TI MAPEADA · 300 MAPAS MENTAIS DE TI

Módulo 05

Segurança da Informação



30 mapas · mapas 122 a 151

Neste módulo:

122 Princípios da Segurança
123 Ameaça, Vulnerabilidade e Risco
124 Malwares
125 Engenharia Social
126 DoS e DDoS
127 Ataques de Rede
128 Criptografia Simétrica
129 Criptografia Assimétrica
130 Funções Hash
131 Assinatura Digital
132 Certificado Digital
133 ICP-Brasil e PKI
134 SSL/TLS
135 Firewall
136 IDS e IPS
137 DMZ
138 Autenticação e MFA
139 Controle de Acesso
140 OAuth 2.0, OpenID e SAML
141 Backup
142 ISO/IEC 27001
143 ISO/IEC 27002
144 Gestão de Riscos
145 Continuidade de Negócios
146 OWASP Top 10
147 SQL Injection e XSS
148 Gestão de Incidentes
149 Pentest
150 SIEM e SOC
151 Zero Trust

Princípios da Segurança

O QUE É

Propriedades que a segurança da informação busca garantir.

1 Confidencialidade

- só quem pode acessa

2 Integridade

- dado não alterado indevidamente

3 Disponibilidade

- acesso quando necessário

4 Autenticidade

- origem confirmada

5 Não repúdio

- autor não pode negar a autoria

⚠ CAI EM PROVA

A tríade CID é confidencialidade, integridade e disponibilidade.

Material de estudo e revisão · uso pessoal

Ameaça, Vulnerabilidade e Risco

O QUE É

Conceitos básicos da análise de segurança.

1 Ativo

- tudo que tem valor para a organização

2 Vulnerabilidade

- fraqueza explorável

3 Ameaça

- causa potencial de incidente

4 Risco

- probabilidade vezes impacto

5 Controle

- medida que reduz o risco

⚠ CAI EM PROVA

Ameaça explora vulnerabilidade; sem vulnerabilidade, a ameaça não tem efeito.

Material de estudo e revisão · uso pessoal

Malwares

O QUE É

Softwares maliciosos que causam danos ou roubam dados.

1 Vírus

- precisa de hospedeiro e execução

2 Worm

- se propaga sozinho pela rede

3 Trojan

- parece legítimo
- abre acesso

4 Ransomware

- cifra dados e pede resgate

5 Outros

- spyware
- keylogger
- rootkit
- botnet

⚠ CAI EM PROVA

Worm se replica sem precisar de arquivo hospedeiro.

Engenharia Social

O QUE É

Manipulação de pessoas para obter informações ou acessos.

1 Phishing

- mensagem falsa em massa

2 Spear phishing

- alvo específico

3 Whaling

- mira executivos

4 Vishing e smishing

- por voz e por SMS

5 Pretexting

- história inventada para ganhar confiança

⚠ CAI EM PROVA

Engenharia social explora o fator humano, não falhas técnicas.

Material de estudo e revisão · uso pessoal

DoS e DDoS

O QUE É

Ataques que tentam tornar um serviço indisponível.

1 DoS

- origem única

2 DDoS

- muitas origens
- botnets

3 Volumétricos

- UDP flood
- amplificação DNS

4 Protocolo

- SYN flood
- ping da morte

5 Aplicação

- HTTP flood

⚠ CAI EM PROVA

DDoS ataca a disponibilidade.

Ataques de Rede

O QUE É

Ataques que interceptam ou falsificam comunicações.

1 Man-in-the-middle

- intermediário intercepta

2 Sniffing

- captura de pacotes

3 Spoofing

- falsifica IP, MAC, DNS ou e-mail

4 Session hijacking

- rouba a sessão

5 Replay

- reenvia mensagens capturadas

⚠ CAI EM PROVA

Criptografia de ponta a ponta dificulta o man-in-the-middle.

Material de estudo e revisão · uso pessoal

Criptografia Simétrica

O QUE É

Usa a mesma chave para cifrar e decifrar.

