Estratégia Concursos

Aula 00

TJ-RO - Passo Estratégico de Conhecimentos Transversais (Noções de Informática) - 2024 (Pós-Edital)

Autor:
Diego Carvalho, Equipe Informática 2 (Diego Carvalho)

16 de Novembro de 2024

Índice

APRESENTAÇÃO

Faaaaaaaala, galera! Tudo tranquilo?

Eu sou o Prof. Diego Carvalho e, com imensa satisfação, serei o seu analista do Passo Estratégico! Eu também sou Coordenador da Equipe de TI do Estratégia Concursos, além de ministrar as disciplinas de Informática e Engenharia de Software. Para que você conheça um pouco sobre mim, segue um resumo da minha experiência profissional e acadêmica:

Estou extremamente feliz de ter a oportunidade de trabalhar na equipe do "Passo", porque tenho convicção de que nossos relatórios e simulados proporcionarão uma preparação diferenciada aos nossos alunos!

PROF. DIEGO CARVALHO

www.instagram.com/professordiegocarvalho

O QUE É O PASSO ESTRATÉGICO?

O Passo Estratégico é um material escrito e enxuto que possui dois objetivos principais:

a) orientar revisões eficientes;

b) destacar os pontos mais importantes e prováveis de serem cobrados em prova.

Assim, o Passo Estratégico pode ser utilizado tanto para **turbinar as revisões dos alunos mais adiantados nas matérias, quanto para maximizar o resultado na reta final de estudos por parte dos alunos que não conseguirão estudar todo o conteúdo do curso regular.**

Em ambas as formas de utilização, como regra, **o aluno precisa utilizar o Passo Estratégico em conjunto com um curso regular completo.**

Isso porque nossa didática é direcionada ao aluno que já possui uma base do conteúdo.

Assim, se você vai utilizar o Passo Estratégico:

a) **como método de revisão**, você precisará de seu curso completo para realizar as leituras indicadas no próprio Passo Estratégico, em complemento ao conteúdo entregue diretamente em nossos relatórios;

b) **como material de reta final**, você precisará de seu curso completo para buscar maiores esclarecimentos sobre alguns pontos do conteúdo que, em nosso relatório, foram eventualmente expostos utilizando uma didática mais avançada que a sua capacidade de compreensão, em razão do seu nível de conhecimento do assunto.

Seu cantinho de estudos famoso!

Poste uma foto do seu cantinho de estudos nos stories do Instagram e nos marque:

@passoestrategico

Vamos repostar sua foto no nosso perfil para que ele fique famoso entre milhares de concurseiros!

ANÁLISE ESTATÍSTICA

Vejamos na tabela apresentada a seguir o percentual de cobrança em prova das aulas que estudaremos em nosso curso:

TÓPICO	% DE COBRANÇA [CONSULPLAN]
Segurança da informação: noções de procedimentos de segurança; boas práticas de segurança cibernética, incluindo autenticação de dois fatores e gestão de senhas.	02%
Noções de vírus, worms e outras pragas virtuais;	08%
Noções de Informática: Noções do sistema operacional Windows 11. Conceitos de organização e de gerenciamento de informações: arquivos, pastas e programas.	53%
Navegadores web: Mozilla Firefox e Google Chrome.	31%
Google Workspace/Drive: compartilhamento de arquivos; criar arquivos, editar, compartilhamento de arquivos e permissões; Google Agenda - Criar eventos, convidar participantes, ajustar horários, anexar documentos, adicionar videoconferência; Google Tarefas; Google Meet; Gmail - configurações rápidas, painel de visualização, marcadores; editor de texto (documentos Google).	06%

O QUE É MAIS COBRADO DENTRO DO ASSUNTO?

Considerando os tópicos que compõem o nosso assunto, possuímos a seguinte distribuição percentual:

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

COMO NÃO TEMOS QUESTÕES SUFICIENTES DA BANCA ORGANIZADORA DO CONCURSO, INSERIMOS ACIMA AS ESTATÍSTICAS DE BANCAS SEMELHANTES.

