

Aula 04

*TJ-PR (Técnico Judiciário) Passo
Estratégico de Informática - 2025
(Pós-Edital)*

Autor:
Diego Carvalho

20 de Agosto de 2025

Índice

| | |
|---|----|
| 1) O que é mais cobrado no assunto - Segurança da Informação - AOCP | 3 |
| 2) Roteiro de Revisão - Segurança da Informação | 4 |
| 3) Aposto Estratégica - Segurança da Informação | 11 |
| 4) Questões Estratégicas - Segurança da Informação - AOCP | 12 |
| 5) Questionário de Revisão - Segurança da Informação | 17 |
| 6) Lista de Questões Estratégicas - Segurança da Informação - AOCP | 26 |
| 7) Gabarito de Questões Estratégicas - Segurança da Informação - AOCP | 28 |
| 8) Referências Bibliográficas - Segurança da Informação | 29 |



O QUE É MAIS COBRADO DENTRO DO ASSUNTO?

A análise estatística refere-se ao período de 2021 a 2025, abrangendo provas realizadas pela banca organizadora do concurso de níveis médio e superior (em informática, não há diferenciação do nível de questões). Por fim, quando não há quantidade razoável de questões para analisar, nós consideramos percentuais de incidências de bancas similares.

| TÓPICO | % DE COBRANÇA [AOCF] |
|---------------------|-------------------------|
| Confidencialidade | 10% |
| Integridade | 10% |
| Disponibilidade | 09% |
| Autenticidade | 03% |
| Irretratabilidade | 04% |
| Criptografia | 21% |
| Autenticação | 17% |
| Assinatura Digital | 09% |
| Certificado Digital | 17% |



ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

DEFINIÇÕES DE SEGURANÇA DA INFORMAÇÃO

Proteção de informações e de sistemas de informações contra acesso, uso, divulgação, interrupção, modificação ou destruição não autorizados.

Salvaguarda de dados organizacionais contra acesso não autorizado ou modificação para assegurar sua disponibilidade, confidencialidade e integridade.

Conjunto de estratégias para gerenciar processos, ferramentas e políticas necessárias para prevenir, detectar, documentar e combater ameaças às informações organizacionais.

Galera, selecionar e implementar controles de segurança adequados inicialmente pode ajudar uma organização a reduzir seus riscos a níveis aceitáveis. A seleção de possíveis controles deve se basear na avaliação de riscos. Os controles podem variar em natureza, mas – fundamentalmente – são formas de proteger a confidencialidade, integridade ou disponibilidade de informações. **Em geral, eles são divididos em dois tipos¹:**

| | |
|--------------------------|---|
| CONTROLES FÍSICOS | São barreiras que impedem ou limitam o acesso físico direto às informações ou à infraestrutura que contém as informações. Ex: portas, trancas, paredes, blindagem, vigilantes, geradores, sistemas de câmeras, alarmes, catracas, cadeados, salas-cofre, alarmes de incêndio, crachás de identificação, entre outros. |
| CONTROLES LÓGICOS | Também chamados de controles técnicos, são barreiras que impedem ou limitam o acesso à informação por meio do monitoramento e controle de acesso a informações e a sistemas de computação. Ex: senhas, firewalls, listas de controle de acesso, criptografia, biometria ² , IDS, IPS, entre outros. |

Na Segurança da Informação, utiliza-se um jargão muito específico. Caso – no decorrer da aula – vocês tenham alguma dúvida, é só retornar aqui e descobrir o significado. Vejamos

| TERMINOLOGIA | DESCRIÇÃO |
|-------------------|---|
| ATIVO | Qualquer coisa que tenha valor para instituição, tais como: informações, pessoas, serviços, software, hardware, documentos físicos, entre outros. |
| INFORMAÇÃO | Ativo que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, por isso, deve ser adequadamente protegido. |
| AGENTE | Fonte produtora de um evento que pode ter um efeito adverso sobre um ativo de informação, como um funcionário, meio ambiente, hacker, etc. |

¹ Nunca vi em bibliografias consagradas, mas já encontrei em uma prova a cobrança de controles de segurança processuais, que tratam basicamente de... processos de segurança (Ex: troca de senha a cada 30 dias).

² A biometria é polêmica: há algumas classificações que a colocam como controle lógico e outras como físico ou lógico a depender do que ela se propõe a proteger.



| | |
|------------------------|--|
| VULNERABILIDADE | Fragilidades presentes ou associadas a ativos que, quando exploradas por ameaças, levam à ocorrência de incidentes de segurança. |
| AMEAÇA | A ameaça é um agente externo que, se aproveitando das vulnerabilidades, poderá quebrar a confidencialidade, integridade ou disponibilidade da informação, causando um desastre ou perda significativa em um ambiente, sistema ou ativo de informação. |
| ATAQUE | Evento decorrente da exploração de uma vulnerabilidade por uma ameaça com o intuito de obter, alterar, destruir, remover, implantar ou revelar informações sem autorização de acesso. |
| EVENTO | Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação. |
| INCIDENTE | Fato decorrente de um ataque bem-sucedido, com consequências negativas, uma ocorrência indicando uma violação, uma falha ou situação desconhecida, algo que possa ser relevante para a segurança da informação. |
| IMPACTO | Abrangência dos danos causados por um incidente de segurança sobre um ou mais processos de negócio. |
| RISCO | Probabilidade potencial da concretização de um evento que possa causar danos a um ou mais ativos da organização. |

Os princípios de segurança têm como objetivo proteger dados e sistemas contra acessos não autorizados, modificações indevidas e garantir sua acessibilidade e autenticidade.

| 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. |



PEGADINHA CLÁSSICA: CONFIDENCIALIDADE X DISPONIBILIDADE



A confidencialidade garante que a informação somente esteja acessível para usuários autorizados. Já a disponibilidade garante que a informação esteja disponível aos usuários autorizados sempre que necessário.

