

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

GT 3 - Campanhas de Capacitação e Conscientização sobre Proteção de Dados Pessoais na Rede Municipal de Saúde

Ano 2025

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

Campanhas de Capacitação e Conscientização sobre Proteção de Dados Pessoais na Rede Municipal de Saúde

Composição:

- 1- Alessandra Almeida Lapa
- 2- Fernanda Philippi
- 3- Rafael Pereira
- 4- Walter Gaspar
- 5- Carlos Alexandre

Relatora:
Alessandra Lapa

Sumário

Introdução	04
Apresentação do problema	04
Benckmarck / Boas Práticas	05
Recomendações	11
Conclusão	12
Assinaturas	13

1. Introdução

Este documento constitui o relatório final do Grupo de Trabalho 3 (GT3), focado em “Campanhas de Capacitação e Conscientização sobre Proteção de Dados Pessoais”. O presente relatório expande as discussões iniciadas no documento preliminar, incorporando uma pesquisa aprofundada de boas práticas e modelos de planos de capacitação aplicáveis tanto ao setor público quanto ao privado.

O objetivo é fornecer ao Conselho Municipal de Proteção de Dados Pessoais um conjunto de diretrizes e recomendações estratégicas para fomentar uma cultura robusta e perene de proteção de dados pessoais no âmbito da administração municipal, com especial atenção à Rede Municipal de Saúde.

A conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, transcende a mera adequação de processos e tecnologias, exigindo uma transformação cultural que só pode ser alcançada por meio da educação e conscientização contínua de todos os agentes envolvidos no tratamento de dados.

Este relatório, portanto, visa consolidar um referencial prático para a estruturação de iniciativas pedagógicas eficazes, alinhadas às melhores práticas nacionais e internacionais, e adaptadas à realidade do serviço público municipal.

2. Apresentação do Problema

A administração pública municipal, em particular a Rede Municipal de Saúde, lida diariamente com um volume massivo de dados pessoais, incluindo uma parcela significativa de dados sensíveis. A natureza crítica dessas informações, aliada à complexidade dos fluxos de tratamento e à diversidade de agentes envolvidos (servidores, estagiários, terceirizados, parceiros), cria um cenário de risco elevado de incidentes de segurança e tratamento inadequado de dados.

A ausência de uma cultura de privacidade e proteção de dados consolidada representa uma vulnerabilidade significativa, que pode resultar não apenas em sanções administrativas, mas também em danos à reputação do órgão e, fundamentalmente, na quebra da confiança do cidadão nos serviços públicos.

O desafio central, portanto, é transformar a conformidade com a LGPD de uma obrigação legal em um valor organizacional intrínseco, internalizado por cada colaborador.

Para tanto, é imperativo desenvolver e implementar um programa de capacitação e conscientização que seja:

- Contínuo e Abrangente: Alcançando todos os níveis hierárquicos e funcionais da organização.

- Acessível e Relevante: Utilizando linguagem clara e exemplos práticos do cotidiano dos servidores.

- Engajador e Eficaz: Empregando metodologias que incentivem a participação ativa e a mudança de comportamento.

- Mensurável: Permitindo a avaliação do impacto e o aprimoramento contínuo das iniciativas.

Este relatório aborda este problema, propondo soluções estruturadas e baseadas em benchmarks consolidados.

3. Benchmark / Boas Práticas

A análise de benchmarks é fundamental para a construção de um programa de capacitação eficaz. Foram investigadas práticas consolidadas tanto no setor público, que compartilha desafios de governança e bases legais similares, quanto no setor privado, conhecido por sua agilidade e inovação em metodologias de treinamento.

3.1. Setor Público: Diretrizes e Modelos

O setor público possui particularidades importantes, como o tratamento de dados para a execução de políticas públicas, que frequentemente dispensa o consentimento do titular, mas não exime o poder público de cumprir os demais princípios e obrigações da LGPD.

A principal referência de boas práticas para a administração pública é o Guia prático para a fase de conscientização e treinamento da adequação à Lei Geral de Proteção de Dados para a Administração Pública Municipal [1], elaborado pelo Fórum de Proteção de Dados Pessoais dos Municípios, e o Guia de Boas Práticas da Lei Geral de Proteção de Dados (LGPD) [2] do Governo Federal.

