segurança da Informação.



Obs.: Este material foi elaborado pela equipe pedagógica do Gran Cursos Online, de acordo com a aula preparada e ministrada pelo professor Maurício Franceschini Duarte.

ANOTAÇÕES