**Políticas e Diretrizes de Governança de Dados Pessoais**

Este relatório tem como objetivo apresentar um conjunto de políticas e diretrizes para a governança de dados pessoais aplicáveis a órgãos governamentais, com base na Lei Geral de Proteção de Dados Pessoais (LGPD), nas normas ISO pertinentes e nos entendimentos da Autoridade Nacional de Proteção de Dados (ANPD). Os princípios e recomendações aqui apresentados são fundamentados nas políticas de privacidade da Caesb, SERPRO e PGDF além das melhores práticas em conformidade com regulamentações nacionais e internacionais.

**1. Introdução**

A governança de dados pessoais é fundamental para garantir a privacidade e a proteção dos direitos dos titulares dos dados. Este relatório estabelece diretrizes gerais para a implementação de um sistema robusto de governança, com base nos princípios da LGPD, nas normas ISO 27701 (Sistema de Gestão de Privacidade da Informação) e ISO 27001 (Sistema de Gestão de Segurança da Informação), além das regulamentações da ANPD.

**2. Princípios Fundamentais de Governança de Dados**

**2.1 Finalidade e Necessidade**

A coleta e o tratamento de dados pessoais devem ser realizados para propósitos legítimos, específicos, explícitos e informados ao titular, limitando-se ao mínimo necessário para atingir essas finalidades. O tratamento posterior deve ser compatível com a finalidade informada ao titular, conforme previsto na LGPD.

**2.2 Descrição das Hipóteses de Tratamento de Dados**

Artigo 7º, Inciso III

* **Obrigações trabalhistas e previdenciárias**: Dados de funcionários e colaboradores podem ser tratados para cumprimento de exigências legais, como a gestão de folha de pagamento, recolhimento de impostos e contribuições sociais.
* **Exigências fiscais e contábeis**: Tratamento de dados para atender obrigações de auditoria, prestação de contas e outras normativas exigidas por legislações aplicáveis à administração pública ou empresas privadas.

Artigo 7º, Parágrafo V

* **Execução de contratos**: Tratamento de dados para execução de contratos firmados com terceiros ou cidadãos.
* **Proteção ao crédito**: Tratamentos relacionados à garantia do crédito, quando aplicável.

Artigo 23

**Execução de políticas públicas**: Tratamento de dados realizado pela Administração Pública para a execução de políticas públicas previstas em leis, regulamentos, ou quando delegadas à unidade por órgãos competentes.

* **Proteção da segurança pública e nacional**: Tratamento de dados necessários para garantir a segurança pública, defesa nacional e prevenção de crimes.

Para exemplificar:

* **Cadastro de cidadãos** para políticas públicas (saúde, educação, programas sociais);
* **Armazenamento de dados** para garantir transparência e prestação de contas nas políticas públicas;
* **Compartilhamento de dados** com outras entidades públicas ou privadas para execução de políticas interinstitucionais.

Essas bases legais garantem que o tratamento de dados seja feito de maneira adequada, atendendo às normativas específicas da LGPD, e sempre respeitando os princípios da transparência, segurança, e minimização de dados.

**2.3 Transparência e Livre Acesso**

Os titulares de dados pessoais têm o direito de obter informações claras e acessíveis sobre como seus dados estão sendo tratados. Devem ser garantidos mecanismos de livre acesso para consulta sobre os dados armazenados e o tratamento a que estão sujeitos.

**2.4 Qualidade dos Dados**

A precisão, clareza, relevância e atualização dos dados devem ser asseguradas pelos responsáveis pelo tratamento, para que os dados sejam mantidos exatos e adequados às finalidades propostas.

**2.5 Segurança**

Medidas técnicas e administrativas apropriadas devem ser implementadas para garantir a segurança dos dados pessoais, prevenindo acessos não autorizados, perdas acidentais ou ilícitas, além de situações de alteração, destruição ou comunicação indevida de dados.

**2.5.1 Decreto distrital nº 45.771 - art. 20.**

A segurança da informação é um aspecto central da Lei Geral de Proteção de Dados.

* **Identificar e proteger dados pessoais** contra ameaças e vulnerabilidades de segurança.
* **Detectar, responder e recuperar** de incidentes de segurança, incluindo violações de dados pessoais, em conformidade com as obrigações da LGPD.
* **Controles técnicos e organizacionais** que ajudam a assegurar a proteção dos dados pessoais.
* **Estratégias de monitoramento e auditoria** para avaliar a eficácia das medidas de segurança implementadas.

**2.5.2 Plano de Resposta a Incidentes (Decreto Distrital nº 45.771 - art. 21, III)**

Estabelecer um plano claro e estruturado para identificar, responder, mitigar e relatar incidentes de segurança da informação, garantindo a proteção dos dados pessoais e a conformidade com a LGPD, com o objetivo de minimizar o impacto de incidentes de segurança, garantir a integridade, assegurar a notificação adequada às partes interessadas e restaurar as operações normais da organização.