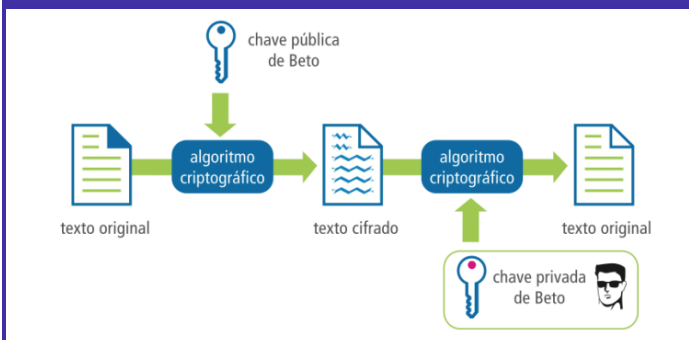
| PRINCÍPIOS ADICIONAIS | DESCRIÇÃO |
|--------------------------|---|
| AUTENTICIDADE | Propriedade que trata da garantia de que um usuário é de fato quem alega ser. Em outras palavras, ela garante a identidade de quem está enviando uma determinada informação. |
| IRRETRATABILIDADE | Também chamada 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. |

AUTENTICIDADE + INTEGRIDADE = IRRETRATABILIDADE

Esteganografia: trata-se de uma técnica utilizada para esconder informações. **Seu objetivo é que as informações sejam transmitidas de forma invisível, sem que possam ser capturadas ou monitoradas.** Trata-se de uma técnica para ocultar uma mensagem dentro de outra, de forma que não sejam percebidas por terceiros. Em geral, escondem-se mensagens dentro de imagens, sons, vídeos, textos, entre outros.

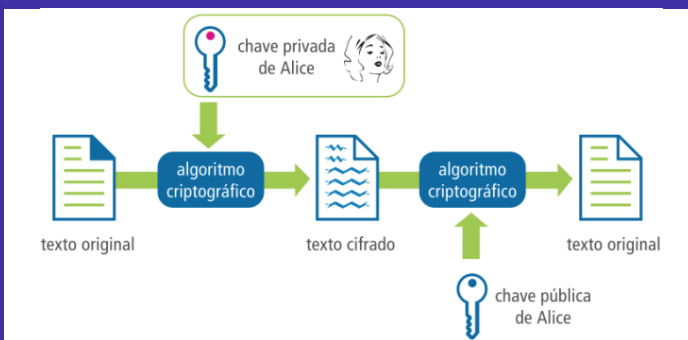
| TIPO DE CRIPTOGRAFIA | DESCRIÇÃO |
|---|--|
| CRIPTOGRAFIA SIMÉTRICA (CHAVE SECRETA) | Utiliza um algoritmo e uma única chave secreta para cifrar/decifrar que tem que ser mantida em segredo. Principais algoritmos: DES, 3DES, AES, IDEA, RC4, Blowfish, Cifragem de Júlio César, etc. |
| CRIPTOGRAFIA ASSIMÉTRICA (CHAVE PÚBLICA) | Utiliza um algoritmo e um par de chaves para cifrar/decifrar - uma pública e a outra tem que ser mantida em segredo. Principais algoritmos: RSA, DSA, ECDSA, Diffie-Hellman (para troca de chaves), etc. |
| 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



O emissor criptografa o texto original com a chave pública do receptor de forma que somente ele

CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA AUTENTICIDADE



O emissor criptografa o texto original com sua chave privada de forma que o receptor possa descryptografá-lo com a chave pública do emissor.



consiga descriptografá-lo com sua chave privada para visualizar o texto original.

A seguir, vejamos uma lista de algoritmos:

| ALGORITMO | DESCRIÇÃO |
|-----------------------|--|
| DES | Algoritmo simétrico de chave privada com 56 bits de tamanho de chave. Desenvolvido na década de 1970, é considerado fraco pelos padrões atuais de segurança. |
| 3DES | Versão atualizada do DES, que usa três vezes a cifra DES para melhorar a segurança. Suas chaves podem ter 112 ou 168 bits. |
| AES | Algoritmo simétrico de chave privada que substituiu o DES como padrão de criptografia em 2001. Suas chaves podem ter 128, 192 ou 256 bits. |
| IDEA | Algoritmo simétrico de chave privada desenvolvido na década de 1990, com chave de 128 bits. Foi uma alternativa ao DES, mas é menos utilizado atualmente. |
| RC4 | Algoritmo simétrico de chave privada usado em várias aplicações, como redes sem fio e SSL/TLS. Possui chaves de 40 a 2048 bits. |
| RSA | Algoritmo assimétrico de chave pública usado para criptografia e assinaturas digitais. É um dos algoritmos mais amplamente usados na criptografia moderna. |
| Diffie-Hellman | Algoritmo de troca de chaves que permite a comunicação segura em um canal inseguro. É amplamente utilizado em sistemas criptográficos baseados em chave pública. |
| Blowfish | Algoritmo simétrico de chave privada usado em diversas aplicações de segurança, com chaves de 32 a 448 bits. É conhecido por sua velocidade e segurança. |
| MD5 | Algoritmo de hash criptográfico que gera um resumo de 128 bits da mensagem original. É amplamente usado para verificar a integridade de arquivos. |
| SHA | Família de algoritmos de hash criptográficos que geram resumos de tamanho fixo (160, 256, 384 ou 512 bits) da mensagem original. É amplamente usado em diversas aplicações de segurança. |

