Estratégia Concursos

Aula 00

CVM (Analista TI - Infraestrutura e Segurança - Perfil 9) Passo Estratégico de Conhecimentos Específicos

Autor:
Fernando Pedrosa Lopes

24 de Outubro de 2024

SEGURANÇA DA INFORMAÇÃO

Sumário

CONTEÚDO

Segurança da Informação. Conceitos Básicos. Terminologia. Princípios. Criptologia. Assinatura Digital. Certificado Digital.

ANÁLISE ESTATÍSTICA

Inicialmente, convém destacar o percentual de incidência do assunto, dentro da disciplina **Segurança da Informação** em concursos/cargos similares. Quanto maior o percentual de cobrança de um dado assunto, maior sua importância.

Obs.: *um mesmo assunto pode ser classificado em mais de um tópico devido à multidisciplinaridade de conteúdo*.

Assunto	Relevância na disciplina em concursos similares
Criptografia	**11.4 %**
Análise de Vulnerabilidade e Gestão de Riscos	**11.4 %**
Plano de Continuidade de Negócios	**8.6 %**
Norma 27005	**8.6 %**
Backup em Segurança da Informação	**5.7 %**
Conceitos Básicos em Segurança da Informação	**5.7 %**
Políticas de Segurança de Informação	**5.7 %**
Norma ISO 27001	**5.7 %**
Certificação Digital em Segurança da Informação	**5.7 %**
Ataques e ameaças	**5.7 %**
Planos de contingência	**2.9 %**
Sistemas de Prevenção-Detecção de Intrusão	**2.9 %**
Segurança de sistemas de informação	**2.9 %**
Infraestrutura de Chaves Públicas (PKI)	**2.9 %**
Controles de segurança	**2.9 %**
Assinatura Digital	**2.9 %**
Malware	**2.9 %**

GLOSSÁRIO DE TERMOS

Faremos uma lista de termos que são relevantes ao entendimento do assunto desta aula. Caso tenha alguma dúvida durante a leitura, esta seção pode lhe ajudar a esclarecer.

Segurança da informação: Refere-se à prática de prevenir o acesso não autorizado, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição de informações.

Controle físico: São medidas tomadas para proteger os ativos de hardware de uma organização contra ameaças físicas. Isso pode incluir medidas como fechaduras, sistemas de alarme, câmeras de segurança, entre outros.

Controle técnico: São as medidas, geralmente implementadas por meio de software, usadas para proteger e controlar o acesso a informações em uma rede. Exemplos de controles técnicos incluem firewalls, criptografia, software antivírus, etc.

Controle administrativo: São políticas e procedimentos destinados a gerenciar o comportamento das pessoas em relação à segurança da informação. Isso pode incluir políticas de segurança, treinamento de conscientização, planos de continuidade de negócios, etc.

Confidencialidade: É a garantia de que a informação é acessível apenas para aqueles autorizados a terem acesso.

Integridade: Garante que a informação é precisa e completa e que não foi alterada de maneira não autorizada.

Disponibilidade: Garante que a informação e os recursos relacionados estão acessíveis quando necessário.

Autenticidade: Garante a veracidade da origem da informação.

Irretratabilidade (não-repúdio): Garante que uma entidade não pode negar ter participado de uma transação ou comunicação.

Criptologia: É o estudo da criptografia e da criptoanálise.

Criptografia: É a prática e o estudo de técnicas para comunicação segura na presença de adversários.

Criptoanálise: É o estudo das técnicas usadas para quebrar a criptografia.

Esteganografia: É a prática de esconder informações dentro de outra informação.

Criptografia simétrica: É um método de criptografia onde a mesma chave é usada para criptografar e descriptografar a informação.

Criptografia assimétrica: É um método de criptografia onde chaves diferentes são usadas para criptografar e descriptografar a informação.

DES, 3DES, AES, IDEA, RC4, Blowfish: São diferentes algoritmos usados para criptografia simétrica.

Cifra de César: É uma das técnicas de criptografia mais simples e mais amplamente conhecidas.

RSA, DSA, Diffie-Hellman: São diferentes algoritmos usados para criptografia assimétrica.

Autenticação: É o processo de verificar a identidade de uma pessoa ou sistema.

MFA (Multi-Factor Authentication): É um método de autenticação que requer mais de um método de verificação de identidade.

Assinatura Digital: É um método matemático usado para validar a autenticidade e a integridade de uma mensagem, software ou documento digital.

Hash: É uma função que converte uma entrada de letras e números em uma saída de um comprimento fixo.

Certificado Digital: É um documento eletrônico que usa uma assinatura digital para vincular uma identidade pública com uma identidade física ou jurídica.

ICP (Infraestrutura de Chaves Públicas): É um conjunto de procedimentos, métodos, e sistemas usados para emitir certificados digitais.

AC Raiz: É a Autoridade Certificadora de nível mais alto em uma hierarquia de ACs.

AC (Autoridade Certificadora): É uma entidade que emite certificados digitais.

AR (Autoridade de Registro): É uma entidade que verifica as informações do requerente de um certificado digital antes que o certificado seja emitido pela AC.

Categoria A: Refere-se a certificados digitais usados para assinatura.

Categoria S: Refere-se a certificados digitais usados para criptografia.

ROTEIRO DE REVISÃO

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.

Introdução e Conceitos Básicos

Segurança da Informação refere-se à prática de **prevenir o acesso, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição não autorizada de informações**. Isso é especialmente relevante no mundo dos negócios, onde a informação é um ativo valioso que precisa ser protegido. As organizações devem garantir que as informações sejam protegidas contra vários tipos de ameaças para garantir a continuidade dos negócios, minimizar o risco de negócios e maximizar o retorno sobre investimentos e oportunidades de negócios.

Um exemplo prático de porque a Segurança da Informação é importante pode ser encontrado na indústria financeira. Os bancos mantêm dados extremamente sensíveis sobre os seus clientes, incluindo informações de conta bancária, números de segurança social e históricos de transações financeiras. Se esses dados caírem em mãos erradas, devido a um ataque cibernético ou a uma violação de segurança, as consequências podem ser devastadoras. Clientes podem sofrer perdas financeiras substanciais e a reputação do banco pode ser irrevogavelmente danificada.

Outro exemplo pode ser visto no setor de saúde, onde as informações dos pacientes são altamente sensíveis e devem ser mantidas em sigilo. Uma violação de segurança que expõe os dados de saúde de um paciente pode levar a violações da privacidade, danos à reputação e até ações legais.

Em um nível pessoal, todos nós confiamos em um grau de segurança da informação em nossa vida diária. Quando fazemos compras online, esperamos que nossos dados de cartão de crédito sejam protegidos. Quando usamos as redes sociais, contamos com a segurança de nossos dados para proteger nossa privacidade.

Veja mais algumas definições de Segurança da Informação que já foram cobradas em prova:

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.

Terminologia

Ativo: No contexto da segurança da informação, um ativo se refere a qualquer dado, dispositivo ou outro componente do ambiente que é valioso para a organização. Isso inclui informações como dados de clientes, propriedade intelectual, infraestrutura de TI e até mesmo a reputação de uma empresa.

Informação: É o ativo mais valioso que uma organização possui. Pode assumir muitas formas, como dados eletrônicos, documentos impressos, conhecimento dos funcionários, etc. A segurança da informação visa proteger esses ativos de informações.

Agente: Em segurança da informação, um agente é a entidade que causa uma ameaça. Os agentes podem ser pessoas, sistemas ou processos que podem causar danos aos ativos de informação.

Vulnerabilidade: Uma vulnerabilidade é uma fraqueza ou falha em um sistema que pode ser explorada para causar danos ou ganhar acesso não autorizado. As vulnerabilidades podem ser causadas por uma variedade de fatores, incluindo falhas de software, configurações de sistema inseguras, e falta de controles de segurança adequados.

Ameaça: Uma ameaça é qualquer coisa que tenha o potencial de causar danos a um ativo de informação. As ameaças podem ser intencionais (como ataques cibernéticos) ou acidentais (como um desastre natural ou erro humano).

Ataque: Um ataque é um ato que explora uma vulnerabilidade para prejudicar um ativo de informação. Isso pode incluir atividades como hacking, phishing, DDoS e outras formas de atividades maliciosas.

Evento: Em segurança da informação, um evento é qualquer observação notável em um sistema ou rede. Nem todos os eventos são indicativos de um problema; eles podem ser tanto normais quanto anormais.

Incidente: Um incidente de segurança é um evento que viola a política de segurança de uma organização. Isso pode incluir acesso não autorizado a sistemas ou dados, introdução de malware, ou interrupção de serviços.

Impacto: O impacto é a consequência ou o efeito de um incidente de segurança sobre a organização. Isso pode incluir perda financeira, danos à reputação, interrupção dos negócios, e perda ou corrupção de dados.

Risco: O risco é a probabilidade de uma ameaça explorar uma vulnerabilidade e o impacto resultante disso na organização. A gestão de risco é um componente essencial da segurança da informação.

Política de Segurança: Uma política de segurança é um documento que estabelece as regras para proteger os ativos de informação de uma organização. Ela define as expectativas da organização em relação à segurança e fornece um plano de ação para lidar com incidentes de segurança.

Controles de Segurança

Controles de segurança são medidas de proteção ou salvaguardas implementadas para **mitigar os riscos à segurança das informações de uma organização**. Eles ajudam a reduzir a probabilidade de uma ameaça conseguir explorar uma vulnerabilidade, ou limitam o impacto caso uma ameaça seja bem-sucedida. Os controles de segurança são uma parte vital de qualquer estratégia de segurança da informação e são essenciais para a proteção de ativos valiosos.

Existem três categorias principais de controles de segurança:

1. Controles Físicos: Esses controles estão relacionados à segurança do ambiente físico. Isso pode incluir coisas como trancas e chaves, cercas de segurança, sistemas de CCTV, iluminação adequada, controle de acesso biométrico, e muito mais. São projetados para prevenir acessos físicos não autorizados e proteger contra danos físicos (como incêndios ou inundações).

2. Controles Técnicos: Envolvem o uso de tecnologia para proteger as informações e os sistemas de informação. Eles incluem firewalls, software antivírus, criptografia, autenticação de dois fatores, e mais. Estes são muitas vezes a primeira linha de defesa contra ameaças cibernéticas.

3. Controles Administrativos: Referem-se a políticas e procedimentos que uma organização implementa para gerenciar e controlar as operações diárias de segurança da informação. Isso pode incluir políticas de segurança, treinamento de conscientização de segurança, planos de resposta a incidentes, e procedimentos de backup e recuperação.

Princípios Fundamentais

Confidencialidade

Confidencialidade é um dos pilares fundamentais da segurança da informação. Trata-se de **garantir que o acesso às informações seja restrito apenas àqueles que têm permissão para visualizá-las**. Se um indivíduo ou sistema puder ver, modificar ou divulgar informações sem autorização, a confidencialidade dessas informações foi comprometida.

Um exemplo comum de confidencialidade é a proteção das informações de saúde de um paciente em um hospital. Essas informações são sensíveis e confidenciais, e apenas os médicos e enfermeiros que estão cuidando do paciente devem ter acesso a elas.

Outro exemplo poderia ser uma empresa que mantém a confidencialidade dos dados de seus clientes, tais como informações de cartão de crédito, endereços, números de telefone e outros detalhes pessoais. A empresa deve tomar medidas para garantir que apenas os funcionários autorizados tenham acesso a essas informações e que elas sejam protegidas contra acesso externo.

Existem várias estratégias e ferramentas para ajudar a garantir a confidencialidade das informações. Algumas das mais comuns incluem:

1. Controle de Acesso: Apenas indivíduos autorizados devem ter acesso a informações confidenciais. O controle de acesso pode ser físico (como trancas nas portas) ou lógico (como nomes de usuário e senhas).