1 Algoritmos

- AES
- DES
- 3DES
- Blowfish

2 AES

- blocos de 128 bits
- chaves 128, 192 ou 256

3 Vantagem

- rápida

4 Problema

- distribuir a chave com segurança

5 Modos

- ECB
- CBC
- GCM

⚠ CAI EM PROVA

DES é considerado inseguro por ter chave de 56 bits.

Material de estudo e revisão · uso pessoal

Criptografia Assimétrica

O QUE É

Usa par de chaves: pública e privada.

1 Algoritmos

- RSA
- ECC
- Diffie-Hellman

2 Confidencialidade

- cifra com a pública do destinatário

3 Assinatura

- cifra o hash com a privada do remetente

4 Vantagem

- resolve a troca de chaves

5 Desvantagem

- mais lenta

⚠ CAI EM PROVA

Para sigilo usa-se a chave pública do destinatário.

Material de estudo e revisão · uso pessoal

Funções Hash

O QUE É

Geram resumo de tamanho fixo e são de mão única.

1 Propriedades

- irreversível
- resistente a colisão

2 Algoritmos

- SHA-256
- SHA-3

3 Fracos

- MD5
- SHA-1

4 Uso

- integridade
- senhas
- assinatura digital

5 Senhas

- com salt e funções lentas como bcrypt

⚠ CAI EM PROVA

Hash garante integridade, não confidencialidade.

Assinatura Digital

O QUE É

Mecanismo que garante autenticidade, integridade e não repúdio.

1 Passo 1

- gera o hash da mensagem

2 Passo 2

- cifra o hash com a chave privada

3 Verificação

- decifra com a chave pública e compara

4 Garante

- autenticidade
- integridade
- não repúdio

5 Não garante

- confidencialidade

⚠ CAI EM PROVA

Assinatura digital sozinha não garante sigilo.

Certificado Digital

O QUE É

Documento eletrônico que liga uma chave pública a uma identidade.

1 Padrão

- X.509

2 Conteúdo

- chave pública
- titular
- validade
- emissor

3 Emissor

- autoridade certificadora assina o certificado

4 Tipos ICP-Brasil

- A1 (software)
- A3 (token ou cartão)

5 Revogação

- LCR e OCSP

⚠ CAI EM PROVA

O certificado contém a chave pública, nunca a privada.

Material de estudo e revisão · uso pessoal

ICP-Brasil e PKI

O QUE É

Infraestrutura de chaves públicas que dá validade jurídica a documentos digitais.

1 AC Raiz

- ITI, topo da cadeia

2 AC

- autoridade certificadora emite certificados

3 AR

- autoridade de registro valida a identidade

4 Base legal

- MP 2.200-2/2001

5 Cadeia de confiança

- raiz
- intermediárias
- usuário

⚠ CAI EM PROVA

A AR identifica o titular; quem emite o certificado é a AC.

SSL/TLS

O QUE É

Protocolos que protegem a comunicação na camada de transporte.

1 Garante

- confidencialidade
- integridade
- autenticação do servidor

2 Handshake

- negocia algoritmos e troca chaves

3 Versões atuais

- TLS 1.2 e 1.3

4 Obsoletos

- SSL 2 e 3
- TLS 1.0 e 1.1

5 Uso

- HTTPS
- e-mail seguro
- VPN

⚠ CAI EM PROVA

O TLS usa assimétrica para trocar a chave e simétrica para os dados.

Material de estudo e revisão · uso pessoal

Firewall

O QUE É

Controla o tráfego entre redes conforme regras.

1 Filtro de pacotes

- IP, porta e protocolo
- sem estado

2 Stateful

- acompanha o estado das conexões

3 Proxy de aplicação

- inspeciona a camada 7

4 NGFW

- inspeção profunda
- aplicações
- IPS integrado

5 WAF

- protege aplicações web

⚠ CAI EM PROVA

Firewall stateful sabe se o pacote pertence a uma conexão válida.

