APRESENTAÇÃO DO MATERIAL

Queridos alunos!!

Sabemos que os **resumos** das disciplinas **são fundamentais para fixação de conteúdos** e, também, para **realização de revisões**. Um resumo bem feito garante que os principais pontos de cada matéria sejam revisados de forma rápida, **aumentando a produtividade dos estudos e a eficiência das revisões**.

Além disso, sabemos que, principalmente para os grandes concursos, o número de matérias cobradas no edital é muito grande. Dessa forma, além de revisar os pontos marcados em seus materiais, um bom resumo pode encurtar o tempo de revisão, garantindo, assim, que todo o material possa ser revisado em um período de tempo mais curto.

Com isso em mente, apresentamos a vocês o **Resumo de Informática - SegInfo - Parte 1 - Princípios Básicos**. Trata-se de um material pensado para lhe ajudar em todo esse processo, visando, inclusive, uma economia de tempo de confecção de materiais, tempo que é o bem mais precioso de um concurseiro, não é mesmo?

Esperamos poder ajudá-los!

Conte sempre com o Estratégia em sua caminhada!

Estratégia Concursos

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 09.

Esse é um material resumido. Em momento algum ele substitui o estudo do material completo. Trata-se de um complemento aos estudos e um facilitador de revisões!

Resumo de Informática

Boatos (Redes de Rumores)

- **Princípios de Segurança:**

PRINCÍPIOS DE SEGURANÇA	DESCRIÇÃO
CONFIDENCIALIDADE	Capacidade de um sistema de não permitir que informações estejam disponíveis ou sejam reveladas a entidades não autorizadas – incluindo usuários, máquinas, sistemas ou processos.
INTEGRIDADE	Capacidade de garantir que a informação manipulada está correta, fidedigna e que não foi corrompida – trata da salvaguarda da exatidão e completeza da informação.
DISPONIBILIDADE	Propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada.

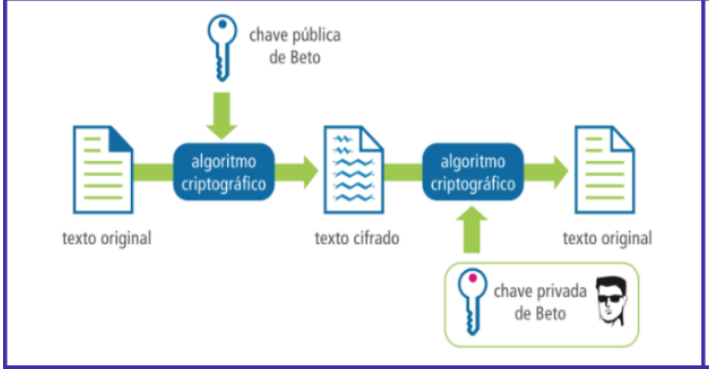
**Este material contempla assuntos dispostos no livro digital (pdf) da aula 09.

- **Princípios Adicionais:**

PRINCÍPIOS ADICIONAIS	DESCRIÇÃO
AUTENTICIDADE	Propriedade que trata da garantia de que um usuário é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação.
IRRETRATABILIDADE	Também chamada de Irrefutabilidade ou Não-repúdio, trata da capacidade de garantir que o emissor da mensagem ou participante de um processo não negue posteriormente a sua autoria.

