INVENTÁRIO DE DADOS PESSOAIS

RELATOS DE EXPERIÊNCIAS

Produzido pela Câmara Técnica da Lei Geral de Proteção de Dados (LGPD) do Conaci

SUMÁRIO

APRESENTAÇÃO 1

AUDITORIA GERAL DO ESTADO DA BAHIA 3

CONTROLADORIA GERAL DO MUNICÍPIO DE SÃO PAULO 26

CONTROLADORIA E OUVIDORA GERAL DO ESTADO DO CEARÁ 59

CONTROLADORIA GERAL DO ESTADO DE GOIÁS 66

CONTROLADORIA GERAL DO ESTADO DE MINAS GERAIS 83

SECRETARIA DE ESTADO DE TRANSPARÊNCIA E CONTROLE DO MARANHÃO 88

Conaci
CONSELHO NACIONAL DE CONTROLE INTERNO

APRESENTAÇÃO

A relação entre proteção de dados pessoais e controle interno está, justamente, na maneira como as organizações gerenciam e protegem as informações pessoais dos indivíduos que interagem com elas.

O controle interno se refere aos processos, políticas e procedimentos estabelecidos por uma organização para garantir a eficiência operacional, a conformidade com as leis e regulamentos aplicáveis e a mitigação de riscos. Ele abrange uma gama de atividades, incluindo monitoramento, avaliação de riscos, controles internos financeiros, conformidade legal e ética, entre outros.

A proteção de dados pessoais, por sua vez, refere-se às medidas adotadas para garantir a privacidade e a segurança das informações pessoais dos indivíduos. Isso inclui a coleta adequada de dados, o armazenamento seguro, a utilização restrita para fins específicos, o acesso limitado e a adoção de salvaguardas técnicas e organizacionais para proteger esses dados contra acesso não autorizado, perda, divulgação ou uso indevido.

Quando se trata de proteção de dados pessoais, o controle interno desempenha um papel fundamental. As organizações precisam estabelecer controles adequados para garantir a conformidade com a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no Brasil.

Esses controles incluem a designação de um encarregado pelo tratamento de dados pessoais, a implementação de políticas claras de privacidade e proteção de dados, o registro das operações de tratamento de dados pessoais, a realização de avaliações de impacto à proteção de dados, a segurança da informação, entre outros.

O controle interno também é essencial para garantir a efetividade dessas medidas de proteção de dados pessoais. Ele envolve o monitoramento contínuo das práticas de coleta e processamento de dados, a identificação e a mitigação de riscos de segurança, a resposta a incidentes de segurança, a revisão e a melhoria contínua dos processos relacionados à proteção de dados pessoais.

Nesse contexto, a efetividade do direito fundamental à proteção de dados, especialmente previsto pela Constituição Federal e pela LGPD, é um constante desafio e uma obra ainda a ser escrita.

Vale ressaltar que a autonomia dos entes federativos trouxe a cada órgão diferentes possibilidades organizacionais à sua implementação e promoção.

É com um intuito colaborativo a essa jornada que a Câmara Técnica sobre a LGPD, do Conselho Nacional de Controle Interno (Conaci), vem desenvolvendo ações que visam a orientar os órgãos de controle interno de todo o país.

Entre essas ações, está a consolidação de práticas já adotadas por órgãos de controle interno nacionais relativas ao desenvolvimento do processo de inventário de dados pessoais - também conhecido como registro das operações de tratamento de dados pessoais e mapeamento de dados pessoais.

Esse instrumento se constitui como a identificação categorial dos dados pessoais existentes e tratados em uma organização e como um dos passos essenciais à implementação de um programa de governança em privacidade e em proteção de dados pessoais no âmbito dos Poderes Executivos dos entes federativos brasileiros.

O Inventário de Dados Pessoais representa um passo primordial para documentar o tratamento de dados pessoais realizados pela instituição, e está em alinhamento ao previsto pela LGPD:

> "Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse."

O inventário consiste em uma excelente forma de fazer um balanço sobre o que o órgão ou a entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e quais operações são realizadas com eles.

Para tanto, em 20 de junho de 2023, durante a 46ª Reunião Técnica do Conselho Nacional de Controle Interno, a Câmara deliberou, por unanimidade, a aprovação e a publicação, como boas práticas metodológicas já adotadas à elaboração do processo de inventário de dados pessoais, das práticas adotadas pelos seguintes órgãos de controle interno: (i) Auditoria Geral do Estado da Bahia (AGE/BA); (ii) Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE); (iii) Controladoria-Geral do Estado de Goiás (CGE/GO); (iv) Controladoria Geral do Estado de Minas Gerais (CGE/MG); (v) Controladoria Geral do Município de São Paulo (CGM/SP); e (vi) Controladoria-Geral do Distrito Federal (CGDF).

Apesar de as realidades organizacionais constituírem-se diferentemente em cada um dos órgãos supracitados e as distinções metodológicas divergirem, por via de consequência, é possível o entendimento convergente sobre o conceito e sobre os requisitos essenciais à estruturação de um processo de inventário de dados pessoais – os quais são, nesse sentido, pontuados pelos tópicos existentes em cada uma das experiências reportadas e documentadas.

Histórico - origem, contexto e motivações

Segundo o “Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD) ” da Controladoria Geral da União, a adequação dos órgãos e entidades em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação envolve: considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução e promover ações de conscientização de todo corpo funcional, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

A primeira ação executada foi a sensibilização dos gestores em relação aos principais aspectos e exigências da lei. Em seguida foi planejado o processo do Inventário de Dados pessoais – IDP, etapa essencial para diagnosticar qual o nível de maturidade em privacidade em que se encontrava a SEFAZ.

O IDP consiste no registro das operações de tratamento dos dados pessoais realizadas pela instituição e fornece subsídio para avaliação de impacto à proteção de dados pessoais, com vistas a verificar a conformidade da instituição quanto ao preconizado pela LGPD.

Em alinhamento com a alta gestão, das medidas necessárias à adequação à LGPD foi priorizada a realização do IDP pelo Grupo de Trabalho, tendo início em fevereiro de 2021, com a adoção de formulários adaptados e desenvolvimento colaborativo com os gestores de área.

As fases 1 e 2 do processo de IDP da Auditoria Geral do Estado da Bahia foram executadas em 03 meses, por meio de 03 entrevistas, que resultaram no levantamento de 19 processos que envolvem tratamento de dados pessoais.

Objetivo / escopo

A alta gestão definiu os fatores críticos a serem identificados no levantamento de processos de negócios que tratam dados pessoais. Os tipos de dados relatados pelos gestores de área em cada processo foram cadastrados visando identificar:

1. Há dados publicados em sites, diário oficial, jornais?
2. Há compartilhamento de dados com órgãos externos?
3. Há compartilhamento de dados com outros setores na SEFAZ?
4. Há tratamento de dados de mais de 250 indivíduos[1]?

Com base nas informações levantadas, foi elaborada uma matriz de ponderação dos fatores críticos, para classificar os processos de negócios que apresentam maiores riscos para que o Inventário fosse priorizado e detalhado nos seguintes aspectos:

- De que forma os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados
- Escopo e Natureza dos Dados Pessoais
- Finalidade do Tratamento de Dados Pessoais
- Categoria de Dados Pessoais - descrição, tempo de retenção, fonte de retenção e nome da base de dados
- Medidas de Segurança/Privacidade
- Contrato (s) de serviços e/ou soluções de TI que trata (m) dados pessoais do serviço/processo de negócio

[1] Número sugerido pela empresa de consultoria Gartner

Estrutura do órgão

No Poder Executivo do Estado da Bahia a coordenação do sistema de controle interno é exercida pela Auditoria Geral do Estado (AGE), com atribuição de órgão central. A AGE está vinculada à Secretaria da Fazenda do Estado da Bahia – SEFAZ e tem por finalidade proceder à análise dos atos e fatos administrativos e financeiros dos órgãos e entidades da administração direta e indireta em conformidade com a legislação vigente, coordenar, como órgão central, o sistema estadual formado pelas unidades setoriais de controle, tendo como competência coordenar, capacitar, monitorar e avaliar estas unidades e gerir o portal Transparência Bahia, principal instrumento ativo de cumprimento da Lei de Acesso à informação, além de competências voltadas ao controle interno preventivo e gerenciamento de riscos.

A equipe é composta por 43 colaboradores distribuídos em 03 coordenações.
O Grupo de Trabalho – LGPD é composto por 04 membros, sendo que 02 são lotados na AGE, inclusive o Encarregado de Proteção de Dados.

Governança

Em dezembro de 2020, foi criado um Grupo de Trabalho - GT multidisciplinar, por meio da Portaria do Secretário da Fazenda, com o objetivo de realizar avaliação e propor estratégias de aperfeiçoamento de rotinas potencialmente impactadas pela LGPD. A portaria que instituiu o GT, teve um caráter temporário e foi renovada por períodos de três meses até janeiro de 2023.

O GT foi composto por membros com conhecimentos nas matérias: cultura organizacional e processos de negócios, gestão de riscos, segurança da informação e jurídico.

O GT foi formado com vinculação ao Gabinete do Secretário da Fazenda e seu funcionamento se deu em paralelo às demais atividades e atribuições dos membros nos seus respectivos setores.

Em fevereiro 2021, o Encarregado de Proteção de Dados Pessoais foi indicado, também por Portaria e teve seus dados publicados no site da SEFAZ.

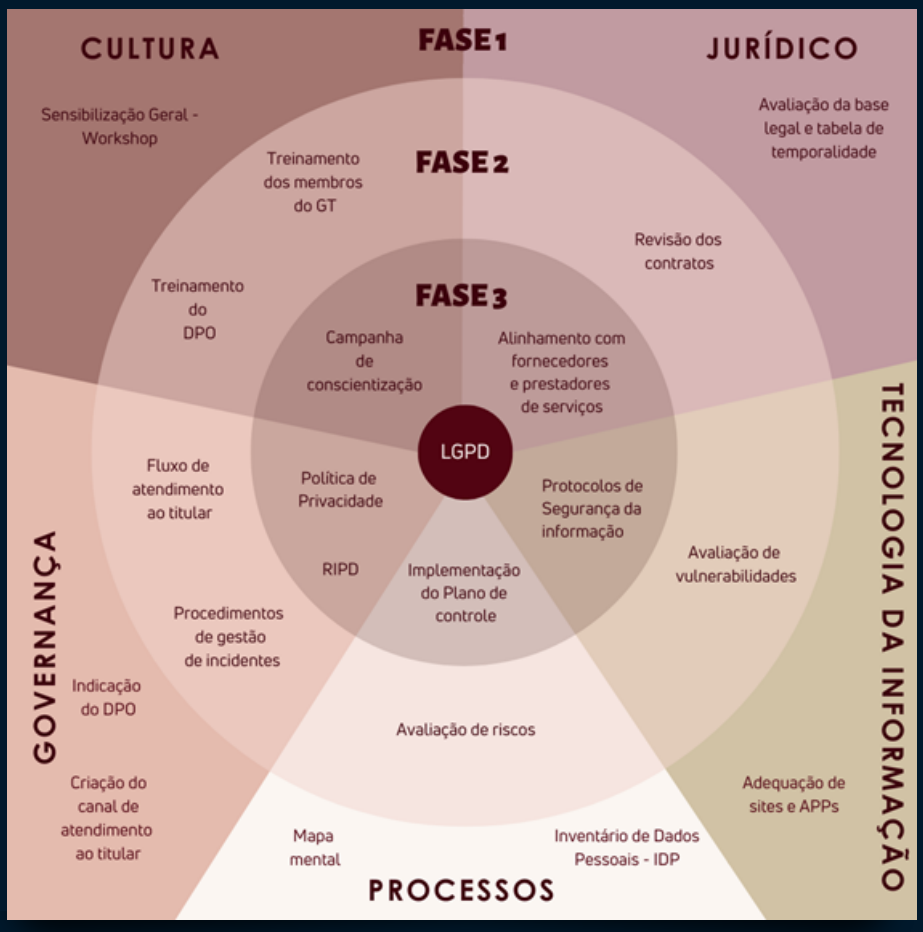
Capacitação - Treinamento

Os membros buscaram participar de eventos e seminários disponíveis na internet e realizaram os cursos Introdução à Lei Brasileira de Proteção de Dados Pessoais e Proteção de Dados Pessoais no Setor Público oferecidos pela Escola Virtual de Governo da Escola Nacional da Administração Pública – ENAP.

A partir de 2022, com a elaboração do Plano de Capacitação da AGE, tendo em vista a premissa de incentivo aos servidores para serem membros de associações profissionais e para desenvolvimento acadêmico, foi incluída a previsão de curso com certificação para o Encarregado de proteção de dados e cursos para os demais membros.

Processo

Em alinhamento com a alta gestão da Secretaria da Fazenda, a adequação da organização à LGPD foi dividida em cinco eixos e três fases, conforme figura 1.



Fonte: Cristina Cardoso, AGE-BA

O IDP constitui ação da Fase 1, no eixo Processos e se integra com as demais ações planejadas para a adequação da SEFAZ à LGPD.

A conclusão do primeiro IDP da AGE ocorreu em maio de 2021.

Método

Para a condução de sensibilização dos gestores em relação aos conceitos e termos concernentes ao IDP, além de nortear o levantamento dos processos de negócio das unidades foram adaptados os formulários disponibilizados pela CGU e empresa de consultoria Gartner.

Como referenciais teóricos foram utilizados:

- Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD) [versão 2.0]
- Guia de Elaboração de Inventário de Dados Pessoais
- Modelo simplificado de inventário de dados pessoais - Template

Os formulários citados foram adequados às necessidades da SEFAZ, com a remoção e/ou customização de seções do inventário de dados pessoais.

Anexo I – Categorização de processos
Anexo II – Inventário de dados pessoais do processo de negócio
Anexo III – Documentação das medidas de segurança, privacidade e controle

Fluxo

O IDP foi desenvolvido com base no fluxo abaixo:

Principais desafios

A LGPD é um reflexo de novas demandas da sociedade e sua compreensão envolve conceitos até então desconhecidos pela maioria das pessoas, tornando complexa a criação e o desenvolvimento da cultura de privacidade na organização. A adequação dos processos de trabalho pressupõe uma mudança na forma como são tratados os dados pessoais que estão sob a responsabilidade do órgão e sendo tamanha a quebra de paradigmas, demandará, para além das normas, o envolvimento e comprometimento dos colaboradores e alterações nas práticas diárias.

O fato de haver pouca regulamentação da matéria de maneira geral, assim como a ausência de arcabouço legal no Estado que pudesse dar suporte às ações de adequação das instituições à LGPD, impactaram no escopo e no alcance dos objetivos traçados inicialmente pela Secretaria. A falta de uma estrutura de governança de dados formal causa fragilidade às ações empreendidas, visto que quando houver a regulamentação, pode resultar em retrabalho ou adequações relevantes.

O processo de construção da metodologia demandou a busca por conhecimentos que não estavam presentes na organização. Para enfrentar este desafio, a capacitação direcionada e conduzida institucionalmente dos envolvidos poderia contribuir para o aprimoramento do processo, agregar valor e dar agilidade às ações.

Outra limitação é que os membros do GT acumularam as ações do IDP com as demais atribuições de suas respectivas áreas, sendo observado que as atividades planejadas poderão ser mais efetivas com a criação de uma estrutura permanente na instituição, como um comitê de privacidade.

Resta claro que a realização do IDP é um passo importante na direção da adequação do órgão à LGPD, entretanto, tendo em vista o caráter dinâmico de um programa de proteção de dados, mesmo implementado de maneira efetiva, ele deve ser revisado periodicamente, estando sujeito a constantes atualizações.

