SEGURANÇA DA INFORMAÇÃO III

CONFIDENCIALIDADE

Uma informação considerada confidencial é aquela à qual apenas pessoas autorizadas devem ter acesso. Por exemplo, imagina-se uma informação impressa ou na tela de um computador, classificada como confidencial.

Supõe-se que este computador seja deixado ligado e a pessoa responsável saia da sala, permitindo que alguém não autorizado acesse e visualize a informação. Considera-se que a pessoa trabalha em um órgão de segurança pública e há uma operação planejada para um bairro específico. Se alguém que trabalha na empresa, independentemente do nível hierárquico, mas não autorizado a ter acesso àquela informação, visualizar os detalhes da operação, isso compromete a confidencialidade. Mesmo que essa pessoa não tenha copiado fisicamente a informação, o simples fato de tê-la acessado já viola a confidencialidade.

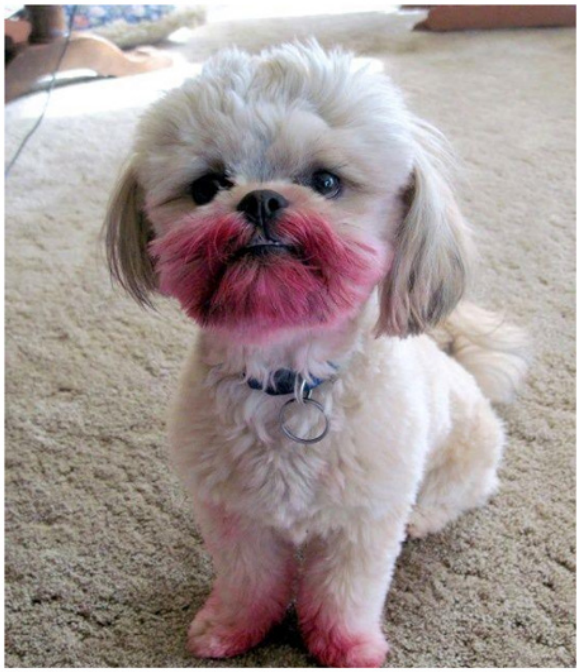
Portanto, conclui-se que a confidencialidade é perdida assim que alguém não autorizado obtém acesso a qualquer informação. A garantia é que a informação não será acessada por pessoas não autorizadas.

NÃO REPÚDIO OU IRRETRATABILIDADE

Para compreender o conceito de não repúdio, é necessário inicialmente compreender o significado de repudiar, que é negar ou recusar. Imagina-se um caso onde alguém está em uma loja com um amigo ou amiga e essa pessoa começa a protestar alegando que o preço do produto está diferente do anunciado no site, exigindo desconto, gerando um alvoroço desnecessário. Nesse momento, chega alguém, possivelmente um segurança do estabelecimento, e a pessoa se distancia, alegando não conhecer ou ter qualquer relação com a pessoa que está causando o problema. Essa atitude de negar o vínculo ou a associação é um exemplo de repúdio.

No contexto da segurança da informação, supõe-se que alguém envie um texto contendo informações incorretas ou que tenha insultado outra pessoa por impulso. Se confrontado sobre isso, a pessoa pode negar ter realizado tal ação, mesmo que tenha sido ela quem o fez.

Nesse contexto, o não repúdio garante à pessoa que recebe a informação que o remetente não poderá negar a autoria do que foi enviado. É uma forma de assegurar que suas ações não possam ser rejeitadas posteriormente, sendo irretratáveis nesse sentido.



Neste exemplo, o cachorro está negando a autoria do fato, mesmo que seja evidente.

DICAN

- **D –** Disponibilidade
- **I –** Integridade
- **C –** Confidencialidade
- **A –** Autenticidade
- **N –** Não repúdio ou irretratabilidade

