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

Gestão de Riscos de Segurança e Privacidade na Administração Pública Municipal

Diagnóstico e Recomendações

2024

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

Gestão de Riscos de Segurança e Privacidade na Administração Pública Municipal – Diagnóstico e recomendações

Composição:

José Lopes
Rodrigo Dias de Pinho Gomes
Dicler Ferreira
Carlos Chagas
Fernando Bourguy
Theonácio Lima Júnior
Antonio Sergio de Oliveira Luiz
Pedro Gueiros
Rafael Moraes
Marco Túlio
Fernanda Paes Leme

Relator:
Rodrigo Dias de Pinheiro Gomes

Sumário

1. Introdução

Na atualidade, cada vez mais organizações de todos os segmentos, sejam estas públicas ou privadas, têm seus processos suportados majoritariamente pelo tratamento de informações por intermédio de ativos tecnológicos, principalmente os ativos de Tecnologia da Informação e Comunicação.

É importante destacar que as informações tratadas por estas organizações muitas vezes consistem de dados pessoais e sensíveis dos indivíduos como RGs, CPFs, nomes, endereços e informações relativas à saúde. Esse tipo de dado requer um nível elevado de proteção para assegurar a privacidade dos cidadãos e o cumprimento das legislações vigentes, como a Lei Geral de Proteção de Dados (LGPD).

Dentro desse novo cenário, amparado pelo poder cada vez maior de armazenamento e processamento das novas tecnologias digitais, a diversidade e quantidade de operações de tratamento de informações, inclusive pessoais e pessoais sensíveis, fazem com que a gestão dos riscos operacionais destas operações torne-se vital à eficiência, eficácia e efetividade das organizações.

Neste contexto, pode-se traduzir este conjunto de riscos sob o título de Riscos de Segurança e Privacidade, fazendo com que Gestão de Riscos de Segurança e Privacidade se tornasse tema estratégico para todas as organizações, e não seria diferente para o Município do Rio de Janeiro.

2. Apresentação do Problema

A Administração Pública Municipal está em uma jornada de Transformação Digital, onde seus processos, inclusive os primários, que efetivamente materializam os serviços disponibilizados ao cidadão carioca em todas as suas áreas de atuação, são cada vez mais fruto do tratamento de informações suportado por ativos de Tecnologia da Informação e Comunicação.

O Governo Digital já é uma realidade em âmbito municipal, com cerca de 90% dos serviços municipais sendo prestados de forma totalmente digital, fazendo com que a Gestão de Riscos de Segurança e Privacidade seja um tema vital à eficiência, eficácia, efetividade, e por que não, à credibilidade dos serviços prestados aos cidadãos cariocas.

Em agosto de 2022, um incidente de segurança, que comprometeu grande parte dos serviços municipais[1], ratificou de forma incontestável a criticidade da efetiva implantação de Programas de Segurança e Privacidade que possam garantir a melhoria contínua da maturidade da Administração Pública Municipal na Gestão de Riscos de Segurança e Privacidade visando à resiliência de sua missão em todas as suas vertentes[2].

Considerando esta nova realidade descrita acima, este relatório tem por objetivo, a partir de um diagnóstico básico da Gestão de Riscos de Segurança e Privacidade na Administração Pública Municipal, compor um conjunto de recomendações que possam colaborar na melhoria do seu nível de maturidade.

---

[1] *"Prefeitura do Rio está há uma semana com serviços parados por conta de ataque hacker."* Disponível em https://g1.globo.com/rj/rio-de-janeiro/noticia/2022/08/22/prefeitura-do-rio-esta-ha-uma-semana-com-servicos-parados-por-conta-de-ataque-hacker.ghtml. Acesso em 02 nov. 2024.

[2] Em resposta ao incidente, a Prefeitura implementou medidas para reforçar a segurança da informação. Em dezembro de 2023, foi publicado o Decreto RIO nº 53.700, instituindo a Política de Segurança da Informação (PSI) no âmbito do Poder Executivo Municipal, visando prevenir, tratar e responder a incidentes futuros de forma mais eficaz.