Por fim, não se pode afastar que a LGPD abriu um novo panorama de teorias jurídicas e desafios na aplicação das leis, principalmente, no serviço público. A coexistência entre a obrigação de garantir a transparência pública, em razão da Lei de Acesso à Informação – LAI e o direito do indivíduo à privacidade vai exigir que os órgãos compreendam suas convergências e promovam a harmonização entre as duas legislações.

Resultados alcançados

Entre os fatores de sucesso atribuídos à metodologia escolhida para realização do IDP, certamente a definição dos perfis dos membros do grupo de trabalho que conduziu as atividades se revelou determinante. Diferentes visões e multidisciplinariedade dos conhecimentos enriqueceram o processo e possibilitaram a superação dos obstáculos.

Do mesmo modo, a inclusão de um componente com profundo conhecimento da cultura organizacional e dos processos de negócios da organização, permitiu boa articulação e receptividade nas áreas para execução das atividades propostas pelo GT.

Em relação à metodologia, a decisão de realizar reuniões de sensibilização e entrevista, com o acompanhamento direto para o levantamento de processos de trabalho que tratam dados pessoais, permitiu maior envolvimento e comprometimento dos gestores.

Como consequência, durante as etapas do IDP, além de identificar riscos à privacidade, foram promovidas mudanças nos processos a partir do entendimento dos gestores sobre a matéria, mesmo antes da concepção do plano de controle, inclusive com revisão de processos.

A exemplo, podem ser citados redefinição dos parâmetros de configuração de cookies para os sites, alteração de formulários relativos a serviços públicos disponibilizados, anonimização de dados no Portal da Transparência, alteração de nível de acesso a processos que tratam dados pessoais.

O processo de IDP foi permeado pela convicção de que esse assunto tão atual, traz a oportunidade de repensar os processos de trabalho e a forma como são tratados os dados pessoais que estão sob a responsabilidade da Administração Pública, para garantir o exercício dos direitos dos cidadãos ao seu livre desenvolvimento.

Afinal, a privacidade passou a ser um direito fundamental da pessoa natural e é o que vai proporcionar os meios necessários à construção e consolidação de sua liberdade individual de escolha e de visão de mundo.

ANEXO I

Categorização de processos

Levantamento de atividades - IDP						
Existe alguma atividade no seu setor que envolva qualquer informação das seguintes categorias de forma regular? Marque X	Processo 1		Processo 2		Processo 3	
	Dados	Peso	Dados	Peso	Dados	Peso
Informações de contato pessoal						
Nome		0		0		0
E-mail		0		0		0
Endereço		0		0		0
Telefone		0		0		0
Informações pessoais de funcionários						
Salário		0		0		0
Cargo		0		0		0
Função		0		0		0
Setor		0		0		0
Informações de dispositivos						
Informações de dispositivos conectados		0		0		0
Aparelhos conectados		0		0		0
Informações financeiras						
Conta bancária		0		0		0
Cartão de Crédito		0		0		0
Transações Financeiras		0		0		0

Levantamento de atividades - IDP						
Existe alguma atividade no seu setor que envolva qualquer informação das seguintes categorias de forma regular? Marque X	Processo 1		Processo 2		Processo 3	
	Dados	Peso	Dados	Peso	Dados	Peso
Informação comportamental						
Comportamento de navegação na web		0		0		0
Relacionamentos de e-mails		0		0		0
Uso de aplicativos e de comunicações		0		0		0
Informações atribuídas por instituições governamentais						
CPF		0		0		0
RG		0		0		0
Passaporte		0		0		0
Placa de carro		0		0		0
Registro em conselhos profissionais		0		0		0
Matrícula		0		0		0
Informações de diretório ou dados de autenticação - ID						
Contas de usuário - login		0		0		0
Senhas		0		0		0
Fotos		0		0		0
Foto ou vídeo no contexto						
Câmera de vigilância		0		0		0
Leitor de placa de veículo		0		0		0

Levantamento de atividades - IDP						
Existe alguma atividade no seu setor que envolva qualquer informação das seguintes categorias de forma regular? Marque X	Processo 1		Processo 2		Processo 3	
	Dados	Peso	Dados	Peso	Dados	Peso
Informações de geolocalização						
Informações usadas em dispositivos GPS para rastreamento de veículos ou posicionamento interno		0		0		0
Informações de saúde		0		0		0
Histórico de saúde		0		0		0
Prescrição		0		0		0
Atestado		0		0		0
Relatório médico		0		0		0
Parecer de saúde		0		0		0
Dados biométricos que pertencem diretamente a indivíduos		0		0		0
Impressão digital		0		0		0
Impressão palmar		0		0		0
Reconhecimento facial e/ou de íris		0		0		0
Dados que revelam origem racial ou étnica		0		0		0
Dados que revelam convicção religiosa		0		0		0
Dados que revelam opinião política		0		0		0
Dados que revelam filiação a sindicato						
Dados que revelam filiação ou crença filosófica						
Dados referentes à vida sexual						
Dados genéticos						

Levantamento de atividades - IDP						
Existe alguma atividade no seu setor que envolva qualquer informação das seguintes categorias de forma regular? Marque X	Processo 1		Processo 2		Processo 3	
	Dados	Peso	Dados	Peso	Dados	Peso
Dados pessoais de crianças e de adolescentes		0		0		0
Grande volume de dados		0		0		0
Compartilhamento de dados		0		0		0
Publicação site / DOE / Jornais de grande circulação		0		0		0
Total de pontos		0		0		0

ANEXO II

Inventário de dados pessoais do processo de negócio

Inventário de Dados Pessoais	
Essa guia é um modelo de um formulário operacional a ser reproduzido, adaptado e preenchido de acordo com a sua atividade de tratamento de dados pessoais. São fornecidos comentários adicionais como notas para auxiliar no preenchimento do formulário.	
1 - Identificação dos serviços / processo de negócio de tratamento de dados pessoais	
1.1 - Nome do serviço / Processo de negócio	
1.2 - N° Referência / ID	
1.3 - Data de Criação do Inventário	
1.4 - Data Atualização do Inventário	

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador					
2.2 - Encarregado					
2.3 - Operador					

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					

4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados	
4.1 - Descrição do Fluxo do tratamento dos dados pessoais	

5 - Escopo e Natureza dos Dados Pessoais	
5.1 - Abrangência da área geográfica do tratamento	
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento	
6.2 - Finalidade	
6.3 - Previsão legal	
6.4 - Resultados pretendidos para o titular de dados	
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo	

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				
7.2 -Dados Financeiros	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.2.1 - Dados de identificação financeira				
7.2.2 - Recursos financeiros				
7.2.3 - Dívidas e despesas				
7.2.4 - Situação financeira (Solvência)				
7.2.5 - Empréstimos, hipotecas, linhas de crédito				

7.2 -Dados Financeiros	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.2.6 - Assistência financeira				
7.2.7 - Detalhes da apólice de seguro				
7.2.8 - Detalhes do plano de pensão				
7.2.9 - Transações financeiras				
7.2.10 - Compensação				
7.2.11 - Atividades profissionais				
7.2.12 - Acordos e ajustes				
7.2.13 - Autorizações ou consentimentos				
7.3 - Características Pessoais	**Descrição**	**Tempo Retenção dos Dados**	**Fonte Retenção**	**Nome Base de Dados**
7.3.1 - Detalhes pessoais				
7.3.2 - Detalhes militares				
7.3.3 - Situação de Imigração				
7.3.4 - Descrição Física				

7.4 - Hábitos Pessoais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.4.1 - Hábitos				
7.4.2 - Estilo de vida				
7.4.3 - Viagens e deslocamentos				
7.4.4 - Contatos sociais				
7.4.5 - Posses				
7.4.6 - Denúncias, incidentes ou acidentes				
7.4.7 - Distinções				
7.4.8 - Uso de mídia				
7.5 - Características Psicológicas	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.5.1 - Descrição Psicológica				
7.6 - Composição Familiar	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.6.1 - Casamento ou forma atual de coabitação				
7.6.2 - Histórico conjugal				
7.6.3 - Familiares ou membros da família				

7.7 - Interesses de lazer	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.7.1 - Atividades e interesses de lazer				
7.8 - Associações	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.8.1 Associações (exceto profissionais, políticas, em sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis)				
7.9 - Processo Judicial/Administrativo/ Criminal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.9.1 - Suspeitas				
7.9.2 - Condenações e sentenças				
7.9.3 - Ações judiciais				
7.9.4 - Penalidades Administrativas				
7.10 - Hábitos de Consumo	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.10.1 - Dados de bens e serviços				
7.11 - Dados Residenciais	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.11.1 - Residência				

7.12 - Educação e Treinamento	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.12.1 - Dados acadêmicos/escolares				
7.12.2 Registros financeiros do curso/treinamento				
7.12.3 - Qualificação e experiência profissional				
7.13 - Profissão e emprego	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.13.1 - Emprego atual				
7.13.2 - Recrutamento				
7.13.3 - Rescisão de trabalho				
7.13.4 - Carreira				
7.13.5 - Absentismo e disciplina				
7.13.6 -Avaliação de Desempenho				
7.13.6 -Avaliação de Desempenho	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.14.1 - Vídeo e imagem				
7.14.2 - Imagem de Vigilância				
7.14.3 - Voz				

7.15 -Outros (Especificar)	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
7.15.1 - Outros (Especificar)				

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou étnica				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferência política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

9 - Frequência e totalização das categorias de dados pessoais tratados	
9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		

11 - Compartilhamento de Dados Pessoais	Dados pessoais compartilhados	Finalidade do compartilhamento
11.1 - Nome da Instituição 1		
11.2 - Nome da Instituição 2		
11.3 - Nome da Instituição 3		
11.4 - Nome da Instituição 4		

12 - Medidas de Segurança/Privacidade	Tipo de medida de segurança e privacidade	Descrição do(s) Controle(s)
12.3 - Medida de Segurança/Privacidade 1		
12.2 - Medida de Segurança/Privacidade 2		
12.3 - Medida de Segurança/Privacidade 3		

13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			

14 - Contrato (s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/processo de negócio	Nº Processo Contratação	Objeto do Contrato	E-mail do Gestor do Contrato
14.2 - Contrato nº 1			
14.2 - Contrato nº 2			

ANEXO III

Documentação das medidas de segurança, privacidade e controle

QUESTIONAMENTOS	RESPOSTAS
ARMAZENAMENTO	
1- Os dados pessoais estão armazenados de que maneira? (Bancos de dados, repositório local ou na nuvem, e-mails, aplicativos, redes sociais...)	
2- Os dados pessoais armazenados, estão em uma forma de dados estruturados ou não estruturados?	
3- Os dados pessoais armazenados, estão em repouso ou em trânsito?	
4- Há políticas de backup?	
5- Há um plano de continuidade e realização de testes com frequência?	
6- Há uma política de armazenamento de dados?	
7- É realizada a classificação de dados?	
8- Os sistemas operacionais são atualizados com frequência? Há alguma política?	
9- Para dados armazenados em cloud, foram revistas as políticas de acesso e configurações para garantir a devida proteção?	
10- São armazenados dados para fins estatísticos e de pesquisa? Estes estão anonimizados?	

QUESTIONAMENTOS	RESPOSTAS
SEGURANÇA	
1- Como são gerenciados os perfis de acessos e autorizações?	
2- Há gestão de identidades e acessos?	
3- Há implementação de criptografia? (cenários em repouso e em trânsito) Considerar também backups e logs.	
4- Nos aplicativos e sistemas que o usuário final Pessoa Física pode acessar, já foram realizados testes de intrusão (pentest)?	
5- Existem procedimentos estabelecidos para atualizações (patches)?	
6- Existem ferramentas para segurança de rede?	
7- Como as senhas de usuários e as internas são armazenadas e gerenciadas?	
8- Existem processos para gestão de vulnerabilidades?	

CONTROLADORIA GERAL DO MUNICÍPIO DE SÃO PAULO (CGM/SP)

Histórico - origem, contexto e motivações

A implementação da proteção de dados pessoais no âmbito da Controladoria Geral do Município de São Paulo (CGM/SP) teve início com a edição do Decreto Municipal nº 59.767/2020, que regulamentou a Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709, de agosto de 2018) no âmbito da Administração Pública Municipal e designa o Controlador Geral do Município como Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município. O Decreto Municipal também previu, dentre as atribuições do Encarregado, a de editar diretrizes à elaboração do Plano de Governança em Privacidade e em Proteção de Dados Pessoais dos órgãos da Administração Pública Municipal. Foi com esse objetivo que a CGM/SP editou, em 21 de julho de 2022, a Instrução Normativa CGM/SP nº 01/2022, que é o ato normativo que dispõe, essencialmente, de padrões à realização, por cada órgão da Administração Pública Municipal, do referido Plano de Governança.

Nesse sentido, a Instrução Normativa estabeleceu, em seus anexos, padrões à realização de um "Mapeamento de Dados Pessoais" (também conhecido, justamente, como "Inventário de Dados Pessoais" e como "Registro das Operações de Tratamento de Dados Pessoais") e de um "Relatório de Impacto à Proteção de Dados" para cada órgão da Administração Pública Municipal direta, em caráter obrigatório, e para cada entidade da Administração Pública Municipal indireta, em caráter orientativo. No Anexo III deste Report, apartado a este documento, está, justamente, o layout utilizado à realização "Mapeamento de Dados Pessoais".

Com o intuito de trazer orientações detalhadas aos órgãos e às entidades, a CGM/SP, em 13 de janeiro de 2023, também disponibilizou aos agentes públicos da Administração Pública Municipal Guias Orientativos que objetivam a implementação das disposições da LGPD e, de modo mais específico, do Decreto Municipal nº 59.767/2020 e da Instrução Normativa CGM/SP nº 01/2022.

Nesse sentido, foram publicados o "Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo" e o "Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo".

O “Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo” é um Manual destinado à orientação de todos os agentes públicos do Poder Executivo Municipal sobre os direitos fundamentais à privacidade e à proteção de dados pessoais e sobre como esses direitos afetam a sua atuação no âmbito da Administração Pública do Município.

O “Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo”, por sua vez, é um Manual que objetiva orientar os agentes públicos do Poder Executivo Municipal que estão a estruturar, no âmbito de cada órgão e de cada entidade da Administração Pública do Município, o seu Programa de Governança em Privacidade e em Proteção de Dados Pessoais. Para tanto, traz passo-a-passo para a implementação de ações como “Mapeamento de Processos”, “Mapeamento de Dados Pessoais” (“Inventário de Dados Pessoais” ou “Registro das Operações de Tratamento de Dados Pessoais”), “Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais” e “Relatório de Impacto à Proteção de Dados Pessoais”. Esse Guia Orientativo traz, assim, a pedra fundamental à estruturação de uma Governança que demarque como esses direitos dos cidadãos estão sendo efetivados pela Prefeitura do Município de São Paulo.

Com relação à operacionalização dos procedimentos estabelecidos pela Instrução Normativa CGM/SP nº 01/2022, se destaca o Mapeamento de Dados Pessoais da CGM/SP, resultado direto de diversas interações com os agentes públicos que, a partir de Questionários, Entrevistas e Reuniões Técnicas, resultou em um Mapeamento de Dados Pessoais robusto, a conter 130 processos que envolvem tratamento de dados pessoais.

Objetivo / escopo

O objetivo principal das ações provenientes da Instrução Normativa CGM/SP nº 01/2022 e dos Guias Orientativos, publicados pela CGM/SP, é o de orientar os agentes públicos do município de São Paulo que estão a estruturar, no âmbito de cada órgão e de cada entidade da Administração Pública do Município, o seu Programa de Governança em Privacidade e em Proteção de Dados Pessoais.

