# Lista de exercícios – Semana 3

# Exercícios Teóricos

**1. Conceitos da Tríade CIA**
Explique com suas palavras o que significa cada letra da Tríade CIA e forneça um exemplo prático de cada uma.

---

**2. Vulnerabilidades e Ameaças**
Liste e descreva três tipos principais de vulnerabilidades em sistemas de informação, dando um exemplo real para cada uma.

---

**3. Controles de Segurança**
Diferencie os controles preventivos, detectivos e corretivos, citando pelo menos um exemplo de cada.

---

**4. Valor Empresarial da Segurança**
Por que investir em segurança de TI é considerado um investimento estratégico e não apenas um gasto? Cite dois benefícios para a empresa.

---

# Exercícios Práticos

**5. Identificação de Malware**

Para cada tipo de malware abaixo, indique suas características principais e como ele se propaga:

a) Vírus
b) Worm
c) Trojan Horse
d) Spyware
e) Keylogger

---

**6. Cenário de Vulnerabilidade**

Um funcionário recebe um e-mail de phishing e clica em um link malicioso, comprometendo sua senha de acesso ao sistema da empresa.

a) Qual componente da Tríade CIA foi violado?
b) Que tipo de vulnerabilidade foi explorada?
c) Que controle poderia ter prevenido o incidente?

---

**7. Aplicação de Ferramentas de Segurança**

Associe cada ferramenta a sua função principal:

| | |
|---|---|
| a) Firewall | 1) Detecta e previne intrusões na rede |
| b) IDS/IPS | 2) Codifica informações sensíveis |
| c) VPN | 3) Centraliza e analisa eventos de segurança |
| d) Criptografia | 4) Túnel seguro para comunicação remota |
| e) SIEM | 5) Barreira contra acessos não autorizados |

---

**8. Estrutura de Segurança Organizacional**

Organize as 6 etapas essenciais de um plano de segurança em ordem lógica de implementação:

- Monitoramento e Auditoria
- Análise de Riscos
- Treinamento de Usuários
- Definição de Políticas
- Implementação de Controles
- Plano de Contingência

# Gabarito – Segurança em Sistemas de Informação

**1. Conceitos da Tríade CIA**

- **Confidencialidade (C):** Somente pessoas autorizadas têm acesso à informação.
  *Exemplo:* Criptografia de senhas no banco de dados.
- **Integridade (I):** Garantia de que os dados permanecem corretos e não foram alterados indevidamente.
  *Exemplo:* Controle de versão (Git) para arquivos de código.
- **Disponibilidade (A):** Sistemas e dados acessíveis quando necessário.
  *Exemplo:* Servidores com redundância e alta disponibilidade.

---

**2. Vulnerabilidades e Ameaças**

- **Falhas de Software:** Bugs não corrigidos ou falta de atualizações.
  *Exemplo:* WannaCry explorou vulnerabilidade do Windows.
- **Configurações Inseguras:** Senhas fracas, portas abertas, permissões excessivas.
  *Exemplo:* Servidor de banco de dados com senha “123456”.
- **Falha Humana:** Funcionário cai em phishing ou executa ação insegura.
  *Exemplo:* Envio de informações sensíveis para e-mail errado.

---

**3. Controles de Segurança**

- **Preventivos:** Evitam que problemas ocorram.
  *Exemplo:* Firewall, autenticação multifator, políticas de senha.
- **Detectivos:** Identificam problemas ou incidentes.
  *Exemplo:* IDS (detecção de intrusão), auditoria de logs, monitoramento.
- **Corretivos:** Corrigem problemas após a ocorrência.
  *Exemplo:* Backups, planos de recuperação de desastres, restauração de sistemas.

---

**4. Valor Empresarial da Segurança**

- Segurança é um investimento estratégico porque protege os ativos críticos da organização e garante continuidade operacional.
- **Benefícios:**
  1. Proteção da reputação e confiança do cliente.
  2. Continuidade operacional e conformidade legal, evitando multas.

---

**5. Identificação de Malware**

| Tipo de Malware | Características | Propagação / Exemplo |
|---|---|---|
| Vírus | Infecta arquivos, precisa ser executado | Executando programa infectado |
| Worm | Se espalha automaticamente, explora vulnerabilidades | Rede ou internet |
| Trojan Horse | Disfarçado de software legítimo, executa ações maliciosas | Download ou e-mail |
| Spyware | Monitora atividades, envia dados para terceiros | Instalado sem consentimento |
| Keylogger | Registra teclas digitadas, captura senhas | Software ou hardware instalado |

---

**6. Cenário de Vulnerabilidade**

- **Tríade CIA violada:** Confidencialidade.
- **Tipo de vulnerabilidade:** Falha humana / Engenharia social (phishing).
- **Controle preventivo aplicável:** Autenticação multifator (MFA), treinamento de conscientização de segurança.

---

**7. Aplicação de Ferramentas de Segurança**

| Ferramenta | Função Principal |
|---|---|
| Firewall | 5) Barreira contra acessos não autorizados |
| IDS/IPS | 1) Detecta e previne intrusões na rede |
| VPN | 4) Túnel seguro para comunicação remota |
| Criptografia | 2) Codifica informações sensíveis |
| SIEM | 3) Centraliza e analisa eventos de segurança |

---

**8. Estrutura de Segurança Organizacional – Ordem Lógica**

1. **Análise de Riscos**
2. **Definição de Políticas**
3. **Implementação de Controles**
4. **Treinamento de Usuários**
5. **Monitoramento e Auditoria**
6. **Plano de Contingência**

---