3. Métodos e Melhores Práticas

O diagnóstico foi realizado com base em entrevistas pontuais com agentes municipais que atuam em Segurança da Informação/Cibernética, Proteção de Dados Pessoais, Administração de Serviços de Tecnologia da Informação e Comunicação, Desenvolvimento de Sistemas e Governança de Tecnologia da Informação e Comunicação.

Para suporte a este processo de entrevistas, e visando garantir que dele se pudesse efetivamente produzir um diagnóstico básico representativo e em conformidade com as melhores práticas de segurança e privacidade vigentes, optou-se por utilizar a ferramenta disponibilizada pelo Governo Federal - **Framework de Privacidade e Segurança da Informação**[3]**.**

Este Framework compreende 18 controles de Segurança da Informação/Cibernética e 13 controles de privacidade descritos abaixo:

- **Controles de Segurança da Informação/Cibernética:**
    1. Inventário e controle de ativos institucionais;
    2. Inventário e controle de ativos de software;
    3. Proteção de dados;
    4. Configuração segura de ativos institucionais e de software;
    5. Gestão de contas;
    6. Gestão do controle de acesso;
    7. Gestão contínua de vulnerabilidades;
    8. Gestão de registros de auditoria;
    9. Proteção de e-mail e navegadores Web;
    10. Defesas contra malware;
    11. Recuperação de dados;
    12. Gestão da Infraestrutura de rede;
    13. Monitoramento e defesa da rede;
    14. Conscientização e treinamento de competências sobre segurança;
    15. Gestão de provedor de serviços;
    16. Segurança de aplicações;
    17. Gestão de resposta a incidentes; e
    18. Testes de invasão.

- **Controles de Privacidade/Proteção de Dados Pessoais:**
    1. Inventário e mapeamento;
    2. Finalidade e hipóteses legais;
    3. Governança;

[3] Disponível em https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias-e-modelos. Acesso em 02 nov. 2024.

4. Políticas, processos e procedimentos;
5. Conscientização e treinamento;
6. Minimização de dados;
7. Gestão do tratamento;
8. Acesso e qualidade;
9. Compartilhamento, transferência e divulgação;
10. Supervisão em terceiros;
11. Abertura, transparência e notificação;
12. Avaliação de impacto, monitoramento e auditoria; e
13. Segurança aplicada à privacidade.

A partir da análise das respostas relativas a cada um dos controles descritos acima, realizou-se a seleção do subconjunto de controles que definiram nosso escopo de análise e recomendações. De forma geral, optou-se por tratar os controles que nos pareceram mais relevantes que avançassem mais rapidamente no cenário atual de riscos de segurança e privacidade ao qual o Município está exposto.

Foi realizada ainda uma análise básica das estruturas de governança e gestão de segurança e privacidade, uma vez que têm papel crucial na garantia da efetividade de qualquer programa de segurança ou privacidade.

4. Diagnóstico da Gestão de Riscos de Privacidade

4.1 Da governança e gestão

Do ponto de vista normativo, dentre os atos administrativos de suporte à Gestão de Riscos de Privacidade em âmbito municipal, podemos destacar o decreto Rio nº 49.558 de 06 de Outubro de 2021, que estabeleceu os procedimentos iniciais a serem adotados pela Administração Pública Municipal visando à construção de uma cultura de proteção de dados pessoais, e o decreto Rio nº 54.984 de 21 de Agosto de 2024, que estabeleceu o Programa Municipal de Proteção de Dados Pessoais e instituiu a Política Municipal de Proteção de Dados Pessoais.

Foi possível constatar que a Gestão de Riscos de Privacidade já é suportada por uma estrutura ativa de governança e gestão, que tem como seu principal pilar o Programa Municipal de Proteção de Dados Pessoais (PMPDP), que já se encontra em execução com ações em diversos eixos, por exemplo, elaboração dos instrumentos previstos pela Lei Geral de Proteção de Dados (LGPD), gerenciamento de riscos no tratamento de dados pessoais, capacitação e sensibilização de agentes públicos, inclusive dos encarregados setoriais de dados dos órgãos e entidades municipais.