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 tipos**[1]:

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, biometria2, 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

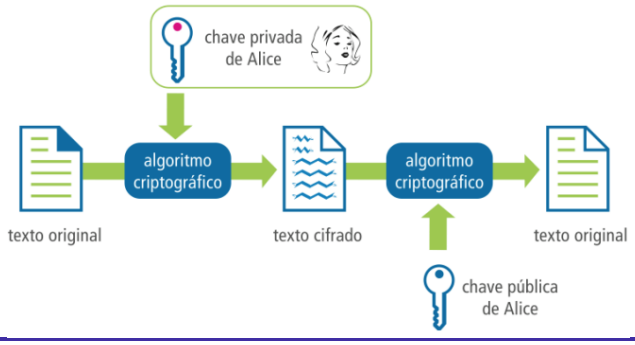
A confidencialidade garante que a informação somente esteja acessível para usuários autorizados. Já a disponibilidade garante que a informação esteja disponível aos usuários autorizados sempre que necessário.

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	CRIPTOGRAFIA ASSIMÉTRICA UTILIZADA PARA GARANTIR O PRINCÍPIO DA AUTENTICIDADE
	
O emissor criptografa o texto original com a chave pública do receptor de forma que somente ele	O emissor criptografa o texto original com sua chave privada de forma que o receptor possa descriptografá-lo com a chave pública do emissor.

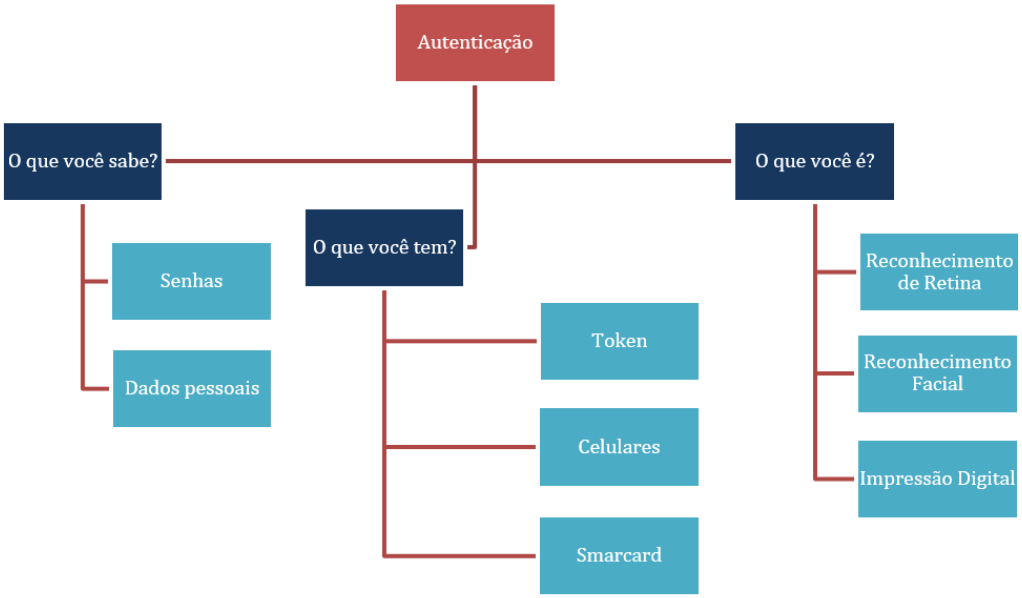
consiga descriptografá-lo com sua chave privada para visualizar o texto original.	