Destacam-se as seguintes diretrizes extraídas desses documentos:

A implementação de um programa de adequação à LGPD, significa mudar a mentalidade e a perspectiva de todo um órgão público. Proteger efetivamente as informações pessoais sob domínio público significa que todos os servidores e agentes públicos devem fazer sua parte. E um dos primeiros passos para essa mudança de mindset, visando atingir toda a Administração - Equipes de gestão e demais servidores - é uma boa ação educativa sobre o tema, afinal, educação é a base de tudo! [1]

As boas práticas para o setor público enfatizam:

- Apoio da Alta Gestão: O engajamento de líderes (secretários, diretores, coordenadores) é o principal fator de sucesso. A capacitação deve começar pelos níveis estratégico e tático.

- Diferenciação de Formatos: A escolha do modelo de ação educativa (palestra, workshop, curso) deve ser intencional e adequada ao público e ao objetivo. Workshops são recomendados para o contato inicial por serem dinâmicos e permitirem a troca de informações [1].

- Conteúdo Direcionado: A abordagem deve ser didática, evitando o "juridiquês" e utilizando exemplos práticos do cotidiano do servidor público. Para a área da saúde, é crucial abordar o tratamento de dados sensíveis, o manuseio de prontuários e os dilemas éticos específicos.

- Continuidade:** A conscientização não é um evento único, mas um processo contínuo que deve ser integrado aos programas de formação continuada e desenvolvimento dos servidores.

- Criação de Materiais de Apoio:** O desenvolvimento de cartilhas, guias e manuais com linguagem acessível serve como material de consulta permanente, reforçando a cultura de proteção de dados.

3.2. Setor Privado: Inovação e Engajamento

O setor privado, especialmente empresas de tecnologia e saúde, oferece insights valiosos sobre como tornar a capacitação mais engajadora e eficaz. A agilidade e a cultura de mensuração de resultados impulsionam a adoção de metodologias inovadoras que podem ser adaptadas para a realidade do serviço público.

As principais práticas observadas são:

- Gamificação (Gamification):** Utilização de elementos de jogos, como quizzes, desafios, pontuações e rankings, para tornar o aprendizado mais lúdico e competitivo, aumentando o engajamento.

- Microlearning:** Entrega de conteúdo em pequenas doses, por meio de vídeos curtos, podcasts ou pílulas de conhecimento, facilitando a absorção da informação em rotinas de trabalho exigentes.

- Simulações e Estudos de Caso:** Criação de cenários práticos, como simulações de ataques de phishing ou estudos de caso sobre vazamentos de dados, para treinar a resposta a incidentes e a tomada de decisão.

- Cultura de Privacidade desde a Integração (Onboarding):** Inclusão de módulos sobre proteção de dados no processo de integração de novos colaboradores, garantindo que a cultura de privacidade seja assimilada desde o início.

•**Métricas de Impacto:** Avaliação da eficácia dos treinamentos não apenas pela taxa de conclusão, mas por indicadores de mudança de comportamento, como a redução no número de cliques em e-mails de phishing ou o aumento de relatos de potenciais incidentes.

3.2.1. Benchmarks de Empresas Privadas

Além das práticas gerais de inovação em capacitação, algumas empresas privadas brasileiras divulgaram de forma transparente suas estratégias de adequação à LGPD, especialmente em relação à conscientização e educação de colaboradores. A seguir, destacam-se quatro casos relevantes:

Itaú Unibanco

O Itaú Unibanco estruturou um programa permanente de capacitação em proteção de dados, integrando treinamentos presenciais e online, materiais educativos e campanhas internas. O banco adota o conceito de cultura de privacidade, reforçando a necessidade de todos os colaboradores compreenderem seus papéis no tratamento de dados pessoais. Entre as medidas destacam-se:

- Treinamentos obrigatórios em LGPD para todo o corpo funcional, renovados periodicamente.
- Campanhas de comunicação digital e uso de pílulas de microlearning, que permitem reforçar conceitos de forma ágil.
- Envolvimento da alta gestão, com executivos participando de workshops e divulgando mensagens de engajamento.
- Monitoramento de resultados com métricas de participação e testes de retenção de conhecimento.

Essas práticas foram relatadas em seus Relatórios de Sustentabilidade, como parte de sua estratégia de governança e risco [3].