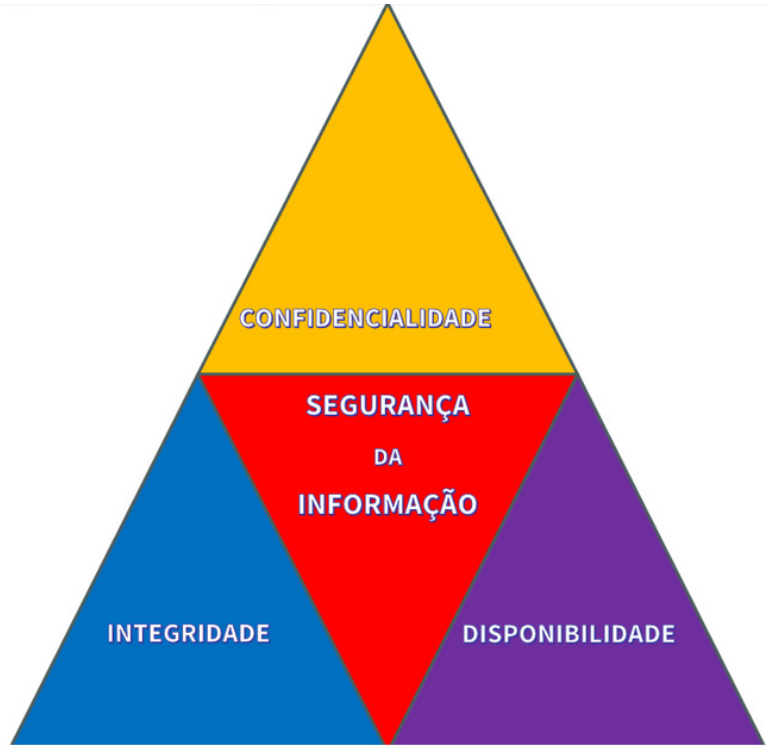
5m

CID

ou

CIA

Confidencialidade, integridade e disponibilidade, também conhecidas pela sigla em inglês CIA, são consideradas os três principais pilares.



A segurança da informação é fundamentada nos pilares da confidencialidade, integridade e disponibilidade. Esses princípios orientam a abordagem em várias questões relacionadas. Os três principais pilares da segurança da informação são esses mencionados, sendo importante lembrar que a sigla CIA em inglês não inclui autenticidade, mas sim disponibilidade, além de confidencialidade e integridade.

DIRETO DO CONCURSO

4. (2024/MS CONCURSOS/SAAE/MANHUAÇU/AJUDANTE ADMINISTRATIVO) Tendo em vista os princípios da Segurança da Informação, analise as afirmativas e depois assinale a alternativa verdadeira.

I – Confidencialidade: trata de assegurar que apenas as partes autorizadas têm acesso à informação.
II – Não repúdio: refere-se a uma informação de autenticação confiável, de forma a não permitir contestações posteriores.
III – Integridade: significa que as informações devem estar acessíveis, quando for necessário.

a. Apenas as afirmativas I e II estão corretas.
b. Apenas as afirmativas II e III estão corretas.
c. Apenas a afirmativa III está correta.
d. As afirmativas I, II e III estão corretas.

Os conceitos são simples, porém podem causar confusão. Não é incomum que em provas as pessoas troquem um conceito pelo outro. Por isso, sempre é recomendado resolver várias questões para familiarizar-se com os termos, o vocabulário e suas nuances.
I – Antes de abordar os conceitos apresentados, é aconselhável lembrar o que significa algo confidencial. Às vezes, o conteúdo pode ser abordado de maneira diferente, utilizando sinônimos e ampliando o contexto.
II – Não repúdio refere-se à incapacidade de negar ter feito algo.
III – A integridade da informação significa que ela deve ser mantida na forma em que foi originada. Se foi transmitida como "AB" maiúsculo, deve ser recebida como "AB" maiúsculo; se foi transmitida como "ab" minúsculo, deve ser recebida como "ab" minúsculo.

5. (2024/CEBRASPE/INPI/ANALISTA DE PLANEJAMENTO – GESTÃO DE T.I – SEGURANÇA DA INFORMAÇÃO) A ocorrência, em uma empresa, da perda de comunicação com um sistema importante, seja pela queda de um servidor, seja pela aplicação crítica de negócio configura exemplo de perda de integridade.

Existe uma distinção entre a incapacidade de acessar e a situação em que alguém acessa indevidamente o banco de dados e altera a informação.
Há o número do PIX, por exemplo. Se alguém substituir o número do PIX da pessoa pelo seu próprio número de PIX, o nome da pessoa fica associado ao PIX do atacante. Nesse caso, houve uma violação na integridade da informação; ela não está mais íntegra. A informação continua disponível, porém comprometida. Em um outro cenário, se o servidor cair, conforme mencionado anteriormente, os dados não estarão acessíveis para o usuário.