2. Criptografia: A criptografia é uma técnica para proteger a confidencialidade das informações. Ela transforma informações legíveis (plaintext) em um código ininteligível (ciphertext) que só pode ser revertido com uma chave de descriptografia.

3. Treinamento de Segurança: Ensinar aos funcionários sobre a importância da segurança da informação e as melhores práticas pode ajudar a prevenir violações de confidencialidade. Isso pode incluir treinamento sobre como identificar e evitar phishing e outros ataques cibernéticos.

4. Políticas e Procedimentos: Implementar políticas claras de segurança da informação pode ajudar a garantir a confidencialidade. Isso pode incluir políticas sobre o uso de senhas fortes, bloqueio de computadores quando não estiverem em uso, e restrições ao compartilhamento de informações sensíveis.

Integridade

Integridade é outro pilar fundamental da segurança da informação. O princípio da integridade refere-se à **garantia de que as informações sejam mantidas precisas e completas, e que não sejam alteradas de forma inadequada ou não autorizada**. Este princípio se aplica não apenas aos dados em si, mas também aos sistemas que processam e armazenam esses dados.

Um exemplo clássico de integridade pode ser visto no setor bancário. É de suma importância que os registros das transações e dos saldos das contas dos clientes sejam mantidos com total precisão. Se um hacker alterar os registros de transações ou os salários dos clientes, isso seria uma violação da integridade dos dados.

Outro exemplo é um hospital que mantém registros médicos de seus pacientes. Se os dados desses registros médicos fossem alterados, isso poderia resultar em diagnósticos ou tratamentos incorretos, o que pode colocar a vida dos pacientes em risco.

Estratégias e ferramentas que podem ser usadas para garantir a integridade:

1. Controle de Acesso: Assim como na confidencialidade, o controle de acesso é essencial para a integridade. Limitar quem pode alterar informações pode ajudar a prevenir alterações não autorizadas.

2. Backups e Recuperação: Manter cópias de backup dos dados e dos sistemas ajuda a garantir que, se os dados forem alterados ou perdidos, eles possam ser restaurados para um estado anterior.

3. Verificação de Integridade dos Dados: Ferramentas como funções de hash e somas de verificação podem ser usadas para garantir a integridade dos dados. Essas ferramentas geram um valor único para um conjunto de dados, que pode ser usado para verificar se os dados foram alterados.

4. Assinaturas Digitais: Assinaturas digitais podem ser usadas para verificar a integridade dos dados, garantindo que os dados não foram alterados desde que a assinatura foi aplicada.

5. Atualizações e Patches: Manter os sistemas e softwares atualizados com as últimas correções de segurança ajuda a proteger contra ameaças que poderiam comprometer a integridade dos dados.

Disponibilidade

- O princípio da disponibilidade, o terceiro pilar da segurança da informação, trata de garantir que as **informações e os sistemas estejam sempre acessíveis para aqueles que precisam delas, quando precisam**. Se um sistema estiver fora do ar ou se um arquivo estiver indisponível quando necessário, então a disponibilidade dessas informações foi comprometida.

Um exemplo de disponibilidade pode ser um site de comércio eletrônico que deve estar disponível 24 horas por dia, 7 dias por semana, para permitir que os clientes façam compras a qualquer momento. Se o site estiver fora do ar, isso pode resultar em perda de vendas e danos à reputação da empresa.

Outro exemplo poderia ser um sistema de registros médicos eletrônicos em um hospital. Se o sistema estiver indisponível, os profissionais de saúde podem não ser capazes de acessar as informações vitais dos pacientes, o que pode resultar em atrasos no tratamento ou mesmo em erros médicos.

Estratégias e ferramentas que podem ser usadas para garantir a disponibilidade:

1. Redundância de Dados: A redundância de dados envolve manter múltiplas cópias dos dados em diferentes locais ou sistemas. Isso pode ajudar a garantir que, se um sistema falhar, haverá outra cópia dos dados disponíveis.

2. Balanceamento de Carga: O balanceamento de carga envolve distribuir o tráfego de rede ou as solicitações de processamento entre vários servidores, para evitar que qualquer servidor individual seja sobrecarregado.

3. Recuperação de Desastres e Continuidade dos Negócios: Ter um plano de recuperação de desastres e continuidade dos negócios pode ajudar a garantir a disponibilidade em caso de um evento significativo, como uma falha de hardware, um desastre natural ou um ataque cibernético.

4. Manutenção Regular do Sistema: A manutenção regular dos sistemas, incluindo atualizações e patches, pode ajudar a prevenir falhas que podem levar à indisponibilidade.

5. Prevenção e Mitigação de DoS (Denial of Service): As técnicas para prevenir e mitigar os ataques de negação de serviço (DoS) podem ajudar a proteger contra ameaças que visam tornar os sistemas indisponíveis.

Outros Princípios

Além do pilar clássico CID - Confidencialidade, Integridade e Disponibilidade - algumas questões de prova também abordam os princípios derivados de **Autenticidade e Irretratabilidade**.

Autenticidade

A autenticidade é outro princípio importante na segurança da informação. Esse princípio **garante que os usuários, sistemas ou entidades sejam quem eles afirmam ser**. A autenticidade é um requisito crucial para estabelecer a confiança em um sistema de segurança, pois ela valida a identidade dos usuários e garante que as informações venham de uma fonte confiável.

Um exemplo clássico de autenticidade é o processo de login em um sistema ou plataforma online. Quando um usuário insere seu nome de usuário e senha, o sistema verifica essas credenciais para garantir que a pessoa é realmente quem afirma ser.

Outro exemplo é a assinatura digital. Uma assinatura digital pode ser usada para autenticar a origem de uma mensagem ou documento, garantindo que ele veio da fonte que afirma ter vindo e não foi forjado.

Estratégias e ferramentas que podem ser usadas para garantir a autenticidade:

1. Autenticação de Usuários: A autenticação de usuários é um método fundamental para garantir a autenticidade. Isso geralmente envolve um nome de usuário e senha, mas pode também incluir autenticação de dois fatores ou multifatores, que usam mais de um método de verificação.

2. Certificados Digitais: Os certificados digitais são usados para autenticar a identidade de um usuário, sistema ou organização na internet. Eles são emitidos por Autoridades de Certificação (ACs), que verificam a identidade da entidade antes de emitir o certificado.

3. Assinaturas Digitais: As assinaturas digitais podem ser usadas para autenticar a origem de uma mensagem ou documento, garantindo que veio de uma fonte específica e não foi alterado durante o trânsito.

4. Criptografia: A criptografia pode ajudar a garantir a autenticidade através da verificação de que uma mensagem ou documento não foi alterado. Isso é geralmente feito usando um processo conhecido como hashing.

Irretratabilidade (Não-Repúdio)

A irretratabilidade, também conhecida como não-repúdio, é um princípio de segurança da informação que **garante que uma entidade envolvida em uma comunicação não possa negar a autoria de sua participação**. Em termos simples, o princípio da irretratabilidade fornece a prova incontestável de que uma ação ou evento ocorreu.

Um exemplo de irretratabilidade é uma transação financeira online. Quando uma pessoa faz uma compra ou uma transferência de dinheiro, ela não pode negar que a transação ocorreu, pois existem registros eletrônicos que comprovam a transação.

Outro exemplo é o envio de um e-mail. Quando um e-mail é enviado, há um registro da mensagem sendo enviada do remetente para o destinatário. Através do uso de mecanismos de irretratabilidade, o remetente não pode negar que enviou a mensagem.

Estratégias e ferramentas que podem ser usadas para garantir a irretratabilidade:

1. Assinaturas Digitais: As assinaturas digitais são uma forma comum de garantir a irretratabilidade. Quando uma mensagem é assinada digitalmente, é criada uma "impressão digital" única que é quase impossível de falsificar. Isso permite que o remetente da mensagem seja identificado de forma inequívoca.

2. Registros de Auditoria: Fornecem prova de que uma ação específica ocorreu em um determinado momento.

3. Timestamping: O timestamping, ou carimbo de tempo, é uma maneira de registrar o momento exato em que uma ação ocorreu. Quando combinado com outros mecanismos de irretratabilidade, o timestamping pode fornecer uma forte garantia de que uma ação ocorreu em um determinado momento.

4. Certificados Digitais: Os certificados digitais, emitidos por uma Autoridade Certificadora (CA), podem ser usados para confirmar a identidade de uma entidade, fornecendo uma camada adicional de irretratabilidade.

A tabela a seguir resume os princípios que vimos até aqui:

Princípio	Descrição	Como Garantir
Confidencialidade	**Garante que as informações sejam acessíveis apenas por pessoas autorizadas**	**Controle de acesso, criptografia, políticas de segurança, treinamento de conscientização**
Integridade	**Garante que as informações sejam mantidas precisas e completas, e que não sejam alteradas de forma inadequada ou não autorizada**	**Controle de acesso, backups e recuperação, verificação de integridade dos dados, assinaturas digitais, atualizações e patches**
Disponibilidade	**Garante que as informações e os sistemas estejam sempre acessíveis para aqueles que precisam deles**	**Redundância de dados, balanceamento de carga, recuperação de desastres e continuidade dos negócios, manutenção regular do sistema, prevenção e mitigação de DoS**
Autenticidade	**Garante que os usuários, sistemas ou entidades sejam quem afirmam ser**	**Autenticação de usuários, certificados digitais, assinaturas digitais, criptografia**
Irretratabilidade	**Garante que uma entidade não possa negar a autoria de sua participação em uma comunicação ou transação**	**Assinaturas digitais, registros de auditoria, timestamping, certificados digitais**

Criptologia

A criptologia é o estudo e a aplicação das técnicas que permitem a comunicação segura em presença de adversários. Este campo é composto por duas áreas distintas, mas intimamente relacionadas: a criptografia e a criptoanálise.

A **criptografia** é a ciência de codificar mensagens de forma que só o destinatário pretendido possa decifrá-las. Ela tem sido usada ao longo da história para comunicação secreta, desde o uso de códigos simples na antiguidade até os complexos sistemas de codificação usados hoje

em dia. A criptografia se tornou uma ferramenta crucial na era digital, pois permite a segurança das informações que são transmitidas e armazenadas online.

Por outro lado, a **criptoanálise** é a ciência de decifrar códigos e cifras sem conhecer a chave usada para criptografar a mensagem original. A criptoanálise utiliza várias técnicas, incluindo análise de frequência, ataques de força bruta e análise estatística para quebrar códigos e decifrar mensagens.

A interação entre a criptografia e a criptoanálise é dinâmica, com avanços em um campo geralmente levando a avanços correspondentes no outro. À medida que os métodos criptográficos se tornam mais sofisticados, o mesmo ocorre com as técnicas de criptoanálise.

Antes de estudarmos técnicas mais avançadas de criptografia e criptoanálise, vamos fazer uma breve discussão Esteganografia, umas das técnicas mais antigas relacionadas à criptologia.

Esteganografia

Esteganografia é a **prática de ocultar uma mensagem ou informação dentro de outra** de forma que a existência da mensagem oculta seja imperceptível. O termo vem das palavras gregas "*steganos*", que significa "coberto" ou "secreto", e "*graphein*", que significa "escrever".

Diferentemente da criptografia, que se concentra em manter o conteúdo de uma mensagem inacessível através da codificação, a esteganografia se concentra em **manter a existência da própria mensagem oculta**.

Ela pode ser aplicada a imagens, arquivos de áudio, vídeo, texto e até mesmo protocolos de rede. O objetivo é que a pessoa que esteja vendo ou ouvindo não perceba que há uma mensagem oculta.