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



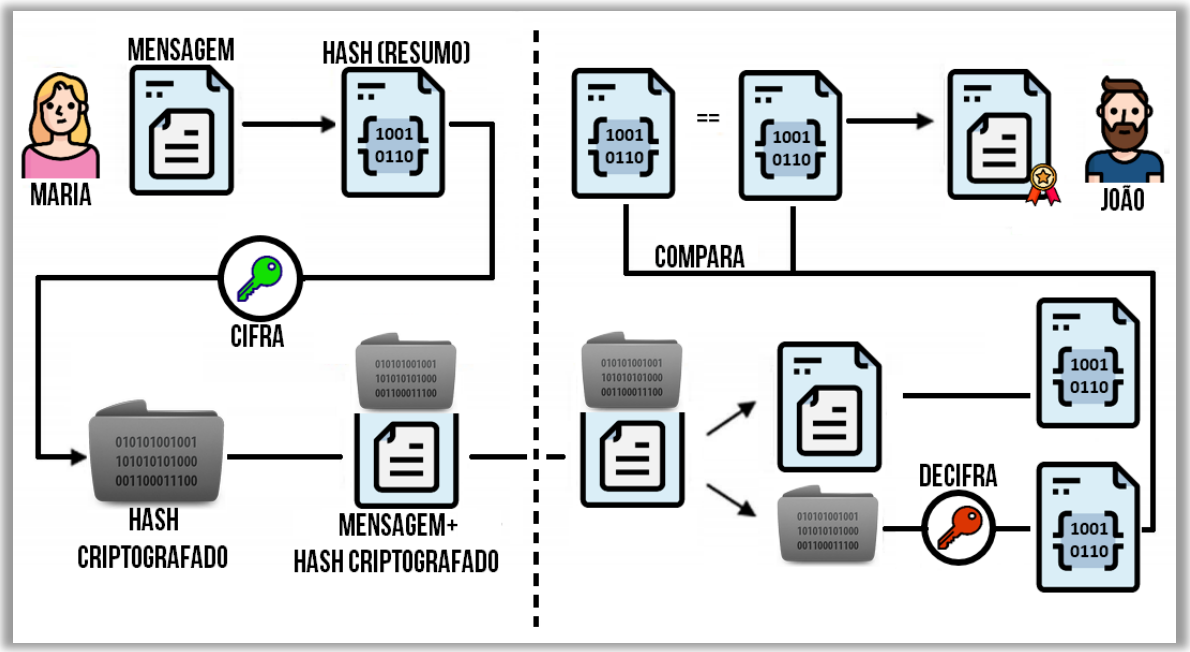
MÉTODOS DE AUTENTICAÇÃO	DESCRIÇÃO
O QUE VOCÊ SABE?	Trata-se da autenticação baseada no conhecimento de algo que somente você sabe, tais como: senhas, frases secretas, dados pessoais aleatórios, entre outros.
O QUE VOCÊ É?	Trata-se da autenticação baseada no conhecimento de algo que você é, como seus 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 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.

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 os pontos com maior probabilidade de cobrança no contexto de **Segurança da Informação**. Estas são as minhas apostas:

1. Eu acredito que pode aparecer uma questão sobre os três princípios fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade, que asseguram a proteção dos dados. Isso é um clássico de provas de concurso!

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.

2. Vale a pena revisar os conceitos de autenticidade (garantir que o usuário é quem alega ser) e irrefutabilidade (impossibilidade de negar a autoria de uma ação).

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.

3. Eu imagino que pode haver uma questão sobre o uso de criptografia simétrica, que utiliza uma única chave para cifrar e decifrar os dados, sendo mais rápida, mas menos segura se a chave for comprometida.

4. Eu aposto em questões sobre criptografia assimétrica, que utiliza um par de chaves (pública e privada), garantindo a confidencialidade e autenticidade.

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.

5. Eu revisaria o conceito de algoritmos de criptografia, como AES, RSA, e MD5, destacando suas utilizações e segurança.

6. Pode haver uma pergunta sobre os métodos de autenticação que incluem o que o usuário sabe (senhas), o que possui (tokens) e o que é (biometria).

7. Eu aposto em questões sobre assinatura digital, que garante a autenticidade e integridade das informações através do uso de hash e criptografia.

8. Vale a pena revisar como certificados digitais são utilizados para garantir segurança nas transações online, verificando a identidade do emissor.