IDS e IPS

O QUE É

Sistemas de detecção e de prevenção de intrusão.

1 IDS

- detecta e alerta
- passivo

2 IPS

- detecta e bloqueia
- em linha

3 Assinatura

- compara com ataques conhecidos

4 Anomalia

- desvio do comportamento normal

5 Local

- NIDS na rede
- HIDS no host

⚠ CAI EM PROVA

Detecção por anomalia pode achar ataques novos, mas gera mais falsos positivos.

Material de estudo e revisão · uso pessoal

DMZ

O QUE É

Zona desmilitarizada: rede intermediária para serviços expostos.

1 Hospeda

- web
- e-mail
- DNS públicos

2 Objetivo

- isolar a rede interna

3 Arquitetura

- um firewall com 3 interfaces ou dois firewalls

4 Regra

- Internet acessa a DMZ, não a rede interna

5 Bastion host

- servidor reforçado exposto

⚠ CAI EM PROVA

Comprometer a DMZ não deve dar acesso direto à rede interna.

Material de estudo e revisão · uso pessoal

Autenticação e MFA

O QUE É

Comprovar a identidade de usuários e sistemas.

1 Algo que sabe

- senha
- PIN

2 Algo que tem

- token
- celular
- cartão

3 Algo que é

- biometria

4 MFA

- fatores de categorias diferentes

5 SSO

- um login para vários sistemas

⚠ CAI EM PROVA

Senha mais PIN não é MFA: os dois são algo que você sabe.

Controle de Acesso

O QUE É

Define quem pode acessar o quê e como.

1 DAC

- dono do recurso decide

2 MAC

- rótulos e níveis definidos pelo sistema

3 RBAC

- permissões por papel

4 ABAC

- atributos e contexto

5 Princípios

- menor privilégio
- segregação de funções

⚠ CAI EM PROVA

No MAC o usuário não consegue alterar as permissões.

OAuth 2.0, OpenID e SAML

O QUE É

Padrões de autorização e identidade federada.

1 OAuth 2.0

- autorização delegada
- access token

2 Papéis OAuth

- dono
- cliente
- servidor de autorização
- recurso

3 OpenID Connect

- autenticação sobre OAuth
- ID token JWT

4 SAML

- SSO com asserções em XML

5 JWT

- token assinado
- cabeçalho, payload e assinatura

⚠ CAI EM PROVA

OAuth 2.0 é de autorização; quem autentica é o OpenID Connect.

Material de estudo e revisão · uso pessoal

Backup

O QUE É

Cópias de segurança para recuperar dados.

1 Completo

- copia tudo

2 Incremental

- muda desde o último backup de qualquer tipo

3 Diferencial

- muda desde o último completo

4 Regra 3-2-1

- 3 cópias
- 2 mídias
- 1 fora do local

5 Restauração

- testar sempre

⚠ CAI EM PROVA

Restaurar incremental exige o completo e todos os incrementais.

ISO/IEC 27001

O QUE É

Norma certificável de requisitos de um sistema de gestão de segurança (SGSI).

1 Ciclo

- PDCA de melhoria contínua

2 Cláusulas

- 4 a 10 obrigatórias

3 Anexo A

- 93 controles na versão 2022

4 Temas do Anexo A

- organizacionais
- pessoas
- físicos
- tecnológicos

5 Declaração de aplicabilidade

- controles escolhidos e por quê

⚠ CAI EM PROVA

A 27001 é certificável; a 27002 é guia de boas práticas.

ISO/IEC 27002

O QUE É

Guia de boas práticas de controles de segurança da informação.

1 Versão 2022

- 93 controles em 4 temas

2 Organizacionais

- 37 controles

3 Pessoas

- 8 controles

4 Físicos

- 14 controles

5 Tecnológicos

- 34 controles

⚠ CAI EM PROVA

A 27002 não é certificável.