As ações da CGM/SP, nesse escopo, se direcionaram a:

1. Dar cumprimento à Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei Federal nº 13.709, de 14 de agosto de 2018 – que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural;
2. Regulamentar a aplicação da LGPD no âmbito da Administração Pública Municipal, conforme o Decreto Municipal nº 59.767/2020;
3. Ser, a partir do Encarregado pela Proteção de Dados Pessoais da Prefeitura, o canal de comunicação entre a Prefeitura, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD);
4. Disponibilizar metodologia e layouts de "Mapeamento de Dados Pessoais" ("Inventário de Dados Pessoais" ou "Registro das Operações de Tratamento de Dados Pessoais") e de "Relatório de Impacto à Proteção de Dados Pessoais", que objetivam padronizar a implementação dessas práticas no âmbito da Prefeitura;
5. Estabelecer aspectos elementares sobre as operações de tratamento de dados pessoais realizadas no âmbito da Prefeitura, especialmente relacionados à realização de seus respectivos "Mapeamento de Processos", "Mapeamento de Dados Pessoais" e "Planos de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"; E
6. Fomentar a cultura de privacidade e da proteção de dados pessoais no âmbito das atividades de tratamento provenientes do serviço público.

Especificamente com relação ao objetivo e ao escopo de atuação da CGM/SP quanto à realização de "Mapeamento de Dados Pessoais", após a padronização de metodologia e de layout desta ação, a CGM/SP iniciou a sua implementação no âmbito do órgão.

Para tanto, preliminarmente, foi necessária a padronização de metodologia e de layout de "Mapeamento de Processos" pelo órgão (vide Anexo I deste report), os quais foram, então, seguidos no âmbito da própria CGM/SP – ação que resultou no mapeamento de 130 processos atualmente existentes no órgão. Para tanto, cada divisão da CGM/SP (vide item 03, abaixo) realizou o mapeamento dos processos existentes em sua unidade, isto após Reunião Técnica de capacitação dos agentes públicos, ministrada pela área de proteção de dados pessoais do órgão, com relação à metodologia aplicada.

Tendo, então, em consideração o “Mapeamento de Processos” realizado no âmbito do órgão, somado à metodologia de “Mapeamento de Dados Pessoais” realizada também pela CGM/SP, deu-se início à atividade pela utilização de um Questionário (vide Anexo II deste report), composto por 18 quesitos, que objetivou a coleta de informações sobre o tratamento de dados pessoais existente em cada um dos 130 processos mapeados. Para tanto, cada divisão da CGM/SP (vide item 03, abaixo) respondeu aos questionários que diziam respeito aos processos a ela relacionados, isto após Reunião Técnica de capacitação dos agentes públicos, ministrada pela área de proteção de dados pessoais do órgão, com relação à metodologia aplicada. Nesse sentido, ao final, 130 questionários, cada qual relacionado a um processo existente na CGM/SP, foram gerados.

Em seguida, a área de proteção de dados pessoais realizou a compilação dos dados coletados a partir das etapas anteriores e a sua interpretação, isto de modo a integrá-las no layout “Mapeamento de Dados Pessoais”, integrante da Instrução Normativa CGM/SP nº 01/2022, o qual foi finalizado e é, juntamente a todas as etapas precedentes, subsídio à realização da próxima etapa do Plano de Governança em Privacidade e em Proteção de Dados Pessoais prevista pela Instrução Normativa e pelos Guias Orientativos aludidos – que é a “Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais”.

Estrutura do órgão

A Controladoria Geral do Município de São Paulo (CGM), um órgão da Administração Pública Municipal direta, que possui como missão exercer o controle interno do Município, promover a integridade, a transparência e a participação social e proteger os dados pessoais dos cidadãos, possui a seguinte estrutura básica:

o Gabinete do Controlador Geral;
- Assessoria Jurídica (AJ);
- Assessoria Técnica (AT);
- Assessoria de Comunicação (ASCOM); e
- Assessoria de Assessoria de Produção de Informações e Inteligência (APRI).

o Corregedoria Geral do Município (CORR);
o Ouvidoria Geral do Município (OGM);
o Coordenadoria de Auditoria Geral (AUDI);
o Coordenadoria de Promoção da Integridade (COPI);
o Coordenadoria de Defesa do Usuário do Serviço Público Municipal (CODUSP); e
o Coordenadoria de Administração e Finanças (CAF);

Governança

Com relação ao Plano de Governança em Privacidade e em Proteção de Dados Pessoais, vale o destaque prévio, contextual, de que:

- A Controladoria Geral do Município de São Paulo (CGM/SP) é o órgão responsável por coordenar, supervisionar e fiscalizar o cumprimento da LGPD e do Decreto Municipal nº 59.767/2020 no âmbito da Administração Pública Municipal;
- O Controlador Geral do Município de São Paulo é o Encarregado pela Proteção de Dados Pessoais da Prefeitura, sendo o canal de comunicação entre a Prefeitura, os titulares dos dados pessoais e a ANPD;
- A Instrução Normativa CGM/SP nº 01/2022, o "Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo" e o "Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo" estabelecem as diretrizes para a implementação do Programa de Governança em Privacidade e em Proteção de Dados Pessoais no âmbito da Administração Pública Municipal.

O Programa de Governança, de modo geral, tem como objetivo garantir o cumprimento dos princípios, dos direitos e das obrigações previstas na LGPD e no Decreto Municipal nº 59.767/2020.

O já citado Decreto Municipal nº 59.767/2020 dispõe do que é denominado de um "Plano de Adequação", que é conjunto entre as boas práticas e o Programa de Governança em Privacidade e Proteção de Dados Pessoais adotado pela Prefeitura do Município de São Paulo. Conforme o seu art. 2º, inc. XIII, é o "conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais." O art. 4º, inc. III, e o art. 10, inc. II, do Decreto Municipal, por sua vez, dispuseram da obrigação do Poder Executivo, por meio da Administração Pública Municipal direta e indireta, de realizá-lo e de mantê-lo atualizado.

O Decreto Municipal, em seu art. 15, também estabeleceu os requisitos mínimos a serem observados nos “Planos de Adequação” da Administração Pública Municipal direta e indireta: (i) publicidade das informações relativas ao tratamento de dados pessoais em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades na Internet, bem como no Portal da Transparência, em seção específica (art. 15, inc. I); (ii) atendimento das exigências que vierem a ser estabelecidas pela ANPD (art. 15, inc. II); e (iii) manutenção de dados pessoais em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral (art. 15, inc. III).

Com relação à Administração Pública Municipal direta, dispôs o art. 4º, caput, do Decreto Municipal, que cada Secretaria e cada Subprefeitura devem realizá-lo e mantê-lo atualizado, observadas as diretrizes editadas pelo Controlador Geral do Município, enquanto Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, após deliberação favorável da Comissão Municipal de Acesso à Informação (CMAI).
Com relação à Administração Pública Municipal indireta, apesar de possuírem os seus próprios Encarregados, conforme o art. 10, caput, do Decreto Municipal, também devem realizar e manter atualizados os seus Planos de Adequação, observadas as diretrizes do Controlador Geral do Município, nos termos do art. 10, inc. II.

Nesse sentido, a estruturação do Programa de Governança em Privacidade e em Proteção de Dados Pessoais está articulada a partir das regras dispostas pelo Decreto Municipal e pelas diretrizes editadas pelo Controlador Geral do Município, enquanto Encarregado, de modo que tanto as diretrizes previstas pela Instrução Normativa CGM/SP nº 01/2022, quanto as diretrizes previstas pelo “Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo” e pelo “Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo” valem para todo Poder Executivo do Município – em caráter mandatório para a Administração Pública Municipal direta e em caráter orientativo para a Administração Pública Municipal indireta.

Capacitação e Conscientização

A promoção da cultura da privacidade e da proteção de dados pessoais aos agentes públicos está a ser realizada a partir de dois níveis: (i) pela conscientização, a partir : (i.i) de campanha informativa, pelas redes sociais e por mailing list a todos os agentes públicos, sobre a proteção de dados pessoais; e (i.i) pela divulgação do "Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo", destinado à orientação sobre os direitos fundamentais à privacidade e à proteção de dados pessoais e sobre como esses direitos afetam a sua atuação no âmbito da Administração Pública do Município; e (ii) pela capacitação, isto a partir da divulgação do "Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo".

Também há a previsão de lançamento de dois cursos online, assíncronos, que objetivam aprimorar o entendimento dos agentes públicos perante o material didático já elaborado, ou seja, relativamente ao "Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo" e ao "Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo".

Processo

A CGM/SP, com relação ao desenvolvimento de seu Programa de Governança em Privacidade e em Proteção de Dados Pessoais, estruturou um Plano de Adequação com a previsão das ações necessárias à sua estruturação, e que se pautam, essencialmente, nas seguintes atividades:

Fase 1 - Atos Preparatórios e Contínuos da Controladoria Geral do Município:

1. Comprometimento de Alta Administração da Controladoria Geral do Município;
2. Ato Normativo que disponha sobre o Programa de Governança em Privacidade e Proteção de Dados Pessoais da Prefeitura do Município (Instrução Normativa CGM/SP nº 01/2022);
3. Capacitação de agentes públicos da Prefeitura do Município:
3.1. Conscientização e capacitação de agentes públicos da Prefeitura do Município relativa à privacidade e proteção de dados pessoais:
3.1.1. Curso em Privacidade e em Proteção de Dados Pessoais;
3.1.2. Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais; e
3.1.3. Campanha de Conscientização em Privacidade e Proteção de Dados Pessoais;
3.2. Capacitação de agentes públicos da Prefeitura do Município relativa à Instrução Normativa CGM/SP nº 01/2022:
3.2.2. Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022.
4. Fixação de responsabilidades e pontos focais na Controladoria Geral do Município:

Fase 2 - Mapeamento de Processos e de Mapeamento de Dados Pessoais da Controladoria Geral do Município:

1. Elaboração do Mapeamento de Processos da Controladoria Geral do Município;
2. Elaboração do Registro das Operações de Tratamento de Dados Pessoais ("Record Of Processing Activities" - RoPA) da Controladoria Geral do Município, com base no Anexo I da Instrução Normativa CGM/SP nº 01/2022:
2.1. Extração e elaboração gráfica de inteligência do Registro das Operações de Tratamento de Dados Pessoais (RoPA) da Controladoria Geral do Município.
3. Execução do Mapeamento do Fluxo de Dados Pessoais da Controladoria Geral do Município:
3.1. Extração e elaboração gráfica de inteligência do Mapeamento do Fluxo de Dados Pessoais da Controladoria Geral do Município.
Fase 3 - Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da Controladoria Geral do Município:
1. Elaboração de Plano de Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da Controladoria Geral do Município;
1.1. Execução de Plano de Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da Controladoria Geral do Município;
2. Elaboração de Diretrizes aos Planos de Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais de CGM/AUDI, CGM/CAF, CGM/CORR, CGM/OGM, CGM/CODUSP, CGM/COPI e CGM/GAB, por CGM/COPI;
3. Elaboração de Planos de Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais por CGM/AUDI, CGM/CAF, CGM/CORR, CGM/OGM, CGM/CODUSP, CGM/COPI e CGM/GAB:
3.1. Execução dos Planos de Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais por CGM/AUDI, CGM/CAF, CGM/CORR, CGM/OGM, CGM/CODUSP, CGM/COPI e CGM/GAB.
4. Elaboração de Plano de Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da Controladoria Geral do Município:
4.1. Execução do Plano de Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da Controladoria Geral do Município:
4.1.1. Elaboração de Plano de Gestão das Hipóteses de Tratamento de Dados Pessoais da Controladoria Geral do Município:
4.1.1.1. Execução de Plano de Gestão das Hipóteses de Tratamento de Dados Pessoais da Controladoria Geral do Município:
4.1.1.1.1. Elaboração de Avaliação de Legítimo Interesse ("Legitimate Interests Assessment" - LIA).
4.1.2. Elaboração do Plano de Gestão das Bases de Dados Pessoais Legadas ("Legacy Database") da Controladoria Geral do Município:
4.1.2.1. Execução do Plano de Gestão das Bases de Dados Pessoais Legadas ("Legacy Database") da Controladoria Geral do Município.

4.1.3. Elaboração do Plano de Gestão da Segurança da Informação da Controladoria Geral do Município (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.3.1. Execução do Plano de Gestão da Segurança da Informação da Controladoria Geral do Município (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.3.1.1. Política de Segurança da Informação;
4.1.3.1.2. Política de Gestão de Ativos;
4.1.3.1.3. Política de Controle de Acesso;
4.1.3.1.4.Política de "Backup"; e
4.1.3.1.5.Política "Bring Your Own Device" (BYOD).
4.1.4. Elaboração de Plano de Gestão dos websites geridos pela Controladoria Geral do Município à Privacidade e à Proteção de Dados Pessoais (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.4.1. Execução de Plano de Gestão dos websites geridos pela Controladoria Geral do Município à Privacidade e à Proteção de Dados Pessoais (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.4.1.1. Políticas de Privacidade e Avisos de Privacidade; e
4.1.4.1.2. Políticas de Cookies e Avisos de Cookies.
4.1.5. Elaboração do Plano de Gestão dos Contratos Administrativos e Instrumentos Congêneres da Controladoria Geral do Município à Privacidade e à Proteção de Dados Pessoais (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.5.1. Execução do Plano de Gestão dos Contratos Administrativos e Instrumentos Congêneres da Controladoria Geral do Município à Privacidade e à Proteção de Dados Pessoais (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.5.1.1. Elaboração de Cláusulas-Padrão relativas à Privacidade e à Proteção de Dados Pessoais para os Contratos Administrativos e Instrumentos Congêneres;
4.1.5.1.2. Elaboração de Termos de Aditamento para os Contratos Administrativos e Instrumentos Congêneres em vigor;
4.1.5.1.3. Elaboração de Termos de Consentimento de Uso de Imagem e Voz para o âmbito de aplicação da LGPD e para o âmbito de exclusão da LGPD;
4.1.6. Ato normativo que procedimentaliza os direitos de acesso, correção e eliminação dos dados pessoais, em observância à LGPD, LAI e Lei de Habeas Data, no âmbito da Prefeitura do Município;
4.1.7. Elaboração do Plano de Resposta aos Incidentes de Segurança relacionados à Privacidade e à Proteção de Dados Pessoais dos órgãos da Administração Pública Municipal (criação de Políticas e Procedimentos Operacionais Padrão):
4.1.7.1. Execução do Plano de Resposta em caso de Incidente de Segurança relacionado à Privacidade e à Proteção de Dados Pessoais dos órgãos da Administração Pública Municipal (criação de Políticas e Procedimentos Operacionais Padrão).

Fase 4 - Relatório de Impacto à Proteção de Dados Pessoais (RIPD) da Controladoria Geral do Município:

1. Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), com base no Anexo II da Instrução Normativa CGM/SP nº 01/2022.

Fase 5 - Relatório do Plano de Governança em Privacidade e em Proteção de Dados Pessoais da Controladoria Geral do Município (Relatório do Plano de Adequação, conforme Instrução Normativa CGM/SP nº 01/2022):

1. Elaboração do Relatório do Plano de Governança em Privacidade e em Proteção de Dados Pessoais da Controladoria Geral do Município.
Fase 6 – Monitoramento:
1. Atualização anual do Relatório do Plano de Governança em Privacidade e em Proteção de Dados Pessoais da Controladoria Geral do Município;
2. Monitoramento contínuo da adequação das práticas da Controladoria Geral do Município à privacidade e à proteção de dados pessoais;
3. Elaboração de Índice de Maturidade sobre o Programa de Governança em Privacidade e em Proteção de Dados Pessoais da Prefeitura do Município;
4. Monitoramento anual do Índice de Maturidade dos órgãos e das entidades da Administração Pública Municipal ao Programa de Governança em Privacidade e em Proteção de Dados Pessoais da Prefeitura do Município;
5. Respostas da Controladoria Geral do Município às demandas provenientes pelos canais oficiais de contato da Controladoria Geral do Município:
5.1. Respostas às demandas que envolvam as atribuições do Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município; e
5.2. Respostas às demandas que envolvam o Programa de Governança em Privacidade e em Proteção de Dados Pessoais da Prefeitura do Município; e
6. Revisão contínua dos Planos de Gestão.