**2.5.3 Regra Geral Sobre Compartilhamento de Dados**

O compartilhamento de dados pessoais com terceiros, internos ou externos à organização, deverá ser realizado apenas quando estritamente necessário para o cumprimento de finalidades legítimas, de acordo com as bases legais previstas na Lei Geral de Proteção de Dados (LGPD).

**2.6 Prevenção**

Devem ser adotadas medidas proativas para evitar a ocorrência de danos relacionados ao tratamento de dados, mediante práticas preventivas que garantam a segurança da informação e a continuidade operacional.

**2.6 Responsabilização e Prestação de Contas**

O agente de tratamento de dados deve demonstrar a adoção de medidas eficazes para garantir a conformidade com a LGPD, além de prestar contas à ANPD e a outros órgãos competentes sempre que solicitado.

**3. Conformidade com a LGPD e Regulamentações Pertinentes**

**3.1 Agentes de Tratamento de Dados**

A governança de dados pessoais envolve a clara definição dos papéis de controladores e operadores, em conformidade com a LGPD. Controladores são responsáveis pelas decisões sobre o tratamento dos dados, enquanto operadores executam o tratamento em nome dos controladores.

**3.2 Encarregado de Dados (DPO)**

O Encarregado de Proteção de Dados deve atuar como elo entre a organização, os titulares dos dados e a ANPD, sendo responsável por garantir a conformidade com a legislação e por prestar esclarecimentos aos titulares sobre o tratamento de seus dados.

**3.3 Relatório de Impacto à Proteção de Dados (RIPD)**

O RIPD deve ser elaborado para processos que possam gerar riscos aos direitos dos titulares, descrevendo medidas de mitigação e mecanismos de segurança implementados.

**4. Implementação das Políticas de Governança de Dados**

**4.1 Gestão da Privacidade da Informação**

Com base na norma ISO 27701, recomenda-se a implementação de um Sistema de Gestão de Privacidade da Informação (SGPI), que garanta a segurança dos processos que envolvem o tratamento de dados pessoais, desde a coleta até a eliminação dos dados.

**4.2 Ferramentas e Tecnologias de Proteção de Dados**

Os órgãos devem adotar ferramentas que garantam a proteção da privacidade, como criptografia, controle de acesso baseado em funções (RBAC), e o uso de sistemas de detecção e prevenção de intrusões. Também é essencial monitorar continuamente o ambiente tecnológico para identificar vulnerabilidades.

**4.3 Treinamento e Capacitação**

A educação, o treinamento e a conscientização dos colaboradores sobre as boas práticas de segurança da informação e proteção de dados são fundamentais. Programas contínuos de capacitação devem ser implementados para garantir que todos os envolvidos no tratamento de dados estejam cientes de suas responsabilidades.

**4.4 Mecanismos de Auditoria e Monitoramento**

A auditoria periódica dos processos de tratamento de dados deve ser realizada para garantir a conformidade com as normas e regulamentos, identificando possíveis falhas e implementando melhorias contínuas no sistema de governança.

**5. Monitoramento e Avaliação**

O monitoramento da conformidade com as políticas de privacidade deve ser contínuo, com avaliações periódicas da eficácia das medidas adotadas. A governança deve incluir relatórios regulares para a alta administração e para a ANPD, conforme requerido.

**5.1 Comitê de Proteção de Dados Pessoais**

Com o objetivo de garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais e promover uma cultura de proteção de dados na organização, será instituído um Comitê de Proteção de Dados Pessoais, que terá as seguintes responsabilidades e estrutura:

1. Responsável por supervisionar a implementação de políticas de proteção de dados, monitorar a conformidade com a LGPD, apoiar o Encarregado de Proteção de Dados em incidentes e comunicação com a ANPD, além de promover a conscientização sobre privacidade e proteção de dados entre colaboradores e partes interessadas.
2. Responsável por avaliar e aprovar políticas, supervisionar medidas de proteção de dados, apoiar na resposta a incidentes e comunicação com a ANPD, acompanhar auditorias e promover treinamentos e campanhas de conscientização sobre a proteção de dados.
3. Produzir relatórios periódicos para a alta administração, apresentando o status da conformidade com a LGPD, incidentes de segurança, ações corretivas e a eficácia dos controles de proteção de dados.

É importante prever que o documento seja revisado periodicamente, além de estabelecer a necessidade expressa de aprovação e publicação pela alta direção do órgão.

**6. Conclusão**

A implementação de um robusto sistema de governança de dados pessoais é essencial para garantir a conformidade com a LGPD e proteger os direitos dos titulares. Este relatório oferece um guia abrangente para órgãos governamentais no desenvolvimento de políticas que assegurem a segurança, privacidade e proteção de dados, promovendo a transparência e a confiança dos cidadãos