Exemplos de Esteganografia:

1. **Imagens Esteganográficas:** Um dos usos mais comuns da esteganografia é em imagens digitais. Por exemplo, um pixel em uma imagem pode ser alterado de uma forma que é indetectável a olho nu, mas que contém informações quando visualizado com o software certo.
2. **Áudio Esteganográfico:** Da mesma forma, a esteganografia pode ser aplicada a arquivos de áudio. Uma técnica comum é alterar o bit menos significativo em cada byte de um arquivo de som para incorporar uma mensagem oculta. Para o ouvido humano, essas alterações são imperceptíveis, mas podem ser detectadas por um software de análise de áudio.

3. **Esteganografia de Protocolo de Rede:** A esteganografia também pode ser aplicada à comunicação de rede. Por exemplo, informações podem ser ocultadas nos campos de cabeçalho de um pacote IP, ou na sequência de pacotes enviados em uma conexão de rede.

Criptografia e Criptoanálise

Criptografia é o estudo e a prática de técnicas para comunicação segura na presença de adversários. Seu objetivo é **garantir que as informações enviadas de um remetente (emissor) a um destinatário (receptor) possam ser lidas apenas por aqueles para quem a mensagem é destinada**. A palavra "criptografia" vem do grego "*kryptós*", que significa "oculto", e "*graphía*", que significa "escrita".

A criptografia serve a várias funções: proporciona **confidencialidade** ao proteger a privacidade da mensagem, mantendo-a inacessível para aqueles que não possuem a chave criptográfica correta; garante **integridade** ao proteger a mensagem de modificações não autorizadas; oferece **autenticação** ao permitir a verificação da identidade de uma parte envolvida em uma comunicação; e assegura **irretratabilidade** (ou não-repúdio) ao proibir uma parte de negar a autoria de sua participação em uma comunicação.

A criptografia tem sido usada ao longo da história da humanidade, de civilizações antigas até a era digital moderna. Veja alguns exemplos históricos do uso de criptografia:

1. **Os Antigos Egípcios:** A primeira evidência conhecida da criptografia vem do antigo Egito, onde hieróglifos foram usados em monumentos funerários. As inscrições não eram destinadas a serem secretas, mas eram uma forma de escrita codificada.
2. **Cifra de César:** Um dos primeiros exemplos de criptografia real vem de Júlio César, que usou o que agora chamamos de Cifra de César para se comunicar com seus generais. Esta cifra envolve um deslocamento simples do alfabeto, onde cada letra é substituída por outra, alguns lugares adiante no alfabeto.
3. **Enigma da Segunda Guerra Mundial:** Durante a Segunda Guerra Mundial, os alemães usaram uma máquina de codificação chamada Enigma para enviar mensagens criptografadas. Os aliados quebraram o código, no entanto, uma façanha que desempenhou um papel crucial na vitória aliada. *Obs.: o filme "O Jogo da Imitação" é um excelente retrato dessa batalha intelectual travada entre os Aliados e o Eixo.*
4. **Era Digital:** Na era digital, a criptografia tornou-se essencial para garantir a segurança da informação em muitas áreas, incluindo comunicações na Internet, sistemas financeiros, militares e de saúde.

Tipos de Criptografia

A criptografia pode ser dividida em dois tipos principais, dependendo do tipo de chaves utilizadas: simétrica e assimétrica.

Criptografia Simétrica: também conhecida como criptografia de chave secreta, usa a mesma chave para criptografar e descriptografar uma mensagem. Isso significa que o remetente e o destinatário devem ambos ter acesso à chave secreta para que a comunicação segura ocorra. Exemplos de algoritmos de criptografia simétrica incluem DES (Data Encryption Standard), AES (Advanced Encryption Standard) e RC4.

A principal vantagem da criptografia simétrica é que ela é rápida e eficiente para grandes volumes de dados. No entanto, a necessidade de compartilhar uma chave secreta de maneira segura entre o remetente e o destinatário pode ser uma desvantagem, especialmente em um ambiente de rede onde há muitos usuários.

Criptografia Assimétrica: também conhecida como criptografia de chave pública, usa duas chaves diferentes: uma chave pública, que pode ser amplamente distribuída, e uma chave privada, que é mantida em segredo pelo proprietário. A chave pública é usada para criptografar a mensagem e a chave privada é usada para descriptografar. Exemplos de algoritmos de criptografia assimétrica incluem RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm) e ECC (Elliptic Curve Cryptography).

A criptografia assimétrica resolve o problema de compartilhamento de chave da criptografia simétrica, já que as chaves públicas podem ser distribuídas livremente sem comprometer a segurança. Além disso, a criptografia assimétrica também permite a criação de assinaturas digitais, o que garante a autenticidade e a irretratabilidade das mensagens. No entanto, a criptografia assimétrica é computacionalmente mais intensiva do que a criptografia simétrica, o que a torna menos adequada para criptografar grandes volumes de dados.

OBSERVAÇÃO IMPORTANTE:

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. Note que nem todos poderão ser garantidos simultaneamente.

Criptografia Simétrica

Criptografia simétrica é uma forma de criptografia em que **a mesma chave é usada tanto para a criptografia (cifragem) quanto para a descriptografia (decifragem) dos dados**. Esta técnica é útil quando a quantidade de dados é substancial, pois a criptografia simétrica é **relativamente rápida se comparada à criptografia assimétrica**.

Além disso, criptografia simétrica é usada para garantir a confidencialidade dos dados. Ela permite que as informações sejam armazenadas ou transmitidas de maneira segura, de modo que apenas as partes que possuem a chave possam acessar os dados originais.

Vantagens:

- Velocidade: A criptografia simétrica é mais rápida e eficiente quando comparada à criptografia assimétrica, o que a torna ideal para cifrar grandes volumes de dados.
- Simplicidade: A criptografia simétrica é mais simples de implementar e usar do que a criptografia assimétrica.

Desvantagens:

- Compartilhamento de chave: A maior desvantagem da criptografia simétrica é a necessidade de compartilhar a chave secreta de forma segura entre as partes que precisam acessar os dados. Se a chave for interceptada durante a transmissão, a segurança dos dados será comprometida.
- Gerenciamento de chaves: Em uma grande rede, o número de chaves necessárias pode ser muito grande, tornando o gerenciamento de chaves um desafio.

Algoritmos de Criptografia Simétrica**:**

DES (Data Encryption Standard): Foi um dos primeiros sistemas de criptografia simétrica amplamente utilizados. Usa uma chave de 56 bits, o que **é considerado inseguro atualmente** devido ao avanço do poder computacional.

3DES (Triple DES): É uma variante do DES que aplica o algoritmo DES três vezes a cada bloco de dados. Isso aumenta a segurança em comparação com o DES padrão, mas também é mais lento.

AES (Advanced Encryption Standard): É o padrão atual para criptografia simétrica, adotado pelo governo dos EUA. É rápido, seguro e usa chaves de 128, 192 ou 256 bits.

IDEA (International Data Encryption Algorithm): É um algoritmo de chave simétrica que usa blocos de 64 bits e uma chave de 128 bits. Foi projetado como um substituto para o DES.

RC4 (Rivest Cipher 4): É um algoritmo de criptografia de fluxo. Embora tenha sido amplamente usado em protocolos como WEP e TLS, **vulnerabilidades descobertas no algoritmo levaram à sua desaprovação em muitos protocolos modernos**.

Blowfish: É um algoritmo de criptografia simétrica que divide os dados em blocos de 64 bits e os criptografa individualmente. É conhecido por sua velocidade e eficácia.

Cifra de César: É uma das técnicas de criptografia mais simples, em que cada letra no texto é 'deslocada' ao longo de um número fixo de posições no alfabeto. Por exemplo, com um deslocamento de 1, A seria substituído por B, B se tornaria C, e assim por diante. Embora seja muito simples e fácil de quebrar com técnicas modernas, a Cifra de César foi eficaz em sua época e é útil para ensinar os conceitos básicos de criptografia.

Mais sobre a Cifra de César

Vamos ver um exemplo prático de aplicação da Cifra de César com o texto "SEGURANCA DA INFORMACAO" e um deslocamento de 3:

Começamos com o texto original: SEGURANCA DA INFORMACAO.

Aplicamos um deslocamento de 3 posições para cada letra. Assim, 'S' se torna 'V', 'E' se torna 'H', 'G' se torna 'J', e assim por diante.

O resultado final (texto cifrado) será: "VHJXUDQFD GD LQIRUPDFDR".

Portanto, a mensagem "SEGURANCA DA INFORMACAO" cifrada com a cifra de César e um deslocamento de 3 se torna "VHJXUDQFD GD LQIRUPDFDR".

Para descriptografar a mensagem, fazemos o processo inverso, ou seja, deslocamos as letras 3 posições para a esquerda no alfabeto.

Criptografia Assimétrica

Criptografia assimétrica, também conhecida como criptografia de chave pública, usa duas chaves diferentes: uma chave pública para criptografar os dados e uma chave privada para descriptografar. Estas chaves são matematicamente relacionadas, mas a chave privada não pode ser derivada da chave pública. Isso permite que a chave pública seja distribuída livremente sem comprometer a segurança dos dados.

Ela é usada para garantir a confidencialidade, a autenticidade e a integridade dos dados. A chave pública geralmente é utilizada para criptografar uma mensagem que só pode ser descriptografada pela correspondente chave privada, garantindo a confidencialidade. A

chave privada pode ser usada para criar uma assinatura digital que pode ser verificada com a chave pública, garantindo a autenticidade e a integridade.

Vantagens:

- Segurança: A chave privada nunca precisa ser transmitida ou compartilhada, reduzindo a chance de ser descoberta.
- Autenticação: Permite a criação de assinaturas digitais que podem ser verificadas para confirmar a identidade do remetente e garantir que os dados não foram alterados.

Desvantagens:

- Velocidade: É significativamente mais lenta do que a criptografia simétrica devido à complexidade computacional dos algoritmos.
- Tamanho da Chave: Requer chaves de tamanho significativamente maior para fornecer o mesmo nível de segurança.

Exemplo:

Imagine que Maria e João querem trocar mensagens de forma segura, mas estão em lugares distantes e o único meio de comunicação é um canal inseguro, por exemplo, a Internet. Eles decidem usar criptografia assimétrica para garantir a segurança das suas mensagens. Aqui está como eles fariam isso:

1. Maria e João geram cada um seu próprio par de chaves - uma chave privada que mantêm em segredo e uma chave pública que podem compartilhar com qualquer pessoa.
2. Maria quer enviar uma mensagem para João. Então, ela obtém a chave pública de João (que pode ser livremente compartilhada) e usa essa chave para criptografar a mensagem.
3. Imagine a chave pública de João como uma caixa com um cadeado aberto. Maria pode colocar a mensagem dentro da caixa e fechar o cadeado. Agora, só alguém com a chave para abrir esse cadeado (a chave privada de João) pode ler a mensagem.
4. Maria envia a caixa trancada (mensagem criptografada) para João através do canal inseguro. Mesmo se alguém interceptar essa caixa durante a transmissão, não será capaz de abri-la e ler a mensagem, pois não possui a chave privada de João.
5. João recebe a caixa trancada e usa sua chave privada (a única que pode abrir o cadeado) para destrancar a caixa e ler a mensagem de Maria.

Esse exemplo ilustra o princípio básico de como a criptografia de chave pública é usada para garantir a confidencialidade das mensagens em um canal inseguro. Também é possível usar criptografia de chave pública para autenticação e integridade (por exemplo, através de assinaturas digitais), mas esses são conceitos mais avançados.

Algoritmos de Criptografia Assimétrica:

RSA (Rivest-Shamir-Adleman): É o algoritmo de chave pública mais comumente usado. É usado tanto para criptografia quanto para assinaturas digitais. A segurança do RSA se baseia na dificuldade de fatorar grandes números primos.

DSA (Digital Signature Algorithm): Como o nome sugere, DSA é usado principalmente para criar assinaturas digitais. Não é usado para criptografia de dados. A segurança do DSA se baseia na dificuldade do problema do logaritmo discreto.