9. Eu acredito que pode haver uma questão sobre a diferença entre criptografia simétrica e assimétrica e suas utilizações em garantir a confidencialidade e autenticidade da comunicação.

10. Eu também aposto que a classificação dos certificados digitais (A1, A2, A3, A4) pode ser cobrada, com detalhes sobre geração de chaves, validade e armazenamento.

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

QUESTÕES ESTRATÉGICAS

1. (CONSULPLAN / TJ-MG – 2017) Segurança da informação é o mecanismo de proteção de um conjunto de informações com o objetivo de preservar o valor que elas possuem para uma pessoa ou organização. Está correto o que se afirma sobre princípios básicos de segurança da informação, EXCETO:

a) Disponibilidade garante que a informação esteja sempre disponível.
b) Integridade garante a exatidão da informação.
c) Confidencialidade garante que a informação seja acessada somente por pessoas autorizadas.
d) Não repúdio garante a informação é autêntica e que a pessoa recebeu a informação.

Comentários:

(a) Correto. Disponibilidade assegura que as informações estejam sempre acessíveis para os usuários autorizados quando necessário;

(b) Correto. Integridade visa a exatidão e a consistência das informações, protegendo-as contra alterações não autorizadas;

(c) Correto. Confidencialidade limita o acesso às informações apenas a pessoas autorizadas, protegendo-as contra acessos não permitidos;

(d) Errado. Não repúdio é o princípio que garante que uma ação ou transação realizada por uma pessoa não possa ser negada posteriormente, mas não garante a autenticidade da informação em si ou que ela foi recebida.

Gabarito: Letra D

QUESTÕES ESTRATÉGICAS

1. (IADES / BRB – 2022) As propriedades que garantem que o dado é correto e consistente com o estado ou informação pretendida, e que asseguram os limites de quem pode obtê-la são definidas respectivamente, como

a) integridade e confidencialidade.
b) integridade e disponibilidade.
c) disponibilidade e integridade.
d) consistência e autenticidade.
e) Consistência e confidencialidade.

Comentários:

(a) Correto. A integridade garante que os dados sejam corretos e consistentes com a informação pretendida, sem alterações não autorizadas. A confidencialidade assegura que o acesso aos dados seja restrito apenas a pessoas ou sistemas autorizados;

(b) Errado. A disponibilidade está relacionada com o acesso contínuo e garantido aos dados, não com a restrição de quem pode obtê-los;

(c) Errado. A integridade está relacionada com a correção e consistência dos dados, mas a disponibilidade trata da acessibilidade dos dados, não da sua proteção contra acessos não autorizados;

(d) Errado. Consistência e autenticidade são conceitos diferentes dos abordados na questão. Consistência refere-se à uniformidade dos dados, enquanto autenticidade garante a identidade de quem acessa;

(e) Errado. Consistência refere-se à uniformidade dos dados, mas confidencialidade, que está correta, é o termo relacionado à proteção dos dados contra acessos não autorizados.

Gabarito: Letra A

2. (FUNDATEC / IPE SAÚDE – 2022) A política de segurança da informação estabelece como as informações são acessadas, tendo como objetivo manter os três pilares da segurança da informação, que são:

a) Confidencialidade, velocidade e armazenamento.
b) Confidencialidade, integridade e disponibilidade.
c) Conectividade, confiabilidade e disponibilidade.
d) Velocidade, controle de acesso e atualização da informação.
e) Velocidade, confiabilidade e controle de acesso.

Comentários:

(a) Errado. Velocidade e armazenamento não são pilares da segurança da informação. Os pilares são confidencialidade, integridade e disponibilidade;

(b) Correto. Os três pilares da segurança da informação são confidencialidade (proteção contra acessos não autorizados), integridade (garantia de dados corretos e não alterados) e disponibilidade (acesso contínuo às informações);

(c) Errado. Conectividade e confiabilidade não fazem parte dos pilares da segurança da informação. O correto é confidencialidade, integridade e disponibilidade;

(d) Errado. Velocidade e atualização da informação não são pilares da segurança da informação. Controle de acesso está relacionado à confidencialidade, mas não define os pilares por completo;

(e) Errado. Confiabilidade e controle de acesso são aspectos importantes, mas não são os pilares centrais da segurança da informação.