A governança e a gestão de riscos de privacidade são realizadas a partir de uma estrutura distribuída. O Município dispõe de um Encarregado de Dados Geral, agente público municipal, indicado pelo Secretário Municipal de Integridade, Transparência e Proteção de Dados. De forma sintética, competem a este encarregado o suporte técnico e a coordenação do PMPDP, assim como a orientação dos Encarregados de Dados Setoriais dos órgãos e entidades.

Cada órgão ou entidade municipal possui, pelo menos, dois Encarregados de Dados Setoriais, um titular e um suplente, e ainda um Comitê de Privacidade e Proteção de Dados Pessoais, liderado por seu respectivo encarregado titular, formado por agentes municipais das diferentes unidades organizacionais do órgão ou entidade. É este Comitê a quem compete implementar o PMPDP no âmbito do órgão ou entidade.

Identificou-se ainda a execução de uma ação de medição de um índice de conformidade à LGPD realizado a partir de um formulário enviado a todos os encarregados setoriais. A partir de medições periódicas deste índice será possível acompanhar a evolução de todos os programas setoriais de privacidade.

Apesar de haver a confirmação de que a estrutura de governança e gestão de privacidade está em plena atividade, fazendo com que sejam

desenvolvidas diversas ações relacionadas ao PMPDP, inclusive as que produzem os artefatos previstos, por exemplo, inventário de dados, avisos e políticas de privacidade, relatórios de impacto à proteção de dados etc, identificou-se que a produção destes artefatos utilizando exclusivamente ferramentas do "tipo Office", gerando arquivos dispersos na rede corporativa, muitas vezes em diversas versões, compromete consideravelmente a capacidade de uma gestão integrada da evolução do PMPDP, assim como a eficiência dos processos de manutenção destes artefatos. Com isso, **recomenda-se** que sejam realizadas ações visando à contratação de uma solução automatizada de gestão de privacidade para suporte ao PMPDP.

4.2 Dos Controles de Proteção de Dados Pessoais

4.2.1 Da Conscientização e Treinamento

Foi possível identificar um programa de treinamento ativo realizado pela Gerência de Proteção de Dados da SMIT e voltado aos encarregados de dados setoriais e aos membros dos Comitês de Proteção de Dados dos órgãos e entidades.

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.

4.2.2 Da Minimização de Dados

Foi possível identificar que ainda não há uma cultura fortemente estabelecida nos órgãos e entidades municipais de análise dos aspectos relacionados aos riscos de privacidade quando da coleta de informações visando ao suporte dos processos e serviços municipais. Com isso, muitas vezes, as operações de tratamento acabam por comprometer o princípio da necessidade, acabando por contemplar, tanto qualitativamente quanto quantitativamente, mais dados pessoais do que seriam imprescindíveis à finalidade prevista.

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.

5. Diagnóstico da Gestão de Riscos de Segurança

5.1 Da Governança e Gestão

Do ponto de vista normativo, dentre os atos administrativos de suporte à Gestão de Riscos de Segurança da Informação em âmbito municipal, podemos destacar o decreto Rio nº 53.700 de 06 de Dezembro de 2023, que institui a nova Política Municipal de Segurança da Informação (PSI), revogando a anterior e dando início a um programa de revitalização das políticas e normas de segurança vigentes, visando compatibiliza-las aos novos cenários de risco, principalmente os advindos da jornada de transformação digital em andamento.