Método

A metodologia desenvolvida pela CGM/SP, consubstanciada no “Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo” e No “Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo”, teve como referencial:

i) Família ABNT/ISO, com destaque para:
a. ISO nº 31.004, de 2015;
b. ISO nº 31.000, de 2018;
c. ISO nº 27.001, de 2018;
d. ISO nº 27.002, de 2013;
e. ISO nº 27.701, de 2013;
f. ISO nº 29.100, de 2020;
g. ISO nº 27.018, de 2021;
h. ISO nº 29.151, de 2020; e
i. ISO nº 31.010, de 2021.

ii) Diretrizes emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), especialmente:
a. Guia Orientativo sobre Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado;
b. Guia Orientativo sobre Tratamento de Dados Pessoais pelo Poder Público;
c. Guia Orientativo sobre Cookies e Proteção de Dados Pessoais; e
d. Estudo Preliminar relativo às hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes.

iii) Normas, nacionais e internacionais, com destaque para:
a. Constituição da República Federativa do Brasil de 1988.
b. Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
c. Lei Federal nº 12.965/2014 – Marco Civil da Internet (MCI);
d. Decreto Municipal nº 59.767/2020; e
e. Regulamento Geral de Proteção de Dados Pessoais (RGPD) da União Europeia.

iv) Doutrina, nacional e internacional, sobre o tema.

Fluxo

Como referido, preliminarmente, foi necessária a padronização de metodologia e de layout de “Mapeamento de Processos” pelo órgão (vide Anexo I deste report), os quais foram, então, seguidos no âmbito da própria CGM/SP – ação que resultou no mapeamento de 130 processos atualmente existentes no órgão. Para tanto, cada divisão da CGM/SP (vide item 03, abaixo) realizou o mapeamento dos processos existentes em sua unidade, isto após Reunião Técnica de capacitação dos agentes públicos, ministrada pela área de proteção de dados pessoais do órgão, com relação à metodologia aplicada.

Tendo, então, em consideração o “Mapeamento de Processos” realizado no âmbito do órgão, somado à metodologia de “Mapeamento de Dados Pessoais” realizada também pela CGM/SP, deu-se início à atividade pela utilização de um Questionário (vide Anexo II deste report), composto por 18 quesitos, que objetivou a coleta de informações sobre o tratamento de dados pessoais existente em cada um dos 130 processos mapeados. Para tanto, cada divisão da CGM/SP (vide item 03, abaixo) respondeu aos questionários que diziam respeito aos processos a ela relacionados, isto após Reunião Técnica de capacitação dos agentes públicos, ministrada pela área de proteção de dados pessoais do órgão, com relação à metodologia aplicada. Nesse sentido, ao final, 130 questionários, cada qual relacionado a um processo existente na CGM/SP, foram gerados.

Em seguida, a área de proteção de dados pessoais realizou a compilação dos dados coletados a partir das etapas anteriores e a sua interpretação, isto de modo a integrá-las no layout “Mapeamento de Dados Pessoais”, integrante da Instrução Normativa CGM/SP nº 01/2022, o qual foi finalizado e é, juntamente a todas as etapas precedentes, subsídio à realização da próxima etapa do Plano de Governança em Privacidade e em Proteção de Dados Pessoais prevista pela Instrução Normativa e pelos Guias Orientativos aludidos – que é a “Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais”.

Principais desafios

Os principais desafios para a aplicação do Programa de Governança em Privacidade e em Proteção de Dados Pessoais nos moldes propostos pela CGM/SP são:

- Conscientizar e capacitar os agentes públicos sobre a importância da privacidade e da proteção de dados pessoais, bem como sobre as normas e as boas práticas aplicáveis ao tratamento dos dados pessoais no âmbito da Administração Pública Municipal;

- Identificar e mapear os fluxos de dados pessoais tratados por cada órgão ou entidade da Administração Pública Municipal, desde a coleta até a eliminação, indicando as hipóteses legais de tratamento, as finalidades, os destinatários, os riscos e as medidas de segurança aplicáveis;

- Elaborar e atualizar os relatórios de impacto à proteção de dados pessoais das operações de tratamento de dados pessoais que possam gerar riscos aos direitos e às liberdades dos titulares, bem como as medidas a serem adotadas para mitigar esses riscos;

- Implementar e monitorar as medidas de segurança necessárias para prevenir e combater incidentes que possam comprometer a segurança, a confidencialidade, a integridade e a disponibilidade dos dados pessoais tratados; e

- Criar e manter canais de contato para com o titular de dados pessoais.

Resultados alcançados

As ações realizadas no âmbito do Programa de Governança em Privacidade e em Proteção de Dados Pessoais da CGM/SP relacionadas à consecução de um Mapeamento de Dados Pessoais no órgão de controle interno municipal resultou, especialmente, em:

- Aprimoramento da cultura do respeito à privacidade e à proteção de dados pessoais entre os agentes públicos do órgão;

- Mapeamento das atividades realizadas pela CGM/SP a partir de metodologia que tornou possível a sua padronização para toda a Prefeitura do Município; e

- Registro das operações de tratamento de dados pessoais de todas as atividades/processos realizadas no âmbito do órgão.

ANEXO I

Contextualização dos Processos

1 - Metodologia

Solicitação de descrição sobre os processos e sobre as etapas dos processos existentes em cada divisão do “órgão/entidade”, com detalhes sobre:

(i) Identificação dos objetivos e das etapas dos processos: etapas existentes em cada processo, com a indicação dos objetivos de cada processo e de cada etapa;

(ii) Recursos humanos das etapas dos processos: divisões do órgão ou entidade e agentes públicos envolvidos em cada etapa de processo;

(iii) Recursos físicos e tecnológicos das etapas dos processos: infraestrutura física e tecnológica utilizada em cada etapa de um processo (e.g., “hardware” e “software” utilizados para documentação de informações em formatos digitais);

(iv) Comunicação e compartilhamento de informações entre as etapas dos processos: modo de comunicação entre os recursos humanos utilizados e o modo de compartilhamento das informações entre as etapas;

(v) Recursos informacionais das etapas dos processos: rol de documentos gerados ou compartilhados em cada etapa de um processo somado ao rol de informações geradas ou compartilhadas em cada etapa de um processo.

É possível que uma etapa, a partir de uma tomada de decisão, possa ser segmentada em distintas possíveis etapas e/ou ser remissiva. Nestes casos, é possível sequenciar as etapas:

(i) com subitens (e.g., etapa 2.1 e etapa 2.2, seguintes à etapa 1); e
(ii) com remissão à(s) etapa(s) precedente(s) ou sucessora(s).

2 - Terminologia

(i) Recursos humanos: entende-se o quantitativo de agentes públicos envolvidos em cada etapa de um processo;

(ii) Recursos físicos e tecnológicos: entende-se a infraestrutura física e tecnológica utilizada em cada etapa de um processo.

(iii) Recursos informacionais: entende-se o rol de “documentos” gerados ou compartilhados em cada etapa de um processo somado ao rol de “informações” geradas ou compartilhadas em cada etapa de um processo;

(iv) Documentos: entende-se o substrato/suporte em que uma informação gerada ou compartilhada é representada a partir de diferentes expressões da percepção humana, como a escrita, a imagem, o áudio e o vídeo; e

(v) Informações: entende-se como informações o conhecimento que é documentado. Neste caso, diz respeito ao objeto/assunto das informações que são geradas ou compartilhadas.

3 - Layout de Mapeamento de Processos

<“Nome do órgão/entidade”/ “Nome da divisão”> /<Versão nº [....]: DD/MM/AAAA>
<“**Nome do Processo**”>
<“Objetivo do Processo”>
Etapa [...]: i. **Objetivo:** <“indicação do objetivo específico desta etapa do processo”> ii. **Recursos humanos utilizados nesta etapa:** <“divisões do órgão ou entidade e agentes públicos envolvidos nesta etapa do processo”>; iii. **Recursos físicos e tecnológicos utilizados nesta etapa:** <“infraestrutura física e tecnológica nesta etapa do processo”>; iv. **Comunicação e compartilhamento das informações:** <“modo de comunicação entre os recursos humanos utilizados e o modo de compartilhamento das informações entre esta etapa com a(s) anterior(es) e a(s) seguinte(s) etapa(s)> v. **Recursos informacionais desta etapa:** a. **Rol de documentos gerados ou compartilhados:** <“documento é o substrato/suporte em que uma informação gerada ou compartilhada é representada a partir de diferentes expressões da percepção humana, como a escrita, a imagem, o áudio e o vídeo”> b. **Rol de informações geradas ou compartilhadas:** “Informação é o conhecimento documentado. Neste caso, diz respeito ao objeto/assunto das informações que são geradas ou compartilhadas”>.

ANEXO II

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

1- Metodologia

Solicitação de resposta, para os responsáveis de cada divisão do "órgão/entidade", aos quesitos do Questionário a partir de cada processo mapeado na etapa "Mapeamento de Processos".

Na eventualidade de dúvidas com relação às respostas do Questionário, a equipe de trabalho poderá dirimi-las a partir da etapa "Entrevistas".

2 - Terminologia

(i) Dados pessoais: informação relacionada a pessoa natural identificada ou identificável. Não se relaciona, portanto, a dados de pessoas jurídicas;

(ii) Dados pessoais sensíveis: categoria especial de dados pessoais de pessoas naturais, cujas subcategorias são relativas à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

(iii) Tratamento de dados pessoais: acesso, armazenamento, arquivamento, avaliação, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, ocultação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização de dados pessoais;

(iv) Agentes de tratamento de dados pessoais: são agentes de tratamento de dados pessoais o controlador e os operadores. Com relação à Administração Pública Municipal direta, o controlador é o Poder Executivo do Município de São Paulo. Servidores e outras pessoas naturais que integram a Administração Pública Municipal direta e cujos atos expressam a sua atuação não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos[2]. Exemplo de operador é a PRODAM – Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo, pessoa jurídica dotada de autonomia e que, quando de sua atuação em regime de direito público, atua no tratamento de dados pessoais em nome do Poder Executivo;

---

[2] BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Brasília, Autoridade Nacional de Proteção de Dados, 2022, p. 60. Disponível aqui. Acesso em: 15 julho 2022.

(v) Encarregado: o Encarregado pela Proteção de Dados Pessoais, no âmbito da Administração Pública Municipal direta, é o Controlador Geral do Município;

(vi) Tempo de retenção: o tempo de retenção de dados pessoais se relaciona à Política Municipal de Gestão Documental, assim como ao Sistema de Arquivo do Município de São Paulo; e

(vii) Fonte de retenção: a fonte de retenção de dados pessoais é o substrato no qual os dados pessoais são representados. São exemplos que poderão ser utilizados, isolada ou cumulativamente, a depender do caso concreto: nuvem (com a especificação do servidor), documento eletrônico DOCX e similares, documento eletrônico PDF e similares, planilha eletrônica EXCEL e similares, mídia eletrônica MP3 e similares, mídia eletrônica MP4 e similares, mídia eletrônica JPEG e similares, disco óptico (CD, DVD, Blu-Ray), “pen-drive”, cartão de memória, HD externo, SSD, fita magnética, disquete, disco fonográfico (vinil, compacto-simples e goma-laca), cilindro fonográfico, material biológico e papel.

3 - *Layout* do Questionário sobre a Privacidade e a Proteção de Dados Pessoais

<“Nome do órgão/entidade”/ “Nome da divisão”> /<Versão nº [....]: DD/MM/AAAA>
<“**Nome do Processo**”>
<“Objetivo do Processo”>
1. **Há operador(es) que atua(m) neste processo? Se sim, identifique-o(s).** **Resposta:** 2. **Em qual(is) fase(s) do ciclo de vida do tratamento de dados pessoais o(s) operador(es) atua(m)?** *<Ciclos de vida representam diferentes ações de tratamento de dados pessoais, como elencadas anteriormente, que se iniciam pela coleta e finalizam-se pela eliminação.>* **Resposta:**

3. Como os dados pessoais são tratados, tendo em vista o ciclo do tratamento de dados pessoais?

<Descrever como os dados pessoais são coletados, produzidos, recepcionados, reproduzidos, extraídos, analisados, guardados, compartilhados, usados e eliminados.>

<Neste quesito, procure refletir sobre o tratamento de dados pessoais conforme as etapas existentes no processo, descritas em "Contextualização de Processos", porque todo processo também possui um ciclo de vida.>

<Exemplo de descrição do fluxo de tratamento de dados pessoais:
1. Os dados pessoais são coletados mediante preenchimento de formulário eletrônico; 2. Os dados pessoais são transferidos, armazenados ou arquivados na nuvem ou em servidores dedicados; 3. A empresa "X" fornece uma quantidade "Y" para armazenamento em nuvem e se compromete a manter o armazenamento em território nacional; 4. Os dados pessoais podem ser eliminados: (i) a pedido do titular, caso não sejam necessários à consecução de interesse público; (ii) após a utilização por desnecessidade de armazenamento; ou (iii) por temporalidade.>

Resposta:

4. Qual é a abrangência da área geográfica do tratamento de dados pessoais?

<Informar se a abrangência dos dados pessoais tratados é nacional, estadual, distrital, municipal ou regional.>

Resposta:

5. Qual é a fonte dos dados pessoais?

<Informar se os dados pessoais tratados se originam dos próprios titulares de dados pessoais, de seus responsáveis legais, ou de outros sujeitos, como, e.g., a partir da Receita Federal, quando de consulta de CPF.>

Resposta:

6. Entre as hipóteses de tratamento elencadas pelo art. 7º[3] e 11[4], da LGPD, qual(is) é (são) a(s) que fundamenta(m) o tratamento de dados pessoais realizado neste processo?

<Copie, nesta resposta, o caput do(s) art.(s) 7º e/ou 11, da LGPD, mais o(s) inciso(s) que fundamenta(m) o tratamento de dados pessoais.>

<O art. 7º diz respeito ao tratamento de dados pessoais, exceto aqueles que se enquadram na categoria de dados pessoais sensíveis.>

---

[3] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

[4] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

<O art. 11 diz respeito ao tratamento de dados pessoais sensíveis, considerados aqueles contenham dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.>

<Excepcionalmente, é possível fundamentar-se em mais de uma hipótese de tratamento, uma vez que um processo poderá ter diferentes tipos de tratamento de dados pessoais.>

<No âmbito da Controladoria Geral do Município de São Paulo, destacam-se as hipóteses de tratamento elencadas no art. 7º, incs. I e II, da LGPD.>

Resposta:

7. Qual(is) é (são) a(s) finalidade(s) do tratamento de dados pessoais deste processo? Qual(is) a(s) previsão(ões) legal(is) que respalda(m) essa(s) finalidade(s)?

Resposta:

8. Quais são os resultados pretendidos, ao titular de dados pessoais, com o tratamento realizado neste processo?

Resposta:

9. Quais os benefícios esperados ao órgão, à Prefeitura do Município e/ou a sociedade, como um todo, com relação a esse tratamento?

Resposta:

10. Informe as categorias ordinárias de dados pessoais tratadas neste processo, de acordo com os enunciados a seguir e os descrevendo com base: (i) no tempo de retenção dos dados pessoais; e (ii) na fonte de retenção dos dados pessoais.