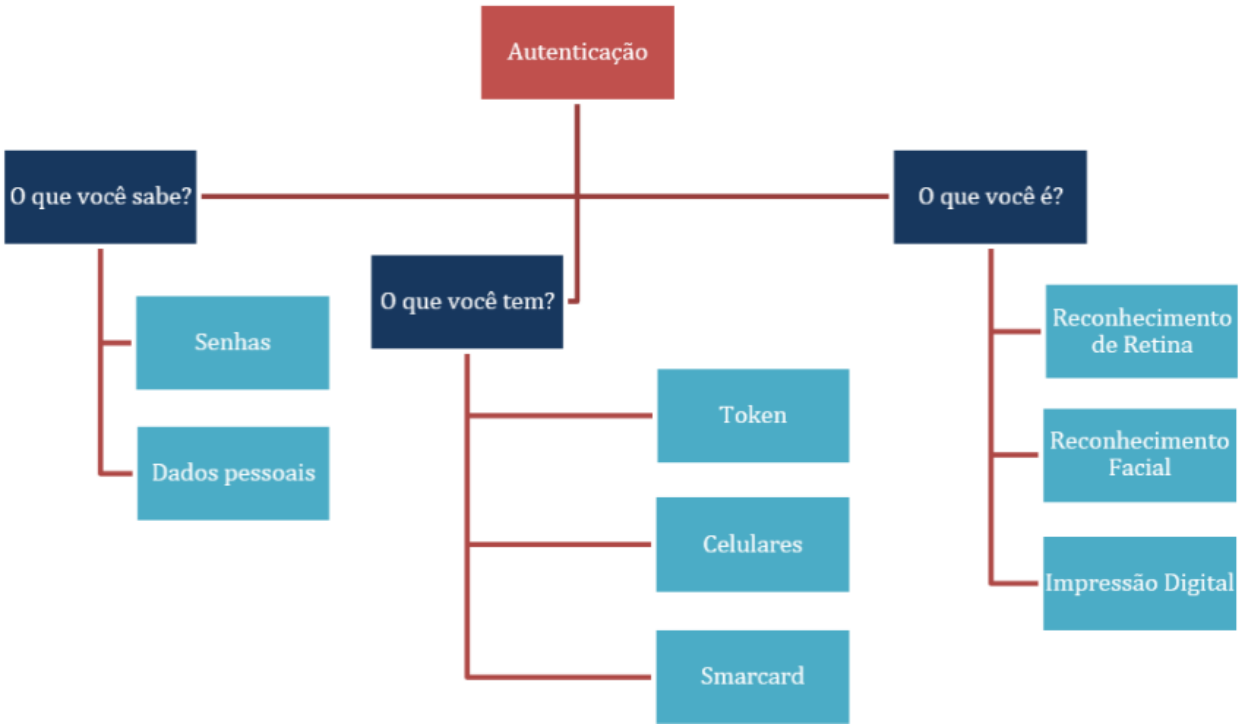
- **Tipo de Criptografia:**

TIPO DE CRIPTOGRAFIA	DESCRIÇÃO
CRIPTOGRAFIA SIMÉTRICA (CHAVE SECRETA)	Utiliza um algoritmo e uma única chave secreta para cifrar/decifrar que tem que ser mantida em segredo.
CRIPTOGRAFIA ASSIMÉTRICA (CHAVE PÚBLICA)	Utiliza um algoritmo e um par de chaves para cifrar/decifrar – uma pública e a outra tem que ser mantida em segredo.
CRIPTOGRAFIA HÍBRIDA (CHAVE PÚBLICA/SECRETA)	Utiliza um algoritmo de chave pública apenas para trocar chaves simétricas – chamadas chaves de sessão – de forma segura. Após a troca, a comunicação é realizada utilizando criptografia simétrica.

CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA CONFIDENCIALIDADE	CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA AUTENTICIDADE
	

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 09.

O emissor criptografa o texto original com a chave pública do receptor de forma que somente ele consiga descriptografá-lo com sua chave privada para visualizar o texto original.	O emissor criptografa o texto original com sua chave privada de forma que o receptor possa descriptografá-lo com a chave pública do emissor.

