

Lista 01 - Princípios em Segurança da Informação

Professor: Fábio Engel de Camargo
Disciplina: Segurança em Tecnologia da Informação
Meio para entrega: Moodle

1. Encriptar dados em dispositivos de armazenamento ou discos rígidos é uma estratégia principal para garantir integridade de dados.
 - a) Verdadeiro
 - b) Falso**
2. Organizações que exigem que representantes de atendimento a cliente acessem seus dados privados podem melhor proteger a privacidade deles e facilitar acesso a outros dados de clientes usando qual dos seguintes controles de segurança?
 - a) Impedir que representantes de atendimento a clientes acessem seus dados privados.
 - b) Bloquear detalhes de dados privados de clientes e permitir acesso apenas aos quatro últimos dígitos dos números de identidade ou número de conta.
 - c) Encriptar todos os dados do cliente.
 - d) Implementar autenticação de segunda camada ao acessar banco de dados de clientes.
 - e) Todos os anteriores.**
3. Qual dos seguintes controles de segurança pode ajudar a reduzir anexos maliciosos de e-mail?
 - a) Filtragem e quarentena de e-mail
 - b) Varredura de antivírus de anexo de e-mail.
 - c) Comprovação com usuários sobre a confiabilidade da fonte de e-mail.
 - d) Impedimento de toda mensagem de e-mail que chegue com anexos desconhecidos.
 - e) Todos os anteriores.**
4. Encriptar comunicações por e-mail será necessário se você estiver enviando informações confidenciais em uma mensagem de e-mail por meio da Internet pública.
 - a) Verdadeiro**
 - b) Falso

5. Políticas, padrões, procedimentos e diretrizes de segurança ajudam as organizações a diminuir riscos e ameaças.

a) Verdadeiro

b) Falso

6. Identifique o princípio (propriedade) de segurança da informação descrito:

Disponibilidade

- Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

Integridade

- Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Confidencialidade

- Propriedade que limita o acesso a informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Autenticidade

- Propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita

Autenticidade

- Propriedade que garante que a informação é proveniente da fonte anunciada.

7. Supondo que lhe foi dada a tarefa de desenvolver um sistema de *e-commerce*, como você poderia garantir a confidencialidade, integridade e disponibilidade de seu sistema?

Confidencialidade:

Controle de acesso: limitar o acesso aos dados somente às pessoas autorizadas;

Criptografia: proteger as informações por meio de técnicas de criptografia;

Política de segurança: definir e implementar uma política clara de segurança da informação.

Integridade:

Backups: fazer cópias de segurança dos dados para evitar perdas em caso de falhas;

Controle de versões: garantir que apenas as versões autorizadas dos dados sejam utilizadas;

Verificação de integridade: realizar verificações periódicas para garantir que os dados não foram corrompidos ou alterados.

Disponibilidade:

Redundância: ter sistemas de backup ou espelhamento para garantir a disponibilidade do sistema em caso de falhas;

Monitoramento: monitorar constantemente o sistema para identificar falhas e corrigi-las rapidamente;

Planejamento de contingência: ter um plano de contingência para lidar com problemas e minimizar o impacto na disponibilidade do sistema.