5ª Reunião do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade da Prefeitura da Cidade do Rio de Janeiro

10/12/2024

Participantes:

1. Rodrigo Henrique Luiz Corrêa - Presidente do Conselho e representante da Secretaria Municipal de Integridade, Transparência e Proteção de Dados;
2. Ana Paula Vasconcellos - representante da Secretaria Municipal de Integridade, Transparência e Proteção de Dados;
3. Alessandra Almeida Lapa - representante da Secretaria Municipal de Saúde;
4. Bruno Monteiro Bruno - representante da Secretaria Municipal de Educação;
5. Nuno Caminada - representante da Secretaria Municipal de Educação;
6. Antonio Sergio de Oliveira Luiz - representante da Empresa Municipal de Informática - IPLANRIO;
7. André Hermanny Tostes - representante da Procuradoria Geral do Município;
8. Geraldo Abreu - representante da Câmara Municipal do Rio de Janeiro;
9. Carlos Fernando das Chagas - representante do Tribunal de Contas do Município do Rio de Janeiro;
10. Leonardo Perseu da Silva Costa - representante do Instituto Brasileiro de Consumidores e Titulares de Dados - IBCTD;
11. José Lopes Ramos - representante do Instituto Brasileiro de Consumidores e Titulares de Dados - IBCTD;
12. Pedro Teixeira Gueiros - representante do Centro Universitário IBMEC;
13. Erica Bakonyi - representante da Fundação Getúlio Vargas - FGV;
14. Walter B. Gaspar - representante da Fundação Getúlio Vargas - FGV;
15. Fernando Felipe Bourguy de Medeiros - representante do TIRio - Sindicato das Empresas de Informática do RJ;
16. Carlos Alexandre Gonzalez - representante do SINDICONTRIO - Sindicato dos Contabilistas do Município do Rio de Janeiro
17. William Lima Rocha - representante do SINDICONTRIO - Sindicato dos Contabilistas do Município do Rio de Janeiro;
18. Vitor Paludetto - representante da Gafisa S.A;
19. Rodrigo Dias de Pinho Gomes - representante da OAB-RJ;
20. Arthur Almeida - representante do Aqualtune Lab;
21. Theonácio Carvalho de Oliveira Lima Júnior - representante do Sindicato das Empresas de Informática do Rio de Janeiro TIRio;
22. Chiara de Teffé - representante do Instituto Tecnologia e Sociedade - ITS.

Local: Reunião on-line pela plataforma Google Meet, com boas-vindas e registro dos presentes às 10h30min e início às 10h38min.

Pontos debatidos:

A pauta previamente enviada para os Conselheiros foi:

I - Abertura, com aprovação da ata da reunião anterior, enviada previamente por e-mail aos Conselheiros;

II - Aprovação dos relatórios dos Grupos de Trabalho pelos seus relatores;

III - Assuntos gerais e informes; e

IV - Encerramento.

I - Abertura, com aprovação da ata da reunião anterior, enviada previamente por e-mail aos Conselheiros

Em relação ao ponto I, foi apresentada a ata da reunião do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade realizada no dia 05/11/2024. A ata foi previamente enviada para apreciação dos integrantes do Conselho Municipal de Proteção de Dados e da Privacidade através de e-mail enviado pela Conselheira Ana Paula Vasconcellos no dia 03/12/2024.

Durante o tempo de análise da referida ata, não houve solicitações de ajustes pelos presentes Conselheiros, e, portanto, a ata foi aprovada por unanimidade. Após, foi informado que ela seria disponibilizada na página da internet, no site em que constam as informações relativas ao Conselho no seguinte endereço eletrônico: https://lgpd.prefeitura.rio/conselho-protecao-de-dados-e-da-privacidade/.

Debatido este ponto, prosseguiu-se para o próximo item da pauta.

II - Aprovação dos relatórios dos Grupos de Trabalho pelos seus relatores

O Presidente do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade da Prefeitura da Cidade do Rio de Janeiro, Rodrigo Corrêa, parabenizou a qualidade do trabalho que foi desenvolvido através dos relatórios realizados pelos grupos de trabalho e agradeceu o claro engajamento dos Conselheiros na realização de pesquisas aprofundadas sobre os temas propostos.