ECDSA (Elliptic Curve Digital Signature Algorithm): É uma versão do DSA que usa curvas elípticas. Isso proporciona o mesmo nível de segurança com chaves significativamente menores, economizando largura de banda e armazenamento.

Diffie-Hellman: É usado para troca segura de chaves pela Internet. Permite que duas partes, cada uma com sua chave pública e privada, gerem uma chave compartilhada que só elas conhecem, mesmo se estiverem comunicando-se através de um canal inseguro. A segurança do Diffie-Hellman também se baseia na dificuldade do problema do logaritmo discreto.

Mais sobre o funcionamento do RSA:

O RSA (Rivest-Shamir-Adleman) é um sistema de criptografia de chave pública que se baseia na **dificuldade computacional de fatorar um número grande em seus fatores primos**. Vamos ver os detalhes do funcionamento do RSA.

1. **Geração das Chaves:**

Primeiro, são escolhidos dois números primos grandes, p e q. Em seguida, esses números são multiplicados para obter um número **n = p * q**. Esse número n faz parte da chave pública e será a "modulus" para as operações de criptografia e descriptografia.

Então, é escolhido um número "e" tal que "e" seja maior que 1 e menor que (p-1)*(q-1) e que "e" e (p-1)*(q-1) sejam coprimos (ou seja, o máximo divisor comum de e e (p-1)*(q-1) deve ser 1). Esse número e é a segunda parte da chave pública.

A chave privada d é o inverso multiplicativo de e modulo (p-1)*(q-1). Em outras palavras, d é um número tal que quando multiplicado por e e depois dividido por (p-1)*(q-1), o resto (ou "resíduo") é 1.

Agora temos as duas chaves. A chave pública é (e, n) e a chave privada é d.

2. **Criptografia:**

Suponha que Maria quer enviar uma mensagem para João. Maria obtém a chave pública de João (e, n) e representa sua mensagem como um número M que seja menor que n.

Maria então criptografa a mensagem fazendo C = M^e mod n, onde C é a mensagem criptografada.

3. **Descriptografia:**

João recebe a mensagem criptografada C. Para descriptografá-la, João faz M = C^d mod n, recuperando a mensagem original M.

A segurança do RSA é baseada no fato de que, **embora seja fácil (com a chave privada) calcular a d-ésima potência de um número C mod n, é extremamente difícil fazer a operação inversa sem conhecer a fatoração de n**. Isso é conhecido como o "problema RSA". Até hoje, ninguém encontrou uma maneira eficiente de resolver o problema RSA, a criptografia RSA é considerada segura para a maioria dos usos práticos.

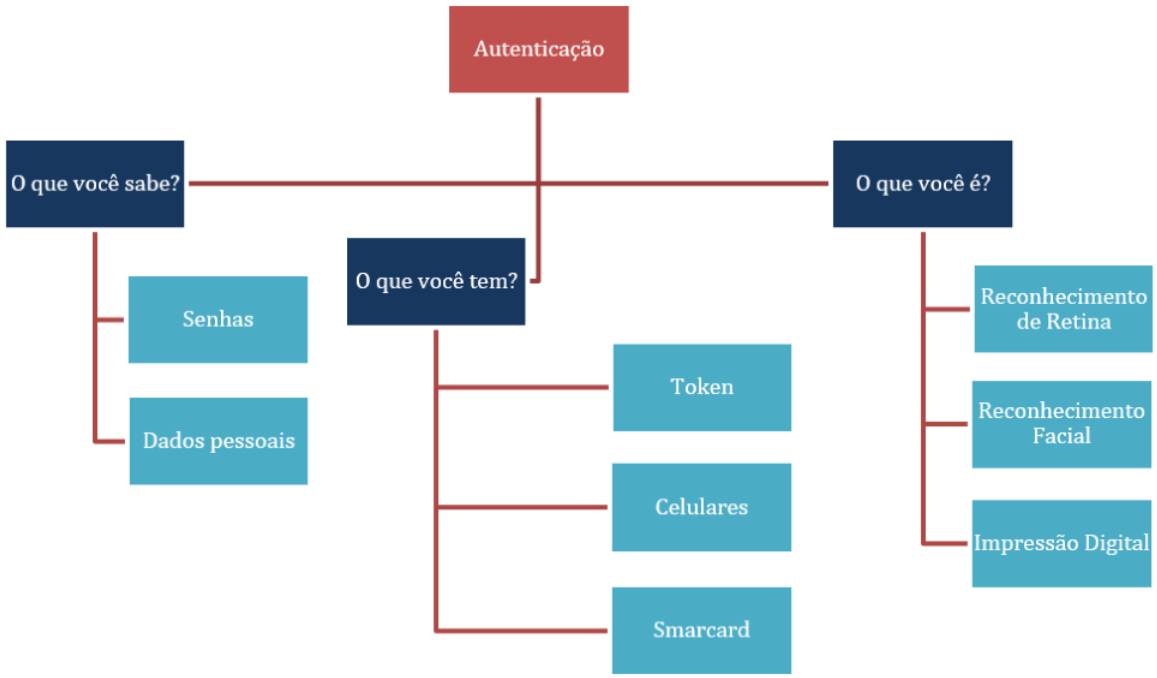
Autenticação

A autenticação é o **processo pelo qual um sistema verifica a identidade de um usuário que tenta acessá-lo**. É um elemento crítico da segurança da informação, porque ajuda a garantir que apenas usuários autorizados possam acessar ou manipular dados. Existem três métodos principais de autenticação, que muitas vezes são descritos como "o que você sabe", "o que você tem" e "o que você é".

1. **O que você sabe**: Esta é a forma mais comum de autenticação e envolve o uso de algo que apenas o usuário conhece, **como uma senha ou um PIN**. No entanto, este método tem suas limitações. As senhas podem ser esquecidas, roubadas ou, se forem simples, até adivinhadas. Além disso, muitas vezes os usuários usam a mesma senha para várias contas, o que significa que se a senha para uma conta for descoberta, todas as contas poderão estar em risco.
2. **O que você tem**: Este método de autenticação envolve o uso de algo que o usuário possui. Isso pode ser um **cartão inteligente, um token de segurança ou até mesmo um celular**. Por exemplo, um banco pode enviar um código de verificação único para o celular de um cliente como parte do processo de autenticação online. Embora este método seja geralmente mais seguro do que a simples utilização de senhas, ele também tem suas limitações. Os dispositivos podem ser perdidos, roubados ou comprometidos.
3. **O que você é**: Esta é uma forma de **autenticação biométrica**, onde características físicas ou comportamentais únicas de um indivíduo são usadas para verificar sua identidade. Isso

pode incluir impressões digitais, reconhecimento facial, reconhecimento de retina ou de íris, reconhecimento de voz e até mesmo a forma de andar de uma pessoa. A vantagem dos sistemas biométricos é que eles são muito difíceis de falsificar ou roubar. No entanto, eles também têm suas limitações. Por exemplo, podem ser afetados por alterações físicas (como um corte no dedo que altera a impressão digital), e alguns sistemas podem ser enganados por imagens de alta qualidade ou gravações.

A figura a seguir resume os tipos de autenticação:



Autenticação Forte

A **autenticação multifator**, também conhecida como autenticação forte, é um método de confirmação da identidade de um usuário que requer a apresentação de dois ou mais fatores de autenticação diferentes. Esses fatores se enquadram em três categorias principais:

- Algo que você sabe (conhecimento), como uma senha ou PIN.
- Algo que você tem (posse), como um cartão inteligente, token ou dispositivo móvel.
- Algo que você é (inerência), referindo-se a características biométricas, como impressões digitais, reconhecimento facial ou de voz.

Usar mais de um método de diferentes categorias aumenta a segurança da autenticação. Para que um invasor acesse uma conta protegida por autenticação multifator, ele precisaria, por exemplo, não apenas saber a senha da vítima (conhecimento), mas também ter acesso ao

dispositivo móvel da vítima (posse) e/ou ser capaz de falsificar suas características biométricas (inerência).

Um exemplo comum de autenticação multifator é a verificação em duas etapas que muitos serviços online usam. Quando você tenta fazer login, é solicitado que você insira sua senha (conhecimento). Em seguida, um código é enviado ao seu celular via SMS ou por meio de um aplicativo autenticador (posse). Você precisa inserir esse código para concluir o processo de login.

Algumas instituições financeiras vão além e usam autenticação de três fatores, que pode incluir a verificação biométrica (inerência) junto com a senha e o dispositivo.

A principal vantagem da autenticação multifator é que ela fornece uma camada adicional de segurança. Mesmo que um invasor consiga descobrir a senha de um usuário, ainda será difícil para ele acessar a conta sem os outros fatores de autenticação. No entanto, a autenticação multifator pode ser menos conveniente para o usuário, pois requer etapas adicionais no processo de login. Além disso, os métodos baseados em posse e inerência podem exigir hardware adicional, como leitores de cartões inteligentes ou scanners biométricos.

Assinatura Digital

Assinatura digital é uma técnica criptográfica usada para **autenticar a identidade de um remetente de uma mensagem ou de um transmissor de um documento eletrônico**. Ela garante que o conteúdo original não foi alterado durante a transmissão (integridade) e confirma a identidade do remetente (autenticidade). Ela desempenha um papel semelhante a uma assinatura física em um documento impresso, mas é executada através de algoritmos de criptografia.

De modo geral, a assinatura digital funciona em dois passos:

- **Criação da Assinatura Digital:** Primeiro, o documento original é processado por um **algoritmo de hash** para criar um resumo da mensagem, que é uma sequência única de caracteres que representa o conteúdo do documento. Em seguida, o remetente usa sua chave privada para criptografar esse resumo da mensagem, criando a assinatura digital. A mensagem original e a assinatura digital são então enviadas ao destinatário.
- **Verificação da Assinatura Digital:** Ao receber a mensagem e a assinatura digital, o destinatário usa a chave pública do remetente para descriptografar a assinatura digital, obtendo o resumo da mensagem original. Paralelamente, o destinatário também processa a mensagem recebida através do mesmo algoritmo de hash para gerar um novo resumo da

mensagem. Se os dois resumos da mensagem correspondem, a assinatura digital é validada. Isso não só confirma que a mensagem é autêntica e veio do remetente indicado, mas também que não foi alterada durante a transmissão.

Exemplo:

Vamos utilizar um exemplo prático envolvendo uma troca de mensagem segura por email entre duas partes, Maria e João. Suponha que Maria deseje enviar uma mensagem importante e sensível para João e queira assegurar que a mensagem é autêntica e não foi alterada durante a transmissão.

1. Primeiro, Maria escreve a mensagem em seu computador. Vamos supor que a mensagem seja "Contrato assinado, aguardo a transferência dos fundos". Maria então processa essa mensagem através de um algoritmo de hash, criando um resumo da mensagem - uma sequência única de caracteres que representa o conteúdo da mensagem.
2. Em seguida, Maria utiliza sua chave privada - que é um código secreto que apenas ela conhece - para criptografar esse resumo da mensagem. O resultado é a assinatura digital.
3. Maria então anexa essa assinatura digital à sua mensagem original e envia ambas para João.
4. Ao receber a mensagem e a assinatura digital, João usa a chave pública de Maria - um código que é conhecido por todos e que corresponde à chave privada de Maria - para descriptografar a assinatura digital. Isso resulta no resumo da mensagem original que Maria enviou.
5. Paralelamente, João também processa a mensagem que recebeu através do mesmo algoritmo de hash para criar um novo resumo da mensagem.
6. João então compara o resumo da mensagem que ele gerou com o resumo da mensagem que ele descriptografou da assinatura digital. Se os dois correspondem, isso confirma que a mensagem é autêntica e não foi alterada durante a transmissão.

Este é um exemplo simples de como a assinatura digital funciona na prática. Note que este processo requer o uso de software de criptografia e certificados digitais, que confirmam a validade das chaves públicas.