10m

6. (2023/FUNATEC/PREFEITURA DE PALMEIRANTE/ASSISTENTE JURÍDICO) Assinale a assertiva que apresenta corretamente o princípio da segurança da informação que é a garantia de que a mensagem não foi alterada durante a transmissão, ou seja, é a garantia da exatidão e completeza da informação.

a. Conformidade.
b. Integridade.
c. Autenticidade.
d. Confidencialidade.

Foram apresentados vários termos aqui que não foram utilizados durante a aula, mas que devem ser associados aos conceitos discutidos.

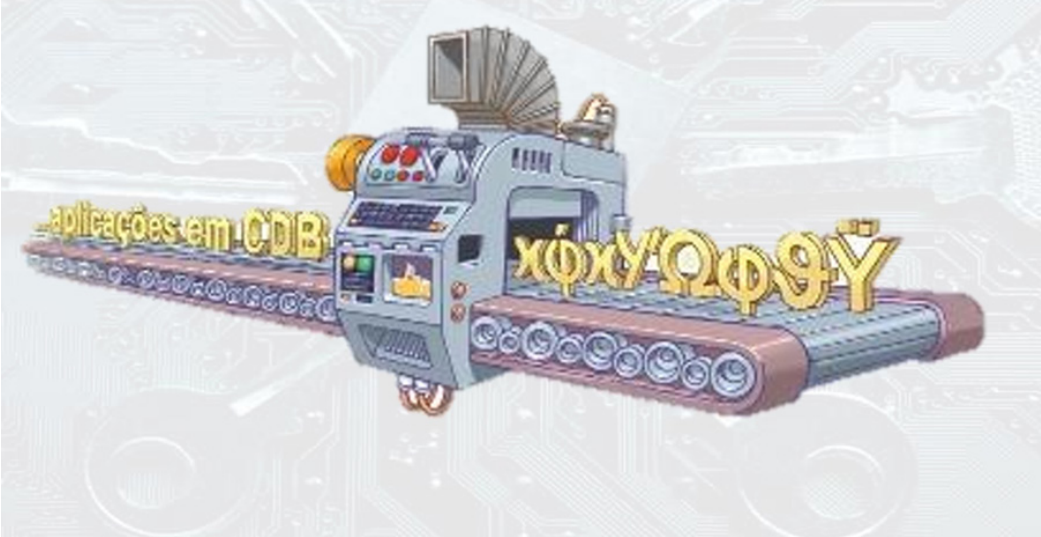
7. (2024/CEBRASPE/INPI/ANALISTA DE PLANEJAMENTO/GESTÃO DE T.I/SEGURANÇA DA INFORMAÇÃO) A confidencialidade da informação garante que, em uma comunicação, a origem e o destino sejam realmente aquilo que alegam ser.

A garantia até o momento é de que quem enviou a informação seja realmente quem disse ser. Pode ocorrer que, em algum momento, as informações tenham sido trocadas entre as partes, mas este não é o foco do texto. Confidencialidade refere-se ao acesso restrito às informações, permitido apenas a pessoas autorizadas. Autenticidade garante a identificação correta do remetente da informação, não do destinatário. Portanto, compreender ambos os conceitos é importante. A confidencialidade é crucial, pois garante o acesso restrito às informações, independentemente das partes envolvidas.

CRIPTOGRAFIA

A criptografia é uma proteção lógica amplamente utilizada e exigida. Isso não diminui a importância dos demais conceitos mencionados até agora, que são frequentemente abordados em provas. Criptografia é derivada das palavras gregas “kryptos”, que significa ocultar, e “graphein”, que se refere à escrita. É uma técnica antiga, utilizada há muito tempo para ocultar informações.

O objetivo da criptografia é transmitir informações de forma que, se interceptadas, não possam ser compreendidas pelo interceptador. Somente a pessoa destinatária, que conhece o código e possui a capacidade de decifrar, pode descriptografar a mensagem com sucesso.



A imagem obtida do CERT-BR, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança da Internet no Brasil, está diretamente relacionada ao tema das ameaças que serão abordados em breve. Ela está relacionada ao processo criptográfico. Na imagem, uma informação inicialmente legível se torna ilegível ao passar por um método criptográfico.

15m

Em algum momento, é importante considerar que, se o processo permanecer dessa forma, ele precisa ser reversível para que a compreensão seja restaurada. Portanto, será necessário aplicar novamente o método inverso para reverter esse processo.