Os relatórios produzidos pelos Grupos de Trabalho trouxeram contribuições muito ricas. Posteriormente será discutida uma forma de disponibilizar a íntegra dos relatórios. Por hora, o presidente do Conselho propõe que seja disponibilizada uma síntese contendo as recomendações apresentadas nos relatórios, de forma objetiva e clara, que seguirá como anexo a ata desta reunião.

O Presidente do Conselho informou ainda que a ata desta reunião, contendo a síntese dos relatórios em anexo, será disponibilizada no site do Conselho Municipal, a fim de que fiquem disponíveis para a população as ideias principais que foram apresentadas nos documentos analisados, de forma que facilite a leitura e a retenção dos muitos aprendizados disponibilizados.

Dito isto, o Presidente do Conselho procedeu à leitura da redação da síntese dos relatórios, que segue como anexo a esta ata.

Debatido este ponto, prosseguiu-se para o próximo item da pauta.

III - Assuntos gerais e informes

O Presidente informou que o Programa de Governança em Privacidade e Proteção de Dados Pessoais da Prefeitura da Cidade do Rio de Janeiro é finalista do Prêmio Inova Gestão Pública, promovido pela Fundação João Goulart e que assim que tiver notícias do resultado da Premiação, a informação será compartilhada com os membros do Conselho.

IV - Encerramento:

O Presidente do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade informou que a data da próxima reunião será enviada com antecedência para todos os Conselheiros através da Secretaria Geral do Conselho e que a intenção é que ela ocorra dentro do primeiro quadrimestre de 2025.

Debatido este ponto, deu-se por encerrada a reunião do presente Conselho Municipal.

Documento assinado de forma física.

ANEXO I

Síntese das propostas elaboradas pelos Grupos de Trabalho do Conselho Municipal de Proteção de Dados Pessoais e da Privacidade

1. **1. Uso do consentimento como base legal para tratamento de dados pessoais e dados pessoais sensíveis pela Administração Pública municipal.**
   Membros do GT: Pedro Gueiros, Fernanda Paes Leme, Erica Bakonyi, André Tostes, André Roberto, Ana Paula Vasconcellos.
   Relator: Pedro Gueiros.
   Recomendação:
   Embora o consentimento esteja previsto na LGPD como uma base legal aplicável ao tratamento de dados, seu uso pela Administração Pública deve ser cauteloso e considerado apenas em situações em que o titular dos dados tenha efetiva liberdade de escolha e onde a revogação desse consentimento não prejudique a execução de políticas públicas essenciais.

2. **Utilização de dados pessoais e dados pessoais sensíveis na rede municipal de saúde e impactos das novas tecnologias.**
   Membros do GT: Alessandra Lapa, Carlos Alexandre, Vitor Paludetto, Walter B. Gaspar, Fernando Bourguy, Horrara Moreira, Rafael Barbosa.
   Relatora: Alessandra Lapa.
   Recomendações:

- Na interoperabilidade referente à oferta de dados pessoais e sensíveis dos pacientes nos diversos locais deverá haver uma infraestrutura tecnológica que possibilite conectar todos os envolvidos no atendimento do sistema de saúde, como médicos, dentistas, psicoterapeutas, hospitais, farmácias e demais usuários, na medida de privilégio de acesso baseado na necessidade de saber (“need to know basis”).
- Minimização de dados: Somente aqueles dados de saúde que são necessários para o respectivo propósito podem ser coletados e processados. Informações desnecessárias ou supérfluas devem ser evitadas;
  Limitação de finalidade: Dados de saúde podem ser processados somente para as finalidades para as quais foram coletados. O uso para outras finalidades é permitido somente em casos excepcionais e sob certas condições.
- Segurança de dados: Medidas técnicas e organizacionais apropriadas devem ser tomadas para garantir a segurança dos dados de saúde. Isso

inclui medidas como criptografia, controles de acesso e verificações de segurança regulares.

