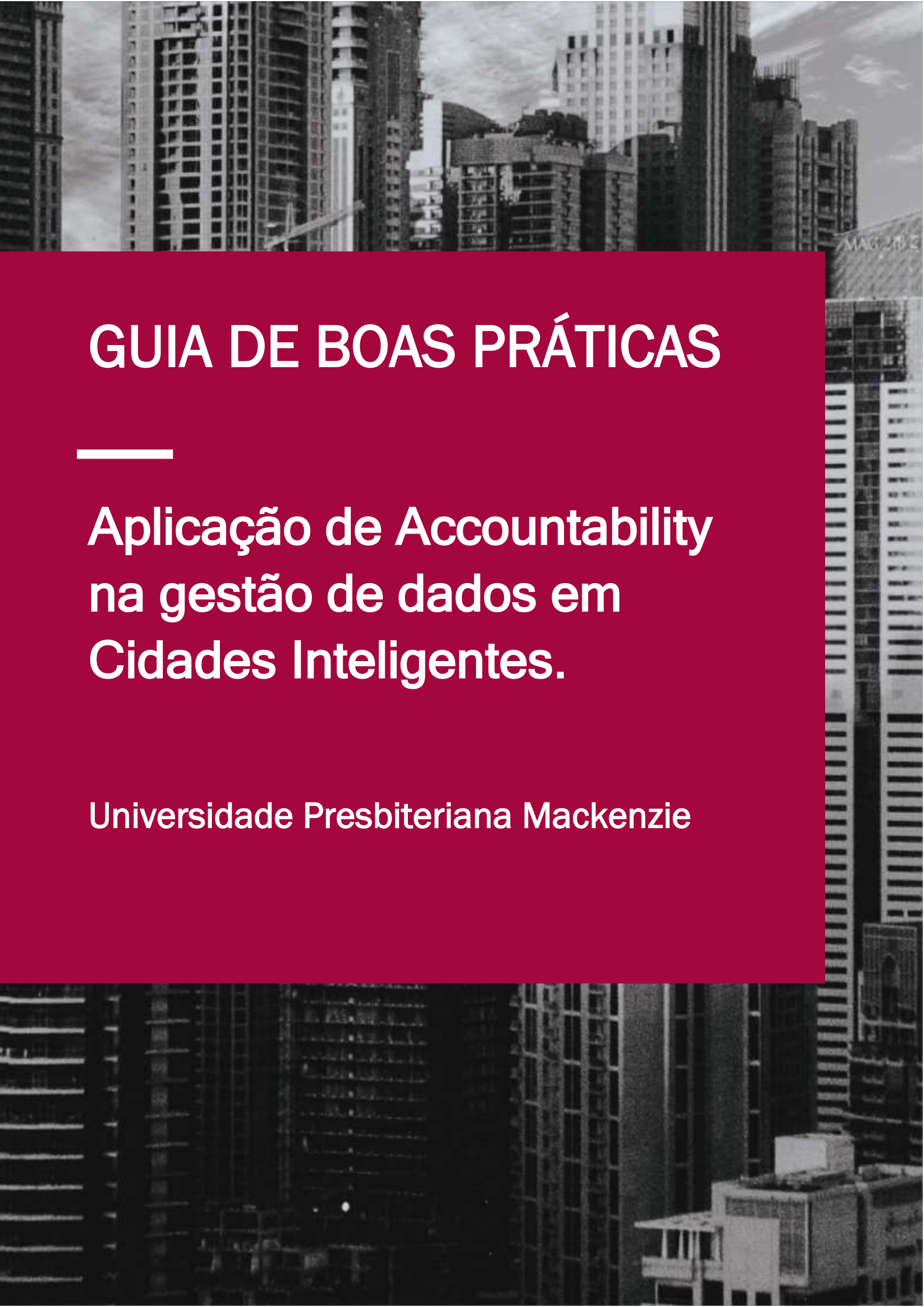

GUIA DE BOAS PRÁTICAS

Aplicação de Accountability na gestão de dados em Cidades Inteligentes.

Universidade Presbiteriana Mackenzie

Guia de Boas Práticas: Aplicação de Accountability na gestão dos dados em Cidades Inteligentes.