Função Hash

Uma função hash é uma função criptográfica especial que recebe uma entrada (ou 'mensagem') e retorna uma string de tamanho fixo de bytes, geralmente na forma de uma **sequência de caracteres alfanuméricos**. A saída é comumente chamada de "hash" ou "digest" da mensagem de entrada.

Existem três propriedades principais que uma função hash deve ter:

1. Deve ser computacionalmente inviável determinar a entrada original a partir do hash gerado.
2. Dado um input e seu hash, deve ser computacionalmente inviável encontrar um segundo input diferente que produza o mesmo hash.
3. Deve ser computacionalmente inviável encontrar dois inputs distintos que produzam o mesmo hash.

Exemplos comuns de funções hash incluem SHA-256 (usado no Bitcoin) e MD5, embora o último não seja mais considerado seguro contra ataques de colisão.

No contexto da assinatura digital, a função hash é usada para gerar um resumo da mensagem que é então criptografado para criar a assinatura digital. Isso tem várias vantagens:

- Economia de tempo: Criptografar o hash de uma mensagem é mais rápido do que criptografar toda a mensagem.
- Segurança: Como mencionado acima, as funções hash são projetadas para serem resistentes a colisões, tornando as assinaturas digitais mais seguras.
- Verificação de integridade: O destinatário pode verificar se a mensagem foi alterada durante a transmissão, gerando o hash da mensagem recebida e comparando-o com o hash descriptografado da assinatura digital.

Exemplo**:**

Vamos supor que Maria queira enviar uma mensagem segura para João. Ela pode usar uma função hash para criar um hash da mensagem original. Por exemplo, se a mensagem original fosse "Olá, João", a função hash poderia gerar o hash "abc123" (esta é uma simplificação, os hashes reais seriam muito mais longos e complexos). Maria então criptografa o hash "abc123" com sua chave privada para criar a assinatura digital. Maria envia a mensagem original "Olá, João" e a assinatura digital para João.

Quando João recebe a mensagem e a assinatura digital, ele pode usar a chave pública de Maria para descriptografar a assinatura digital, o que lhe dá o hash original "abc123". João também pode gerar um novo hash da mensagem recebida "Olá, João". Se o novo hash corresponder ao hash original, João pode ter certeza de que a mensagem não foi alterada durante a transmissão e que veio de Maria.

Certificado Digital

Um certificado digital é uma tecnologia que usa criptografia para **associar uma identidade a uma chave pública**. Esses certificados são emitidos por uma **Autoridade Certificadora** (AC), uma **entidade confiável que valida a identidade do titular do certificado**. Quando uma AC emite um certificado digital, ela está essencialmente atestando que a chave pública contida no certificado pertence à pessoa, sistema ou entidade identificada dentro do certificado.

Os certificados digitais são essenciais para a segurança da informação, pois **fornecem uma maneira de verificar a identidade das partes em uma transação digital**. Eles são comumente usados em uma variedade de aplicações, incluindo SSL/TLS para sites seguros, autenticação de cliente e servidor, assinaturas digitais e criptografia de email.

As Autoridades Certificadoras resolvem um problema fundamental na criptografia de chave pública: **como você pode confiar que uma chave pública realmente pertence à entidade que alega possuí-la**? Sem uma AC, seria muito difícil para as partes verificarem a identidade umas das outras em uma transação digital.

Suponha, por exemplo, que você esteja se comunicando com um site que alega ser o seu banco. O site fornece uma chave pública que você pode usar para criptografar suas informações. Mas como você pode ter certeza de que a chave realmente pertence ao seu banco e não a um atacante que está tentando interceptar suas informações?

Isso é onde as Autoridades Certificadoras entram. Elas verificam a identidade do proprietário da chave pública antes de emitir um certificado. Assim, quando você recebe a chave pública do site, você também recebe um certificado que foi assinado pela AC. Se você confia na AC, então pode confiar que a chave pertence ao seu banco.

Sem uma AC, um atacante poderia potencialmente criar uma chave pública e alegar que pertence ao seu banco. Se você não tiver como verificar essa afirmação, poderá acabar enviando suas informações diretamente para o atacante. Este tipo de ataque é conhecido como "ataque man-in-the-middle" e é uma das muitas ameaças que as Autoridades Certificadoras ajudam a mitigar.

Antes de avançarmos nas explicações sobre certificados digitais, é importante que fique clara a diferença entre assinatura digital e certificado digital:

Assinatura Digital:

- É uma técnica criptográfica que permite ao remetente assinar digitalmente uma mensagem/documento.
- É **usada para verificar a autenticidade e integridade da mensagem/documento**.
- A assinatura digital é única para cada documento; mesmo uma pequena alteração na mensagem resultará em uma assinatura diferente.
- É criada usando a chave privada do remetente e pode ser verificada por qualquer pessoa usando a chave pública correspondente do remetente.

Certificado Digital:

- É uma tecnologia usada para associar uma identidade a uma chave pública.
- **É usado para verificar se uma chave pública pertence a um indivíduo, sistema ou entidade**.
- Um certificado digital é emitido por uma Autoridade Certificadora (AC) e contém informações como o nome do titular, a chave pública, o nome da AC e o período de validade do certificado.
- O certificado é usado para evitar que um atacante se passe por outra entidade ao fornecer uma chave pública diferente.

Aqui está uma tabela que resume essas diferenças:

	Assinatura Digital	Certificado Digital
Função principal	**Verificar a autenticidade e integridade**	**Assegurar que a chave pública pertence ao indivíduo, sistema ou entidade**
É único?	**Sim, para cada mensagem/documento**	**Não, um certificado pode ser usado com várias mensagens/documentos**
Quem cria?	**O remetente da mensagem/documento**	**Uma Autoridade Certificadora (AC)**
O que usa?	**Chave privada do remetente**	**Informações do titular e sua chave pública**

Infraestrutura de Chaves Públicas (ICP-Brasil)

A Infraestrutura de Chave Pública (ICP), também conhecida como Public Key Infrastructure (PKI), é um **conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais**. Ela fornece uma estrutura de segurança digital que garante a autenticação, a privacidade e a integridade das informações trocadas em redes digitais.

A ICP é uma estrutura fundamental para atividades que requerem segurança e confiança, tais como assinatura de documentos digitais, transações financeiras online, troca segura de informações e autenticação de identidade online.

Como funciona a emissão de um certificado?

O processo de emissão de um certificado digital envolve vários passos que garantem a segurança e a autenticidade do certificado. De forma simplificada, funciona assim:

1. **Solicitação**: Primeiro, o solicitante (que pode ser uma pessoa, uma organização ou um servidor web) solicita um certificado a uma Autoridade de Registro (AR), fornecendo todas as informações necessárias e a chave pública que será associada ao certificado. Normalmente, isso envolve preencher um formulário online no site da AR e submeter um par de chaves público-privadas. A chave privada é mantida em segredo pelo solicitante, enquanto a chave pública é enviada para a AR.
2. **Verificação de Identidade**: A AR verifica a identidade e a validade das informações fornecidas pelo solicitante. Este processo pode variar dependendo da política da AR. Para certificados de pessoa física, por exemplo, pode ser necessário apresentar documentos de identificação pessoal. Para certificados de servidor web, a AR pode verificar a propriedade do domínio para o qual o certificado será emitido.
3. **Emissão do Certificado**: Uma vez que a identidade do solicitante e a validade das informações tenham sido verificadas, a Autoridade Certificadora (AC) emite o certificado digital. O certificado contém a chave pública do solicitante, a identidade do solicitante e a assinatura digital da AC. A assinatura digital da AC permite que quem receber o certificado confirme que ele foi realmente emitido por uma AC confiável e que não foi alterado.
4. **Distribuição do Certificado**: O certificado emitido é então distribuído ao solicitante. Depois disso, o solicitante pode usar o certificado para estabelecer conexões seguras, assinar digitalmente documentos e e-mails, entre outros usos, dependendo do tipo de certificado.
5. **Verificação do Certificado**: Quando o certificado é usado, a parte receptora (como um navegador web ou o destinatário de um e-mail assinado) verifica o certificado. Isso envolve verificar a assinatura digital da AC no certificado para confirmar que ele foi emitido por uma AC confiável e não foi alterado.

Qual é a estrutura utilizada no Brasil?

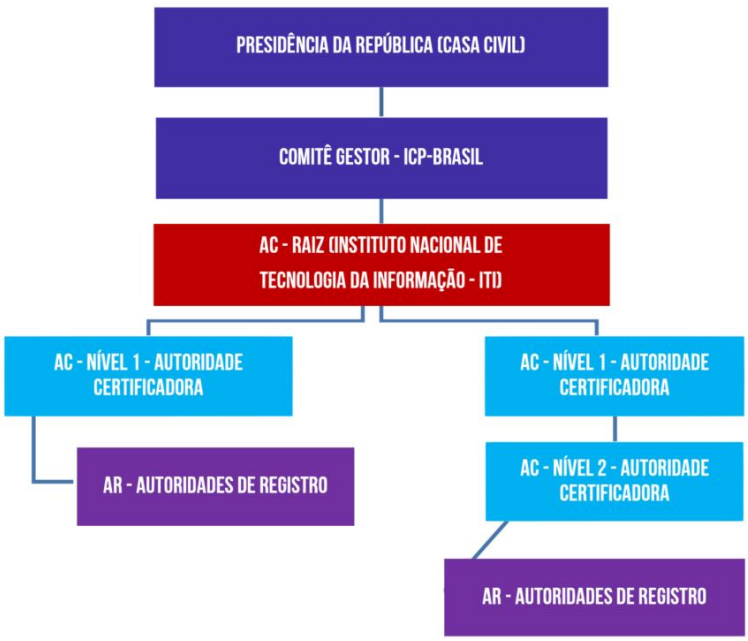
No Brasil, a **ICP-Brasil é a Infraestrutura de Chaves Públicas Brasileira**, que é a hierarquia de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Instituída pela Medida Provisória 2.200-2 de 24 de agosto de 2001, **é uma cadeia hierárquica de confiança que permite a autenticação digital de documentos**.

Por meio de suas ACs (Autoridades Certificadoras), a ICP-Brasil **emite os certificados digitais**, garantindo assim sua validade jurídica. O modelo adotado pelo Brasil, de certificação com o par de chaves criptográficas, é o que garante a autenticidade, a integridade, a confidencialidade e a não repúdio das informações.

A estrutura é organizada **hierarquicamente em camadas**, cada uma delas com suas próprias funções e responsabilidades. Existem três tipos principais de autoridades dentro desta estrutura: Autoridade Certificadora Raiz, Autoridade Certificadora e Autoridade de Registro.

1. **Autoridade Certificadora Raiz (AC Raiz)**: Esta é a entidade no topo da cadeia de confiança de uma ICP. A AC Raiz é responsável por emitir certificados para as Autoridades Certificadoras (ACs) abaixo dela na hierarquia, além de estabelecer as políticas de segurança para a infraestrutura da ICP. Na ICP-Brasil, a AC Raiz é o Instituto Nacional de Tecnologia da Informação (ITI).
2. **Autoridade Certificadora (AC)**: Estas são as entidades certificadas pela AC Raiz para emitir, suspender, renovar ou revogar certificados digitais para usuários finais ou outras ACs. As ACs devem seguir as políticas definidas pela AC Raiz e são auditadas regularmente para garantir a conformidade.
3. **Autoridade de Registro (AR)**: A Autoridade de Registro serve como o elo entre os usuários e a Autoridade Certificadora. Elas são responsáveis por verificar a identidade dos solicitantes antes que a AC emita os certificados. Elas também podem realizar outras funções, como renovação e revogação de certificados.