| ALGORITMO | SEGURANÇA | VELOCIDADE | TAMANHO DA CHAVE | UTILIZAÇÃO | TIPO |
|-----------------------|-----------|------------|------------------|---------------|-------------|
| DES | FRACO | RÁPIDO | 56 BITS | LEGADO | SIMÉTRICO |
| 3DES | MODERADO | LENTO | 112-168 BITS | LEGADO | SIMÉTRICO |
| AES | FORTE | RÁPIDO | 128-256 BITS | ATUAL | SIMÉTRICO |
| IDEA | MODERADO | RÁPIDO | 128 BITS | LEGADO | SIMÉTRICO |
| RC4 | MODERADO | RÁPIDO | 40-2048 BITS | LEGADO | SIMÉTRICO |
| RSA | FORTE | LENTO | 2048-4096 BITS | ATUAL | ASSIMÉTRICO |
| DIFFIE-HELLMAN | FORTE | MODERADO | VARIÁVEL | CHAVE PÚBLICA | ASSIMÉTRICO |
| BLOWFISH | FORTE | RÁPIDO | 32-448 BITS | LEGADO | SIMÉTRICO |
| MD5 | FRACO | RÁPIDO | 128 BITS | LEGADO | HASH |



SHA

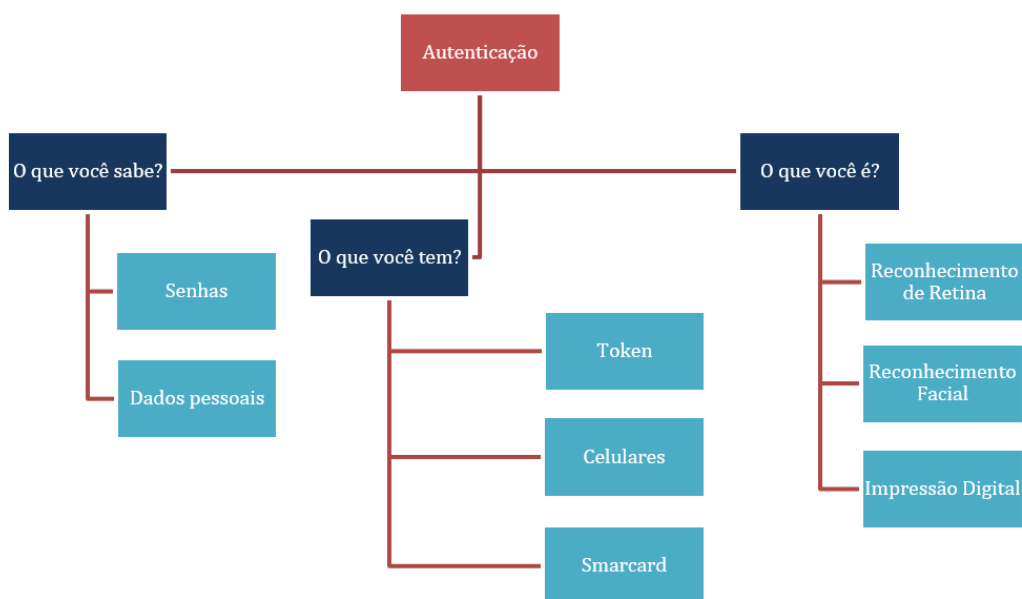
MODERADO

MODERADO

160-512 BITS

ATUAL

HASH



| 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

INTEGRIDADE

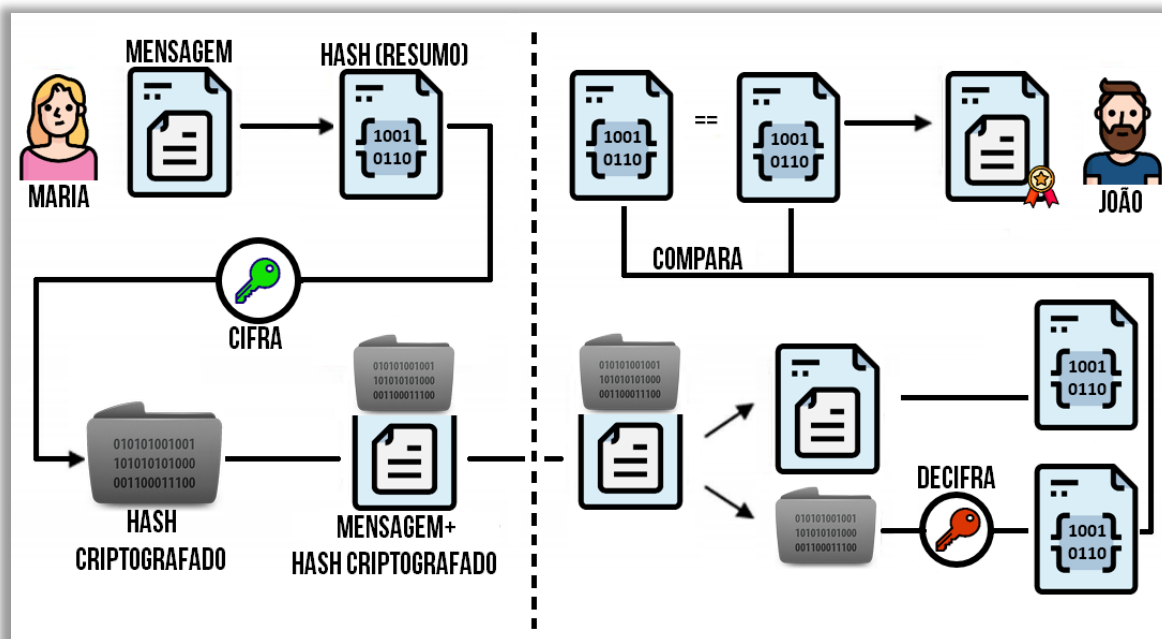
NÃO-REPÚDIO

AUTENTICIDADE



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 descryptografa 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 descryptografou 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.

GARANTIAS

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 MÁXIMA (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 por si só garante apenas **confidencialidade**! No entanto, quando utilizamos algoritmos criptográficos, nós acrescentamos mecanismos que nos ajudam a garantir outros serviços de segurança da informação. Em outras palavras, algoritmos de criptografia simétrica permitem garantir **confidencialidade, autenticidade e integridade**. Já algoritmos de criptografia assimétrica permitem garantir **confidencialidade, autenticidade, integridade e não-repúdio**. Notem que nem todos poderão ser garantidos simultaneamente!



APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais.

Eu listei abaixo o ponto com maior probabilidade de cobrança no contexto de **Segurança da Informação**. Estas são as minhas apostas:

| 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. |

| PRINCÍPIOS DE SEGURANÇA | 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 | DESCRIÇÃO |
|--|--|
| CRIPTOGRAFIA SIMÉTRICA (CHAVE SECRETA) | Utiliza um algoritmo e uma única chave secreta para cifrar/decifrar que tem que ser mantida em segredo. Principais algoritmos: DES, 3DES, AES, IDEA, RC4, Blowfish, Cifragem de Júlio César, etc. |
| 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. Principais algoritmos: RSA, DSA, ECDSA, Diffie-Hellman (para troca de chaves), etc. |



QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.

1. (AOCP / UFFS - 2019) Uma assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada. Sobre Assinaturas digitais, assinale a alternativa correta.

- a) A verificação da assinatura é feita com o uso da chave privada. É a chave privada, então, que deve ser compartilhada com o destinatário.
- b) A assinatura digital baseia-se no fato de que apenas o dono conhece a chave pública utilizada.
- c) Se o texto foi codificado com a chave privada, somente a própria chave privada pode decodificá-lo.