Hospital Israelita Albert Einstein

No setor da saúde, o Hospital Albert Einstein implementou um programa de adequação à LGPD que envolve não apenas processos técnicos, mas também treinamento especializado de profissionais de saúde. O hospital reconhece que a

manipulação de prontuários e dados sensíveis exige atenção especial e, por isso, desenvolveu:

- Treinamentos segmentados por área (médicos, equipe de enfermagem, administrativos), com foco em situações reais do cotidiano.
- Materiais internos de apoio, como cartilhas digitais e guias práticos sobre manuseio de dados sensíveis.
- Criação de um comitê interno de governança em privacidade, responsável por conduzir campanhas de engajamento.
- Adoção de workshops de dilemas éticos em saúde digital, promovendo debates sobre limites do uso de dados.

Essa experiência é reconhecida como referência no setor por unir formação técnica e ética médica [4].

TOTVS

A TOTVS, líder em software de gestão, promoveu uma ampla campanha de educação corporativa em proteção de dados. A empresa adotou metodologias digitais de aprendizagem, incluindo:

- Plataforma de e-learning com módulos sobre LGPD, segurança da informação e boas práticas de governança.
- Campanhas periódicas de conscientização, como simulações de ataques de phishing, para treinar respostas dos colaboradores.
- Desenvolvimento de materiais de apoio destinados não apenas a funcionários, mas também a clientes, como cartilhas digitais e webinars sobre privacidade.
- Inclusão de LGPD nos programas de integração de novos colaboradores (onboarding).

Esse modelo reforça a ideia de que a capacitação deve ser contínua e incorporada ao cotidiano corporativo, e não limitada a treinamentos pontuais [5].

Natura &Co

A Natura &Co incorporou a privacidade e a ética digital como pilares de sua estratégia global de governança. O grupo desenvolveu uma abordagem que alia conscientização, liderança e transparência. Entre as iniciativas estão:

- Treinamentos contínuos e workshops interativos para colaboradores de diferentes níveis hierárquicos.
- Engajamento de lideranças como embaixadores internos de privacidade, transmitindo a mensagem de forma exemplar.
- Criação de canais internos de apoio, para que colaboradores possam esclarecer dúvidas sobre tratamento de dados.
- Inclusão da proteção de dados como tema em seus relatórios anuais de sustentabilidade, vinculando a prática à responsabilidade socioambiental e de governança (ESG).

A empresa enfatiza que a cultura de proteção de dados é um ativo reputacional, e que o investimento em treinamento fortalece a confiança de consumidores e parceiros [6].

3.3. Modelos de Planos de Capacitação

Com base nas boas práticas analisadas, um plano de capacitação eficaz pode ser estruturado em fases e direcionado a diferentes públicos. O Guia prático para a fase de conscientização e treinamento [1] oferece um modelo detalhado que pode ser adaptado.

A seguir, apresentamos uma tabela com um modelo de plano de capacitação, combinando as melhores práticas dos setores público e privado:

Fase do Plano	Público-Alvo	Formato Sugerido	Conteúdo Programático Chave	Métricas de Sucesso
1. Conscientização Inicial	Todos os servidores, estagiários e terceirizados	Workshop presencial/online (4h)	Conceitos fundamentais da LGPD, princípios, direitos dos titulares, exemplos práticos de dados pessoais e sensíveis no dia a dia, responsabilidades do agente público.	Taxa de participação > 95%, Pesquisa de satisfação, Teste de conhecimento inicial.
2. Capacitação por Função	Equipes específicas (TI, Jurídico, RH, Atendimento,	Treinamento técnico (8h-16h), E-learning com módulos	TI: Segurança da informação, gestão de incidentes,	Certificação por conclusão, Avaliação de aprendizado

	Saúde)	específicos	privacy by design. Jurídico: Bases legais, contratos com operadores. RH: Tratamento de dados de servidores. Saúde: Dados sensíveis, prontuários, pesquisa.	baseada em estudos de caso.
3. Engajamento Contínuo	Todos os servidores	Campanhas periódicas, Microlearning (vídeos, podcasts), Gamificação (quizzes), Simulações de phishing	Atualizações sobre a LGPD, lembretes sobre boas práticas (senhas fortes, mesa limpa), divulgação de casos de incidentes (anonimizados).	Taxa de abertura de comunicados, Participação em atividades de gamificação, Redução de cliques em phishing.
4. Formação de Multiplicadores	Servidores com aptidão e interesse ("Embaixadores da LGPD")	Workshop avançado, Reuniões periódicas	Aprofundamento em temas da LGPD, Técnicas de comunicação e treinamento, Como atuar como ponto focal de dúvidas em seus setores.	Número de "embaixadores" formados, Número de dúvidas respondidas pelos multiplicadores.