Veja a estrutura graficamente:



Tipos de Certificado Digital

Certificados digitais vêm em muitos tipos, cada um projetado para atender a diferentes necessidades e requisitos de segurança. Veja alguns exemplos:

Certificados de Servidor Web / SSL (Secure Sockets Layer): usados para estabelecer uma conexão segura entre um servidor web e o navegador de um usuário. Eles permitem que os dados sejam transmitidos de forma segura e criptografada, prevenindo interceptação e manipulação de dados. São comumente usados em sites de comércio eletrônico e bancos online.

Certificados de E-mail / S/MIME (Secure/Multipurpose Internet Mail Extensions): usados para garantir a segurança do e-mail, permitindo que os usuários assinem digitalmente e criptografem e-mails. Eles garantem que o e-mail não foi alterado durante o trânsito e confirmam a identidade do remetente.

Certificados de Assinatura de Código: usados por desenvolvedores de software para assinar digitalmente seu software. Eles confirmam a identidade do autor do software e garantem que o software não foi alterado desde que foi assinado.

Certificados de Autenticação de Cliente: usados para autenticar usuários em servidores ou sistemas. Eles são uma alternativa mais segura às senhas tradicionais, pois são mais difíceis de falsificar ou roubar.

Certificados de Dispositivo / Máquina: usados para autenticar dispositivos em uma rede. Eles são comumente usados em redes corporativas para garantir que apenas dispositivos autorizados possam acessar a rede.

Certificados de Identidade Pessoal: usados por indivíduos para provar sua identidade online. Eles podem ser usados para uma variedade de fins, como assinar documentos digitalmente, acessar serviços online seguros e autenticar-se em redes ou sistemas.

Cada tipo de certificado digital contém informações específicas sobre o titular do certificado e a entidade que emitiu o certificado (a Autoridade Certificadora). A Autoridade Certificadora assina digitalmente o certificado para confirmar sua autenticidade.

Categorias de Certificado Digital

Os certificados digitais no Brasil são classificados em categorias, designadas como "A" e "S". Cada categoria possui subdivisões para especificar ainda mais o nível de segurança e as funcionalidades associadas a cada tipo de certificado. Aqui está uma breve descrição:

1. **Categoria A**: São os certificados de **assinatura digital**, usados para garantir a integridade, a autenticidade e a não repúdio das informações assinadas. Eles são subdivididos em três tipos:
    - **A1**: Este certificado é gerado e armazenado no computador do usuário. Tem validade de um ano e não exige mídia criptográfica para armazenamento, sendo assim menos seguro que o A3.
    - **A3**: Este certificado tem validade de até cinco anos e é gerado e armazenado em uma mídia criptográfica segura (como um smartcard ou token), não podendo ser exportado, o que proporciona um maior nível de segurança.
    - **A4**: Similar ao A3, mas com validade de até 10 anos. Esta categoria é teoricamente possível, mas normalmente não é utilizada na ICP-Brasil.
2. **Categoria S**: São os certificados de sigilo ou criptografia, usados para garantir o sigilo das informações. Assim como os certificados da categoria "A", os certificados da categoria "S" também são subdivididos em S1, S2, S3 e S4, com o mesmo nível de segurança e características de armazenamento. A principal diferença entre a categoria "S" e a categoria "A" é que a categoria "S" é usada para cifrar os dados, garantindo que eles sejam lidos apenas por quem possua a chave de descriptografia correspondente.

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[1].

Um certificado digital é uma tecnologia de segurança da informação que utiliza a criptografia de chave pública para associar a identidade de um indivíduo, organização ou dispositivo a uma chave pública. Funciona como uma forma de carteira de identidade digital emitida por uma Autoridade Certificadora (AC) confiável. Dentro de seu escopo, o certificado contém informações vitais como o nome do titular, a chave pública, o período de validade do

[1] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.

certificado e a assinatura digital da AC que o emitiu. Esta assinatura garante a autenticidade do certificado, permitindo que outras partes confiem nas informações nele contidas.

Os certificados digitais são fundamentais para várias operações de segurança na internet, facilitando transações seguras, comunicações criptografadas e a autenticação digital de usuários e dispositivos. Eles são amplamente utilizados em ambientes que requerem altos níveis de segurança, como no comércio eletrônico, nas transações bancárias online e nos serviços governamentais digitais, onde garantem que as comunicações e transações sejam realizadas de maneira segura. Além disso, os certificados digitais desempenham um papel crucial na implementação de assinaturas digitais, proporcionando uma maneira eficaz de verificar a integridade e a origem dos documentos eletrônicos, essencial para a validade jurídica em ambientes digitais.

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. **(FGV / SEAD-AP – 2022)** Com relação aos métodos de criptografia de chave pública, considere as afirmativas a seguir.

I. Cada participante em um sistema de chave pública possui um par de chaves, uma pública e outra, privada. II. Qualquer participante pode criptografar e decriptografar uma mensagem usando a própria chave privada. III. Quando o participante P1 envia uma mensagem criptografada para P2, é preciso que P2 conheça a chave privada de P1.

É correto somente o que se afirma em

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

Comentários:
(I) Correto; (II) Errado, só é possível decriptografar uma mensagem usando a própria

chave privada se ela foi criptografada usando sua chave pública; (III) Errado, a chave privada é... privada, logo P2 não pode conhecer a chave privada de P1.

Gabarito: A

2. **(FGV / TCE-TO – 2022)** O auditor José recebeu o arquivo AnexoJ em formato digital. Antes de proceder com a abertura do AnexoJ, José determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do AnexoJ por ele recebido com os dados do AnexoJ transmitido pelo emissor.

Essa avaliação feita por José em AnexoJ está diretamente relacionada com o seguinte princípio da segurança de informações:

a) integridade
b) confidencialidade
c) autenticidade
d) disponibilidade
e) qualidade

Comentários:
José quer saber se os dados recebidos são fidedignos em relação aos dados enviados, logo se trata de uma preocupação com relação à integridade.

Gabarito: A

3. **(FGV / TCE-TO – 2022)** As funções de hash são comumente empregadas nos mecanismos de segurança da informação.

Quanto às suas propriedades básicas, para que o algoritmo de hash seja considerado forte, é correto afirmar que:

a) a mesma entrada deve produzir saídas diferentes
b) deve ser difícil encontrar duas entradas que produzam o mesmo hash
c) deve ser possível produzir a entrada original a partir do hash resultante
d) pequenas mudanças na entrada devem produzir pequenas mudanças no hash resultante
e) mesmo que as entradas possuam o mesmo tamanho, os resultados de hash terão tamanhos diferentes

Comentários:
(a) Errado, deve produzir a mesma saída; (b) Correto; (c) Errado, idealmente deve ser impossível produzir a entrada original a partir do hash resultante; (d) Errado, pequenas

mudanças na entrada devem produzir grandes mudanças no hash resultante; (e) Errado, o hash resultante sempre terá o mesmo tamanho.

Gabarito: B

4. **(FGV / TCE-TO – 2022)** Bernardo e João são auditores recém-concursados no TCE/TO. Bernardo precisa enviar documentos sigilosos para João e vice-versa, contudo, nenhum deles utilizou ainda a ferramenta de criptografia disponível na instituição.

Sabendo-se que é utilizada a criptografia por chave pública, o procedimento que deve ser seguido por cada auditor antes de tramitar os documentos é:

a) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave pública do destinatário

b) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; enviar a chave privada para o destinatário; e encriptar um documento utilizando a chave privada enviada

c) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave privada do remetente

d) gerar a chave pública para encriptação e decriptação dos documentos; enviar a chave pública para o destinatário; e encriptar os documentos utilizando a chave pública enviada

e) combinar uma senha entre eles; encriptar e decriptar os documentos utilizando a senha combinada

Comentários:
(a) Correto; (b) Errado, não se envia sua chave privada para o destinatário, porque a chave é privada. E encripta-se o documento utilizando a chave pública do destinatário; (c) Errado, encripta-se os documentos utilizando a chave pública do destinatário; (d) Errado, deve-se gerar o par de chaves e não é necessário enviar a chave pública para o destinatário; (e) Errado, não faz nenhum sentido.

Gabarito: A

5. **(FGV / TRT-MA – 2022)** Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma privada e uma pública. Com relação às categorias de uso dos criptossistemas de chave pública, analise as afirmativas a seguir:

I. Criptografia/descriptografia: um emissor criptografa uma mensagem com a chave pública do seu destinatário.

II. Assinatura digital: um emissor assina uma mensagem com sua chave pública. A assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem.

III. Troca de chave: dois lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são possíveis, envolvendo as chaves públicas de uma ou de ambas as partes.

Está correto o que se afirma em

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

Comentários:
(I) Correto; (II) Errado. Se ele assinar com a própria chave pública, só ele poderá descriptografar. O intuito da assinatura digital é permitir que qualquer pessoa identifique a autenticidade de uma mensagem, logo ele deve assinar uma mensagem com a sua chave privada para que qualquer pessoa com a sua chave pública possa descriptografá-la e conferir a autenticidade; (III) Errado. Envolvem as chaves privadas de uma ou de ambas as partes.

Gabarito: A

6. **(FGV / MPE-GO – 2022)** João quer usar um serviço de armazenamento em nuvem que ofereça o recurso de verificação de sua identidade em duas etapas. Para isso, João escolheu um serviço que usa um aplicativo autenticador instalado em seu dispositivo móvel.

O tipo de verificação em duas etapas do serviço escolhido por João é o(a):

a) código de verificação
b) token gerador de senhas
c) cartão de segurança
d) dispositivo confiável
e) chave de recuperação

Comentários:
(a) Correto. Existem vários aplicativos autenticadores (Ex: Google Authenticator, Microsoft Authenticator, entre outros) que permitem fazer a verificação em duas etapas: em geral, o usuário insere login e senha na primeira etapa e depois insere um código de verificador gerado pelo aplicativo na segunda etapa;
(b) Errado, token gerador de senha é um dispositivo físico e, não, um autenticador instalado em seu dispositivo móvel que usa um serviço de armazenamento em nuvem;
(c) Errado, cartão de segurança é um cartão físico que contém um conjunto de códigos que permitem a autenticação em duas etapas – não tem relação com aplicativo autenticador;
(d) Errado, dispositivo confiável é um computador ou dispositivo móvel que você frequentemente usa para acessar suas contas. Pode ser necessário inserir um código de segurança no primeiro acesso. Ele não será necessário nos demais, pois seu dispositivo será "lembrado" – não tem relação com um aplicativo autenticador;
(e) Errado, chave de recuperação é um código que permite recuperar uma senha ou o acesso a alguma aplicação – não tem relação com um aplicativo autenticador.

Gabarito: A

7. **(FGV / TJDFT – 2022)** Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

a) confidencialidade
b) autenticidade
c) integridade
d) disponibilidade
e) irretratabilidade

Comentários:
Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado Irretratabilidade ou Não-Repúdio, que é a garantia de que o autor não possa negar que ele realizou as operações.

Gabarito: E

8. **(FGV / SEFAZ-BA – 2022)** Os métodos criptográficos, de acordo com a chave utilizada, podem ser classificados em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Assinale a opção que indica um exemplo de método criptográfico da categoria que utiliza chaves assimétricas.

a) Blowfish
b) RSA
c) 3DES

d) IDEA
e) AES

Comentários:
(a) Errado, é um algoritmo de criptografia simétrica; (b) Correto, é um algoritmo de criptografia assimétrica; (c) Errado, é um algoritmo de criptografia simétrica; (d) Errado, é um algoritmo de criptografia simétrica; (e) Errado, é um algoritmo de criptografia simétrica.

Gabarito: B

9. **(FGV / TJ-RS – 2020)** Certificados Eletrônicos, no Brasil, são emitidos:

a) por autoridades certificadoras
b) pela Receita Federal
c) pela Polícia Federal
d) pelas prefeituras
e) pelos cartórios

Comentários:
Questão ruim! Certificados eletrônicos são emitidos por autoridades certificadoras, mas a Receita Federal é uma autoridade certificadora.

