**DESEVOLVIMENTO 6 BANCO DE DADOS II**

**No ano de 2022, diversas empresas sofreram tentativas de ataques cibernéticos que poderiam impactar diretamente a segurança dos dados. Portanto, é recomendado que funcionários e clientes de lojas virtuais sempre mantenham suas senhas de acesso atualizadas, alterando-as a cada três meses. Pensando nisso, cite pelo menos três métodos para melhorar essas senhas, com foco em fortalecê-las.**

**Resposta:**

Aqui estão três métodos para fortalecer senhas:

**- Comprimento e Complexidade:** Incentive o uso de senhas longas e complexas, que contenham uma combinação de letras maiúsculas e minúsculas, números, caracteres especiais e símbolos. Quanto maior e mais complexa for a senha, mais difícil será para os hackers quebrá-la usando ataques de força bruta.

**- Autenticação de Dois Fatores (2FA):** Implemente a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança exigindo não apenas uma senha, mas também um segundo fator de autenticação, como um código enviado por SMS, um token de segurança ou uma chave de segurança física.

**- Evitar Informações Pessoais Óbvias:** Instrua os usuários a não utilizar informações pessoais óbvias em suas senhas, como nomes de familiares, datas de nascimento, números de telefone ou endereços. Essas informações são facilmente acessíveis ou podem ser descobertas por meio de redes sociais e outras fontes, tornando as senhas mais vulneráveis a ataques de força bruta e engenharia social.

Ao implementar esses métodos, as senhas dos funcionários e clientes das lojas virtuais serão fortalecidas, reduzindo significativamente o risco de comprometimento da segurança dos dados.