Política de Mapeamento e Uso de Dados — Projeto MERURU TCG

1. Introdução

Esta política tem como objetivo estabelecer as diretrizes de **mapeamento, tratamento e proteção de dados pessoais** no âmbito do projeto **MERURU TCG**, garantindo conformidade com a **Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 — LGPD)**.

O documento descreve as práticas adotadas para coleta, classificação, armazenamento, transformação e compartilhamento de informações relacionadas a **funcionários e usuários internos do sistema**, considerando aspectos de segurança, auditoria e governança de dados.

2. Dados Pessoais Protegidos pela LGPD

A LGPD protege qualquer informação relacionada a uma pessoa física identificada ou identificável. No contexto do MERURU TCG, são considerados dados pessoais os **identificadores diretos**, como nome, e-mail e ID do usuário, bem como **identificadores indiretos**, como endereço IP, cookies e registros de acesso.

Não há necessidade de coleta de dados sensíveis, tais como CPF, religião, orientação sexual ou outros atributos pessoais que não sejam estritamente necessários para o funcionamento do sistema.

3. Criptografia e Hashing

Para garantir a integridade e a confidencialidade das informações, todas as senhas devem ser armazenadas por meio de **hash seguro**, utilizando **BCrypt** , conforme já implementado pelo **Spring Security**.

Tokens de sessão e refresh tokens devem ser armazenados **criptografados ou hashed**, a fim de evitar vazamentos ou uso indevido.
Em casos excepcionais, dados adicionais como e-mails poderão ser criptografados antes de sua persistência no banco de dados, reforçando a proteção contra acesso não autorizado.

4. Logs e Auditoria

A legislação determina que sejam mantidos **registros de acesso e de operações** realizadas sobre dados pessoais.
No MERURU TCG, o backend em **Spring Boot** utilizar um sistema nativo para registrar automaticamente as ações realizadas por cada usuário.

Os logs são considerados dados sensíveis, uma vez que podem conter informações capazes de identificar indivíduos, como endereços IP, timestamps, IDs de usuários ou e-mails de login.
Esses registros devem ser tratados de forma restrita, observando os princípios de **minimização, anonimização, retenção limitada e segurança**.

4.1 Princípios Aplicáveis aos Logs

- **Anonimização ou pseudonimização:** substituir identificadores diretos por códigos irreversíveis em logs técnicos.
- **Retenção limitada:** manter registros pelo prazo máximo de seis meses a um ano, com exclusão ou anonimização automática após o período.
- **Segurança e controle de acesso:** garantir que apenas administradores de segurança e auditores devidamente autorizados possam visualizar logs, que devem ser armazenados em banco seguro e nunca expostos em endpoints públicos.

5. Boas Práticas Complementares

Para aprimorar o controle e a conformidade, o projeto adota as seguintes práticas:

- **Centralização dos logs** em ferramentas como ELK Stack ou Loki, facilitando auditoria e monitoramento.
- **Separação entre logs técnicos e de auditoria**, garantindo que erros de sistema não exponham dados pessoais.
- **Criptografia de IPs e IDs** para reduzir o risco de reidentificação.
- **Notificação interna sobre coleta de dados**, garantindo transparência aos funcionários.
- **Controle de acesso baseado em função (RBAC)**, permitindo que apenas administradores visualizem registros sensíveis.

6. Práticas Proibidas

São expressamente vedadas as seguintes condutas:

- Manter logs indefinidamente, em violação ao princípio da retenção limitada;
- Registrar o corpo completo de requisições, que pode conter informações sensíveis;
- Compartilhar logs ou dados pessoais com terceiros sem contrato formal e cláusulas de proteção de dados;
- Permitir o download bruto de logs, prática que aumenta o risco de vazamentos.

7. Aplicação Prática no Sistema MERURU TCG

A implementação desta política ocorre de forma integrada em todas as camadas do sistema:

- **Banco de dados:** armazenamento de senhas criptografadas e anonimização de usuários excluídos.
- **Backend (Spring Boot):** auditoria de ações, controle de consentimento e uso de papéis (roles) para autorização.
- **Frontend:** exibição de política de privacidade e coleta explícita de consentimento do usuário por meio de checkbox.
- **Infraestrutura (Docker):** uso de HTTPS, isolamento seguro de logs.
- **Administração:** disponibilização de endpoint para deleção ou anonimização de usuários, garantindo o direito ao esquecimento.

8. Conclusão

Esta política estabelece os fundamentos para a **governança, segurança e tratamento ético de dados pessoais** dentro do projeto MERURU TCG. Seu propósito é assegurar que todas as informações coletadas sejam tratadas com **transparência, responsabilidade e conformidade legal**, promovendo um ambiente digital seguro e confiável.

O cumprimento desta política é obrigatório para todos os colaboradores, desenvolvedores e administradores que tenham acesso aos sistemas ou dados do MERURU TCG.