- d) O dono da mensagem conhece a chave privada. Se essa chave foi usada para codificar uma informação, então apenas o dono da mensagem poderia ter feito isso.
- e) Um hash (que possui tamanho fixo e reduzido) pode ser utilizado pra obter a informação original novamente.

Comentários:

- (a) Errado. A verificação da assinatura digital é feita com a chave pública, e não com a chave privada. A chave privada deve ser mantida em segredo pelo dono da assinatura, enquanto a pública pode ser compartilhada;
- (b) Errado. A chave pública não é secreta, pelo contrário, ela deve ser compartilhada para permitir a verificação da assinatura digital;
- (c) Errado. Se um texto foi codificado com a chave privada, ele pode ser decodificado com a chave pública, não com a própria chave privada. Isso é fundamental para a verificação da assinatura digital;



(d) Correto. A assinatura digital utiliza a chave privada do remetente para cifrar um hash da mensagem. Como só o dono da chave privada pode gerar essa assinatura, isso comprova sua autenticidade e integridade;

(e) Errado. Um hash é uma função unidirecional, ou seja, não pode ser revertido para obter a informação original. Ele serve apenas para verificar a integridade dos dados.

Gabarito: Letra D

2. (AOCP / Prefeitura de João Pessoa - PB - 2018) Um dos itens mais importantes é a autenticidade, na qual o transmissor confirma sua identidade para o receptor, assinando digitalmente o documento que vai ser transmitido. A respeito da assinatura digital, assinale a alternativa correta.

a) Para se confeccionar uma assinatura digital, é necessário executar um algoritmo de hash sobre a mensagem e, após isso, criptografar o resumo obtido com a chave privada.

b) Para se confeccionar uma assinatura digital, é necessário executar somente o algoritmo de hash.

c) Para se confeccionar uma assinatura digital, é necessário criptografar um documento com a chave simétrica.

d) Para se confeccionar uma assinatura digital é necessário executar um algoritmo de hash sobre a mensagem e, após isso, criptografar o resumo obtido com a chave pública.

Comentários:

(a) Correto. A assinatura digital é gerada ao aplicar um algoritmo de hash sobre a mensagem para obter um resumo (digest) e, em seguida, criptografar esse hash com a chave privada do remetente. O destinatário pode verificar a autenticidade ao descriptografar o hash com a chave pública do remetente e compará-lo com um novo hash gerado da mensagem recebida;

(b) Errado. Apenas executar um algoritmo de hash gera um resumo da mensagem, mas não garante autenticidade, pois qualquer pessoa poderia gerar um hash idêntico;

(c) Errado. A criptografia simétrica não é usada para assinaturas digitais. Assinaturas digitais utilizam criptografia assimétrica, onde a chave privada assina e a chave pública verifica a assinatura;



(d) Errado. A assinatura digital é gerada ao criptografar o hash com a chave privada, e não com a chave pública. A chave pública é usada pelo destinatário para verificar a assinatura.