Gabarito: Letra B

3. (FADESP / SEFA-PA – 2022) Na assinatura digital são utilizadas:

a) a chave pública do receptor e a chave privada do receptor
b) a chave pública do emissor e a chave privada do emissor.
c) a chave pública do receptor e a chave privada do emissor
d) a chave privada do receptor e a chave pública do emissor.
e) as chaves secretas do emissor.

Comentários:

(a) Errado. A assinatura digital utiliza a chave privada do emissor, não a chave do receptor;

(b) Correto. Na assinatura digital, o emissor assina a mensagem com sua chave privada, e o receptor pode verificar a autenticidade com a chave pública do emissor;

(c) Errado. A chave privada do emissor é usada para assinar a mensagem, e a chave pública do emissor é usada para verificar a assinatura, não a chave pública do receptor;

(d) Errado. A chave privada do receptor não é utilizada no processo de assinatura digital;

(e) Errado. Não se utilizam chaves secretas na assinatura digital, e sim a chave pública e a chave privada do emissor.

Gabarito: Letra B

4. (FADESP / SEFA-PA – 2022) A forma de realizar assinatura digital baseada em logaritmos discretos, em que o trabalho principal para a geração de assinatura que não depende da mensagem pode ser feito durante o tempo ocioso do processador, e a parte da

geração da assinatura que depende da mensagem exige multiplicar um inteiro de 2n bits por um inteiro de n bits, é conhecida como:

a) SCHNORR.
b) ELGAMAL.
c) DSA.
d) Curva Elíptica.
e) RSA-PSS.

Comentários:

(a) Correto. O esquema de assinatura Schnorr é baseado em logaritmos discretos e permite que parte da geração da assinatura (independente da mensagem) seja feita antecipadamente, otimizando o processo durante o tempo ocioso do processador;

(b) Errado. O ElGamal também é baseado em logaritmos discretos, mas não possui a mesma característica de otimização da geração da assinatura durante o tempo ocioso;

(c) Errado. O DSA (Digital Signature Algorithm) é baseado em logaritmos discretos, mas não possui a otimização de pré-cálculo da assinatura como o Schnorr;

(d) Errado. A assinatura com curvas elípticas é eficiente, mas não segue o mesmo princípio descrito na questão;

(e) Errado. RSA-PSS é um esquema de assinatura baseado em RSA, que não utiliza logaritmos discretos.

Gabarito: Letra A

5. (FADESP / SEFA-PA – 2022) A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como:

a) Electronic Codebook (EBC).
b) Cipher Block Chaining (CBC).
c) Cipher Feedback (CFB).
d) Ouput Feedback (OFB).
e) Counter (CTR).

Comentários:

Questão de nível completamente absurdo! É o tipo de questão que eu sugiro simplesmente chutar e ser feliz. Esse nível de aprofundamento não é cobrado nem para analistas de sistemas – talvez para cargos específicos de segurança da informação. De todo modo, existem cinco modos de operação de cifra de bloco: ECB, CBC, CFB, OFB e CTR. A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como CBC (Cipher Block Chaining).