<Em caso de inexistência de tratamento de determinada categoria de dados pessoais, responda "Não há".>

<O tempo de retenção de dados pessoais se relaciona à Política Municipal de Gestão Documental, assim como ao Sistema de Arquivo do Município de São Paulo.>

<A fonte de retenção de dados pessoais é o substrato no qual os dados pessoais são representados. São exemplos que poderão ser utilizados, isolada ou cumulativamente, a depender do caso concreto: nuvem (especificar servidor), documento eletrônico DOCX e similares, documento eletrônico PDF e similares, planilha eletrônica EXCEL e similares, mídia eletrônica MP3 e similares, mídia eletrônica MP4 e similares, mídia eletrônica JPEG e similares, disco óptico (CD, DVD e Blu-Ray), pen-drive, cartão de memória, HD externo, SSD, fita magnética, disquete, disco fonográfico (vinil, compacto-simples e goma-laca), cilindro fonográfico, material biológico e papel.>

<Deve ser especificado o tempo e a fonte de retenção para cada subcategoria de dados pessoais elencada, na eventualidade de serem armazenadas, temporal ou materialmente, de forma distinta. Ou seja, havendo duas subcategorias de dados pessoais em "Detalhes de identificação pessoal", como "nome" e "endereço residencial", devem ser descritos os distintos tempos e fontes de retenção dessas duas subcategorias.>

Identificação pessoal: <**há** ou **não há**.>

a. Detalhes de identificação pessoal: *<Descrever se são tratados dados como nome, endereço residencial, histórico de endereços anteriores, número de telefone fixo residencial, número de celular pessoal, e-mail pessoal, etc.>*
Tempo de retenção:
Fonte de retenção:

i. Dados de identificação pessoal atribuídos por instituições governamentais: *<Descrever se são tratados dados de identificação como CPF, RG, número de passaporte, número de carteira de motorista, número de registro em conselho profissional, etc.>*
Tempo de retenção:
Fonte de retenção:

b. Dados de identificação eletrônica: *<Descrever se são tratados dados como endereços IP, cookies, etc.>*
Tempo de retenção:
Fonte de retenção:

c. Dados de localização eletrônica: *<Informar se são tratados dados de comunicação de torres de celulares (e.g., GSM), dados de GPS, etc.>*
Tempo de retenção:
Fonte de retenção:

Corpo: <**há** ou **não há**.>

a. Detalhes biográficos: <*Descrever se são tratados dados pessoais como idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.*>
Tempo de retenção:
Fonte de retenção:

b. Detalhes militares: <*Descrever se são tratados dados como situação militar, patente militar e distinções militares.*>
Tempo de retenção:
Fonte de retenção:

c. Descrição física: <*Dados de descrição física são informações físicas de uma pessoa com possibilidade de serem visivelmente identificadas. Descrever se são tratados dados como altura, peso, cor do cabelo, cor dos olhos, características distintivas, etc.*>
Tempo de retenção:
Fonte de retenção:

d. Detalhes imigratórios: <*Descrever se são tratados dados como detalhes sobre visto, autorização de trabalho, limitações de residência ou movimentação, condições especiais relacionadas à autorização de residência, etc.*>
Tempo de retenção:
Fonte de retenção:

Mente: <**há** ou **não há**.>

a. Descrição psicológica: <*Descrever se são tratados dados sobre personalidade ou caráter.*>
Tempo de retenção:
Fonte de retenção:

Imagem: <**há** ou **não há**.>

a. Vídeo e imagem: <*Descrever se são tratados arquivos de vídeos, fotos digitais, fitas de vídeo, etc.*>
Tempo de retenção:
Fonte de retenção:

i. Vídeo e imagem enquanto relacionados à segurança pública: <*Descrever se são tratadas imagens e/ou vídeos de câmeras de segurança/vigilância (e.g., CFTV), etc.*>
Tempo de retenção:
Fonte de retenção:

b. Voz: *<Descrever se são tratadas fitas e arquivos digitais de voz, bem como outros registros de gravações de voz.>*
Tempo de retenção:
Fonte de retenção:

Hábitos: <**há** ou **não há**.>

a. Detalhes sobre hábitos pessoais: *<Descrever se são tratados dados como uso de tabaco, uso de álcool, hábitos alimentares e dieta alimentar.>*
Tempo de retenção:
Fonte de retenção:

b. Detalhes sobre estilo de vida: **<Descrever se são tratados dados como informações sobre o uso de bens ou serviços e comportamentos característicos dos titulares dos dados.>**
Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre distinções: *<Descrever se são tratados dados como distinções civis, administrativas ou militares.>*
Tempo de retenção:
Fonte de retenção:

d. Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais: *<Descrever se são tratados dados sobre bens e outros direitos enquanto relacionados aos hábitos pessoais do titular.>*
Tempo de retenção:
Fonte de retenção:

e. Detalhes sobre viagens e deslocamentos: *<Descrever se são tratados dados sobre antigas residências e deslocamentos, visto de viagem, autorizações de trabalho, etc.>*
Tempo de retenção:
Fonte de retenção:

f. Detalhes sobre denúncias, incidentes ou acidentes: *<Descrever se são tratados dados como informações sobre um acidente, incidente ou denúncia na qual o titular dos dados está envolvido, a natureza dos danos ou ferimentos, pessoas envolvidas, testemunhas, etc.>*
Tempo de retenção:
Fonte de retenção:

g. Detalhes sobre núcleos sociais: <*Descrever se são tratados dados como amigos, parceiros de negócios, relacionamentos com pessoas que não sejam familiares próximos, etc.*>
Tempo de retenção:
Fonte de retenção:

h. Detalhes sobre uso de mídias: <*Descrever se são tratados dados que definem o comportamento de uso de mídias e meios de comunicação.*>
Tempo de retenção:
Fonte de retenção:

Lazer: <**há** ou **não há**.>

a. Detalhes sobre interesses de lazer: <*Descrever se são tratados dados sobre hobbies, esportes, dentre outros interesses.*>
Tempo de retenção:
Fonte de retenção:

Consumo: <**há** ou **não há**.>

a. Detalhes sobre bens e serviços enquanto relacionados aos hábitos de consumo: <*Descrever se são tratados dados sobre bens e serviços consumidos pelo titular de dados.*>
Tempo de retenção:
Fonte de retenção:

Finanças: <**há** ou **não há**.>

a. Dados de identificação financeira: <*Descrever se são tratados dados como números de identificação, números de contas bancárias, números de cartões de crédito ou débito, códigos secretos, etc.*>
Tempo de retenção:
Fonte de retenção:

b. Detalhes sobre recursos financeiros: <*Descrever se são tratados dados como renda, posses, investimentos, renda total, renda profissional, poupança, datas de início e término dos investimentos, receita de investimento, dívidas sobre ativos, etc.*>
Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre dívidas e despesas: *<Descrever se são tratados dados como total de despesas, aluguéis, empréstimos, hipotecas e outras formas de crédito.>*
Tempo de retenção:
Fonte de retenção:

d. Detalhes sobre a situação financeira: *<Descrever se são tratados dados de solvência, ou seja, avaliação do rendimento e avaliação de capacidade de pagamento.>*
Tempo de retenção:
Fonte de retenção:

e. Detalhes sobre empréstimos, hipotecas e linhas de crédito: *<Descrever se são tratados dados como natureza do empréstimo, valor emprestado, saldo remanescente, data de início, período do empréstimo, taxa de juros, visão geral do pagamento e detalhes sobre as garantias.>*
Tempo de retenção:
Fonte de retenção:

f. Detalhes sobre assistência financeira: *<Descrever se são tratados dados como de benefícios, assistência, bonificações, subsídios, etc.>*
Tempo de retenção:
Fonte de retenção:

g. Detalhes de apólice de seguro: *<Descrever se são tratados dados como natureza da apólice de seguro, detalhes sobre os riscos cobertos, valores segurados, período segurado, data de rescisão, pagamentos feitos, recebidos ou perdidos, situação do contrato, etc.>*
Tempo de retenção:
Fonte de retenção:

h. Detalhes de plano de pensão: *<Descrever se são tratados dados como data efetiva do plano de pensão, natureza do plano, data de término do plano, pagamentos recebidos e efetuados, opções, beneficiários, etc.>*
Tempo de retenção:
Fonte de retenção:

i. Detalhes sobre transações financeiras: *<Descrever se são tratados dados como valores pagos e a pagar pelo titular dos dados, linhas de crédito concedidas, avais, forma de pagamento, visão geral do pagamento, depósitos e outras garantias, etc.>*
Tempo de retenção:
Fonte de retenção:

j. Detalhes sobre compensações: *<Descrever se são tratados dados como de detalhes sobre compensações reivindicadas, valores pagos ou outros tipos de compensação, etc.>*
Tempo de retenção:
Fonte de retenção:

k. Detalhes sobre atividades profissionais: *<Descrever se são tratados dados de atividades profissionais executadas pelo titular de dados, como natureza da atividade, natureza dos bens ou serviços utilizados ou entregues pela pessoa em registro, relações comerciais, etc.>*
Tempo de retenção:
Fonte de retenção:

l. Detalhes sobre acordos e ajustes comerciais: *<Descrever se são tratados dados como detalhes sobre acordos ou ajustes comerciais, acordos sobre representação ou acordos legais, etc.>*
Tempo de retenção:
Fonte de retenção:

m. Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros: *<Descrever se são tratados dados financeiros baseados no consentimento de seu titular>.*
Tempo de retenção:
Fonte de retenção:

Residência: <**há** ou **não há**.>

a. Detalhes residenciais: *<Descrever se são tratados dados sobre natureza da residência, propriedade própria ou alugada, duração da residência nesse endereço, aluguel, custos, classificação da residência, detalhes sobre a avaliação, nomes das pessoas que possuem as chaves.>*
Tempo de retenção:
Fonte de retenção:

Família: <**há** ou **não há**.>

a. Detalhes sobre relacionamentos atuais: *<Descrever se são tratados dados como nome do cônjuge ou companheiro(a), nome de solteiro(a), do cônjuge ou companheiro (a), data de casamento, data do contrato de coabitação, número de filhos, etc.>*
Tempo de retenção:
Fonte de retenção:

b.Detalhes sobre relacionamentos anteriores: <*Descrever se são tratados dados sobre casamentos ou parcerias anteriores, divórcios, separações, nomes de parceiros anteriores, etc.*>
Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre núcleo familiar: <*Descrever se são tratados dados sobre outros familiares ou membros da família do titular de dados.*>
Tempo de retenção:
Fonte de retenção:

Educação: <**há** ou **não há**.>

a. Dados acadêmicos: <*Descrever se são tratados dados sobre diplomas, certificados obtidos, resultados de exames, avaliação do progresso dos estudos, histórico escolar, grau de formação, etc.*>
Tempo de retenção:
Fonte de retenção:

b. Dados financeiro-acadêmicos: <*Descrever se são tratados dados sobre taxas de inscrição e custos pagos, financiamento, formas de pagamento, registros de pagamento, etc.*>
Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre qualificações e experiências acadêmico-profissionais: <*Descrever se são tratados dados sobre certificações profissionais, interesses profissionais, interesses acadêmicos, interesses de pesquisa, experiência de ensino, etc.*>
Tempo de retenção:
Fonte de retenção:

Trabalho: <**há** ou **não há**.>

a. Detalhes sobre ocupações atuais: <*Descrever se são tratados dados sobre empregador, descrição do cargo e função, antiguidade, data de recrutamento, local de trabalho, especialização ou tipo de empresa, modos e condições de trabalho, cargos anteriores e experiência anterior de trabalho no mesmo empregador, etc.*>
Tempo de retenção:
Fonte de retenção:

b. Detalhes sobre processos de seleção: <*Descrever se são tratados dados sobre data de seleção, método de seleção, fonte de seleção, referências, detalhes relacionados à período de estágio, etc.*>

Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre rescisões: <*Descrever se são tratados dados sobre data de rescisão, motivo, período de notificação, condições de rescisão, etc.*>
Tempo de retenção:
Fonte de retenção:

d. Detalhes sobre ocupações anteriores: <Descrever se são tratados dados sobre ocupações anteriores e empregadores, períodos sem emprego, serviço militar, etc.>
Tempo de retenção:
Fonte de retenção:

e. Detalhes sobre avaliações de desempenho: <*Descrever se são tratados dados sobre avaliações de desempenho ou qualquer outro tipo de análise de qualificação ou habilidades profissionais.*>
Tempo de retenção:
Fonte de retenção:

f. Detalhes sobre disciplina e absenteísmo: <*Descrever se são tratados dados sobre registros de absentismo, motivos de ausência, medidas disciplinares, etc.*>
Tempo de retenção:
Fonte de retenção:

Filiações: <**há** ou **não há**.>

a. Detalhes sobre associações as quais é filiado o titular de dados pessoais (exceto profissionais, políticas, sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis): <*Descrever se são tratados dados sobre participação em organizações de caridade ou benevolentes, clubes, parcerias, grupos, etc.*>
Tempo de retenção:
Fonte de retenção:

Conflitos: <**há** ou **não há**.>

a. Detalhes sobre processos judiciais em curso: <*Descrever se são tratados dados sobre suspeitas de violações, conexões conspiratórias com criminosos conhecidos, inquéritos ou ações judiciais (civis ou criminais) empreendidas por ou contra o titular de dados, etc.*>
Tempo de retenção:
Fonte de retenção:

b. Detalhes sobre decisões judiciais: <*Descrever se são tratados dados sobre decisões cíveis e criminais que envolvam o titular de dados.*>
Tempo de retenção:
Fonte de retenção:

c. Detalhes sobre processos administrativos em curso: <*Descrever se são tratados dados sobre processos administrativos em curso que envolvam o titular de dados.*>
Tempo de retenção:
Fonte de retenção:

d. Detalhes sobre decisões administrativas: <*Descrever se são tratados dados de decisões administrativas, como em processos administrativos disciplinares, e sanções respectivas, como advertências e multas, além de qualquer outro tipo de sanção administrativa prevista em normas ou regulamentos administrativos.*>
Tempo de retenção:
Fonte de retenção:

Outros: <***Há*** *ou* ***não há****. Especifique se há outras categorias de dados pessoais tratadas que não tenham sido contempladas anteriormente.*>

11. Informe as categorias de dados pessoais sensíveis tratadas neste processo, de acordo com os enunciados a seguir e os descrevendo com base: (i) no tempo de retenção dos dados pessoais; e (ii) na fonte de retenção dos dados pessoais.