Gabarito: Letra A

3. (AOCP / Câmara de Rio Branco - AC - 2016) Os atributos da segurança da informação, segundo os padrões internacionais (ISO/ IEC 17799:2005), norteiam práticas de segurança. Nesse contexto, são atributos da segurança da informação, EXCETO

- a) irretratabilidade ou não repúdio.
- b) autenticidade.
- c) legitimidade.
- d) integridade.
- e) disponibilidade.

Comentários:

(a) Errado. Irretratabilidade (não repúdio) é um atributo da segurança da informação, garantindo que uma ação realizada por um usuário não possa ser negada posteriormente;

(b) Errado. Autenticidade é um atributo essencial, garantindo que os dados e identidades são legítimos e confiáveis;

(c) Correto. Legitimidade não é um atributo formalmente reconhecido pela norma ISO/IEC 17799:2005 como parte dos princípios da segurança da informação;

(d) Errado. Integridade é um dos três pilares da segurança da informação, assegurando que os dados não sejam modificados indevidamente;

(e) Errado. Disponibilidade é fundamental, garantindo que a informação esteja acessível sempre que necessário.

Gabarito: Letra C

4. (AOCP / CISAMUSEP - PR - 2016) Para acessarmos serviços online (webmail, redes sociais, sites de e-commerce etc.), geralmente utilizamos um "nome de usuário" ou "login" que representa uma conta e, para garantir que somos o dono da conta, utilizamos uma "senha". Qual dos elementos apresentados a seguir NÃO deve ser utilizado na elaboração de uma senha:

- a) Números aleatórios.



- b) Fazer substituições de caracteres.
- c) Grande quantidade de caracteres.
- d) Sequências de teclado.
- e) Diferentes tipos de caracteres.

Comentários:

(a) Errado. Números aleatórios aumentam a complexidade da senha, tornando-a mais difícil de ser adivinhada por ataques de força bruta ou dicionário;

(b) Errado. Substituir caracteres (por exemplo, trocar "A" por "@") pode aumentar a segurança da senha, embora padrões previsíveis possam ser explorados por atacantes;

(c) Errado. Senhas longas são mais seguras, pois aumentam o número de combinações possíveis, dificultando ataques de força bruta;

(d) Correto. Sequências de teclado (como "123456", "qwerty" ou "asdfgh") são extremamente previsíveis e facilmente descobertas, tornando a senha fraca;

(e) Errado. O uso de diferentes tipos de caracteres (maiúsculas, minúsculas, números e símbolos) torna a senha mais resistente a ataques.

Gabarito: Letra D

5. (AOCP / SEJUS - CE - 2017) Preencha a lacuna e assinale a alternativa correta. Um(a) _____ se usado(a) de forma maliciosa e instalado(a) pode permitir estabelecer conexões cifradas com sites fraudulentos, sem que o navegador emita alertas indicativos de risco.

- a) certificado EV SSL
- b) certificado auto-assinado
- c) criptografia de chaves assimétricas
- d) criptografia de chave simétrica

Comentários:

(a) Errado. O certificado EV SSL (Extended Validation SSL) é um certificado digital validado por uma autoridade certificadora confiável, exibindo informações detalhadas sobre a entidade certificada e aumentando a segurança para o usuário;



(b) Correto. Um certificado autoassinado, quando instalado de forma maliciosa, pode permitir conexões cifradas com sites fraudulentos sem que o navegador exiba alertas de segurança. Isso ocorre porque navegadores normalmente alertam sobre certificados autoassinados, mas se o usuário ou um atacante instalá-lo manualmente no sistema, ele pode ser aceito sem notificações;

(c) Errado. A criptografia de chaves assimétricas é um conceito mais amplo usado para segurança de comunicação e não é, por si só, um elemento que engana navegadores para aceitar conexões maliciosas;

(d) Errado. A criptografia de chave simétrica protege dados com uma única chave compartilhada, mas não está diretamente relacionada à validação de conexões seguras em navegadores.

Gabarito: Letra B



QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível! Vamos ao nosso questionário:

Perguntas

1. Quais são os três princípios fundamentais da segurança da informação?
2. Quais são os dois tipos de controles de segurança?
3. O que são controles físicos?
4. O que são controles lógicos (ou técnicos)?
5. O que é o princípio da confidencialidade?
6. O que é o princípio da integridade?
7. Qual a relação entre confidencialidade e integridade?
8. O que é o princípio da disponibilidade?
9. Qual a diferença entre confidencialidade e disponibilidade?
10. Quais são os atributos do Hexagrama Parkeriano?
11. O que é autenticidade?
12. O que é o princípio da irretratabilidade?
13. Como a irretratabilidade pode ser garantida?
14. Autenticidade e irretratabilidade são a mesma coisa?
15. Como a integridade está relacionada à irretratabilidade?
16. O que é criptologia?
17. O que é esteganografia?
18. Qual é a diferença entre esteganografia e criptografia?