CRIPTOGRAFAR

Existe um processo conhecido como criptografia, também chamado de codificação ou cifragem da informação. Inicialmente, tem-se um texto legível, denominado texto em branco, que pode ser compreendido por qualquer pessoa capaz de ler.

Esse texto é então submetido a um algoritmo criptográfico, que é um programa de computador projetado para realizar essa transformação. Assim como existem programas para edição de imagens ou aplicativos de mensagens como o WhatsApp, cada um com sua finalidade específica, o algoritmo criptográfico tem a função de converter o texto legível em um formato cifrado. Para garantir que o processo seja reversível, uma senha é aplicada ao algoritmo, personalizando essa transformação.

Portanto, após a aplicação da senha, o texto se torna criptografado. É relevante destacar que, como mencionado anteriormente, se o processo não for reversível, ele perde a utilidade na maioria dos contextos.

DESCRIPTOGRAFAR

E então vem o processo de descriptografar, decodificar ou decifrar. É importante ter cuidado com o termo "decifrar", pois pode implicar tentativas de adivinhação sem ter a senha. Existe um tipo de ataque chamado força bruta, que consiste justamente em tentativas repetidas até obter sucesso na decifração.

Dependendo do método criptográfico utilizado, pode haver a necessidade de compartilhar essa chave entre pessoas autorizadas para acessar a informação. Se alguém interceptar a informação no meio do caminho sem possuir a chave, poderá tentar decifrá-la. A segurança da criptografia é medida em bits, como 1024 bits, 2048 bits, entre outros. Quanto maior a força criptográfica, mais difícil é o processo de decifração.

Em alguns contextos, especialmente em níveis mais avançados como pós-graduação, pode-se considerar matematicamente impossível decifrar a informação criptografada devido ao tempo necessário e ao poder computacional exigido. Nesses casos, embora não se fale em segurança absoluta ou impossibilidade completa, trabalha-se com a ideia de quase impossibilidade de decifração.

Após receber a informação criptografada, que não é legível, o processo de descriptografia se inicia. Utiliza-se o mesmo algoritmo criptográfico aplicado na codificação, juntamente com a senha apropriada, que pode ser a mesma utilizada anteriormente. Com isso, a informação se torna legível novamente. Portanto, ocorreu o processo de criptografia seguido pela descriptografia, resultando na codificação e posterior decodificação, ou cifragem e decifragem do texto.

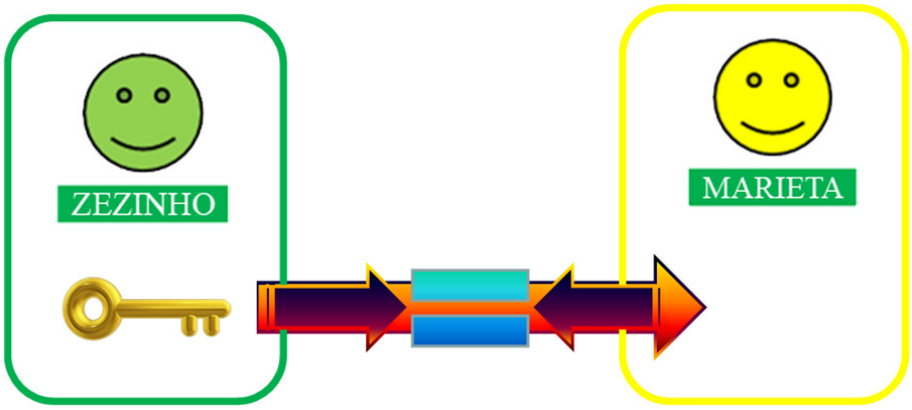
PRINCIPAIS MÉTODOS CRIPTOGRÁFICOS

- **CRIPTOGRAFIA SIMÉTRICA**
- **CRIPTOGRAFIA ASSIMÉTRICA**

CRIPTOGRAFIA SIMÉTRICA

Simetria refere-se à igualdade entre os lados. Em segurança da informação, significa que ambos os lados utilizam a mesma chave. A chave usada para criptografar é a mesma utilizada para descriptografar. Isso implica que a criptografia simétrica é mais veloz. No entanto, quando algo é mais rápido em segurança da informação, acarreta certos riscos. Embora seja um processo criptográfico mais simples, utilizando uma única chave, não é tão seguro quanto o outro método. Porém atente-se, menos seguro não implica necessariamente ser inseguro.