<Dado pessoal sensível é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.>

<Em caso de inexistência de tratamento de determinada categoria de dados pessoais, responda "Não há".>

<O tempo de retenção de dados pessoais se relaciona à Política Municipal de Gestão Documental, assim como ao Sistema de Arquivo do Município de São Paulo.>

<A fonte de retenção de dados pessoais é o substrato no qual os dados pessoais são representados. São exemplos que poderão ser utilizados, isolada ou cumulativamente, a depender do caso concreto: nuvem (especificar servidor), documento eletrônico DOCX e similares, documento eletrônico PDF e similares, planilha eletrônica EXCEL e similares, disco óptico (CD, DVD e Blu-Ray), pen-drive, cartão de memória, HD externo, SSD, fita magnética, disquete, disco fonográfico (vinil, compacto-simples e goma-laca), cilindro fonográfico, material biológico e papel.>

<Deve ser especificado o tempo e a fonte de retenção para cada subcategoria de dados pessoais elencada, na eventualidade de serem armazenadas, temporal ou materialmente, de forma distinta. Ou seja, havendo duas subcategorias de dados pessoais sensíveis, devem ser descritos os distintos tempos e fontes de retenção dessas duas subcategorias.>

Dados pessoais sensíveis: <**há** ou **não há**.>

a. Revelem origem racial ou étnica:
Tempo de retenção:
Fonte de retenção:

b. Revelem convicção religiosa:
Tempo de retenção:
Fonte de retenção:

c. Revelem filiação a organização de caráter religioso:
Tempo de retenção:
Fonte de retenção:

d. Revelem opinião política:
Tempo de retenção:
Fonte de retenção:

e. Revelem filiação a organização de caráter político:
Tempo de retenção:
Fonte de retenção:

f. Revelem filiação a sindicato:
Tempo de retenção:
Fonte de retenção:

g. Revelem filiação a organização de caráter filosófico:
Tempo de retenção:
Fonte de retenção:

h. Refiram-se à saúde ou à vida sexual:
Tempo de retenção:
Fonte de retenção:

i. Refiram-se a dados genéticos:
Tempo de retenção:
Fonte de retenção:

j. Refiram-se a dados biométricos: *<Descrever se são tratados dados de impressões digitais e de voz, digitalizações de íris, reconhecimento facial, reconhecimento de formato de dedo ou mão, assinaturas dinâmicas, etc.>*
Tempo de retenção:
Fonte de retenção:

12. **Com qual frequência os dados pessoais são tratados?**

<Descrever em que frequência os dados são tratados. Isso representa a disponibilidade e horário de funcionamento do sistema automatizado ou processo manual que trata os dados pessoais.>

Resposta:

13. Qual o volume de categorias de dados pessoais tratados?

<Informar o volume total de categorias de dados pessoais e de dados pessoais sensíveis descritos neste mapeamento de dados pessoais relacionados a determinado processo.
Exemplo:
Categorias de dados pessoais tratados:
Idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.
Categorias de dados pessoais sensíveis tratadas:
Tratamento de dados pessoais de saúde como CID10 e data de último exame médico.
Neste caso, a informação que deve ser preenchida é:
São tratadas 6 categorias de dados pessoais (idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade) e 02 categorias de dados pessoais sensíveis (CID10 e data de último exame médico), totalizando 08 categorias tratados pelo processo.>

Resposta:

14. **Quais são as categorias de titulares de dados pessoais deste processo? São tratados dados pessoais de crianças, adolescentes e outros grupos vulneráveis?**

<Informar quem são os titulares de dados pessoais deste processo. Exemplos: crianças e adolescentes, munícipes, servidores ativos e inativos, pacientes, educandos, etc.>

Resposta:

15. Os dados pessoais tratados neste processo são compartilhados? Se sim, com quem?

<Informe o nome da empresa ou instituição com a qual os dados pessoais são compartilhados. Exemplos: Microsoft, Google, IBGE, Ministério Público, Receita Federal, Controladoria-Geral da União e Ministério da Saúde.>

<Apenas devem ser indicadas instituições que não façam parte da Prefeitura do Município de São Paulo, o que inclui sua administração pública direta e indireta. Exclui-se, dessa forma, a PRODAM, mas inclui-se as empresas com as quais esta compartilha os dados pessoais tratados pela Prefeitura do Município.>

Resposta:

16. Em sua análise, há medida(s) de segurança, técnicas e administrativas, atualmente em curso que proteja(m) os dados pessoais tratados neste processo? Se sim, qual(is)?

<Indicar se existem atualmente medidas de segurança, técnicas e administrativas, aptas à proteção dos dados pessoais, isto no âmbito de seu órgão ou entidade, ou, se aplicável, de forma global, na Prefeitura do Município de São Paulo ou em sua entidade. Exemplos: controles de segurança em recursos humanos; controles de acesso físico; controles de acesso lógico; controles de segurança física e do ambiente; controles de segurança nas comunicações; controles de conformidade das licitações, contratos administrativos, convênios e instrumentos congêneres; Política de Segurança da Informação; Política de Senhas; Política de Mesa Limpa; Política de Backup; Política de Privacidade e Proteção de Dados Pessoais; Política de Cookies; e Política de Gestão de Incidentes de Segurança da Informação.>

Resposta:

17. Há transferência internacional dos dados tratados neste processo? Se sim, qual(is) é (são) a(s) categoria(s) de dados pessoais e de dados pessoais sensíveis transferidas? Essa transferência internacional está protegida por alguma garantia?

<Indicar se os dados pessoais tratados neste processo são transferidos, como para armazenamento por provedor de nuvem, para fora do Brasil. Em caso afirmativo, se possível, indicar o país no qual os dados pessoais são tratados.>

<São exemplos de garantias para a realização de transferência internacional de dados pessoais: acordo de cooperação internacional; certificação regularmente emitida; cláusulas contratuais específicas para determinada transferência; cláusulas-padrão contratuais; código de conduta regularmente emitido; cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular; execução de política pública ou atribuição legal do serviço público; exercício regular de direitos em processo judicial, administrativo ou arbitral; fornecimento de consentimento específico pelo titular de dados pessoais; normas corporativas globais; país que fornece um nível adequado de proteção; proteção da vida ou da incolumidade física do titular ou de terceiro; selo regularmente emitido; e transferência autorizada pela Autoridade Nacional de Proteção de Dados (ANPD).>

Resposta:

18. Quais são os contratos de serviços e/ou soluções de tecnologia da informação que possuem relação com o tratamento de dados pessoais deste processo?

<Informe os números e os "links" de acesso dos contratos de serviços e/ou soluções de tecnologia da informação que realizam algum tipo de operação de tratamento com os dados pessoais deste processo.>

Resposta:

CONTROLADORIA E OUVIDORIA GERAL DO ESTADO DO CEARÁ
CGE/CE

Histórico - origem, contexto e motivações

A partir da publicação da Lei Federal Nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD) a Controladoria e Ouvidoria Geral do Estado do Ceará tem buscado tomar medidas para se adequar a referida legislação visando resguardar os direitos dos titulares de dados e a proteção de seus dados pessoais.

Nesse contexto em 09/10/2020 a CGE/CE, por meio da portaria 90/2020, institui e designa Comissão Setorial, com caráter temporário, para propor ações relacionadas à adequação a Lei Geral de Proteção de Dados Pessoais – LGPD, fixando prazo de 30 dias para que seja estabelecido plano de ação visando alavancar as medidas necessárias ao cumprimento da norma vigente.

Desta forma a partir das atividades desenvolvidas no âmbito da Comissão foi estabelecido plano de ação por meio da Portaria 105/2020 de 01/12/2020 conforme abaixo:

PLANO DE AÇÃO LGPD CGE			
1. Processos de Negócio e Ferramentas	Responsável	Data Ínicio	Data Fim
1.1 Criar Inventário contendo as ferramentas tecnológicas da CGE que tratem dados pessoais	Áreas de Negócio e TIC	01/09/2020	14/09/2020
1.2 Identificar quais dados pessoais são tratados por ferramenta tecnológica	Áreas de Negócio e TIC	16/09/2020	16/10/2020
1.3 Identificar a finalidade e as bases legais relacionadas ao tratamento de dados	Áreas de Negócio e TIC	17/10/2020	30/11/2020
1.4 Identificar se existem compartilhamento dos dados pessoais com outras instituições	Áreas de Negócio e TIC	17/10/2020	30/11/2020
1.5 Alterar processos para a exclusão de dados pessoais desnecessários ao negócio da CGE	Áreas de Negócio e TIC	01/01/2021	31/12/2021

PLANO DE AÇÃO LGPD CGE			
1. Processos de Negócio e Ferramentas	Responsável	Data Ínicio	Data Fim
1.6 Ajustar processo de Gerenciamento de projetos para tratar novas funcionalidades que tratem dados pessoais	TIC	01/10/2021	31/12/2021
2. Gestão da Privacidade	Responsável	Data Ínicio	Data Fim
2.1 Identificar os processos onde é necessário obter o consentimento do titular dos dados	Áreas de Negócio	01/01/2021	31/12/2021
2.2 Criar/Ajustar termo de privacidade nas ferramentas tecnológicas	Áreas de Negócio	01/01/2021	31/12/2021
3. Proteção de Dados	Responsável	Data Ínicio	Data Fim
3.1 Revisar o armazenamento atual de dados pessoais	TIC	01/01/2022	30/06/2022
3.2 Identificar medidas técnicas e organizacionais adequadas para proteger os dados	TIC	01/01/2022	30/06/2022
3.3 Implementar medidas técnicas para proteção de dados pessoais	TIC	01/01/2022	30/06/2022
4. Retenção de Dados e Backup	Responsável	Data Ínicio	Data Fim
4.1 Revisão procedimento de Retenção de Backup	TIC	01/01/2022	30/06/2022
4.2 Alterar política de retenção de Backup	TIC	01/01/2022	30/06/2022
4.3 Remover dados pessoais levantados no item 1.5 dos backups existentes	TIC	01/01/2022	30/06/2022

Em tempo, em 28/10/2021 foi instituído pela Portaria 59/2021 o Grupo de Trabalho Setorial que trata a adequação da LGPD no âmbito da CGE/CE que dentre as suas principais atribuições estão o acompanhamento da execução do plano de ação, o mapeamento dos processos não contemplados no plano de ação, promoção de capacitações e promoção de demais ações de adequação à LGPD.

Objetivo/Escopo

A partir das discussões realizadas no âmbito da Comissão Setorial, foi definido como escopo inicial a priorização de ações relacionadas a adequação das ferramentas tecnológicas da CGE considerando principalmente dois critérios importantes:

- a competência da CGE em gerenciar diversas plataformas tecnológicas corporativas que possuem um amplo volume e variedade de dados pessoais, como por exemplo as plataformas de Transparência, Ouvidoria, Acesso à Informação, Contratos, Convênios e Congêneres;

- os mapeamentos dos processos de negócios da CGE/CE não estão totalmente concluídos, trabalho esse que está em andamento no âmbito do Sistema de Gestão da Qualidade da CGE/CE.

Desta forma, considerando este escopo traçou-se os seguintes objetivos específicos no que se refere ao inventário de dados pessoais:

- realizar o inventário das ferramentas tecnológicas que tratem dados pessoais;

- realizar o inventário de dados pessoais que são tratados em cada ferramenta;

- identificar e catalogar as finalidades e bases legais relacionadas ao tratamento dos dados pessoais;

- identificar e catalogar os dados pessoais que são compartilhados com outras instituições.

Estrutura da CGE/CE

Em 2003, o Poder Executivo do Estado do Ceará instituiu por meio da Lei nº. 13.297/2003, seu órgão central de controle interno, inicialmente chamado de Secretaria da Controladoria (Secon). Ao longo dos anos, a Controladoria e Ouvidoria Geral do Estado passou por transformações, ampliando suas competências institucionais, abrigando hoje as ações dos sistemas governamentais de Ouvidoria, Transparência, Controladoria, Auditoria Governamental e Correição.

Sua estrutura organizacional e competências estão dispostas na Lei nº 16.710, de 21 de dezembro de 2018, e regulamentadas no Decreto nº 34.002, de 24 de março de 2021, no esforço contínuo de atender às políticas e estratégias da ação governamental previstas nas suas atribuições.

Sua Missão consiste em Coordenar e exercer atividades de Transparência, Ouvidoria, Correição, Auditoria Governamental, Ética e Controladoria no Poder Executivo, contribuindo para a melhoria da gestão pública e do controle social, em benefício da sociedade.

Governança

Em outubro foi instituído pela Portaria 59/2021 o Grupo de Trabalho Setorial que trata a adequação da LGPD no âmbito da CGE/CE, onde esse grupo é composto por 8 (oito) membros contemplando as áreas de Tecnologia, Assessoria Jurídica, Transparência, Ouvidoria e Gestão Superior.

Capacitação /Treinamento

Durante a jornada de adequação os membros do Grupo de Trabalho Setorial e demais colaboradores da Controladoria foram contemplados com palestras e seminários sobre a LGPD.

O XV Encontro Estadual de Controle Interno promovido pela CGE/CE em dezembro de 2021 teve como tema Controle Interno, Proteção de Dados e Transparência, onde foi apresentando um Painel sobre a Lei Geral de Proteção de Dados no Setor Público.

Não obstante a essas atividades estão sendo planejadas para 2023 capacitações mais específicas para os membros do Grupo de Trabalho Setorial e o Encarregado de Dados Pessoais da CGE/CE.

Metodologia

Para elaboração do IDP de cada ferramenta tecnológica foram realizadas as seguintes atividades:

- elaboração de um formulário padrão para catalogar os dados pessoais contidos em cada ferramenta e as possíveis bases legais que resguardam o tratamento de dados pessoais;
- envio do formulário para a área de negócio responsável por cada ferramenta para preenchimento;
- reuniões entre as áreas de negócio e área de tecnologia para validação do preenchimento do formulário;
- exclusão de dados pessoais que não tinham características aderentes a finalidade dos processos de negócio das ferramentas;

- validação do formulário pela Comissão Setorial;
- criação de Aviso de Privacidade para cada ferramenta.

Principais Desafios

Durante o processo de elaboração do inventário de dados pessoais foram encontradas algumas dificuldades conforme abaixo:

- necessidade de uma compreensão mais ampla acerca dos requisitos da legislação;
- necessidade de um Modelo de Governança de Dados;
- artefatos relacionados a documentação de sistemas, como dicionários de dados, em parte, desatualizados;
- necessidade de atualizar o processo de gerenciamento de projetos de software para contemplar revisões periódicas do inventário de dados pessoais na medida em que novas funcionalidades forem criadas nas ferramentas;
- necessidade de um levantamento mais detalhado contemplando todo ciclo de vida dos dados pessoais, desde o momento em que o dado é coletado até o término do tratamento. A partir dessas informações, pode ser realizada a identificação, avaliação e monitoramento dos riscos a que o órgão/entidade está exposto.

Resultados Alcançados

A partir do trabalho realizado para elaboração do inventário de dados pessoais foi possível fazer uma reflexão acerca de um dos princípios fundamentais da Lei Geral de Proteção de Dados que é o da finalidade. É bastante comum que no processo de desenvolvimento de ferramentas tecnológicas sejam solicitadas funcionalidades que busquem armazenar uma série de dados pessoais que não tenham uma relação direta com a finalidade do sistema ou do negócio, entretanto a partir da LGPD esse modelo precisou ser repensado pois o princípio da finalidade estabelece que somente deverão ser tratados dados pessoais que tenha finalidade relacionada ao negócio da organização, portanto a partir do trabalho de elaboração do inventário foi possível eliminar dos sistemas dados pessoais que fugiam a finalidade da CGE.

Um outro ponto de destaque foi que ao final do trabalho foi possível ter catalogado os dados pessoais que estão sendo tratados, as bases legais que resguardam esse tratamento e a disponibilização desse inventário por meio dos avisos de privacidade que estão disponibilizados em cada ferramenta o que nos permitiu também atender ao princípio da transparência.

Por fim o sucesso desse trabalho se deve principalmente ao engajamento das pessoas, o trabalho em conjunto das áreas de negócio responsáveis por cada ferramenta, área de tecnologia, Comissão Setorial LGPD, além do patrocínio da Alta Gestão da CGE/CE.

Modelo utilizado para elaboração do IDP

INVENTÁRIO DE DADOS PESSOAIS				
Dados Iniciais				
Nome do Sistema:	<Preencha com o nome do Sistema>			
Gestor do Sistema:	<Preencha com o nome do Gestor do Sistema>			
Data da Criação:	<Preencha com a data de criação do IDP>			
Data da última atualização	<Preencha com a data da última atualização do IDP>			
Controlador:	<Preencha com o nome do Controlador, pessoa a quem compete as decisões referente ao tratamento de dados pessoais>			
Operador:	<Preencha com o nome do Operador, pessoa que realiza o tratamento de dados pessoais em nome do Controlador>			
Encarregado de Dados:	<Preencha com o nome do Encarregado, pessoa que será o canal de comunicação com os titulares de dados pessoais>			
Dados Pessoais				
Módulo	Funcionalidade	Dados Pessoal	Sensível	Finalidade/ Base Legal
<Preencha com o módulo do Sistema Ex: Ouvidoria>	<Preencha com a Funcionalidade do Sistema Ex: Criação do Perfil>	<Preencha o Nome do dado pessoal Ex: CPF>	<Preencha com o Sim para indicar se o dado pessoal em questão é classificado como sensível Ex: Sim>	<Preencha com a finalidade e a base legal que resguarde o tratamento do dado pessoal Ex: Preenchimento obrigatório: Caso o cidadão opte por receber a resposta por email; Preenchimento opcional: no restante dos casos. Finalidade: Caso opte por receber a resposta por email e, também, ter uma base de dados que possa ser futuramente utilizada para avaliação de algum serviço, participação de pesquisas, etc. Art. 23 da Lein° 13460/2017>

CONTROLADORIA GERAL DO ESTADO DE GOIÁS
CGE/GO

Este material, elaborado pela equipe do Núcleo de Projetos Governamentais da Controladoria Geral do Estado de Goiás (CGE-GO), busca fazer um apanhado das ações internas referentes ao processo de adequação à Lei Geral de Proteção de Dados Pessoais - LGPD (Lei Federal 13.709/2018) tomadas até o momento, dando especial atenção ao Piloto de Inventário de Dados Pessoais (IDP), providência mais concreta realizada pelo órgão.

