📚 Anotações para Estudo - Segurança em Sistemas de Informação

🎯 1. Conceitos Fundamentais

Definição de Segurança em Sistemas de Informação

- Conjunto de **práticas, políticas, processos e tecnologias** para proteger dados, sistemas, redes e recursos organizacionais
- Objetivo: garantir **Confidencialidade, Integridade e Disponibilidade** (Tríade CIA)
- É um **processo contínuo**, não apenas uma ferramenta pontual

🔐 Tríade CIA - Base de Tudo!

C - Confidencialidade

- **Conceito**: Apenas pessoas autorizadas acessam informações
- **Exemplo prático**: Criptografia de senhas no banco de dados
- **Lembre-se**: "Quem pode ver?"

I - Integridade

- **Conceito**: Dados permanecem corretos e sem alterações indevidas
- **Exemplo prático**: Controle de versão (Git) para arquivos
- **Lembre-se**: "Os dados estão corretos?"

A - Disponibilidade

- **Conceito**: Sistemas acessíveis quando necessário
- **Exemplo prático**: Servidores com redundância
- **Lembre-se**: "Está funcionando quando preciso?"

⚠️ 2. Vulnerabilidades e Ameaças

O que são Vulnerabilidades?

Pontos fracos que podem ser explorados para causar danos.

Tipos Principais:

1. **Falhas de Software**

    - Bugs não corrigidos
    - Falta de atualizações
    - *Exemplo*: WannaCry (2017) - explorou falha do Windows
2. **Configurações Inseguras**
    - Senhas fracas
    - Portas abertas desnecessariamente
    - Permissões excessivas
3. **Falha Humana**
    - Funcionários enganados por phishing
    - Comportamentos inseguros
4. **Infraestrutura Frágil**
    - Ausência de firewall
    - Falta de backups
    - Sistemas sem redundância

🔴 Uso Indevido dos Sistemas

Tipos:

- **Interno**: Funcionário copiando base de clientes
- **Externo**: Hacker invadindo servidor
- **Misto**: Parceiro acessando além do permitido

Impactos:

- Perdas financeiras diretas
- Danos à reputação
- Multas (LGPD no Brasil, GDPR na Europa)

💼 3. Valor Empresarial da Segurança

Por que Investir em Segurança?

Não é gasto, é INVESTIMENTO estratégico!

Benefícios:

- **Proteção da Reputação**: Evita perda de credibilidade
- **Continuidade Operacional**: Reduz paralisações
- **Conformidade Legal**: Evita multas e processos
- **Confiança**: Atrai mais clientes e parceiros

Exemplo Real:

E-commerce com certificado SSL → mais confiança → mais vendas

🛡️ Tipos de Controles

Preventivos (Evitam problemas)

- Firewalls
- Autenticação multifator
- Políticas de senha

Detectivos (Identificam problemas)

- Sistemas de auditoria
- IDS (Detecção de Intrusão)
- Monitoramento

Corretivos (Resolvem problemas)

- Backups
- Planos de recuperação
- Restauração de sistemas

🏗️ 4. Estrutura para Segurança Organizacional

6 Etapas Essenciais:

1. 📊 **Análise de Riscos**
    - Identificar ativos críticos
    - Mapear vulnerabilidades
    - Avaliar impactos
2. 📋 **Definição de Políticas**
    - Regras documentadas
    - Responsabilidades claras
    - Penalidades definidas
3. ⚙️ **Implementação de Controles**
    - Ferramentas técnicas
    - Práticas operacionais
4. 🎓 **Treinamento de Usuários**
    - Conscientização
    - Educação continuada
5. 👁️ **Monitoramento e Auditoria**

    - Supervisão contínua
    - Relatórios regulares
6. 🚨 **Plano de Contingência**
    - Procedimentos de emergência
    - Recuperação rápida

🛠️ 5. Tecnologias e Ferramentas

Ferramentas Básicas:

- **Firewall**: Barreira contra acessos não autorizados
- **Antivírus/Antimalware**: Detecta e remove ameaças
- **IDS/IPS**: Detecção e prevenção de intrusão
- **Criptografia**: Codifica informações sensíveis
- **VPN**: Túnel seguro para comunicação
- **Controle de Acesso**: MFA, biometria, cartões

Tecnologias Avançadas:

- **SIEM**: Centraliza análise de eventos de segurança
- **Backup em Nuvem**: Redundância geográfica
- **Sandboxing**: Ambiente isolado para testes
- **Machine Learning**: Detecção inteligente de ameaças

🦠 6. Malware e Ameaças Avançadas

Tipos de Malware:

Vírus

- Infecta arquivos
- Precisa ser executado
- Se propaga através de outros programas

Worms

- Se espalha automaticamente pela rede
- **Não precisa** ser executado manualmente
- Explora vulnerabilidades do sistema

Trojan Horse (Cavalo de Troia)

- Disfarçado de software legítimo
- Executa ações maliciosas ocultas
- Exemplo: "presente" por email

Spyware

- Monitora atividades do sistema
- Envia informações para terceiros
- Coleta dados sem conhecimento do usuário

Keyloggers

- Registra teclas digitadas
- Captura senhas e dados sensíveis
- Pode ser software ou hardware

🎭 Outras Ameaças:

Hackers vs Crackers

- **Hacker**: Especialista em tecnologia (nem sempre criminoso)
- **Cracker**: Usa conhecimento para fins ilegais

Ataques Comuns:

- **Cibervandalismo**: Alteração não autorizada de páginas
- **Spoofing**: Falsificação de identidade/site
- **Sniffing**: Interceptação de tráfego de rede
- **DoS/DDoS**: Sobrecarga de sistemas para indisponibilidade
- **Botnets**: Redes de dispositivos infectados controlados remotamente

---

📝 Dicas para Memorização:

Para a Tríade CIA:

- **C**onfidencialidade = **C**riptografia
- **I**ntegridade = **I**nalterado
- **A**vailability = **A**cessível

Para Controles:

- **P**reventivo = **P**revine problemas
- **D**etectivo = **D**escobre problemas
- **C**orretivo = **C**orrige problemas

Para Malware:

- **Vírus** = precisa de **hospedeiro**
- **Worms** = se **espalha sozinho**
- **Trojan** = se **disfarça**
- **Spyware** = **espiona**
- **Keylogger** = registra **teclas**