UNIVERSIDADE FEDERAL DA BAHIA
DISCIPLINA: MATA60 – BANCO DE DADOS
DISCENTE: Miguel Santana Fialho Santos (matrícula: 222116289)

PROJETO 1 - DOMÍNIO DE GOVERNANÇA

Link para o GitHub com o projeto: https://github.com/guelfialho/Mata60_ProjetoBD
Vídeo do domínio de governança: https://youtu.be/dSvSkidjI9k

1. POLÍTICA DE BACKUP

A Política de Backup e Restauração de Dados Digitais tem como objetivo estabelecer diretrizes, responsabilidades e competências voltadas à segurança, proteção e disponibilidade dos dados digitais a fim de garantir a continuidade das operações.

Para cumprir essa missão, é essencial implementar mecanismos que permitam a guarda e a recuperação dos dados em situações de indisponibilidade ou perda devido a erro humano, ataques, desastres naturais ou outras ameaças.

Este documento apresenta a Política de Backup e Restauração de Dados Digitais, detalhando o método e a periodicidade de backup dos dados armazenados pelos sistemas computacionais.

2. DECLARAÇÕES DA POLÍTICA

A seguir serão descritas as regras a serem seguidas para garantir a conformidade dos dados e a sua segurança.

PRINCÍPIOS GERAIS

1. **Responsabilidade e Gerenciamento:**
    - A administração da política de backup e recuperação de dados é de responsabilidade da equipe de TI, que deve garantir que os backups sejam realizados de acordo com as diretrizes estabelecidas.
    - Todos os dados críticos devem ser incluídos no plano de backup, e todos os backups devem ser monitorados regularmente para garantir sua integridade e funcionalidade.

2. **Frequência de Backup:**
    - **tbl_categorias, tbl_produtos, tbl_fornecedores, tbl_clientes**: Backup diário, devido à natureza crítica dos dados de cadastro e suas frequentes atualizações.
    - **tbl_produtos_fornecedores, tbl_vendas, tbl_avaliacoes, tbl_interesses, tbl_enderecos**: Backup diário para garantir a preservação de dados transacionais e informações de interesse dos clientes.

3. **Estratégia de Preservação:**
    - **Backup Completo**: Realizado semanalmente para todas as tabelas, armazenando todos os dados existentes em um novo arquivo de backup.
    - **Backup Incremental**: Realizado diariamente, capturando apenas os dados que mudaram desde o último backup completo.
    - **Backup Diferencial**: Realizado a cada dois dias, armazenando todas as alterações feitas desde o último backup completo.

4. **Temporalidade e Retenção:**
    - **tbl_categorias, tbl_produtos, tbl_fornecedores, tbl_clientes**: Retenção mínima de 1 ano para backups completos, permitindo a recuperação de dados por um período extenso.
    - **tbl_produtos_fornecedores, tbl_vendas, tbl_avaliacoes, tbl_interesses, tbl_enderecos**: Retenção mínima de 6 meses, suficiente para garantir a preservação de transações e interações recentes.

5. **Mídia de Backup:**
    - Os backups serão armazenados em mídias diversas para reduzir o risco de perda de dados:
        - **Armazenamento em Nuvem**: Backup diário com criptografia de ponta-a-ponta.
        - **Discos Externos**: Backup semanal mantido fora do local de operação principal (off-site) para recuperação em caso de desastres.
        - **Fitas Magnéticas**: Backup mensal, armazenado em local seguro e de difícil acesso, garantindo uma camada adicional de segurança.

6. **Plano de Recuperação:**
    - Um **Plano de Recuperação de Desastres (DRP)** deverá ser estabelecido e testado semestralmente para assegurar que todos os sistemas críticos possam ser restaurados dentro de um prazo aceitável.
    - O DRP incluirá procedimentos para a recuperação dos seguintes cenários:
        - **Perda Parcial de Dados**: Recuperação de dados perdidos em tabelas específicas, com verificação de integridade.
        - **Perda Total de Dados**: Restauração completa do banco de dados a partir do backup mais recente.
        - **Desastre Natural ou Físico**: Ativação do backup off-site para recuperação completa do ambiente operacional.

7. **Demonstração e Auditoria:**
    - Relatórios de backup devem ser gerados após cada operação, documentando o sucesso ou falha do processo.
    - Auditores internos ou externos deverão revisar os relatórios de backup trimestralmente para garantir conformidade com a política e detectar possíveis melhorias.

8. **Treinamento e Conscientização:**
    - A equipe de TI será regularmente treinada sobre as melhores práticas de backup e recuperação.
    - Todos os funcionários devem estar cientes da importância do backup e seguir as políticas de governança estabelecidas.