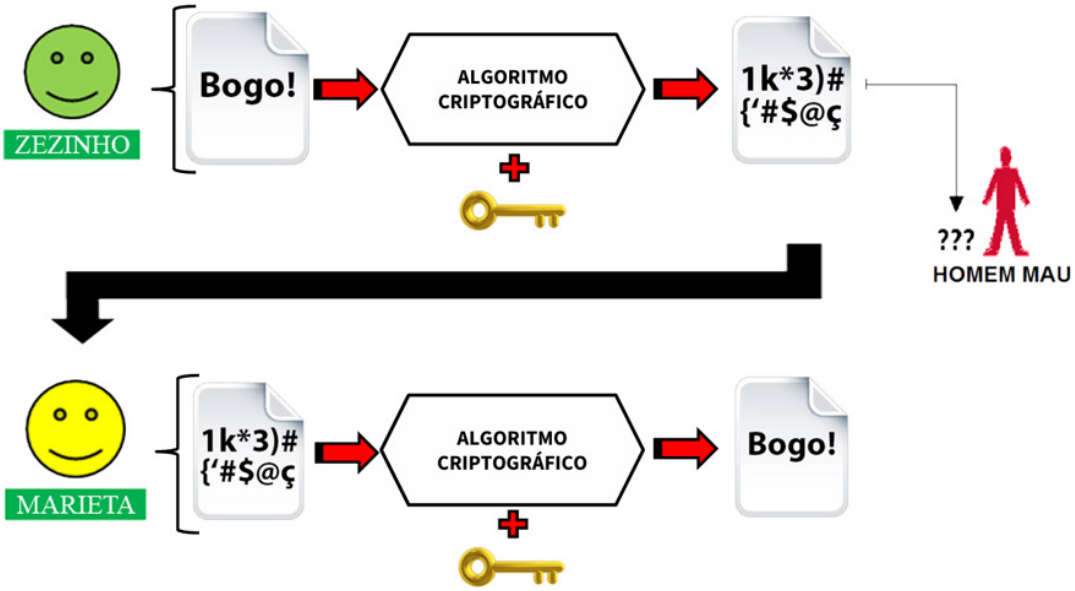
20m



Tem-se dois personagens mencionados anteriormente, Zezinho e Marieta, que utilizarão uma mesma chave. Isso implica que, em algum momento, essa chave será compartilhada entre eles, o que constitui o momento crítico da criptografia simétrica. Ambos utilizarão essa mesma chave.

Para ilustrar, considere sua própria casa, onde várias pessoas possuem cópias da mesma chave. Se uma dessas pessoas perder a chave e alguém a encontrar, essa pessoa poderá entrar na casa. Ela também pode fazer uma cópia da chave perdida e colocá-la de volta no mesmo local. Se a pessoa que perdeu a chave eventualmente a encontrar e pensar que está segura, a cópia já terá sido feita e devolvida ao mesmo lugar, possivelmente até dentro da própria casa, aproveitando um momento de descuido.

Portanto, é crucial lembrar que, embora a criptografia simétrica utilize uma única chave e seja um processo mais rápido, é menos segura. Sua vulnerabilidade reside justamente no uso compartilhado dessa única chave. Uma vez comprometida, seja por qualquer motivo, geralmente não há como evitar o acesso não autorizado às informações protegidas.



Aplica-se um algoritmo criptográfico ao texto legível, resultando em uma informação cifrada. Se alguém não autorizado interceptar essa informação, não conseguirá compreendê-la. Ao enviá-la para o destinatário que também possui a chave correspondente, a mesma utilizada na cifragem, ele conseguirá decifrar o texto. Pode haver mais de duas pessoas envolvidas nesse processo, cada uma possuindo uma cópia da chave, garantindo que apenas pessoas autorizadas acessem a informação.

A seguir, será abordada a criptografia assimétrica. Por razões didáticas, este tópico será encerrado um pouco antes do planejado, a fim de iniciar e concluir o assunto dentro do mesmo bloco. Após a exploração da criptografia simétrica, discutir-se-á a criptografia assimétrica. O prefixo "a" neste contexto indica a falta de igualdade. Enquanto na criptografia simétrica utiliza-se a mesma chave em ambos os lados, na abordagem assimétrica essa prática não será adotada. Este tema será desenvolvido no próximo bloco.

GABARITO

4. a
5. E
6. b
7. E