19. O que é criptografia?
20. Quais são os principais tipos de criptografia?
21. Quais são os fundamentos principais das técnicas de criptografia?
22. O que é criptografia simétrica?
23. Qual o maior desafio da criptografia simétrica?
24. Quais são alguns algoritmos de criptografia simétrica?
25. Qual princípio é garantido pela criptografia simétrica?
26. A criptografia simétrica garante o princípio da integridade?
27. A criptografia simétrica pode garantir autenticidade?
28. O que é criptografia assimétrica?
29. Qual é a vantagem da criptografia assimétrica em relação à simétrica?
30. Na criptografia assimétrica, o que acontece ao criptografar uma mensagem com a chave pública?
31. O que acontece se você criptografar uma mensagem com sua chave privada?
32. Quais são os principais algoritmos de criptografia assimétrica?
33. Qual é a principal desvantagem da criptografia assimétrica?
34. O que é criptografia híbrida?
35. Quais são os três fatores que influenciam a segurança de um sistema criptográfico?
36. O que é um algoritmo de hash criptográfico?
37. O que é o método de autenticação "O que você sabe"?
38. O que é autenticação baseada em "O que você é"?
39. O que é autenticação baseada em "O que você tem"?
40. O que é autenticação forte?
41. O que é autenticação em dois fatores?
42. O que é uma assinatura digital?
43. O que é um algoritmo de hash?
44. O que caracteriza um algoritmo de hash?
45. O que é uma colisão em um algoritmo de hash?
46. Qual é a função de um algoritmo de hash em uma assinatura digital?
47. O que é irretratabilidade?
48. Como a assinatura digital garante autenticidade e integridade?
49. Qual é a diferença entre identificação, autenticação e autorização?
50. O que é uma Autoridade Certificadora (AC)?
51. O que é um certificado digital?
52. O que é a Lista de Certificados Revogados (LCR)?
53. Qual a diferença entre assinatura digital e certificado digital?
54. O que é uma Infraestrutura de Chave Pública (ICP)?
55. Qual é o papel da Autoridade Certificadora Raiz (AC-Raiz)?
56. O que faz uma Autoridade de Registro (AR)?
57. O que é um certificado autoassinado?
58. O que é uma Cadeia/Teia de Confiança (Web of Trust)?
59. Quais são os dois tipos de certificados digitais principais?
60. Qual a função do certificado digital em uma página web?



Perguntas com Respostas

1. Quais são os três princípios fundamentais da segurança da informação?

Confidencialidade, Integridade e Disponibilidade (CID).

2. Quais são os dois tipos de controles de segurança?

Controles físicos e controles lógicos.

3. O que são controles físicos?

São barreiras que impedem ou limitam o acesso físico direto a informações ou infraestrutura. Ex: portas, trancas, sistemas de câmeras.

4. O que são controles lógicos (ou técnicos)?

São barreiras que limitam o acesso à informação por meio de monitoramento e controle de sistemas. Ex: senhas, firewalls, criptografia.

5. O que é o princípio da confidencialidade?

É a capacidade de um sistema de não permitir que informações sejam acessadas ou reveladas a entidades não autorizadas.

6. O que é o princípio da integridade?

É a capacidade de garantir que a informação está correta, fidedigna e não foi corrompida durante seu percurso, mantendo suas características originais.

7. Qual a relação entre confidencialidade e integridade?

São princípios independentes. A quebra de um não implica a quebra do outro.

8. O que é o princípio da disponibilidade?

É a propriedade de uma informação estar acessível e utilizável sob demanda por uma entidade autorizada.

9. Qual a diferença entre confidencialidade e disponibilidade?

A confidencialidade garante que apenas usuários autorizados tenham acesso à informação; a disponibilidade garante que a informação esteja acessível quando necessário.

10. Quais são os atributos do Hexagrama Parkeriano?

Confidencialidade, Integridade, Disponibilidade, Autenticidade, Posse ou Controle, e Utilidade.



11. O que é autenticidade?

É a propriedade que garante que o emissor de uma mensagem é quem ele alega ser.

12. O que é o princípio da irretratabilidade?

Também conhecido como não-repúdio, é a garantia de que o emissor da mensagem não poderá negar posteriormente sua autoria.

13. Como a irretratabilidade pode ser garantida?

Com mecanismos de integridade e autenticidade, como a assinatura digital e sistemas de criptografia.

14. Autenticidade e irretratabilidade são a mesma coisa?

Não. A autenticidade garante a identidade do emissor, enquanto a irretratabilidade impede que ele negue posteriormente o envio da mensagem.

15. Como a integridade está relacionada à irretratabilidade?

A integridade garante que a mensagem não foi alterada, o que, junto com a autenticidade, garante a irretratabilidade.

16. O que é criptologia?

Criptologia é o estudo da ocultação de informações (criptografia e esteganografia) e da quebra dessas técnicas (criptoanálise).

17. O que é esteganografia?

Esteganografia é uma técnica de ocultar uma mensagem dentro de outra, de forma que ela não seja percebida, como esconder uma mensagem dentro de uma imagem.

18. Qual é a diferença entre esteganografia e criptografia?

Esteganografia esconde a existência da mensagem, enquanto a criptografia torna a mensagem ininteligível para quem não possui a chave de descryptografia.

19. O que é criptografia?

Criptografia é a técnica de tornar uma mensagem ininteligível para qualquer pessoa que não tenha a chave para descryptografá-la.

20. Quais são os principais tipos de criptografia?

Criptografia simétrica, criptografia assimétrica e criptografia híbrida.



21. Quais são os fundamentos principais das técnicas de criptografia?

Substituição, onde elementos são mapeados para outros, e transposição, onde elementos são reorganizados.

