Atividade em Grupo (3 pessoas) – Introdução aos Princípios de Segurança da Informação

Tema da Semana 1

- Apresentação da disciplina
- Conceitos e princípios básicos de Segurança da Informação (CID – Confidencialidade, Integridade e Disponibilidade)
- Metodologia de ensino e plataformas de apoio

Proposta da Atividade

1. **Formação dos Grupos**: Organizar os estudantes em grupos de 3 integrantes.
2. **Leitura de Cenário**: Cada grupo deverá receber (ou criar) um **cenário fictício** que represente o cotidiano de uma empresa ou situação pessoal onde a informação seja fundamental (ex.: escritório contábil, e-commerce, clínica médica, rede social).
3. **Identificação de Riscos e Conceitos**
    a. **Passo 1**: Ler o cenário e identificar possíveis **riscos e incidentes** de Segurança da Informação, apontando quais princípios (CID – Confidencialidade, Integridade, Disponibilidade) estariam em risco.
    b. **Passo 2**: Listar **ações ou práticas** que poderiam **minimizar** os riscos identificados (por exemplo, uso de senhas fortes, controle de acesso, backup etc.).
4. **Discussão e Conclusões**
    a. Cada grupo, ao final, prepara um **resumo** (escrito ou apresentado oralmente) que destaque:
    a) As vulnerabilidades encontradas no cenário.
    b) As soluções sugeridas, relacionando-as aos princípios de Confidencialidade, Integridade e Disponibilidade.
    b. Se a turma tiver tempo e estrutura, cada grupo pode apresentar rapidamente (2-3 minutos) seu cenário e conclusões, possibilitando que os demais colegas façam comentários ou sugestões adicionais.
5. **Material de Apoio**
    a. **Ementa da disciplina**: para relacionar o que foi discutido aos temas que serão vistos ao longo do semestre.
    b. **Bibliografia básica** (p. ex., artigos curtos ou capítulos introdutórios de livros) para embasar as definições de Segurança da Informação.
    c. **Orientações** da plataforma virtual (SAVA, por exemplo) para que os alunos saibam onde encontrar mais informações e como fazer pesquisas adicionais.

Objetivos de Aprendizagem

- **Compreender na prática** a importância dos princípios de Segurança da Informação (CID).
- **Refletir** sobre situações reais ou simuladas, reconhecendo vulnerabilidades e propondo soluções básicas.
- **Estimular a colaboração** entre os colegas, promovendo trabalho em equipe e a troca de conhecimento.

Duração Sugerida

- **Tempo total**: 30 a 45 minutos
  → 10 minutos para leitura do cenário e brainstorm do grupo
  → 10 a 15 minutos para a elaboração das soluções
  → 10 a 20 minutos para apresentação e discussão entre grupos

A seguir, apresentamos **7 cenários** fictícios que podem ser utilizados como base para a atividade em grupos sobre os princípios da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade):

1. Agência de Marketing Digital

- **Contexto**: Uma pequena agência de marketing digital gerencia perfis de redes sociais para diversos clientes.
- **Desafios**:
  ✓ Equipe de seis pessoas que compartilha o mesmo computador em alguns momentos do dia.
  ✓ Armazenamento de senhas de clientes em planilhas abertas em uma pasta compartilhada na rede interna.
  ✓ Uso de pendrives pessoais para transferir arquivos de campanhas entre os funcionários.

2. Clínica de Fisioterapia

- **Contexto**: Uma clínica de fisioterapia possui prontuários de pacientes em formato digital.
- **Desafios**:
  ✓ Os computadores utilizados pelos fisioterapeutas não possuem bloqueio de tela automático.
  ✓ Os dados dos pacientes (histórico clínico, exames, evolução) são salvos em um único computador sem backup.
  ✓ Wi-Fi da clínica é livre para pacientes e funcionários sem segmentação de rede.

3. E-commerce de Produtos Artesanais

- **Contexto**: Um casal iniciou um pequeno e-commerce de produtos artesanais, vendendo via site próprio.
- **Desafios**:
  - ✓ Falta de certificado SSL no site, o que pode expor dados dos clientes durante a compra.
  - ✓ Armazenamento de informações de cartão de crédito em um servidor sem medidas adequadas de segurança.
  - ✓ Senhas fracas (ou repetidas) para acessar a área de administração do site.

4. Ambiente de Coworking

- **Contexto**: Um espaço de coworking recebe profissionais de diversas áreas que trabalham em salas compartilhadas.
- **Desafios**:
  - ✓ Rede Wi-Fi única para todos os usuários, sem controle de acesso ou autenticação robusta.
  - ✓ Alguns visitantes costumam conectar notebooks desconhecidos e podem compartilhar arquivos sem verificação de vírus.
  - ✓ Equipamentos como impressora e projetor ficam conectados na mesma rede sem quaisquer restrições.

5. Secretaria Municipal

- **Contexto**: Uma secretaria municipal responsável por emitir documentos oficiais e arquivar dados sensíveis da população local.
- **Desafios**:
  - ✓ Empregados frequentemente compartilham logins de um mesmo computador para agilizar o fluxo de trabalho.
  - ✓ Ausência de procedimentos de backup regulares dos arquivos digitais que contêm dados pessoais.
  - ✓ Documentos impressos com dados sensíveis ficam à vista em mesas e não são descartados adequadamente.

6. Startup de Desenvolvimento de Software

- **Contexto**: Uma startup desenvolve um aplicativo para gerenciamento financeiro de empresas.
- **Desafios**:
  - ✓ Parte da equipe trabalha remotamente, acessando servidores críticos via VPN, mas sem verificação de múltiplos fatores de autenticação.

- ✓ O repositório de código-fonte está na nuvem; algumas credenciais de serviços estão hardcoded (inseridas diretamente no código).
- ✓ Logs contendo dados sensíveis de testes são mantidos sem criptografia em pastas públicas do servidor.

7. Rede Doméstica com Smart Devices

- **Contexto**: Uma família possui diversos dispositivos IoT (smart TV, assistente virtual, câmeras de segurança) conectados ao roteador doméstico.
- **Desafios**:
  - ✓ Senha-padrão do roteador nunca foi alterada desde a instalação.
  - ✓ As câmeras de segurança podem ser acessadas remotamente via aplicativo, mas sem segurança adequada (senhas simples e sem atualizações).
  - ✓ O backup de fotos da família é feito apenas em um HDD externo, sem nenhuma solução em nuvem ou criptografia.

Como Utilizar os Cenários

1. **Dividir os grupos** e designar a cada um cenário (ou permitir que escolham).
2. **Leitura/Análise** do cenário: identificar os principais pontos de vulnerabilidade ou risco.
3. **Aplicar os Conceitos CID**: relacionar como a Confidencialidade, Integridade e Disponibilidade podem ser afetadas nessas situações.
4. **Propor Soluções**: cada grupo elabora sugestões para mitigar esses problemas, discutindo boas práticas de segurança e ações efetivas de proteção de dados.