INTRODUÇÃO

Como já dito na Constituição da República Federativa do Brasil (1988): "Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta constituição". Diante do exposto, entende-se que as entidades do setor público e indivíduos nelas presentes são responsáveis pela forma como são geridos os recursos públicos, uma vez que estão exercendo suas funções com a finalidade de representação dos interesses coletivos.

O termo accountability surge neste contexto e consiste no dever que um órgão e/ou Instituição tem de prestar contas, em decorrência das responsabilidades oriundas de uma delegação de poder. O princípio do accountability implica que o controlador de dados deve aplicar as medidas técnicas e organizacionais adequadas para cumprir e demonstrar a conformidade com os regulamentos aplicáveis à proteção de dados pessoais, tendo em conta o risco que o seu tratamento acarreta.

No centro desse movimento, parece estar a crescente habilidade de utilizar dados para melhorar os serviços oferecidos pelos governos locais. Nas cidades inteligentes estes dados são usados em tempo real para controlar e orientar de várias maneiras ou funções de rotina que esses sistemas usam. Entretanto, apesar dos benefícios que podem propiciar para a vida nas cidades, as atividades de coleta e tratamento de dados levantam preocupações com a privacidade dos cidadãos. Isso porque potencializam significativamente as possibilidades de utilização desses dados para finalidades que atendam aos interesses de diversos outros atores, tanto do setor público como do setor privado.

A QUEM O GUIA É DIRECIONADO E COMO DEVE SER UTILIZADO?

A proposta deste Guia de Boas Práticas é auxiliar entidades do setor público e indivíduos nelas presentes, na aplicação e execução do princípio accountability durante a manipulação e gestão de dados em uma Cidade Inteligente. Sua utilização consiste no entendimento e na implementação das boas práticas citadas no decorrer do guia para garantir aos cidadãos a segurança de que, ao optar por uma Cidade Inteligente, seus dados/privacidade estarão seguros e serão regidos pelo princípio de accountability – responsabilidade, ética e transparência. O principal objetivo deste guia é promover o accountability como prática padrão na privacidade de dados em cidades inteligentes e como uma questão estratégica de negócios e conformidade legal.

BOAS PRÁTICAS: APLICAÇÃO DE ACCOUNTABILITY NA GESTÃO DE DADOS EM CIDADES INTELIGENTES

O accountability é mundialmente reconhecido como um bloco-chave para a regulação eficaz da privacidade de dados e sua implementação correspondente. É considerado como uma jornada e um processo de gerenciamento de mudanças internas para incorporar a privacidade de dados no DNA da instituição, sendo necessário um esforço contínuo impulsionado por avaliações contínuas de risco e a necessidade de melhoria constante, que exige que as instituições se adaptem constantemente a fatores internos e externos; abordar mudanças regulatórias, legais e tecnológicas; e mitigar novos riscos.

- **Responsabilidade;**

É imprescindível que os colaboradores entendam que proteger dados pessoais e praticar o uso responsável de dados é um esforço coletivo e responsabilidade de todos (e não apenas da responsabilidade dos oficiais de privacidade e das equipes jurídicas). Quando a responsabilidade se torna uma prática de trabalho, o comportamento de accountability provoca uma mudança real de cultura na organização e aumenta a confiabilidade com os titulares dos dados (cidadãos), administradores de dados (funcionários) e instituições relacionadas.

- **Transparência:**

O objetivo fundamental da transparência baseia-se na construção de canais de comunicação fortes e eficazes, facilitando a compreensão dos titulares dos dados, especialmente aumentando a clareza, acessibilidade, relevância e pontualidade da comunicação. A transparência desempenha um enorme papel no accountability através do compromisso com as partes interessadas no que diz respeito ao fornecimento e acesso às informações disponíveis.

As principais decisões tomadas devem ser acessíveis ao público em geral através da Internet, no entanto, simplesmente disponibilizar informações é claramente percebido como não suficiente para dar ao público acesso ao porquê e como as decisões podem afetar os cidadãos.