Do mesmo modo, o trabalho pretende abordar o contexto de adequação estadual à norma, tratando sobre o seu aparato legal, estrutura de governança e cronograma de ações, sempre dando ênfase na participação da CGE-GO dentro deste processo.

Contexto do estado de Goiás

A Lei Geral de Proteção de Dados – LGPD (Lei Federal nº 13.709/2018), que dispõe sobre a proteção de dados pessoais da pessoa natural tratados pelo poder público e instituições privadas, exige uma série de providências legais, de governança e segurança da informação.

De forma geral, a Lei requer que as empresas e órgãos públicos aperfeiçoem a forma como lidam com dados pessoais e informações sensíveis, prevendo requisitos legais e de segurança da informação, bem como sanções administrativas e pecuniárias àqueles que não se adequarem ao dispositivo.

No âmbito do estado de Goiás, foi publicado o Decreto nº 10.092 de 6 de junho de 2022, que dispõe sobre a aplicação da LGPD na administração pública direta e indireta do Poder Executivo.

O dispositivo disciplina a respeito das diretrizes e competências a serem observadas, bem como sobre a criação da Rede de Encarregados pelo Tratamento de Dados Pessoais e do Comitê Estadual de Proteção de Dados Pessoais, composto pela Controladoria-Geral do Estado (que o preside), Secretaria do Estado e Administração, Secretaria de Estado da Ciência, Tecnologia e Inovação e Procuradoria-Geral do Estado

DECRETO ESTADUAL N° 10.092/22

REDE DE ENCARREGADOS PELO TRATAMENTO DE DADOS PESSOAIS

COMITÊ ESTADUAL DE PROTEÇÃO DE DADOS PESSOAIS

CONTROLADORIA-GERAL

SECRETÁRIA DO ESTADO DE DESENVOLVIMENTO E

PROCURADORIA-GERAL DO ESTADO

SECRETÁRIA DO ESTADO DE ADMINISTRAÇÃO

Desde a publicação do Decreto estadual n° 10.092/22,
foram tomadas diversas ações a fim de iniciar o processo de adequação à LGPD, dentre elas, destacam-se:

Nomeação do Comitê Estadual de Proteção de Dados Pessoais (CEPD)

Aprovação do Regimento Interno

Criação do Cronograma Macro de Ações

Capacitação do CEPD, por meio da Escola de Governo do Estado de Goiás (EGOV)

Inclusão da aba "LGPD" e das informações dos encarregados em todos os sites institucionais do governo

Criação do site "LGPD Goiás", plataforma voltada à comunicação entre os órgãos e o CEPD

Criação do site "LGPD Goiás", plataforma voltada à comunicação entre os órgãos e o CEPD

Para realizar a autenticação do usuário, solicita-se o login pelo "**gov.br**" e é necessário que o cidadão possua o "**selo prata**"

Considerando a vigência tanto da LGPD, quanto do Decreto estadual n° 10.092/22, e, acima de tudo, a necessidade de garantir ao cidadão goiano os direitos fundamentais de liberdade, privacidade e não discriminação, a CGE-GO, por meio do Núcleo de Projetos Governamentais e de outros setores, iniciou o seu processo interno de adequação, promovendo ações de planejamento, diagnóstico e conscientização sobre o tema da proteção de dados pessoais.

A Controladoria tem um papel estratégico na adequação estadual como presidente do CEPD, possuindo pioneirismo no estado no que se refere à LGPD.

Estrutura

A Controladoria Geral do Estado de Goiás (CGE-GO) é o órgão central dos sistemas de controle interno, correição, transparência e ouvidoria, órgão de assessoramento ao Governador do Estado, na forma da Lei n° 20.491, de 25 de junho de 2019. Destacam-se nas suas competências a defesa do patrimônio público e a prevenção e o combate à corrupção.

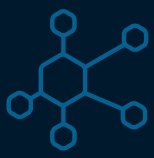
A formação desta Controladoria como unidade administrativa do Poder Executivo aconteceu em 2011, sendo criada com a função de dar assistência ao Governador no desempenho das suas atribuições atinentes à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, às atividades de ouvidoria, ao incremento da transparência da gestão.

Em 2019, foi aprovado o seu regulamento interno, com o estabelecimento de suas competências e a criação das Assessorias de Controle Interno nos órgãos.

No ano de 2021, o órgão se consolidou ainda mais, com a aprovação de sua Lei Orgânica, que dispõe sobre as funções e a carreira específica da CGE-GO também sobre os Sistemas de Controle Interno, de Ouvidoria e de Correição.

A CGE-GO possui **autonomia administrativa e** está ligada diretamente ao Chefe do Poder Executivo.

Áreas fins:
Controle Interno, Correição, Transparência, Controle Social e Ouvidoria



Quadro de servidores:
73,6% de efetivos (145)
26,4% comissionados (52)

Capacitação e treinamento

A Controladoria conta com um Plano de Conscientização em LGPD que visa reforçar o conhecimento sobre a legislação e adequar a sua aplicabilidade às atividades rotineiras dos servidores.

As ações estão divididas em duas frentes:

Conscientização geral, por veículos de comunicação interna

REDES SOCIAIS

REUNIÕES

INTRANET E CHAT GOIÁS

SITE

EVENTOS

Conscientização presencial direcionada a cada área

REUNIÕES

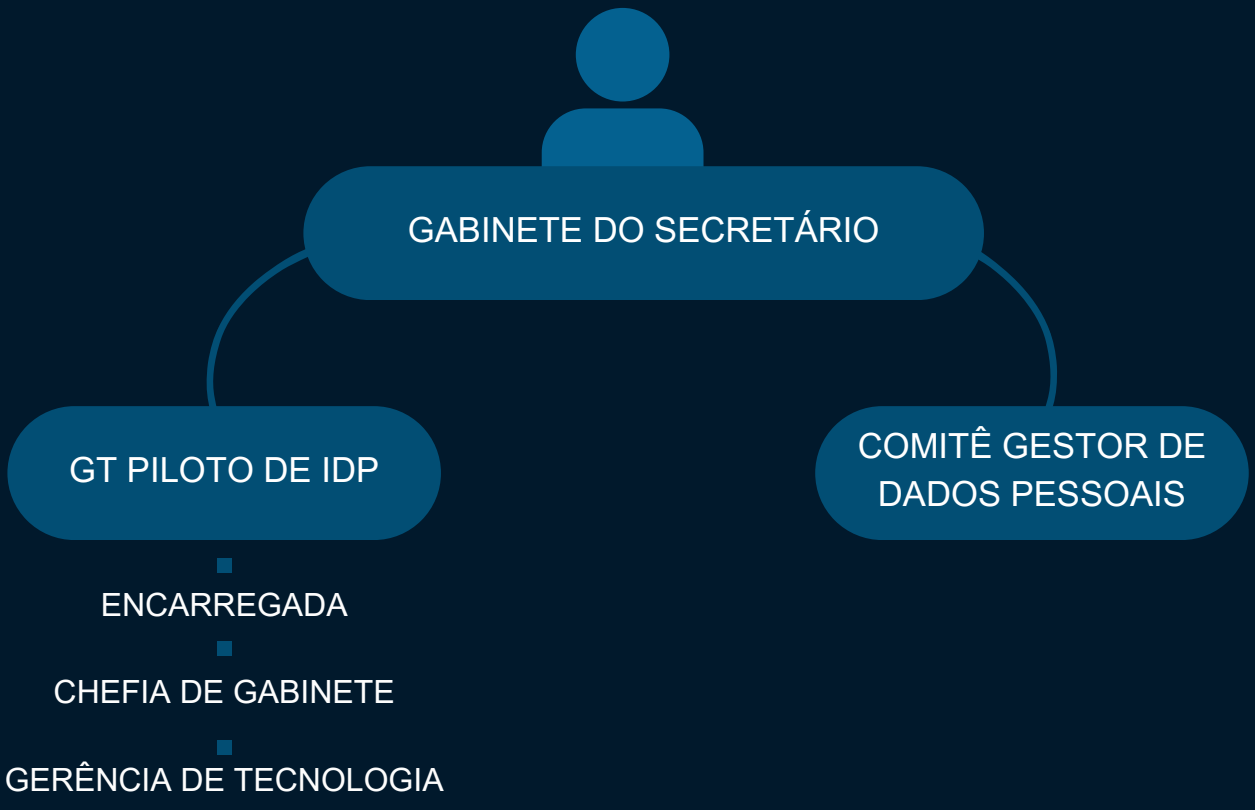
DEBATES EM GRUPO

INTRANET E CHAT GOIÁS

VISITA DA ENCARREGADA

Governança LGPD

A Controladoria conta com um Plano de Conscientização em LGPD que visa reforçar o conhecimento sobre a legislação e adequar a sua aplicabilidade às atividades rotineiras dos servidores. As ações estão divididas em duas frentes:



Processo de adequação à LGPD

O processo de adequação da Controladoria Geral do Estado à LGPD obedece ao Plano de Adequação que está dividido em 6 etapas, conforme figura abaixo:

1. Preparação e institucionalização da Política Geral de Proteção de Dados
2. Avaliação inicial e planejamento
3. Elaboração do Inventário de Dados Pessoais
4. Políticas de Governança de Dados Pessoais
5. Aprofundamento
6. Conformidade

Piloto de inventário de dados pessoais

Com o objetivo de dar prosseguimento na adequação à LGPD e em atendimento ao artigo 37 da Lei, que dispõe sobre a necessidade de manter o registro das operações de tratamento de dados pessoais, seguiu-se a execução da Etapa 2 – Avaliação Inicial e Planejamento, do Plano de Adequação à LGPD da CGE-GO. Para isso, elaborou-se o Projeto Piloto do Inventário de Dados Pessoais (Piloto de IDP).

O Inventário de Dados Pessoais (IDP) consiste na realização de um balanço que identifica os dados tratados pelo órgão, quais são as operações realizadas, o caminho percorrido, incluindo os processos e procedimentos pelos quais os dados pessoais transitam e seus requisitos legais para tratamento.

Esse registro mantido pelo IDP envolve descrever informações em relação ao tratamento de dados pessoais realizado pelo órgão ou entidade, tais como:

Agentes de tratamento (controlador e operador)

Hipótese e Previsão Legal (art. 7°, 11 e outros)

Finalidade

Tempo de retenção

Dados pessoais tratados e categorias dos titulares

Compartilhamento de dados e transferência internacional

Objetivo

O propósito do Piloto de IDP foi identificar os principais processos de negócio da CGE e determinar quais seriam incluídos na primeira avaliação do impacto geral.

Por ter umas duração menor do que a de um ciclo normal, também serviu para validar na prática o processo de trabalho proposto no Plano de Adequação à LGPD e para identificar peculiaridades do trabalho de adequação que não puderam ser antevistas durante a concepção do planejamento.

Método

O Piloto de IDP foi realizado por meio de formulário na plataforma “Smartsheet” contendo perguntas e respostas com opções de seleções pré-definidas e descritivas, visando facilitar e orientar as respostas a serem preenchidas pelos responsáveis da atividade (processo).

A plataforma utilizada proporciona a execução de trabalho com uma interface semelhante a uma planilha que ajuda as equipes a planejar, rastrear e gerenciar projetos em tempo real. Apresenta-se ainda como vantagem da utilização do software o baixo custo de contratação, base de dados própria do sistema, acesso à internet de qualquer navegador, painéis de controle de fácil visualização, e controle de acesso.

O Piloto de IDP foi realizado em 24 unidades administrativas da CGE-GO, por meio de entrevistas conduzidas pela Encarregada pelo Tratamento de Dados Pessoais, juntamente com profissionais de Tecnologia da Informação (GT do Piloto de IDP) que orientaram os participantes do processo no preenchimento do formulário.

Nesta primeira etapa, foram inventariados os principais processos que envolvem maior volume de dados pessoais tratados por cada unidade administrativa, com o propósito de conhecer o fluxo dos dados pessoais das principais atividades de cada área.

Método

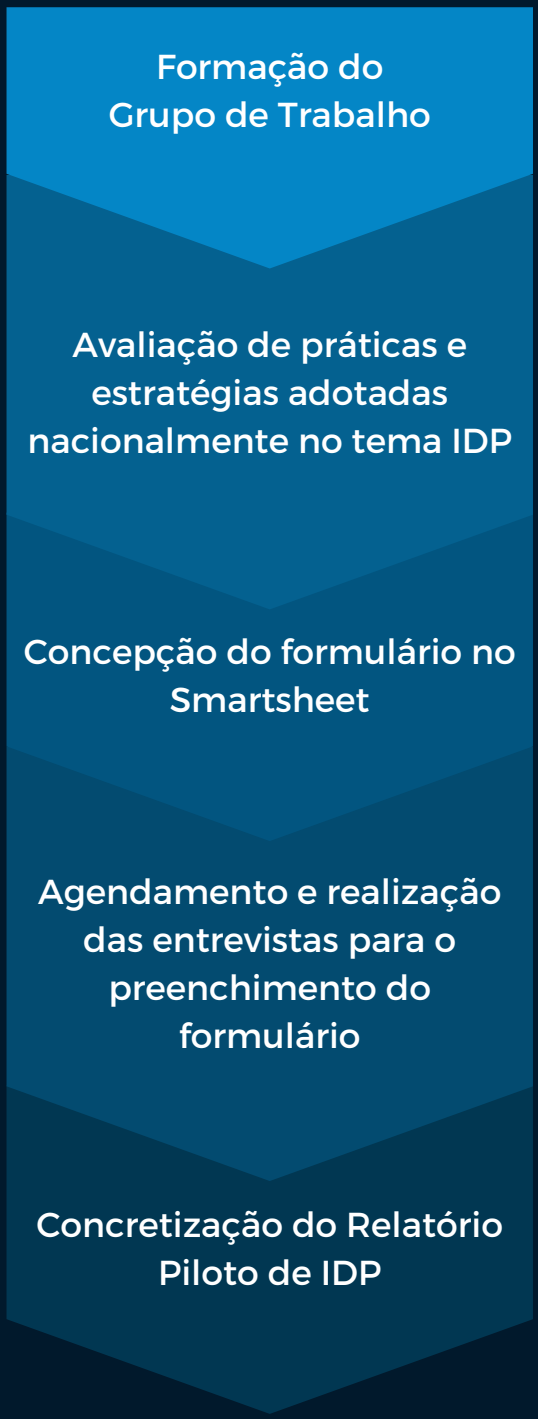
Grupo de Trabalho composto pela Encarregada pelo Tratamento de Dados Pessoais e profissionais de Tecnologia da Informação

Formulário na Plataforma Smartsheet

Entrevistas para o preenchimento do formulário

Mapeamento dos principais processos de 68,5% das unidades da CGE, priorizando as gerências

Fluxo de realização do piloto do IDP



Desafios

Legislação recente

A Lei Geral de Proteção de Dados Pessoais é um ordenamento jurídico novo no cenário brasileiro e sua implementação requer a todos os envolvidos no processo a compreensão e interpretação de seus requisitos e obrigações.