Gabarito: Letra B

6. (FADESP / SEFA-PA – 2022) A forma de controle de acesso lógico, em que o dono dos dados e os usuários individuais são capazes de definir, ao seu critério, qual acesso será permitido aos seus dados independentemente da política, é definida como um controle de acesso:

a) mandatório
b) baseado na função.
c) discricionário
d) baseado em reivindicações
e) seletista

Comentários:

(a) Errado. O controle de acesso mandatório (MAC) é restritivo e definido por uma política central, onde os usuários não têm controle sobre as permissões de acesso;

(b) Errado. O controle de acesso baseado em função (RBAC) define permissões com base em funções atribuídas a usuários, não permitindo que os usuários individuais decidam quem acessa os dados;

(c) Correto. O controle de acesso discricionário (DAC) permite que o proprietário dos dados defina quem pode acessá-los, concedendo permissões conforme seu critério;

(d) Errado. O controle de acesso baseado em reivindicações (Claim-Based) usa atributos ou declarações do usuário para decidir o acesso, mas não é controlado pelo proprietário dos dados;

(e) Errado. "Seletista" não é um termo utilizado para descrever um modelo de controle de acesso.

Gabarito: Letra C

7. (FADESP / SEFA-PA – 2022) Considerando os passos utilizados pelo algoritmo de assinatura digital RSA, julgue verdadeira (V) ou falsa (F) cada uma das afirmativas a seguir.

I. A mensagem a ser assinada é inserida em uma função de hash que produz um código hash seguro de tamanho variado.

II. O código hash gerado é encriptado usando a chave privada do emissor para formar a assinatura digital.

III. O destinatário recebe a mensagem e produz um código hash. Ele também decripta a mensagem usando a chave pública do emissor. Se o código hash calculado coincidir com a assinatura decriptada, ela é aceita como válida.

A sequência correta é:

a) I - F; II - F; III - F.
b) I - F; II - F; III - V.
c) I - V; II - V; III - F.
d) I - F; II - V; III - V.
e) I - V; II - V; III - V.

Comentários:

I. Falso. O código hash produzido por uma função de hash segura tem tamanho fixo, não variado, independentemente do tamanho da mensagem de entrada;

II. Verdadeiro. No RSA, o código hash gerado a partir da mensagem é encriptado usando a chave privada do emissor para criar a assinatura digital;

III. Verdadeiro. O destinatário gera o código hash da mensagem recebida e decripta a assinatura usando a chave pública do emissor. Se o código hash calculado coincidir com o decriptado, a assinatura é válida.

Gabarito: Letra D

Figura 1 – Notícia da Agência Brasil

8. (FUNDATEC / ISS-Porto Alegre – 2022) A Figura 1 apresenta notícia a respeito da 2ª fase da Operação Spoofing, na qual os policiais federais cumpriram dois mandados de prisão temporária e outros de busca e apreensão em endereços de pessoas ligadas à organização criminosa investigada. Os criminosos invadiram os celulares de autoridades, tendo acessado e tomado conhecimento de informações, muito delas sensíveis, sem autorização dos respectivos proprietários. Nesse caso, é correto afirmar que o seguinte princípio básico da Segurança da Informação foi violado:

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

Comentários:

(a) Correto. O princípio da confidencialidade (sigilo) foi violado, pois os criminosos acessaram informações sensíveis sem autorização dos proprietários, comprometendo o acesso restrito aos dados;

(b) Errado. A integridade refere-se à precisão e consistência dos dados, o que não foi o principal aspecto comprometido neste caso;

(c) Errado. Não repúdio refere-se à incapacidade de negar uma ação, o que não está relacionado ao acesso não autorizado de informações;

(d) Errado. A autenticidade está relacionada à verificação da identidade dos envolvidos, que não é o foco da violação descrita;

(e) Errado. A disponibilidade refere-se à garantia de acesso contínuo às informações, que não foi o princípio afetado neste caso.

Gabarito: Letra A

Figura 2 – Venda de certificados digitais

9. (FUNDATEC / ISS-Porto Alegre – 2022) Um certificado digital "e-CNPJ", do tipo "A1", após devidamente emitido, pode ser armazenado:

I. Diretamente no computador do titular do certificado.
II. Em um token.
III. Em um cartão smart card.

Quais estão corretas?

a) Apenas I.
b) Apenas III.
c) Apenas I e II.

d) Apenas II e III.
e) I, II e III.