A implementação da transparência implica em comunicar aos indivíduos informações críticas sobre seu programa de privacidade de dados, procedimentos e proteções, bem como os benefícios e/ou potenciais riscos de processamento de dados e informações sobre direitos individuais por meios de fácil acesso (por exemplo, avisos de privacidade, políticas e ferramentas de transparência, como painéis e portais

- **Emissão de Relatórios:**

Publicação de relatórios de transparência sobre o acesso do governo aos dados e desenvolvimento de ferramentas visuais para ajudar as partes interessadas externas a entender melhor como funcionam as atividades de processamento de dados da organização. Colocar informações em sites é relativamente fácil, o esforço empreendido pelas instituições deve ir além do fornecimento de informações e produzir informações que não só sejam acessíveis, mas também avaliadas e bem compreendidas por todas as partes interessadas. Todos as instituições assumem um papel ativo em tornar as informações inteligíveis e utilizáveis pelo público.

- **Compromisso de Líderes:**

Essa prática consiste no compromisso claro e formalizado dos líderes da instituição responsável pela administração dos dados gerados nas cidades inteligentes, com relação a proteção da privacidade destes dados. Deve haver um comprometimento desde o topo da organização, com a elaboração de um código de negócio, práticas e valores institucionais que devem ser seguidos por todos os funcionários. As instituições responsáveis pela gestão dos dados devem comunicar regularmente sobre a importância da privacidade para toda a organização através da intranet, vídeos e e-mails. Em particular, eles também devem envolver-se pessoalmente em atividades de privacidade de dados, como participar da supervisão de reuniões de comitê, solicitando relatórios de privacidade.

- **Treinamentos e Certificados:**

Os funcionários devem receber oportunidades de treinamentos e certificações, permitindo também que eles participem de conferências e eventos de privacidade e se envolva com a comunidade de privacidade mais ampla. Treinamentos e conscientização são elementos-chave para incorporar a privacidade e a responsabilização de dados na cultura das instituições que administram dados públicos.

A implementação consiste em garantir treinamento contínuo e comunicação a funcionários e outros que lidam com dados processados pela organização sobre o programa de privacidade, seus objetivos e controles.

- **Avaliar os riscos de privacidade de dados relacionados a parceiros de negócios:**

Avaliar os riscos relacionados à privacidade dos parceiros de negócios também é importante. Estes incluem fornecedores, clientes ou qualquer outro parceiro com quem a organização possa compartilhar os dados pessoais. Comumente, os oficiais de privacidade trabalham com aquisições para incluir questões de privacidade nos questionários de due diligence existentes. Essas perguntas ajudam os oficiais de privacidade a identificar se o terceiro fornece o nível adequado de proteção de acordo com o risco identificado e para os padrões de proteção da organização que está fragmentando os dados pessoais. O risco é frequentemente medido pela triagem de terceiros em diferentes categorias de alto-médio-baixo risco, dependendo de circunstâncias como: se eles processam grandes volumes de dados pessoais, os tipos de dados processados, as medidas técnicas que eles têm em vigor, se eles tiveram uma recente violação de dados etc. Avaliações mais detalhadas, incluindo visitas no local e revisões de infraestrutura, podem ser realizadas se o terceiro for classificado como de médio ou alto risco. As certificações de segurança, gerenciamento de informações e privacidade também são fatores positivos importantes na avaliação de riscos.

- **Implementação de Políticas de Privacidade**

As políticas de privacidade estabelecem princípios e requisitos que os funcionários devem seguir ao se envolver em atividades de processamento de dados. As organizações também adotam políticas adicionais de privacidade específicas para regiões, países, tipos de negócios, produtos e serviços. As políticas de privacidade são frequentemente alinhadas com padrões externos, como os estabelecidos pela OCDE, LGPD, normas ISO ou qualquer outra lei nacional. As políticas e procedimentos devem ser revisados e atualizados para levar em conta as mudanças comerciais, legais e regulatórias.

A aplicação desta prática consiste em construir e mantém políticas e procedimentos de privacidade de dados que refletem leis, regulamentos, normas, valores e metas organizacionais aplicáveis e implementar mecanismos para operacionalizá-los em toda a organização. Isso inclui políticas e procedimentos para garantir um processamento justo e considerações éticas.

REFERÊNCIAS:

As boas práticas citadas neste guia correspondem à uma coletânea de várias práticas que estão disponíveis nos frameworks ITIL, TOGAF, COBIT, OECD e CIPL.

Desenvolvidor por: Fernando S. Nóbrega, Loren F. Ferreira, Fábio S. Lopes.