4. Recomendações

Com base na análise do relatório preliminar e no benchmark realizado, o Grupo de Trabalho 3 recomenda as seguintes ações estratégicas para o Conselho Municipal de Proteção de Dados Pessoais, a serem propostas à administração municipal:

1. Instituir um Programa de Capacitação e Conscientização Contínuo:

Formalizar, por meio de portaria ou decreto, um programa permanente de educação em proteção de dados, garantindo sua continuidade e alocação de recursos. O programa deve seguir o modelo estruturado em fases apresentado na seção 3.3.

2. Adotar o "Guia prático para a fase de conscientização e treinamento" como

Referência Principal: Utilizar o guia [1] como o documento norteador para a implementação das ações educativas, adaptando suas recomendações (público-alvo, formato, conteúdo) à realidade da administração municipal.

3. Priorizar a Capacitação da Alta Gestão e das Equipes da Saúde: Iniciar o programa de capacitação pelos secretários, subsecretários, coordenadores e diretores para garantir o patrocínio e o engajamento das lideranças. Em paralelo, desenvolver e aplicar um módulo de treinamento específico e aprofundado para todos os profissionais da Rede Municipal de Saúde, dada a sensibilidade dos dados tratados.

4. Incorporar Metodologias Inovadoras de Engajamento: Além dos formatos tradicionais, investir em plataformas de e-learning que permitam a aplicação de gamificação e microlearning. Realizar campanhas de simulação de phishing para treinar e medir a prontidão dos servidores.

5. Criar a Figura dos "Embaixadores da LGPD": Identificar e capacitar servidores em diferentes secretarias para atuarem como multiplicadores e pontos focais de conhecimento, descentralizando a expertise e facilitando a disseminação da cultura de privacidade.

6. Desenvolver e Disponibilizar Materiais de Apoio: Produzir uma cartilha oficial de boas práticas em proteção de dados para a administração municipal, bem como guias rápidos e vídeos curtos, que sirvam como material de consulta permanente para todos os servidores.

7. Estabelecer Métricas e Monitorar o Progresso: Definir um conjunto de indicadores-chave de desempenho (KPIs) para monitorar a eficácia do programa, incluindo taxas de participação, resultados de testes de conhecimento, métricas de engajamento e redução de incidentes de segurança. Os resultados devem ser reportados periodicamente ao Conselho.

5. Conclusão

A criação de uma cultura de proteção de dados é um pilar indispensável para a conformidade com a LGPD e para a construção de uma relação de confiança entre a administração pública e o cidadão.

A capacitação e a conscientização não são despesas, mas investimentos estratégicos na segurança jurídica do município e na proteção dos direitos fundamentais da população.

Este relatório buscou fornecer um caminho claro e estruturado, baseado em referências sólidas e boas práticas de mercado, para que o Conselho Municipal de Proteção de Dados Pessoais possa liderar a implementação de um programa de educação transformador.

A execução das recomendações aqui propostas contribuirá decisivamente para que a proteção de dados pessoais seja internalizada como um valor essencial em toda a administração municipal.

6. Referências Bibliográficas

[1] RIBEIRO, Adriano Aquino; BOTEMBERGER, Sahmara Liz. Guia prático para a fase de conscientização e treinamento da adequação à Lei Geral de Proteção de Dados para a Administração Pública Municipal. Versão 1.0. [S. l.]: Fórum de Proteção de Dados Pessoais dos Municípios, 2023. Disponível em: <https://www.municipioslgpd.com.br/>. Acesso em: 10 set. 2025.

[2] BRASIL. Secretaria de Governo Digital. Guia de Boas Práticas: Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Governo Federal, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 10 set. 2025.

[3] ITAÚ UNIBANCO. Relatório Anual de Sustentabilidade 2021. Disponível em: <https://www.itaui.com.br/relacoes-com-investidores/relatorio-anual/> Acesso em: 25 set. 2025.

[4] HOSPITAL ISRAELITA ALBERT EINSTEIN. LGPD na Saúde. 2021. Disponível em: <https://www.einstein.br/Pages/lgpd.aspx> Acesso em: 01 set. 2025.

[5] TOTVS. Relatório Anual de Sustentabilidade 2022. Disponível em: <https://ri.totvs.com/> Acesso em: 10 set. 2025.

[6] NATURA &Co. Relatório de Sustentabilidade 2022. Disponível em: <https://naturaeco.com/relatorios/> Acesso em: 10 set. 2025.

7. Assinaturas