1. **Objetivo**
   Garantir a proteção dos dados pessoais e sensíveis armazenados no sistema, bem como definir diretrizes para controlar o acesso às informações e funcionalidades, de modo a cumprir as legislações vigentes, como a LGPD (Lei Geral de Proteção de Dados).

2. **Princípios Fundamentais**

    - **Confidencialidade**: Os dados armazenados devem ser acessíveis apenas a usuários autorizados conforme seu nível de acesso.
    - **Integridade**: Garantir que os dados sejam precisos e não sejam alterados de forma não autorizada.
    - **Disponibilidade**: As informações e funcionalidades devem estar disponíveis para os usuários autorizados sempre que necessário.
    - **Transparência**: Informar aos titulares dos dados como suas informações serão utilizadas.
3. **Perfis de Acesso**
   Os níveis de acesso foram definidos para garantir a segurança e a funcionalidade do sistema:

    - **ADM (Administrador do Sistema)**:

        - Acesso total a todas as tabelas e funcionalidades do sistema.
        - Responsável pela gestão de usuários, auditoria de atividades e resolução de problemas.
        - Pode criar, alterar, excluir e visualizar todos os registros.
    - **Responsável**:

        - Acesso completo às tabelas relacionadas a eventos, inscrições, atividades e usuários.
        - Permissão para visualizar, cadastrar, alterar e excluir informações nessas tabelas.
        - **Restrições**: Não pode acessar ou alterar dados da tabela de pagamentos (TAB_PAGAMENTO).
    - **Usuário**:

        - Permissão apenas para **visualizar** dados das tabelas de usuários (TAB_USUARIO) e atividades (TAB_ATIVIDADE).
        - Não pode realizar alterações ou acessar informações de outras tabelas.
4. **Proteção dos Dados Pessoais**

    - **Dados Sensíveis**: Informações como CPF, nome social, escolaridade e dados sobre deficiência serão armazenados de forma criptografada.

- **Consentimento**: Todos os dados pessoais só serão coletados com o consentimento explícito do titular.
- **Retenção**: Os dados serão armazenados pelo tempo necessário para os fins definidos, sendo excluídos após o término do uso ou mediante solicitação do titular.
- **Acesso Restrito**:
  - Administradores têm acesso irrestrito aos dados sensíveis.
  - Responsáveis podem acessar dados pessoais exceto os relacionados à tabela de pagamentos.
  - Usuários não têm acesso a dados sensíveis.

5. **Gestão de Credenciais**

   - Autenticação obrigatória para acesso ao sistema.
   - **Senhas**:
     - Devem ser fortes, com comprimento mínimo de 8 caracteres, contendo letras, números e caracteres especiais.
     - Troca obrigatória a cada 90 dias.
   - **2FA (Autenticação em Dois Fatores)**: Disponível para Administradores e Responsáveis.
   - Bloqueio de contas após 5 tentativas de login mal-sucedidas.
6. **Segurança das Transações**

   - **Pagamentos**:
     - Apenas Administradores podem acessar informações completas relacionadas aos pagamentos.
     - Responsáveis e Usuários não têm acesso a dados financeiros sensíveis.
   - Conexões criptografadas (HTTPS) são obrigatórias para todas as transações.
7. **Controle de Certificados**

   - Certificados estarão disponíveis apenas para participantes que cumprirem os critérios estabelecidos.
   - Organizadores podem consultar os certificados relacionados aos eventos sob sua responsabilidade.
8. **Auditoria e Logs**

   - Todas as operações no sistema serão registradas, incluindo:
     - Data, hora, usuário e tipo de ação.
   - Apenas Administradores têm acesso completo aos logs.
   - Logs serão revisados periodicamente para identificar acessos não autorizados.
9. **Direitos dos Titulares de Dados**

   - Os titulares poderão solicitar:
     - Acesso aos seus dados pessoais.
     - Correção de informações imprecisas ou incompletas.

        - Exclusão de seus dados, desde que não estejam em uso para fins legais ou contratuais.
        - Revogação do consentimento para o uso de seus dados a qualquer momento.

10. **Responsabilidades dos Usuários**

    - Os usuários devem manter suas credenciais seguras e não compartilhá-las.
    - É proibido acessar ou tentar acessar informações para as quais o usuário não tenha permissão explícita.

11. **Penalidades para Descumprimento**

    - Violações das políticas de acesso ou privacidade resultarão em:
        - Suspensão ou revogação do acesso ao sistema.
        - Comunicação aos órgãos competentes em casos de violação da lei.
        - Ações legais, conforme aplicável.

12. **Revisão e Atualização**

    - A política será revisada anualmente ou sempre que houver mudanças significativas no sistema ou na legislação aplicável.

Observações

- Esta política foi ajustada para refletir os níveis de acesso configurados no PostgreSQL para os usuários **ADM**, **Responsavel** e **Usuario**, garantindo que as permissões estejam alinhadas aos papéis e responsabilidades de cada perfil.
-