- Processamento terceirizado: se os provedores de serviços processarem dados pessoais em nome dos controladores destes dados (por exemplo, provedores de serviços de TI), eles devem respeitar o contrato de prestação de serviços celebrado, com cláusulas claras e rígidas de confidencialidade e responsabilidade na proteção de dados pessoais e sensíveis dos pacientes;
- Direitos dos titulares dos dados: Os pacientes têm o direito à informação sobre seus dados armazenados, o direito à retificação de dados.
- imprecisos, o direito à exclusão sob certas condições e o direito à portabilidade dos dados, se for o caso.
- Em se tratando de interoperabilidade de prontuários médicos e informações de saúde do paciente, como é o caso do HCI da SMS-Rio, os pacientes deverão ter acesso ao seu HCI quando todas as integrações tiverem sido finalizadas e ter disponível para sua ciência todo o histórico de usuários que acessaram o seu HCI, garantindo assim, a transparência legal.
- Notificação de violação de proteção de dados: No caso de violações de dados que representem um risco aos direitos e liberdades dos titulares dos dados, deverá haver uma comunicação pública e informação clara sobre o ocorrido a ANPD, nos termos da resolução CD/ANPD nº 15/2024.
- Avaliação de impacto na proteção de dados: A Secretaria Municipal de Saúde (SMS-Rio) deverá analisar a pertinência de elaboração de um relatório de impacto de dados pessoais (RIPD) quanto ao processamento de dados de saúde em ambientes de interoperabilidade, avaliando se representa um alto risco para os direitos e liberdades dos titulares dos dados. A integração de sistemas deverá estar condicionada à realização deste relatório, que deverá justificar a sua adequação e necessidade tendo em vista os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
- Em casos de incidentes de segurança de dados pessoais e sensíveis deverá haver um plano de restabelecimento dos serviços, assim como documentação e avaliação sobre as falhas e vulnerabilidades ocorridas e medidas adotadas em resposta. Ademais, deverá haver um plano de contingência para retomada das atividades parcial ou total dos serviços aos pacientes.
- Nos hospitais de médio e grande porte, sob a responsabilidade da Secretaria Municipal de Saúde, deverá haver uma sala de back-up local a fim de garantir a continuidade dos atendimentos, principalmente emergenciais, devido à sua sensibilidade no resultado.

3. **Proteção dos dados pessoais de crianças e adolescentes e boas práticas na rede municipal de educação**
   Membros: Léo Perseu, Horrara Moreira, Chiara de Teffé, Bruno Monteiro, Nuno Caminada, Ana Paula Vasconcellos.
   Relatora: Chiara de Teffé.
   Recomendações:

- Discussão permanente acerca da Política Municipal de Privacidade e Proteção de Dados, envolvendo diferentes atores, e maior amadurecimento do marco institucional já existente no âmbito da administração pública municipal.
- Monitoramento e aperfeiçoamento contínuo das políticas de compartilhamento de dados pessoais com terceiros.
- Capacitação e Sensibilização da Comunidade Escolar: recomenda-se o investimento em capacitação de professores, alunos e responsáveis sobre boas práticas em segurança e proteção de dados pessoais. A conscientização sobre o uso responsável das tecnologias digitais e a adoção de práticas seguras deverão ser integradas ao espaço escolar.
- Conscientização dos Alunos Sobre Privacidade e Proteção de Dados: Educar os alunos sobre a importância da proteção de dados pessoais e da privacidade digital é essencial. Algumas iniciativas podem incluir: a) integrar a educação digital na programação e no currículo escolar; b) promover campanhas escolares e atividades lúdicas, como concursos de desenho ou redação, para engajar os alunos no tema de privacidade e segurança digital; e c) desenvolver, em parceria com organizações especializadas, materiais didáticos e oficinas voltadas para diferentes faixas etárias, focando nos direitos e deveres digitais.
- Aplicação de Sistemas de Gestão Educacional: recomenda-se a adoção, sempre que possível, de sistemas de gestão educacional que utilizam criptografia forte, autenticação multifatorial e outros fatores de segurança para proteger o acesso aos dados dos envolvidos na atividade educacional. Recomenda-se também o estabelecimento de uma governança robusta para a gestão de dados pessoais, com supervisão contínua de um comitê de proteção de dados.

4. **Abertura de dados na Administração Pública municipal, respeitando a LGPD e as diretrizes de proteção de dados pessoais**
   Membros: Ana Paula Vasconcellos, José Lopes, Marco Túlio, Carlos Alexandre, Rafael Moraes, Bruno Monteiro, Rafael Barbosa, William Rocha.
   Relatora: Ana Paula Vasconcellos.
   Recomendações:

- Iniciar o engajamento interno e dar andamento às discussões, com o fortalecimento da atuação dos grupos de trabalho e o fomento para que tais

grupos possam avançar nas discussões. Um exemplo que pode ser aproveitado do caso do Ministério do Desenvolvimento Social é o da realização de reuniões do GT com representantes dos órgãos e entidades, de modo a assegurar que todas as unidades envolvidas estejam alinhadas com a Política de Dados Abertos.