Comentários:

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

(I) Correto, ele pode ser armazenado no disco rígido do computador do titular do certificado; (II) Errado, não pode ser armazenado com um token; (III) Errado, não pode ser armazenado em um smartcard.

Gabarito: Letra A

10. (FUNDATEC / DPE SC – 2018) A certificação digital é utilizada para garantir, de forma eletrônica, a autoria de determinado documento, como por exemplo, o perito responsável por determinado laudo. Um dos componentes da certificação digital é a utilização de criptografia. Diante do exposto, é correto afirmar que, para verificar a assinatura digital de um perito em relação a um laudo pericial emitido por ele, a primeira etapa é a aplicação:

a) Da chave criptográfica privada do perito.
b) Da chave criptográfica pública do perito.
c) Da chave criptográfica simétrica de quem quer validar.
d) De um algoritmo de hash simétrico de tamanho qualquer.
e) De um algoritmo de hash assimétrico de tamanho mínimo de 128 bits.

Comentários:

(a) Errado. Para verificar a assinatura digital do perito, eu não posso utilizar sua chave privada porque somente ele tem acesso a ela;

(b) Correto. Para verificar a assinatura digital do perito, utiliza-se a chave pública dele correspondente à chave privada, de modo que seja possível identificá-lo inequivocamente;

(c) Errado. Não se utiliza criptografia simétrica na certificação digital;

(d) Errado. Algoritmo de Hash é apenas o algoritmo utilizado no processo de assinatura digital e não é capaz de verificar a assinatura do perito – e não existe algoritmo de hash simétrico;

(e) Errado. Algoritmo de Hash é apenas o algoritmo utilizado no processo de assinatura digital e não é capaz de verificar a assinatura do perito – e não existe algoritmo de hash assimétrico;

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 descriptografia.

19. O que é criptografia?

Criptografia é a técnica de tornar uma mensagem ininteligível para qualquer pessoa que não tenha a chave para descriptografá-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. (CONSULPLAN / TJ-MG – 2017) Segurança da informação é o mecanismo de proteção de um conjunto de informações com o objetivo de preservar o valor que elas possuem para uma pessoa ou organização. Está correto o que se afirma sobre princípios básicos de segurança da informação, EXCETO:

a) Disponibilidade garante que a informação esteja sempre disponível.
b) Integridade garante a exatidão da informação.
c) Confidencialidade garante que a informação seja acessada somente por pessoas autorizadas.
d) Não repúdio garante a informação é autêntica e que a pessoa recebeu a informação.

LISTA DE QUESTÕES ESTRATÉGICAS

1. **(IADES / BRB – 2022) As propriedades que garantem que o dado é correto e consistente com o estado ou informação pretendida, e que asseguram os limites de quem pode obtê-la são definidas respectivamente, como**

a) integridade e confidencialidade.
b) integridade e disponibilidade.
c) disponibilidade e integridade.
d) consistência e autenticidade.
e) Consistência e confidencialidade.

2. **(FUNDATEC / IPE SAÚDE – 2022) A política de segurança da informação estabelece como as informações são acessadas, tendo como objetivo manter os três pilares da segurança da informação, que são:**

a) Confidencialidade, velocidade e armazenamento.
b) Confidencialidade, integridade e disponibilidade.
c) Conectividade, confiabilidade e disponibilidade.
d) Velocidade, controle de acesso e atualização da informação.
e) Velocidade, confiabilidade e controle de acesso.

3. **(FADESP / SEFA-PA – 2022) Na assinatura digital são utilizadas:**

a) a chave pública do receptor e a chave privada do receptor
b) a chave pública do emissor e a chave privada do emissor.
c) a chave pública do receptor e a chave privada do emissor
d) a chave privada do receptor e a chave pública do emissor.
e) as chaves secretas do emissor.

4. **(FADESP / SEFA-PA – 2022) A forma de realizar assinatura digital baseada em logaritmos discretos, em que o trabalho principal para a geração de assinatura que não depende da mensagem pode ser feito durante o tempo ocioso do processador, e a parte da geração da assinatura que depende da mensagem exige multiplicar um inteiro de 2n bits por um inteiro de n bits, é conhecida como:**

a) SCHNORR.
b) ELGAMAL.
c) DSA.
d) Curva Elíptica.
e) RSA-PSS.