Gabarito: A

10. **(FGV / Prefeitura de Niterói - RJ – 2018)** AES, RSA e RC4 são exemplos, respectivamente, de algoritmos de:

a) criptografia simétrica, de criptografia assimétrica e de dispersão criptográfica
b) criptografia simétrica, de criptografia assimétrica e de criptografia simétrica
c) criptografia simétrica, de criptografia de chave pública e de criptografia assimétrica

d) criptografia assimétrica, de criptografia simétrica e de criptografia assimétrica
e) criptografia assimétrica, de criptografia simétrica e de dispersão criptográfica

Comentários:
AES: criptografia simétrica; RSA: criptografia assimétrica; RC4:criptografia simétrica.

Gabarito: 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 auto explicação 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. O que é Segurança da Informação?
2. Quais são os três tipos de controles na segurança da informação?
3. Defina os princípios de confidencialidade, integridade e disponibilidade.
4. O que é Autenticidade e como ela é importante na segurança da informação?
5. O que significa Irretratabilidade ou não-repúdio na segurança da informação?
6. O que é Criptologia?
7. O que é Esteganografia?
8. Quais são as diferenças entre a criptografia simétrica e a criptografia assimétrica?
9. O que é a Cifra de César?
10. Quais são os diferentes métodos de autenticação?
11. O que é a autenticação multifator (MFA)?
12. O que é uma assinatura digital?
13. O que é uma função Hash?
14. O que é um Certificado Digital?
15. O que é uma Infraestrutura de Chave Pública (ICP)?
16. O que é uma Autoridade Certificadora Raiz?
17. O que é uma Autoridade Certificadora (AC)?
18. O que é uma Autoridade de Registro (AR)?
19. Quais são as categorias de certificados digitais?
20. Qual é a diferença entre assinatura digital e certificado dial?

Perguntas e Respostas

1. O que é Segurança da Informação?
   Resposta: Segurança da Informação é a prática de prevenir o acesso, uso, divulgação, interrupção, modificação, inspeção, gravação ou destruição não autorizados de informações.
2. Quais são os três tipos de controles na segurança da informação?
   Resposta: Controles físicos, controles técnicos e controles administrativos.
3. Defina os princípios de confidencialidade, integridade e disponibilidade.
   Resposta: Confidencialidade garante que a informação é acessível apenas para aqueles autorizados a terem acesso. Integridade garante que a informação é precisa e completa e que não foi alterada de maneira não autorizada. Disponibilidade garante que a informação e os recursos relacionados estão acessíveis quando necessário.

4. O que é Autenticidade e como ela é importante na segurança da informação?
   Resposta: Autenticidade é a garantia de que a origem da informação é verdadeira. É crucial para prevenir a falsificação de dados e garantir a veracidade das transações.
5. O que significa Irretratabilidade ou não-repúdio na segurança da informação?
   Resposta: Irretratabilidade ou não-repúdio é a garantia de que uma entidade não pode negar ter participado de uma transação ou comunicação.
6. O que é Criptologia?
   Resposta: Criptologia é o estudo da criptografia e da criptoanálise.
7. O que é Esteganografia?
   Resposta: Esteganografia é a prática de esconder informações dentro de outra informação.
8. Quais são as diferenças entre a criptografia simétrica e a criptografia assimétrica?
   Resposta: Na criptografia simétrica, a mesma chave é usada para criptografar e descriptografar a informação. Na criptografia assimétrica, duas chaves diferentes são usadas - uma para criptografar e outra para descriptografar a informação.
9. O que é a Cifra de César?
   Resposta: A Cifra de César é uma das técnicas de criptografia mais simples e mais amplamente conhecidas. Ela é um tipo de criptografia de substituição em que cada letra no texto é 'deslocada' um certo número de lugares para baixo no alfabeto.
10. Quais são os diferentes métodos de autenticação?
    Resposta: Alguns métodos de autenticação incluem: O que você sabe (senhas e dados pessoais), O que você tem (Token, Celulares, Smartcard) e O que você é (Reconhecimento de Retina, Facial e Impressão Digital).
11. O que é a autenticação multifator (MFA)?
    Resposta: A autenticação multifator é um método de autenticação que requer mais de um método de verificação de identidade.
12. O que é uma assinatura digital?
    Resposta: Uma assinatura digital é um método matemático usado para validar a autenticidade e a integridade de uma mensagem, software ou documento digital.
13. O que é uma função Hash?
    Resposta: Uma função hash é uma função que converte uma entrada de letras e números em uma saída de um comprimento fixo.
14. O que é um Certificado Digital?
    Resposta: Um certificado digital é um documento eletrônico que vincula as chaves de criptografia a uma entidade.
15. O que é uma Infraestrutura de Chave Pública (ICP)?
    Resposta: A ICP é um conjunto de procedimentos, métodos e sistemas usados para emitir certificados digitais.
16. O que é uma Autoridade Certificadora Raiz?
    Resposta: A Autoridade Certificadora Raiz é a AC de nível mais alto em uma hierarquia de ACs.

17. O que é uma Autoridade Certificadora (AC)?
Resposta: A AC é uma entidade que emite certificados digitais.

18. O que é uma Autoridade de Registro (AR)?
Resposta: A AR é uma entidade que verifica as informações do requerente de um certificado digital antes que o certificado seja emitido pela AC.

19. Quais são as categorias de certificados digitais?
Resposta: As categorias de certificados digitais incluem categoria A (usada para assinatura) e categoria S (usada para criptografia).

20. Qual é a diferença entre assinatura digital e certificado digital?
Resposta: A assinatura digital é um método para validar a autenticidade e a integridade de um documento, enquanto o certificado digital é um documento que vincula as chaves de criptografia a uma entidade.

LISTA DE QUESTÕES ESTRATÉGICAS

1. **(FGV / SEAD-AP – 2022)** Com relação aos métodos de criptografia de chave pública, considere as afirmativas a seguir.

I. Cada participante em um sistema de chave pública possui um par de chaves, uma pública e outra, privada. II. Qualquer participante pode criptografar e decriptografar uma mensagem usando a própria chave privada. III. Quando o participante P1 envia uma mensagem criptografada para P2, é preciso que P2 conheça a chave privada de P1.

É correto somente o que se afirma em

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

2. **(FGV / TCE-TO – 2022)** O auditor José recebeu o arquivo AnexoJ em formato digital. Antes de proceder com a abertura do AnexoJ, José determinou a fidedignidade do referido arquivo, avaliando a conformidade dos dados do AnexoJ por ele recebido com os dados do AnexoJ transmitido pelo emissor.

Essa avaliação feita por José em AnexoJ está diretamente relacionada com o seguinte princípio da segurança de informações:

a) integridade
b) confidencialidade
c) autenticidade
d) disponibilidade
e) qualidade

3. **(FGV / TCE-TO – 2022)** As funções de hash são comumente empregadas nos mecanismos de segurança da informação.

Quanto às suas propriedades básicas, para que o algoritmo de hash seja considerado forte, é correto afirmar que:

a) a mesma entrada deve produzir saídas diferentes
b) deve ser difícil encontrar duas entradas que produzam o mesmo hash
c) deve ser possível produzir a entrada original a partir do hash resultante
d) pequenas mudanças na entrada devem produzir pequenas mudanças no hash resultante
e) mesmo que as entradas possuam o mesmo tamanho, os resultados de hash terão tamanhos diferentes

4. **(FGV / TCE-TO – 2022)** Bernardo e João são auditores recém-concursados no TCE/TO. Bernardo precisa enviar documentos sigilosos para João e vice-versa, contudo, nenhum deles utilizou ainda a ferramenta de criptografia disponível na instituição.

Sabendo-se que é utilizada a criptografia por chave pública, o procedimento que deve ser seguido por cada auditor antes de tramitar os documentos é:

a) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave pública do destinatário

b) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; enviar a chave privada para o destinatário; e encriptar um documento utilizando a chave privada enviada

c) gerar um par de chaves a ser usado para encriptação e decriptação dos documentos; importar a chave pública no registrador público da instituição; guardar a chave privada; e encriptar os documentos utilizando a chave privada do remetente

d) gerar a chave pública para encriptação e decriptação dos documentos; enviar a chave pública para o destinatário; e encriptar os documentos utilizando a chave pública enviada

e) combinar uma senha entre eles; encriptar e decriptar os documentos utilizando a senha combinada

5. **(FGV / TRT-MA – 2022)** Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma privada e uma pública. Com relação às categorias de uso dos criptossistemas de chave pública, analise as afirmativas a seguir:

I. Criptografia/descriptografia: um emissor criptografa uma mensagem com a chave pública do seu destinatário.

II. Assinatura digital: um emissor assina uma mensagem com sua chave pública. A assinatura é feita por um algoritmo criptográfico aplicado à mensagem ou a um pequeno bloco de dados que é uma função da mensagem.

III. Troca de chave: dois lados cooperam para trocar uma chave de sessão. Várias técnicas diferentes são possíveis, envolvendo as chaves públicas de uma ou de ambas as partes.

Está correto o que se afirma em

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

6. **(FGV / MPE-GO – 2022)** João quer usar um serviço de armazenamento em nuvem que ofereça o recurso de verificação de sua identidade em duas etapas. Para isso, João escolheu um serviço que usa um aplicativo autenticador instalado em seu dispositivo móvel.

O tipo de verificação em duas etapas do serviço escolhido por João é o(a):

a) código de verificação
b) token gerador de senhas
c) cartão de segurança
d) dispositivo confiável
e) chave de recuperação

7. **(FGV / TJDFT – 2022)** Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em

contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

a) confidencialidade
b) autenticidade
c) integridade
d) disponibilidade
e) irretratabilidade

8. **(FGV / SEFAZ-BA – 2022)** Os métodos criptográficos, de acordo com a chave utilizada, podem ser classificados em duas categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Assinale a opção que indica um exemplo de método criptográfico da categoria que utiliza chaves assimétricas.

a) Blowfish
b) RSA
c) 3DES
d) IDEA
e) AES

9. **(FGV / TJ-RS – 2020)** Certificados Eletrônicos, no Brasil, são emitidos:

a) por autoridades certificadoras
b) pela Receita Federal
c) pela Polícia Federal
d) pelas prefeituras
e) pelos cartórios

10. **(FGV / Prefeitura de Niterói - RJ – 2018)** AES, RSA e RC4 são exemplos, respectivamente, de algoritmos de:

a) criptografia simétrica, de criptografia assimétrica e de dispersão criptográfica
b) criptografia simétrica, de criptografia assimétrica e de criptografia simétrica
c) criptografia simétrica, de criptografia de chave pública e de criptografia assimétrica
d) criptografia assimétrica, de criptografia simétrica e de criptografia assimétrica
e) criptografia assimétrica, de criptografia simétrica e de dispersão criptográfica

Gabaritos

1. A

2. A

3. B

4. A

5. A

6. A

7. E

8. B

9. A

10. B

Questões Adicionais

As questões apresentadas a seguir integram o Banco de Questões do Passo Estratégico. Recomenda-se utilizá-las como um recurso complementar para a prática e consolidação dos conhecimentos adquiridos no material teórico, de acordo com o estilo adotado pela banca organizadora.

Bom estudo!

1. O que caracteriza um certificado digital emitido por uma Autoridade Certificadora (AC)?

A) Ele contém a chave privada do titular.
B) Ele é usado exclusivamente para criptografar dados.
C) Ele é gerado automaticamente por qualquer dispositivo conectado à internet.
D) Ele garante a disponibilidade dos dados na rede.
E) Ele certifica a identidade do titular e contém a chave pública.