Foi possível identificar, a partir de iniciativas da Secretaria Municipal da Casa Civil, um conjunto de ações em andamento visando à construção de uma estrutura de Governança e Gestão de Tecnologia da Informação e Comunicação em âmbito municipal que suportará a Gestão de Riscos de Segurança da Informação. No entanto, uma vez que tal estrutura não está implementada, não foi identificada a existência de agentes setoriais responsáveis por coordenar programas de segurança, de comitês de segurança setoriais ou quaisquer estruturas internas semelhantes às existentes no suporte à Gestão de Riscos de Privacidade e Proteção de Dados, com exceção da IplanRio, onde constatou-se a existência de uma Gerência de Segurança Cibernética, atuando em nível operacional, e do Escritório de Riscos, Conformidade e Segurança, atuando em nível tático e estratégico.

Em resumo, apesar da PSI estabelecer um conjunto de competências relacionadas ao tema para os diversos órgãos e entidades municipais, sua estrutura de governança e gestão, fundamental à sua efetiva implementação, ainda não se encontra implementada.

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.

5.2 Dos Controles de Segurança e Recomendações

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.

5.2.1 Da Gestão de Ativos Institucionais e de Software

Apesar de termos identificado uma solução de gerenciamento de inventário de ativos tecnológicos (equipamentos e software) em produção, seu escopo de cobertura ainda é pequeno em relação ao número de ativos tecnológicos que compõem a rede corporativa municipal.

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.

Identificou-se ainda uma heterogeneidade grande principalmente no tocante ao perfil de configuração dos equipamentos que compõem as redes locais dos órgãos e entidades, em especial das suas estações de trabalho. Este tipo de situação aumenta consideravelmente o número de vulnerabilidades distintas presentes na rede corporativa, que tem como consequência um aumento considerável da superfície de ataque. Cabe ainda ressaltar que configurações de perfil mais antigo, muitas vezes, não se compatibilizam com soluções de segurança mais recentes, fazendo com que estes equipamentos tenham sua proteção consideravelmente comprometida, transformando-os em um dos principais “elos fracos da corrente de segurança da informação”.

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.

5.2.2 Da Proteção de Dados

Apesar de prevista como diretriz na Política de Segurança da Informação vigente, não identificou-se um processo formal ativo que permita a classificação da informação quanto ao seu nível de sensibilidade a um incidente de segurança, ou seja, ao comprometimento de sua confidencialidade, integridade ou disponibilidade, que possibilite uma definição precisa dos controles adequados que deveriam suportar seu ciclo de vida: de sua coleta ou criação ao seu descarte.

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.

5.2.3 Da Conscientização e Treinamento em Segurança

Identificou-se algumas ações embrionárias de conscientização em Segurança da Informação, principalmente a partir de palestras e eventos abertos à participação presencial ou virtual, em tese, de todos os funcionários municipais; porém, diante de seu quantitativo e de sua amplitude de distribuição geográfica, entende-se que o controle ainda está muito imaturo em âmbito municipal.

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.

5.2.4 Da Segurança de Aplicações

No “coração” da transformação digital estão os sistemas e aplicações; estes são quem efetivamente suportam os serviços digitais. Identificou-se que o Município tem cerca de 800 (oitocentos) sistemas ou aplicações em produção valendo-se de mais de 10 plataformas/linguagens de desenvolvimento distintas, o que sem dúvida aumenta consideravelmente a superfície de ataque da rede corporativa municipal: quanto maior heterogeneidade de plataformas de desenvolvimento, maior a diversidade de vulnerabilidades e, por conseguinte, maior a superfície de ataque.

Identificou-se alguns movimentos em Desenvolvimento Seguro de Software, que garantem que só entrem em produção aplicações e sistemas que tenham sido aprovadas em testes dinâmicos de segurança; porém, de qualquer forma, considerando o volume, a diversidade, a relevância e a criticidade destes sistemas e aplicações para o suporte à missão do Município, entende-se ser urgente elevar consideravelmente a maturidade deste controle, logo **recomenda-se** que sejam realizadas ações visando à criação e implantação de um Programa de Desenvolvimento Seguro que tenha como metas principais:

a) A definição de um conjunto padrão de plataformas/linguagens de desenvolvimento de software e a criação de um projeto que tenha como finalidade a atualização dos sistemas e aplicações municipais para que entrem em conformidade com este padrão;

b) A implementação de um novo conjunto de métodos de desenvolvimento em conformidade com os princípios de “Security by Design’ e “Privacy by Design” suportado por soluções automatizadas que possam garantir um pipeline seguro de desenvolvimento e atualização para todos os sistemas e aplicações municipais;

c) A garantia de manutenção de um programa contínuo de treinamento e aprimoramento das equipes de desenvolvimento em Desenvolvimento Seguro de Software.