5. **(FADESP / SEFA-PA – 2022) A característica do modo de operação de cifra de bloco em que a entrada do algoritmo de encriptação é o XOR dos próximos 64 bits de texto claro e os 64 bits anteriores de texto cifrado é conhecida como:**

a) Electronic Codebook (EBC).
b) Cipher Block Chaining (CBC).
c) Cipher Feedback (CFB).
d) Ouput Feedback (OFB).
e) Counter (CTR).

6. (FADESP / SEFA-PA – 2022) A forma de controle de acesso lógico, em que o dono dos dados e os usuários individuais são capazes de definir, ao seu critério, qual acesso será permitido aos seus dados independentemente da política, é definida como um controle de acesso:

a) mandatório
b) baseado na função.
c) discricionário
d) baseado em reivindicações
e) seletista

7. (FADESP / SEFA-PA – 2022) Considerando os passos utilizados pelo algoritmo de assinatura digital RSA, julgue verdadeira (V) ou falsa (F) cada uma das afirmativas a seguir.

I. A mensagem a ser assinada é inserida em uma função de hash que produz um código hash seguro de tamanho variado.

II. O código hash gerado é encriptado usando a chave privada do emissor para formar a assinatura digital.

III. O destinatário recebe a mensagem e produz um código hash. Ele também decripta a mensagem usando a chave pública do emissor. Se o código hash calculado coincidir com a assinatura decriptada, ela é aceita como válida.

A sequência correta é:

a) I - F; II - F; III - F.
b) I - F; II - F; III - V.
c) I - V; II - V; III - F.
d) I - F; II - V; III - V.
e) I - V; II - V; III - V.

Figura 1 – Notícia da Agência Brasil

8. (FUNDATEC / ISS-Porto Alegre – 2022) A Figura 1 apresenta notícia a respeito da 2ª fase da Operação Spoofing, na qual os policiais federais cumpriram dois mandados de prisão temporária e outros de busca e apreensão em endereços de pessoas ligadas à organização criminosa investigada. Os criminosos invadiram os celulares de autoridades, tendo acessado e tomado conhecimento de informações, muito delas sensíveis, sem autorização dos respectivos proprietários. Nesse caso, é correto afirmar que o seguinte princípio básico da Segurança da Informação foi violado:

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

Figura 2 – Venda de certificados digitais

9. (FUNDATEC / ISS-Porto Alegre – 2022) Um certificado digital "e-CNPJ", do tipo "A1", após devidamente emitido, pode ser armazenado:

I. Diretamente no computador do titular do certificado.
II. Em um token.
III. Em um cartão smart card.

Quais estão corretas?

a) Apenas I.
b) Apenas III.
c) Apenas I e II.
d) Apenas II e III.
e) I, II e III.

10. (FUNDATEC / DPE SC – 2018) A certificação digital é utilizada para garantir, de forma eletrônica, a autoria de determinado documento, como por exemplo, o perito responsável por determinado laudo. Um dos componentes da certificação digital é a utilização de criptografia. Diante do exposto, é correto afirmar que, para verificar a assinatura digital de um perito em relação a um laudo pericial emitido por ele, a primeira etapa é a aplicação:

a) Da chave criptográfica privada do perito.
b) Da chave criptográfica pública do perito.
c) Da chave criptográfica simétrica de quem quer validar.
d) De um algoritmo de hash simétrico de tamanho qualquer.
e) De um algoritmo de hash assimétrico de tamanho mínimo de 128 bits.

GABARITO

1. LETRA D

GABARITO

1. LETRA D
2. LETRA A
3. LETRA A
4. LETRA A
5. LETRA A
6. LETRA A
7. LETRA E
8. LETRA D
9. LETRA E
10. LETRA C

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.