- Publicar uma Política Municipal de Abertura de Dados, em formato de decreto municipal, que estabeleça as diretrizes gerais para direcionar a construção dos Planos de Dados Abertos, nos moldes da Política de Dados Abertos do Poder Executivo Federal, que foi instituída em 2016 através do Decreto nº 8.777, de 11 de maio de 2016.
- Elaborar Inventário/Catálogo de Bases de Dados: considerando que o Inventário de Dados Pessoais é um dos instrumentos do Programa de Governança em Privacidade e Proteção de Dados Pessoais, ele pode ser aperfeiçoado para, a partir dele, gerar o Inventário de Bases de Dados de cada órgão/entidade municipal. É importante que esse processo conte com o envolvimento de todas as unidades do órgão/entidade, em especial do Comitê de Proteção de Dados Pessoais, das Autoridades de Monitoramento da LAI e dos gestores de ativos da informação, assegurando a conformidade com os padrões estabelecidos para a segurança da informação e para a proteção de dados pessoais. O processo de catalogação observado na experiência do MDS pode ser replicado pela Administração Pública municipal carioca.
- Realizar Consulta Pública: considerando as experiências apresentadas, observou-se que a participação social foi um elemento chave para direcionar os esforços de transparência. Dessa forma, é interessante que os Planos de Dados Abertos municipais passem por consultas à população carioca.
- Elaborar Matriz de Priorização: considerando as experiências apresentadas, elaborar a matriz de priorização, levando em consideração fatores como a relevância dos dados para o cidadão, estímulo ao controle social, projetos estratégicos do governo e potencial de fomento à inovação em governos municipais, para construção de cidades mais inteligentes e inclusivas, além do nível de maturidade da base de dados.

5. **Gestão de riscos à privacidade e à proteção de dados pessoais e aperfeiçoamento da *cybersegurança* no âmbito da Administração Pública municipal**
   Membros do GT: José Lopes, Rodrigo Gomes, Dicler Ferreira, Carlos Chagas, Fernando Bourguy, Theo Carvalho, Antônio Sérgio, Pedro Gueiros, Rafael Moraes, Marco Túlio, Fernanda Paes Leme.
   Relator: Rodrigo Pinho.
   Recomendações:

- Recomenda-se que sejam realizadas ações visando à contratação de uma solução automatizada de gestão de privacidade para suporte ao Programa Municipal de Proteção de Dados Pessoais e da Privacidade (Decreto Rio 54.984/2024 e Resolução SEGOVI 91/22).
- Recomenda-se que sejam realizadas ações no sentido de estender este programa visando alcançar os demais agentes públicos municipais, de forma que cada agente, considerando suas competências e responsabilidades no tocante ao tratamento de dados pessoais, possa adquirir os conhecimentos em Proteção de Dados Pessoais que garantam um tratamento em conformidade com toda a regulamentação e legislação vigentes.
- Recomenda-se que sejam realizadas ações pelos Encarregados setoriais e pelos Comitês de Proteção de Dados Pessoais dos órgãos e entidades no sentido de difundir os conhecimentos relativos à proteção de dados pessoais, em especial enfatizando o caráter fundamental dos princípios da finalidade, adequação e necessidade, cruciais a efetiva implantação de uma cultura de minimização de tratamento de dados pessoais. Cabe ressaltar que merecem atenção especial os gestores de sistemas, processos ou de informação, uma vez que são estes agentes que dão materialidade às decisões dos órgãos e entidades, em sua atuação como controladores, quanto ao tratamento de dados pessoais que suportarão seus respectivos processos e serviços.
- Recomenda-se que seja criado e implantado um Programa Municipal de Segurança da Informação nos moldes do Programa Municipal de Proteção de Dados, especificando seus eixos de atuação e a estrutura de governança e gestão que irá suportá-lo. Cabe ressaltar ainda que entende-se imprescindível que os agentes que venham a exercer papéis nesta estrutura de governança e gestão sejam formalmente treinados.
- Identificou-se que a IplanRio está conduzindo um programa de segurança cibernética tendo como base referencial o CIS Controls em sua versão 7.1 (https://www.cisecurity.org/controls/v7), visando à melhoria contínua dos níveis de segurança da rede corporativa municipal. Recomenda-se que a base referencial de suporte ao programa seja atualizada para a versão 8 ou 8.1.
- Recomenda-se que sejam realizadas ações no sentido possibilitar uma expansão contínua do escopo de cobertura da solução de gerenciamento de inventários, tendo como meta alcançar todos os ativos tecnológicos da rede corporativa municipal.
- Recomenda-se que sejam realizadas ações no sentido da criação de um conjunto de artefatos normativos que estabeleça famílias de configuração padronizadas para os equipamentos que compõem as redes dos órgãos e entidades municipais. Estes padrões de configuração deverão ser atendidos por todos os órgãos e entidades quando da aquisição ou atualização de seus equipamentos.