5.2.5 Do Monitoramento e Defesa da Rede

A rede corporativa municipal abriga aproximadamente 25.000 equipamentos de Tecnologia da Informação e Comunicação entre servidores, estações de

trabalho, roteadores, switches dentre outros. É a partir da integração entre eles e de sua comunicação com ativos externos à rede corporativa que se materializam os processos e serviços que suportam a administração pública municipal. Com isso, torna-se vital manter uma alta capacidade de monitoração desta rede, assim como de identificação e resposta a incidentes.

Identificou-se um grau de maturidade em crescimento no tocante ao monitoramento e defesa da rede, no entanto, considerando as limitações de pessoal verificadas junto às equipes técnicas da IplanRio, a dimensão da rede e seu perfil de funcionamento 24x7, e mais importante, o seu papel cada vez mais vital para a Administração Pública Municipal, **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.

5.2.6 Da Gestão de Resposta a Incidentes

Constatou-se que a Política de Segurança da Informação vigente determina que compete à IplanRio instituir e coordenar o Grupo de Prevenção, Tratamento e Resposta a Incidentes (GPTRI).

Com isso, **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. Conclusão

Conceitualmente, a gestão de riscos de segurança e privacidade, de forma sintética, se ampara em três “pilares/dimensões”: pessoas, processos e tecnologia. As entrevistas e interações com os agentes municipais que permitiram desenvolver o diagnóstico aqui apresentado possibilitam concluir que, apesar identificados cenários de evolução representativos em gestão de riscos de segurança na dimensão da tecnologia desde o incidente de segurança ocorrido em agosto de 2022, ainda há muito a caminhar nos “pilares” pessoas e processos.

Cabe destacar a importância de avançar na gestão de riscos de segurança, que se mostrou em estágio de maturidade bem inferior quando comparado com o de Privacidade. Ademais, considerando ser a segurança um dos princípios basilares no tocante à proteção de dados pessoais, este avanço torna-se imprescindível para que a Administração Pública Municipal possa garantir sua conformidade à Lei Geral de Proteção de Dados.

Quanto à gestão de riscos de privacidade, foi possível identificar um estágio mais maduro, porém, que ainda precisa avançar consideravelmente na dimensão pessoas. Outra questão que parece incontestável é a necessidade imperiosa de, quanto antes, conseguir ser suportada por uma solução automatizada.

Assim, com base nas análises realizadas, sugere-se a implementação de 11 recomendações principais para consolidar uma gestão de riscos de segurança e privacidade mais robusta e eficaz na Administração Pública Municipal. Essas recomendações abrangem desde a contratação de soluções automatizadas para governança de privacidade e segurança até a ampliação de programas de treinamento e conscientização, tanto em proteção de dados quanto em segurança da informação. Incluem, ainda, a adoção de práticas de minimização de dados, padronização de configuração de ativos tecnológicos, classificação de dados sensíveis, e criação de um programa de desenvolvimento seguro de software. Destaca-se, também, a necessidade de monitoramento contínuo através de um Security Operation Center (SOC) e a formação de um grupo integrado para resposta a incidentes.

A execução dessas ações permitirá uma melhoria substancial nos níveis de maturidade da gestão de riscos, promovendo uma cultura institucional alinhada aos princípios da segurança e privacidade e atendendo às exigências legais e regulamentares de forma eficiente e integrada.

Assinaturas dos membros do GT