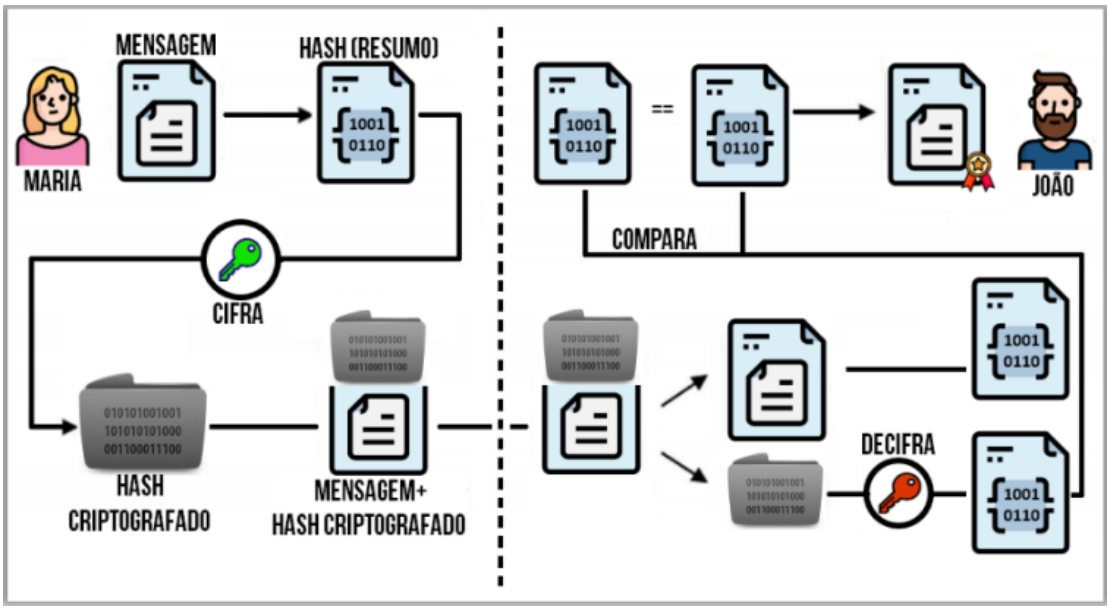


- **Métodos de Autenticação:**

MÉTODOS DE AUTENTICAÇÃO	DESCRIÇÃO
O QUE VOCÊ SABE?	Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.
O QUE VOCÊ É?	Trata-se da autenticação baseada no conhecimento de algo que você é, como seus dados biométricos.
O QUE VOCÊ TEM?	Trata-se da autenticação baseada em algo que somente o verdadeiro usuário possui, tais como: celulares, crachás, Smart Cards, chaves físicas, tokens, etc.

- **Autenticação Forte:** Trata-se de um tipo de autenticação que ocorre quando se utiliza pelo menos dois desses três métodos de autenticação. Um exemplo é a Autenticação em Dois Fatores (ou Verificação em Duas Etapas).

- **Assinatura Digital:** Trata-se de um método matemático de autenticação de informação digital tipicamente tratado como substituto à assinatura física, já que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado. Por meio de um Algoritmo de Hash, é possível garantir a integridade dos dados.



- **Funcionamento da assinatura digital:** Maria possui uma mensagem em claro (sem criptografia). Ela gera um hash dessa mensagem, depois criptografa esse hash utilizando sua chave privada. Em seguida, ela envia para João tanto a mensagem original quanto o seu hash. João gera um hash da mensagem original e obtém um resultado, depois descriptografa o hash da mensagem utilizando a chave pública de Maria e obtém outro resultado. Dessa forma, ele tem dois hashes para comparar: o que ele gerou a partir da mensagem em claro e o que ele descriptografou a partir da mensagem criptografada. Se forem iguais, significa que Maria realmente enviou a mensagem, significa que ela não pode negar que enviou a mensagem e, por fim, significa que a mensagem está íntegra.

- **Certificado Digital:** Certificado Digital é um documento eletrônico assinado digitalmente por uma terceira parte confiável – chamada Autoridade Certificadora – e que cumpre a função de associar uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas com o intuito de tornar as comunicações mais confiáveis e auferindo maior confiabilidade na autenticidade. Ele é capaz de garantir a autenticidade, integridade e não-repúdio, e até confidencialidade.

TIPO	GERAÇÃO DO PAR DE CHAVES	TAMANHO DA CHAVE (BITS)	ARMAZENAMENTO	VALIDADE (ANOS)
CERTIFICADO A1/S1	POR SOFTWARE	RSA 1024 OU 2048	DISCO RÍGIDO (HD) E PENDRIVE	1
CERTIFICADO A2/S2	POR SOFTWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	2
CERTIFICADO A3/S3	POR HARDWARE	RSA 1024 OU 2048	SMARTCARD (COM CHIP) OU TOKEN USB	5
CERTIFICADO A4/S4	POR HARDWARE	RSA 2048 OU 4096	SMARTCARD (COM CHIP) OU TOKEN USB	6

- **Garantias:** A criptografia sempre garante **confidencialidade**! Por meio da utilização de cifras simétricas, é possível garantir a **autenticidade** caso a chave seja conhecida apenas por dois participantes. Por meio de cifras assimétricas, é possível realizar o processo de criptografia (em que se garante a confidencialidade e a integridade por meio de uma função de hash); e realizar o processo de assinatura digital (em que se garante integridade, autenticidade e não-repúdio).

**Este material contempla assuntos dispostos no livro digital (pdf) da aula 09.