22. O que é criptografia simétrica?

Criptografia simétrica é uma técnica onde a mesma chave é usada tanto para criptografar quanto para descriptografar a mensagem.

23. Qual o maior desafio da criptografia simétrica?

Proteger a chave compartilhada entre as partes, já que a segurança da comunicação depende dela.

24. Quais são alguns algoritmos de criptografia simétrica?

DES, 3DES, AES, IDEA, RC4, Blowfish e Cifragem de Júlio César.

25. Qual princípio é garantido pela criptografia simétrica?

A criptografia simétrica garante o princípio da confidencialidade.

26. A criptografia simétrica garante o princípio da integridade?

Não, a criptografia simétrica não garante que a mensagem permaneça inalterada durante a transmissão.

27. A criptografia simétrica pode garantir autenticidade?

Sim, mas apenas se a chave secreta for conhecida por apenas duas entidades.

28. O que é criptografia assimétrica?

Criptografia assimétrica é uma técnica de criptografia que utiliza um par de chaves distintas: uma chave pública para criptografar e uma chave privada para descriptografar as informações.

29. Qual é a vantagem da criptografia assimétrica em relação à simétrica?

Não há necessidade de compartilhar a chave privada, eliminando o risco de interceptação durante a troca de chaves.

30. Na criptografia assimétrica, o que acontece ao criptografar uma mensagem com a chave pública?

Somente a chave privada correspondente pode descriptografar a mensagem, garantindo a confidencialidade.



31. O que acontece se você criptografar uma mensagem com sua chave privada?

Qualquer pessoa com a chave pública poderá descriptografá-la, garantindo o princípio da autenticidade.

32. Quais são os principais algoritmos de criptografia assimétrica?

RSA, DSA, ECDSA, ElGamal, Diffie-Hellman.

33. Qual é a principal desvantagem da criptografia assimétrica?

É mais lenta que a criptografia simétrica, podendo ser até 100 vezes mais lenta devido ao tamanho maior das chaves.

34. O que é criptografia híbrida?

Criptografia híbrida é a combinação de criptografia simétrica e assimétrica, onde a assimétrica é usada para trocar chaves simétricas e a simétrica para a comunicação.

35. Quais são os três fatores que influenciam a segurança de um sistema criptográfico?

A força do algoritmo, o sigilo da chave e o comprimento da chave.

36. O que é um algoritmo de hash criptográfico?

É uma função que transforma dados de tamanho variável em um resumo de tamanho fixo, usado para verificar a integridade dos dados.

37. O que é o método de autenticação "O que você sabe"?

É baseado no conhecimento de algo que apenas o usuário sabe, como senhas, frases secretas ou dados pessoais.

38. O que é autenticação baseada em "O que você é"?

É a autenticação baseada em características físicas únicas, como impressão digital, padrão de retina ou reconhecimento facial.

39. O que é autenticação baseada em "O que você tem"?

É a autenticação baseada em algo que o usuário possui, como celulares, crachás, Smart Cards ou tokens.

40. O que é autenticação forte?

É um método que combina pelo menos dois tipos de autenticação, como "o que você sabe" e "o que você tem", como na autenticação em dois fatores.



41. O que é autenticação em dois fatores?

É um método que combina dois tipos de autenticação, como uma senha (o que você sabe) e um código enviado ao celular (o que você tem).

42. O que é uma assinatura digital?

É uma forma de garantir autenticidade, integridade e irretratabilidade de um documento digital, utilizando criptografia assimétrica e algoritmos de hash.

43. O que é um algoritmo de hash?

É um algoritmo criptográfico que transforma uma entrada de dados de qualquer tamanho em uma saída de tamanho fixo, garantindo integridade.

44. O que caracteriza um algoritmo de hash?

Ele é unidirecional, ou seja, a saída não permite descobrir a entrada, e a mesma entrada sempre gera a mesma saída.

45. O que é uma colisão em um algoritmo de hash?

É quando diferentes entradas geram a mesma saída, algo que deve ser evitado em funções de hash criptográficas.

46. Qual é a função de um algoritmo de hash em uma assinatura digital?

Ele garante a integridade da mensagem, permitindo verificar se o conteúdo foi alterado.

47. O que é irretratabilidade?

É a garantia de que o emissor de uma mensagem ou documento não poderá negar posteriormente sua autoria.

48. Como a assinatura digital garante autenticidade e integridade?

A autenticidade é garantida pela criptografia com a chave privada do emissor, e a integridade é garantida pelo uso do algoritmo de hash.

49. Qual é a diferença entre identificação, autenticação e autorização?

Identificação é apresentar uma informação para ser reconhecido; autenticação é verificar se a identidade é válida; autorização é verificar os privilégios de acesso.

50. O que é uma Autoridade Certificadora (AC)?

É uma entidade responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais, funcionando como um cartório digital.



51. O que é um certificado digital?

É um documento eletrônico que contém informações como o nome, chave pública do proprietário e a assinatura digital de uma Autoridade Certificadora.

52. O que é a Lista de Certificados Revogados (LCR)?

É uma lista publicada pela Autoridade Certificadora contendo certificados que não são mais válidos ou confiáveis.

53. Qual a diferença entre assinatura digital e certificado digital?

A assinatura digital verifica a autenticidade e integridade de uma entidade, enquanto o certificado digital vincula uma chave pública a uma entidade e garante sua autenticidade.