- Recomenda-se ainda que sejam realizadas ações visando à definição formal de critérios de obsolescência para todos os padrões de configuração descritos acima, de forma que estes possam se manter sempre atualizados e, por conseguinte, fomentar nos órgãos e entidades municipais a necessidade de manutenção de um processo de atualização contínuo de seus equipamentos, garantindo sua compatibilidade às soluções de segurança corporativas.
- Recomenda-se que sejam realizadas ações no sentido da criação e implantação de um conjunto de artefatos normativos e operacionais (ex. normas, guias e procedimentos) que possibilitem a classificação das informações tratadas pelo Município com relação a sua sensibilidade, assim como a identificação dos controles a serem implementados durante todo seu ciclo de vida como resultado desta classificação.
- Recomenda-se que as seguintes ações sejam executadas:
  a) A definição e implementação de uma estrutura de suporte à governança e gestão de Segurança da Informação em âmbito municipal, que consiga promover o tratamento do tema por todos os órgãos e entidades.
  b) Valendo-se da estrutura acima, a definição de um programa de conscientização que possa efetivamente chegar a todos os órgãos e entidades.
  c) Considerando o quantitativo de agentes municipais e sua amplitude de distribuição geográfica, recomenda-se a implementação de uma solução automatizada para suporte ao programa de conscientização.
- Recomenda-se que sejam realizadas ações visando à criação e implantação de um Programa de Desenvolvimento Seguro de Software.
- Recomenda-se a contratação de um serviço de Security Operation Center (SOC) que atue em regime de 24x7 e que possa responder de forma imediata aos incidentes de segurança que venham a ser identificados a qualquer tempo.
- Recomenda-se que o GPTRI seja formado por integrantes do provedor do serviço de SOC descrito acima e membros das equipes técnicas da IplanRio, que atuando de forma integrada devem definir e implementar todos os artefatos e processos de suporte à gestão de resposta a incidentes.

6. **Empoderamento Cidadão: análise das melhores práticas em conscientização sobre proteção de dados pessoais e mecanismos de enfrentamento à vulnerabilidade social pela perspectiva da proteção dos dados pessoais e da privacidade**
   Membros do GT: Ana Paula Vasconcellos, Léo Perseu, Horrara, Alessandra Lapa, Walter B. Gaspar, Erica Bakonyi, Carlos Alexandre.
   Co-relatoras: Horrara Moreira e Erica Bakonyi**.**

Recomendações:

- O empoderamento cidadão é um processo que demanda esforço contínuo, com iniciativas sistemáticas que contemplam o envolvimento direto de grupos diversos. Ainda que se reconheçam os desafios e a impossibilidade de conquistar a conscientização de forma homogênea, é essencial iniciar ações de simplificação e orientação da população.
- Realização de atividades de fomento ao empoderamento cidadão como prática contínua.
- Compreensão da vulnerabilidade de forma sistêmica.
- Ampliação do escopo para as chamadas para participação pública, aqui entendidas como mecanismo de aproximação entre instituições públicas e população, bem como de escuta ativa (interlocução atenta e interessada), dedicada à promoção dos direitos da privacidade e da proteção de dados;
- Colaboração entre órgãos públicos, sociedade civil, instituições de ensino e cidadãos.
- Estruturação de Grupo de Trabalho dedicado à documentação e resposta às consultas públicas relacionadas aos programas de conscientização.

Documento assinado de forma física.