Gestão de Riscos

O QUE É

Processo de identificar, analisar, avaliar e tratar riscos.

1 Normas

- ISO 27005
- ISO 31000

2 Etapas

- contexto
- identificação
- análise
- avaliação
- tratamento

3 Tratamento

- mitigar
- transferir
- evitar
- aceitar

4 Risco residual

- o que sobra após o tratamento

5 Apoio

- comunicação e monitoramento contínuos

⚠ CAI EM PROVA

Contratar seguro é transferir o risco.

Material de estudo e revisão · uso pessoal

Continuidade de Negócios

O QUE É

Manter as operações críticas durante e após um desastre.

1 BIA

- análise de impacto nos negócios

2 RTO

- tempo máximo para voltar a operar

3 RPO

- perda máxima de dados aceitável

4 Planos

- PCN
- plano de recuperação de desastres

5 Sites

- hot
- warm
- cold

⚠ CAI EM PROVA

RPO mede dados perdidos; RTO mede tempo parado.

Material de estudo e revisão · uso pessoal

OWASP Top 10

O QUE É

Lista das falhas de segurança web mais críticas.

1 A01

- quebra de controle de acesso

2 A02

- falhas criptográficas

3 A03

- injeção, incluindo XSS

4 Outras

- design inseguro
- configuração incorreta
- componentes vulneráveis

5 Versão

- 2021

⚠ CAI EM PROVA

Na edição 2021, quebra de controle de acesso subiu para o primeiro lugar.

SQL Injection e XSS

O QUE É

Ataques que injetam código em aplicações.

1 SQL injection

- comandos SQL em entradas do usuário

2 Defesa SQL

- consultas parametrizadas
- menor privilégio

3 XSS

- script malicioso no navegador da vítima

4 Tipos XSS

- refletido
- armazenado
- DOM

5 CSRF

- força ação com a sessão da vítima

⚠ CAI EM PROVA

Consultas parametrizadas são a principal defesa contra SQL injection.

Material de estudo e revisão · uso pessoal

Gestão de Incidentes

O QUE É

Tratamento de eventos que comprometem a segurança.

1 Etapas

- preparação
- detecção
- contenção
- erradicação
- recuperação

2 Pós-incidente

- lições aprendidas

3 CSIRT

- equipe de resposta a incidentes

4 Evento x incidente

- incidente tem efeito adverso

5 Evidências

- cadeia de custódia

⚠ CAI EM PROVA

Nem todo evento de segurança é um incidente.

Material de estudo e revisão · uso pessoal

Pentest

O QUE É

Teste de invasão autorizado para encontrar vulnerabilidades.

1 Black box

- sem informação prévia

2 Gray box

- informação parcial

3 White box

- acesso total à informação

4 Fases

- reconhecimento
- varredura
- exploração
- relatório

5 Ferramentas

- Nmap
- Metasploit
- Burp Suite

⚠ CAI EM PROVA

Pentest exige autorização formal; sem ela é crime.

Material de estudo e revisão · uso pessoal

SIEM e SOC

O QUE É

Monitoramento centralizado de eventos de segurança.

1 SIEM

- coleta e correlaciona logs

2 SOC

- equipe que monitora 24x7

3 SOAR

- automatiza respostas

4 Threat intelligence

- informação sobre ameaças

5 EDR

- detecção e resposta nos endpoints

⚠ CAI EM PROVA

O SIEM correlaciona eventos de várias fontes para gerar alertas.

Material de estudo e revisão · uso pessoal

Zero Trust

O QUE É

Modelo que não confia em ninguém por padrão, dentro ou fora da rede.

1 Lema

- nunca confie, sempre verifique

2 Princípios

- menor privilégio
- assumir violação

3 Microssegmentação

- rede dividida em pequenas zonas

4 Verificação contínua

- identidade
- dispositivo
- contexto

5 Referência

- NIST SP 800-207

⚠ CAI EM PROVA

No Zero Trust estar dentro da rede não dá confiança automática.