2. Em relação à Cifra de César, qual alternativa é verdadeira?

A) Trata-se de um algoritmo de criptografia simétrica que realiza a rotação das posições das letras do alfabeto.
B) É uma modalidade de criptografia impossível de ser quebrada.
C) Teve seu primeiro uso difundido durante a Primeira Guerra Mundial.
D) Utiliza o método de chave privada para cifrar e chave pública para decifrar.
E) É um algoritmo de criptografia assimétrica.

3. Em que situação a criptografia assimétrica é geralmente preferida à criptografia simétrica?

A) Para criptografar grandes volumes de dados em tempo real.
B) Para garantir a integridade de grandes bases de dados.
C) Para autenticação e troca segura de chaves.
D) Para proteger dados armazenados em dispositivos móveis.
E) Para criptografar e-mails internamente em uma organização.

4. Qual a utilização preferencial da criptografia de chave pública (assimétrica)?

A) Para transmitir grandes volumes de dados de forma segura.
B) Na geração de assinaturas digitais.
C) Na configuração de redes privadas virtuais (VPN).
D) Na autenticação de usuários em uma rede local.
E) Na codificação de mensagens de correio eletrônico.

5. Qual dos seguintes métodos seria o mais apropriado para garantir a disponibilidade dos serviços online de uma organização em caso de um ataque DDoS, assegurando que os usuários legítimos ainda possam acessar os recursos?

A) Implementação de firewalls para bloquear tráfego de rede malicioso.
B) Uso de redes de distribuição de conteúdo (CDNs) para distribuir o tráfego de rede entre múltiplos servidores.
C) Criação de backups regulares dos dados armazenados.
D) Utilização de criptografia simétrica para proteger os dados transmitidos.
E) Implementação de autenticação multifatorial para todos os usuários.

6. Qual das seguintes práticas de segurança é utilizada especificamente para evitar ataques de negação de serviço (DDoS) em servidores que hospedam serviços críticos?

A) Implementação de criptografia assimétrica para todas as comunicações de rede.
B) Implementação de senhas fortes para todos os usuários do sistema.
C) Configuração de firewalls para monitorar e controlar o tráfego de entrada e saída.
D) Criação de backups regulares dos dados armazenados em servidores críticos.
E) Uso de redes de distribuição de conteúdo (CDNs) para balancear o tráfego.

7. No contexto de segurança da informação, a confidencialidade é um dos principais pilares. Suponha que uma empresa esteja preocupada com a proteção de dados sensíveis durante a transmissão pela internet. Qual das seguintes estratégias seria a mais eficaz para garantir que apenas os destinatários autorizados possam acessar as informações transmitidas?

A) Implementação de uma política de senhas fortes para todos os funcionários.
B) Realização de backups regulares dos dados para prevenir perda de informações.
C) Uso de firewalls para monitorar e controlar o tráfego de entrada e saída na rede da empresa.
D) Criptografia das informações utilizando um algoritmo de chave pública, como RSA, para garantir que apenas os destinatários com a chave privada correspondente possam descriptografar os dados.
E) Utilização de software antivírus para proteger contra malware.

8. A integridade dos dados é crucial para a confiança nas transações eletrônicas. Imagine um sistema de pagamento online que necessita garantir que os dados das transações não sejam alterados durante a transmissão. Qual método seria mais apropriado para assegurar essa integridade?

A) Utilização de um algoritmo de criptografia simétrica para proteger os dados durante a transmissão.
B) Implementação de uma função hash, como SHA-256, para gerar um resumo dos dados que pode ser verificado tanto pelo remetente quanto pelo destinatário.
C) Instalação de firewalls para proteger a rede contra acessos não autorizados.
D) Implementação de políticas de senha forte para todos os usuários do sistema.
E) Criação de backups regulares dos dados transacionais.

9. Quando se considera a implementação de controles de segurança em uma organização, qual dos seguintes controles é especificamente classificado como controle administrativo e por que ele é importante?

A) Implementação de software antivírus para detectar e remover malware.
B) Aplicação de criptografia em dados armazenados e transmitidos.
C) Configuração de firewalls para proteger a rede contra acessos não autorizados.
D) Uso de câmeras de segurança para monitorar as instalações físicas.
E) Treinamento de conscientização de segurança para todos os funcionários da empresa.

10. Qual dos seguintes é um exemplo de ataque que compromete a disponibilidade de um sistema?

A) Interceptação de e-mails durante a transmissão.
B) Modificação não autorizada de dados.
C) Acesso não autorizado a informações confidenciais.
D) Ataque de negação de serviço (DDoS).
E) Falsificação de certificados digitais.

GABARITOS E COMENTÁRIOS

1. O que caracteriza um certificado digital emitido por uma Autoridade Certificadora (AC)?

A) Ele contém a chave privada do titular.
B) Ele é usado exclusivamente para criptografar dados.
C) Ele é gerado automaticamente por qualquer dispositivo conectado à internet.
D) Ele garante a disponibilidade dos dados na rede.
E) Ele certifica a identidade do titular e contém a chave pública.

Gabarito: E

Comentários: Um certificado digital emitido por uma AC certifica a identidade do titular e contém a chave pública, permitindo a autenticação e a comunicação segura.

2. Em relação à Cifra de César, qual alternativa é verdadeira?

A) Trata-se de um algoritmo de criptografia simétrica que realiza a rotação das posições das letras do alfabeto.
B) É uma modalidade de criptografia impossível de ser quebrada.
C) Teve seu primeiro uso difundido durante a Primeira Guerra Mundial.
D) Utiliza o método de chave privada para cifrar e chave pública para decifrar.
E) É um algoritmo de criptografia assimétrica.

Gabarito: A

Comentários: A Cifra de César é conhecida por ser um dos métodos mais antigos de criptografia, sendo um tipo de criptografia de substituição, em que cada letra na mensagem original é 'rotacionada' um certo número de posições no alfabeto.

3. Em que situação a criptografia assimétrica é geralmente preferida à criptografia simétrica?

A) Para criptografar grandes volumes de dados em tempo real.
B) Para garantir a integridade de grandes bases de dados.
C) Para autenticação e troca segura de chaves.
D) Para proteger dados armazenados em dispositivos móveis.
E) Para criptografar e-mails internamente em uma organização.

Gabarito: C

Comentários: A criptografia assimétrica é geralmente preferida para autenticação e troca segura de chaves devido à segurança adicional proporcionada pelo uso de um par de chaves (pública e privada).

4. Qual a utilização preferencial da criptografia de chave pública (assimétrica)?

A) Para transmitir grandes volumes de dados de forma segura.
B) Na geração de assinaturas digitais.
C) Na configuração de redes privadas virtuais (VPN).
D) Na autenticação de usuários em uma rede local.
E) Na codificação de mensagens de correio eletrônico.

Gabarito: B

Comentários: A criptografia de chave pública (assimétrica) é preferencialmente utilizada na geração de assinaturas digitais. As assinaturas digitais usam a chave privada de um usuário para criptografar os dados. Uma vez que esta chave é única para cada usuário, a assinatura digital ajuda a verificar a identidade do remetente e a garantir que os dados não foram alterados durante a transmissão.

5. Qual dos seguintes métodos seria o mais apropriado para garantir a disponibilidade dos serviços online de uma organização em caso de um ataque DDoS, assegurando que os usuários legítimos ainda possam acessar os recursos?

A) Implementação de firewalls para bloquear tráfego de rede malicioso.
B) Uso de redes de distribuição de conteúdo (CDNs) para distribuir o tráfego de rede entre múltiplos servidores.
C) Criação de backups regulares dos dados armazenados.
D) Utilização de criptografia simétrica para proteger os dados transmitidos.
E) Implementação de autenticação multifatorial para todos os usuários.

Gabarito: B

Comentários: O uso de redes de distribuição de conteúdo (CDNs) ajuda a mitigar os efeitos de um ataque DDoS, distribuindo o tráfego de rede entre múltiplos servidores e mantendo a disponibilidade dos serviços.

6. Qual das seguintes práticas de segurança é utilizada especificamente para evitar ataques de negação de serviço (DDoS) em servidores que hospedam serviços críticos?

A) Implementação de criptografia assimétrica para todas as comunicações de rede.
B) Implementação de senhas fortes para todos os usuários do sistema.
C) Configuração de firewalls para monitorar e controlar o tráfego de entrada e saída.
D) Criação de backups regulares dos dados armazenados em servidores críticos.
E) Uso de redes de distribuição de conteúdo (CDNs) para balancear o tráfego.

Gabarito: E

Comentários: O uso de redes de distribuição de conteúdo (CDNs) ajuda a distribuir o tráfego de rede e a evitar que um único servidor seja sobrecarregado, mitigando os efeitos de um ataque de negação de serviço (DDoS).

7. No contexto de segurança da informação, a confidencialidade é um dos principais pilares. Suponha que uma empresa esteja preocupada com a proteção de dados sensíveis durante a transmissão pela internet. Qual das seguintes estratégias seria a mais eficaz para garantir que apenas os destinatários autorizados possam acessar as informações transmitidas?

A) Implementação de uma política de senhas fortes para todos os funcionários.
B) Realização de backups regulares dos dados para prevenir perda de informações.
C) Uso de firewalls para monitorar e controlar o tráfego de entrada e saída na rede da empresa.
D) Criptografia das informações utilizando um algoritmo de chave pública, como RSA, para garantir que apenas os destinatários com a chave privada correspondente possam descriptografar os dados.
E) Utilização de software antivírus para proteger contra malware.

Gabarito: D

Comentários: A criptografia das informações utilizando um algoritmo de chave pública, como RSA, é uma estratégia eficaz para garantir que apenas os destinatários autorizados, que possuem a chave privada correspondente, possam acessar e descriptografar as informações transmitidas.

8. A integridade dos dados é crucial para a confiança nas transações eletrônicas. Imagine um sistema de pagamento online que necessita garantir que os dados das transações não sejam alterados durante a transmissão. Qual método seria mais apropriado para assegurar essa integridade?

A) Utilização de um algoritmo de criptografia simétrica para proteger os dados durante a transmissão.
B) Implementação de uma função hash, como SHA-256, para gerar um resumo dos dados que pode ser verificado tanto pelo remetente quanto pelo destinatário.
C) Instalação de firewalls para proteger a rede contra acessos não autorizados.
D) Implementação de políticas de senha forte para todos os usuários do sistema.
E) Criação de backups regulares dos dados transacionais.

Gabarito: B

Comentários: A implementação de uma função hash, como SHA-256, é a abordagem mais adequada para garantir a integridade dos dados, pois gera um resumo fixo dos dados que pode ser verificado pelo remetente e destinatário para assegurar que os dados não foram alterados.

9. Quando se considera a implementação de controles de segurança em uma organização, qual dos seguintes controles é especificamente classificado como controle administrativo e por que ele é importante?

A) Implementação de software antivírus para detectar e remover malware.
B) Aplicação de criptografia em dados armazenados e transmitidos.
C) Configuração de firewalls para proteger a rede contra acessos não autorizados.
D) Uso de câmeras de segurança para monitorar as instalações físicas.
E) Treinamento de conscientização de segurança para todos os funcionários da empresa.

Gabarito: E

Comentários: O treinamento de conscientização de segurança para todos os funcionários é um controle administrativo crucial. Ele educa os funcionários sobre as melhores práticas de segurança, políticas da empresa e como reconhecer e responder a possíveis ameaças, reduzindo significativamente os riscos de erro humano.

10. Qual dos seguintes é um exemplo de ataque que compromete a disponibilidade de um sistema?

A) Interceptação de e-mails durante a transmissão.
B) Modificação não autorizada de dados.
C) Acesso não autorizado a informações confidenciais.
D) Ataque de negação de serviço (DDoS).
E) Falsificação de certificados digitais.

Gabarito: D

Comentários: Um ataque de negação de serviço (DDoS) compromete a disponibilidade de um sistema ao sobrecarregar o servidor com tráfego, tornando os recursos inacessíveis para usuários legítimos.

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

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.