54. O que é uma Infraestrutura de Chave Pública (ICP)?

É uma entidade que emite chaves públicas, garantindo credibilidade e confiança em transações digitais por meio de certificados digitais.

55. Qual é o papel da Autoridade Certificadora Raiz (AC-Raiz)?

A AC-Raiz emite certificados para outras Autoridades Certificadoras, gerencia certificados e fiscaliza a conformidade das práticas de certificação.

56. O que faz uma Autoridade de Registro (AR)?

A AR valida e encaminha solicitações de emissão ou revogação de certificados digitais e realiza a identificação presencial dos solicitantes.

57. O que é um certificado autoassinado?

É um certificado emitido e assinado pela própria Autoridade Certificadora Raiz, confirmando sua autenticidade.

58. O que é uma Cadeia/Teia de Confiança (Web of Trust)?

É um modelo descentralizado de confiança, onde usuários estabelecem relações de confiança entre si ao assinarem mutuamente seus certificados.

59. Quais são os dois tipos de certificados digitais principais?

Certificado de Assinatura Digital (A), para identificação e autenticação, e Certificado de Sigilo (S), para proteção de informações sigilosas.

60. Qual a função do certificado digital em uma página web?



Verificar a autenticidade do servidor e garantir que a comunicação entre o usuário e a página seja criptografada e segura.



LISTA DE QUESTÕES ESTRATÉGICAS

1. (AOCP / UFFS - 2019) Uma assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isso e que ela não foi alterada. Sobre Assinaturas digitais, assinale a alternativa correta.

- a) A verificação da assinatura é feita com o uso da chave privada. É a chave privada, então, que deve ser compartilhada com o destinatário.
- b) A assinatura digital baseia-se no fato de que apenas o dono conhece a chave pública utilizada.
- c) Se o texto foi codificado com a chave privada, somente a própria chave privada pode decodificá-lo.
- d) O dono da mensagem conhece a chave privada. Se essa chave foi usada para codificar uma informação, então apenas o dono da mensagem poderia ter feito isso.
- e) Um hash (que possui tamanho fixo e reduzido) pode ser utilizado pra obter a informação original novamente.

2. (AOCP / Prefeitura de João Pessoa - PB - 2018) Um dos itens mais importantes é a autenticidade, na qual o transmissor confirma sua identidade para o receptor, assinando digitalmente o documento que vai ser transmitido. A respeito da assinatura digital, assinale a alternativa correta.

- a) Para se confeccionar uma assinatura digital, é necessário executar um algoritmo de hash sobre a mensagem e, após isso, criptografar o resumo obtido com a chave privada.
- b) Para se confeccionar uma assinatura digital, é necessário executar somente o algoritmo de hash.
- c) Para se confeccionar uma assinatura digital, é necessário criptografar um documento com a chave simétrica.
- d) Para se confeccionar uma assinatura digital é necessário executar um algoritmo de hash sobre a mensagem e, após isso, criptografar o resumo obtido com a chave pública.



3. (AOCP / Câmara de Rio Branco - AC - 2016) Os atributos da segurança da informação, segundo os padrões internacionais (ISO/ IEC 17799:2005), norteiam práticas de segurança. Nesse contexto, são atributos da segurança da informação, EXCETO

- a) irretratabilidade ou não repúdio.
- b) autenticidade.
- c) legitimidade.
- d) integridade.
- e) disponibilidade.

4. (AOCP / CISAMUSEP - PR - 2016) Para acessarmos serviços online (webmail, redes sociais, sites de e-commerce etc.), geralmente utilizamos um "nome de usuário" ou "login" que representa uma conta e, para garantir que somos o dono da conta, utilizamos uma "senha". Qual dos elementos apresentados a seguir NÃO deve ser utilizado na elaboração de uma senha:

- a) Números aleatórios.
- b) Fazer substituições de caracteres.
- c) Grande quantidade de caracteres.
- d) Sequências de teclado.
- e) Diferentes tipos de caracteres.

5. (AOCP / SEJUS - CE - 2017) Preencha a lacuna e assinale a alternativa correta. Um(a) _____ se usado(a) de forma maliciosa e instalado(a) pode permitir estabelecer conexões cifradas com sites fraudulentos, sem que o navegador emita alertas indicativos de risco.

- a) certificado EV SSL
- b) certificado auto-assinado
- c) criptografia de chaves assimétricas
- d) criptografia de chave simétrica



GABARITO

1. LETRA D
2. LETRA A
3. LETRA C
4. LETRA D
5. LETRA B



REFERÊNCIAS BIBLIOGRÁFICAS

1. STALLINGS, William. Cryptography and Network Security: Principles and Practices. 7th ed. Boston: Pearson, 2017.
2. SCHNEIER, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed. New York: John Wiley & Sons, 1996.
3. MENEZES, Alfred J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. Handbook of Applied Cryptography. 5th ed. Boca Raton: CRC Press, 2001.
4. HINTZBERGEN, J.; SMULDERS, A.; VROOMEN, R.; WIRKUS, M. Foundations of Information Security: Based on ISO27001 and ISO27002. 2nd ed. Zaltbommel: Van Haren Publishing, 2018.
5. NAKAMURA, Emílio Tissato. Segurança de Redes em Ambientes Cooperativos. 1ª ed. São Paulo: Novatec, 2007.



ESSA LEI TODO MUNDO CONHECE: PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.



1 Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.



2 Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).



3 Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).



4 Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).



5 Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).



6 Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).



7 Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.



8 O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.



Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.