Cultura de Privacidade

A implementação da cultura de privacidade pressupõe que a proteção de dados deve ser incorporada em todas as áreas da organização, o que demanda mudanças no modo pelo qual o servidor se enxerga nesse processo.

Conscientização e Treinamento

O novo panorama trazido pela LGPD demanda conscientização e treinamento sobre a proteção, o manuseio e as responsabilidades de todos os envolvidos diretamente e indiretamente no tratamento de dados pessoais.

Mapeamento de Dados Pessoais

Necessidade de identificar e mapear todos os dados pessoais dos principais processos pela CGE, incluindo a localização, finalidade e base legal para o tratamento de cada tipo de dado

Governança e Gerenciamento

Estabelecer uma estrutura de governança eficaz para a proteção de dados, com a definição de responsabilidades claras em relação ao cumprimento da Lei.

Resultados alcançados

Realização do Piloto de IDP por meio de formulário do Smartsheet

Pesquisas realizadas preliminarmente em outros órgãos/estados, mostraram que os modelos de IDP apresentados foram feitos em planilhas do Word ou Excel, tendo as respostas feitas de modo descritivo. A realização do Piloto de IDP por meio de formulário do Smartsheet com respostas pré-definidas favoreceu na compreensão das informações relevantes para a formulação das respostas pelos servidores. Apresentou também como benefício a disponibilização de todas as informações em um único banco de dados, em que é possível extrair resultados analíticos referente ao tratamento.

Identificação e análise dos principais dados pessoais tratados na CGE

Foi possível identificar, de forma preliminar, os agentes do tratamento das principais processos/atividades da pasta, as categorias mais recorrentes de dados pessoais, o seu fluxo e os principais locais de armazenamento (backups, pastas digitais, armazenamento em nuvem, entre outros).

Compartilhamento e migração da base de dados

Com a identificação das atividades e suas fases (ciclo de vida), será possível definir uma forma (de acordo com as recomendações da ANPD) de compartilhamento e migração dos dados tratados, calculando seu impacto à instituição.

Prazos de armazenamento dos dados pessoais

Por meio da identificação dos dados pessoais pelo Piloto de IDP, haverá mais facilidade na identificação, prazo, armazenamento e eliminação dos mesmos.

Adoção de medidas técnicas e administrativas

A categorização dos dados pessoais por meio do IDP auxiliará na avaliação e adoção de medidas técnicas e administrativas capazes de mitigar riscos e prevenir a ocorrência de danos aos titulares.

Conscientização dos envolvidos

A instrução realizada pelos entrevistadores para a elaboração do Piloto de IDP com os servidores irá auxiliar na realização dos próximos IDPs, onde estes poderão orientar as sua equipe no preenchimento do formulário.

Controle de acesso às informações e medidas de segurança

Foi possível identificar, preliminarrmente, quais são os tipos de controle (medidas preventivas de autorização de acesso às informações) e as medidas de segurança recorrentes nas áreas, as quais serão avaliadas e aprimoradas no decorrer da adequação.

Resultados alcançados

O Piloto de IDP foi executado em 68,5% das áreas da CGE-GO.

As informações resultantes do preenchimento do formulário estão disponíveis em plataforma única, por meio do Smartsheet, ferramenta que possui diversos benefícios, como o baixo custo de contratação, interface acessível e intuitiva, e controle de acesso.

Categorização dos dados recorrentemente tratados pelo órgão.

Identificação dos fluxos de dados e principais locais de armazenamento.

Detecção de algumas vulnerabilidades que, em seguida, passaram a serem tratadas.

Referências Bibliográficas

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível aqui. Acesso em: 02 fev 2023.

GOIÁS (Estado). Decreto n° 10.092, de 6 de junho de 2022. Dispõe sobre a aplicação da Lei federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, no âmbito da administração pública direta e indireta do Poder Executivo estadual. Diário Oficial de Goiás: Goiânia, GO, ano 185, n. 23.810, p. 4, 6 jun. 2022.

Anexo

Este formulário visa identificar as operações de tratamento de dados pessoais realizados por esta instituição no papel de Controlador de Dados (LGPD, art. 5º, VI), no qual será atualizado e auditado regularmente, permitindo que esta pasta atenda ao requisito de manter um registro das operações de tratamento de dados pessoais, nos termos da LGPD, art. 37.

Deve-se preencher 1 FORMULÁRIO PARA CADA ATIVIDADE (PROCESSO) exercido dentro da unidade/setor. Após o envio do formulário, ele será recarregado para uma nova entrada.

1. Identificação do Servidor

1.1. Área 1.2. Nome do Servidor 1.3. Função

2. Identificação do macroprocesso, processo, dados pessoais e titulares de dados pessoais

2.1 Descrição do Macroprocesso
Visão geral do processo, podendo abranger vários processos principais ou secundários.

2.2 Descrição do Processo
Conjunto racionalmente sequenciado de operações (atividades e tarefas).

2.3 O processo realiza o tratamento de dados pessoais? Quais?
Dado pessoal é qualquer informação que permite identificar, direta ou indiretamente, um indivíduo (pessoa física) que esteja vivo.

2.4 O processo realiza o tratamento de dados pessoais sensíveis? Quais?
São os dados que, por sua sensibilidade, podem ser utilizados para fins discriminatórios, exigindo padrões mais rigorosos para o seu tratamento.
Nota: Caso tenha marcado a opção "Não trata dados pessoais" na pergunta anterior, e o seu processo também não trate dados sensíveis, marque a última alternativa.

2.5 Titular de Dados Pessoais

3. Identificação do Encarregado de Dados e Agentes de Tratamento

3.1 Encarregado de Dados
Nome do Encarregado de Dados

3.2 Agentes de Tratamento
De acordo com a LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o Controlador e o Operador.
a) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Neste inventário, o Controlador será a CGE.
b) Operador: empresa, entidade, órgão, fornecedor (direito público ou privado), terceiros (pessoa física ou jurídica) a quem compete o tratamento de dados pessoais em nome do controlador.
Exemplos: CIEE (contratação de estagiários para a CGE); G4F (prestação de serviços em construção de soluções tecnológicas para a CGE); SEDI (prestação de serviços corporativos para a CGE); entre outros.
Nota 1: O operador será sempre uma pessoa distinta do controlador, isto é, não atua como profissionalsubordinado a este ou como membro de seus órgãos.
Nota 2: Caso o tratamento de dados pessoais seja realizado pelos dois agentes (Controlador e Operador)
selecionar as duas opções.
Controlador
Operador

4. Respaldo Legal

4.1 Qual é a Finalidade do tratamento dos dados pessoais?
Finalidade é a razão ou motivo pelo qual é realizado o tratamento dos dados pessoais.

4.2 Qual é a base legal para o tratamento dos dados pessoais?
São os requisitos para o tratamento de dados pessoais dispostos no art. 7° da LGPD.
ATENÇÃO: as opções "Consentimento" e "Interesse Legítimos do Controlador ou de Terceiro" são limitadas no âmbito do setor público.

4.3 Qual é a base legal para o tratamento dos dados pessoais sensíveis?
São os requisitos para o tratamento de dados pessoais sensíveis dispostos no art. 11 da LGPD.

5.1 Indique as fases do ciclo de vida do tratamento de dados pessoais

Trata-se das quatro fases as quais correspondem aos tipos de tratamento de dados estabelecidos no art. 5°, inciso X, LGPD.

- Coleta: obtenção, recepção ou produção de dados pessoais – independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação, etc).
- Retenção: arquivamento ou armazenamento de dados pessoais – independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço, etc.).
- Processamento: qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.
- Compartilhamento: qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.
- Eliminação: qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

6. Coleta, armazenamento e descarte de dados pessoais

6.1 Qual é o motivo da coleta dos dados pessoais?

6.2 Qual a forma de coleta dos dados pessoais?

6.3 Qual é o local de armazenamento dos dados pessoais?

6.4 Qual o período de armazenamento dos dados pessoais?

6.5 Existe descarte dos dados?
Sim
Não

7. Compartilhamento de Dados Pessoais
É a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública.

7.1 Existe compartilhamento de dados pessoais com órgãos e entidades públicas e/ou privadas?
Sim
Não

8. Transferência internacional de dados pessoais

8.1 Existe transferência de dados pessoais para outro(s) país(es)?
Explicação: Trata-se da transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (art. 5º, inciso XV, LGPD).
Exemplos: troca de e-mails com entes internacionais, parcerias institucionais com compartilhamento ou transferência de dados pessoais para o exterior, acesso aos sistemas de uso da CGE no exterior, entre outros.
Sim
Não

9. Controles e medidas de segurança e privacidade

9.1 Qual(is) são os controle de acesso utilizados no tratamento dos dados pessoais?
Controle de acesso é a forma de colocar limites para que cada pessoa só tenha acesso ao que é necessário para o seu trabalho.

9.2 Quais são as medidas de segurança e privacidade utilizados no tratamento dos dados pessoais?
São precauções estabelecidas para proteger os dados coletados, armazenados, processados, compartilhados e transferidos.

Este anexo traz o formulário de forma incompleta.
Acesso ao inteiro teor:
https://app.smartsheet.com/b/form/9e30c649f8a04855b48955889cc3518b

CONTROLADORIA GERAL DO ESTADO DE MINAS GERAIS
CGE/MG

Histórico – origem, contexto e motivações

A adequação à Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) pela Administração Pública pressupõe um trabalho com amplo escopo de atividades, processos e estratégias. A implementação, ou adequação à LGPD, rapidamente se transforma em "as adequações". O conjunto de atividades envolve desde a formação e/ou fortalecimento de cultura institucional, avaliações e diagnósticos quanto aos processos da entidade, identificação de pontos de riscos e falhas, até planos para mitigação, assim como diversas outras ações que mobilizam toda a estrutura organizacional.

Na Controladoria-Geral do Estado de Minas Gerais (CGE-MG), os trabalhos associados à LGPD se iniciaram a partir de um grupo de trabalho[5] do Poder Executivo estadual, que tinha como objetivo conhecer as determinações legais e avaliar as possibilidades e necessidades de adequação da Administração do Estado. Ao lado das outras instituições (Secretaria de Estado de Planejamento e Gestão, Secretaria de Estado de Fazenda, Advocacia Geral do Estado e Companhia de Tecnologia da Informação do Estado de Minas Gerais - Prodemge), a CGE observou a necessidade de instituir um grupo interno de trabalho, no âmbito do órgão, para realizar os processos de adequação que a lei demandaria.

Com o apoio da alta gestão, foi instituído o Comitê Temático, com integrantes de áreas distintas: auditoria, transparência e integridade, corregedoria, tecnologia e comunicação, assessoria estratégica e núcleo de combate à corrupção, conforme Resolução CGE/MG nº 20/2020[6].

As primeiras ações do Comitê envolveram um planejamento e a instituição de um plano de ação. Um diagnóstico cultural e um diagnóstico de maturidade institucional também foram realizados, para que se obtivesse um retrato da situação da CGE diante do processo de adequação e para que se visualizassem as áreas a serem priorizadas.

[5] http://www.pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=188010&marc=LGPD
[6] http://www.pesquisalegislativa.mg.gov.br/LegislacaoCompleta.aspx?cod=191602&marc=lgpd

Pautado pelas orientações do Comitê Estadual de Proteção de Dados Pessoais, o Comitê da CGE iniciou o processo de mapeamento de processos e inventário de dados pessoais (IDP).

Objetivo / escopo

Antes de iniciar o inventário dos dados pessoais, objetivo prioritário, foi realizado (ou atualizado em alguns casos) o levantamento dos processos de trabalho da CGE. O mapeamento dos dados pessoais seria realizado, posteriormente, a partir de cada processo. Assim, seria possível visualizar os fluxos por onde transitam os dados pessoais na instituição e observar, em cada caso, se os dados estavam sendo tratados de modo adequado, nos termos da Lei.

O levantamento dos processos foi realizado pelas áreas e consolidado com o apoio da Assessoria de Gestão Estratégica e do Comitê Temático de LGPD da CGE. Foram considerados tanto os processos de trabalho das áreas finalísticas, como aqueles das áreas meio, como rotinas administrativas.

O objetivo do inventário era ter uma visão sobre os tipos de dados pessoais tratados nos processos de trabalho. A partir disso, o órgão teria um retrato da situação, com informações para subsidiar decisões, como a adoção de medidas de segurança e outras.

Estrutura do órgão

A Controladoria-Geral do Estado de Minas Gerais (CGE) é o órgão central do sistema de controle interno do Poder Executivo mineiro. Tem como competência assistir o Governador no desempenho de suas atribuições quanto aos assuntos e providências atinentes à defesa do patrimônio público, ao controle interno, à auditoria pública, à correição, à prevenção e ao combate à corrupção, ao incremento da transparência e do acesso à informação e ao fortalecimento da integridade e da democracia participativa,

Em sua estrutura orgânica, observam-se as seguintes áreas finalísticas: Auditoria-Geral, Corregedoria-Geral e Subcontroladoria de Transparência e Integridade. Em seu quadro de servidores estatutários, a CGE possui 167 servidores efetivos, 31 com cargos de provimento em comissão, num total de 198 servidores (base: competência 03/2023[7]).

[7] Demonstrativo de despesa de pessoal - 1º trimestre da Subsecretaria de Gestão de Pessoas/SEPLAG-MG (pág. 16 da publicação do jornal oficial Minas Gerais do dia 18/04/2023 Cad. do Executivo)

Governança

Sob o aspecto da governança, o Comitê Estadual de Proteção de Dados Pessoais foi criado com o objetivo de promover a implementação das disposições da Lei no 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

Como desdobramento, cada órgão e entidade do Estado designou Comitês Temáticos, Comissões, Grupos de Trabalho ou Responsáveis para auxiliar na promoção da adequação à LGPD.

No âmbito da CGE, para compor o Comitê Temático de Proteção de Dados Pessoais, foram designados dois servidores das áreas finalísticas (um titular e um suplente), assim como de áreas que poderiam colaborar nas definições e implementação de ações relativas ao tratamento de dados pessoais no órgão: planejamento e finanças, tecnologia da informação e comunicação, assessoria estratégica e núcleo de combate à corrupção. O coordenador do comitê é o atual Encarregado pelo Tratamento de Dados Pessoais da Controladoria, conforme Resoluções CGE-MG nº 24/2021 e 27/2021. O Encarregado responde diretamente ao Gabinete da CGE.

Capacitação – Treinamento

Os integrantes do Comitê da CGE realizaram as capacitações disponibilizadas pela Escola Virtual de Governo (EVG) do Governo Federal: Introdução à Lei Brasileira de Proteção de Dados Pessoais e Proteção de Dados Pessoais no Setor Público. Alguns participaram também de outras capacitações, buscadas individualmente. A formação se deu de forma heterogênea, mesmo dentre o grupo.

Além disso, o Comitê Estadual, ao longo de 2021 e 2022, também ofereceu rodas de conversa periódicas em que, juntamente com a disponibilização de materiais orientativos, trazia explicações sobre os assuntos tratados, tais como:

a) organização de fases de implementação sugeridas;
b) entendimento sobre os atores previstos na norma: controlador, encarregado, titular, operador;
c) orientações sobre as questões de transparência e LGPD;
d) contratos administrativos e a LGPD;
e) metas relacionadas ao alcance de índice de maturidade em determinado período.

Alguns membros do Comitê Temático participaram de tais eventos, a fim de nivelar de conhecimento e receber direcionamento para as ações de adequação à LGPD, no âmbito do Executivo estadual.

Processo

Sendo uma atividade que seria realizada pelas unidades administrativas da CGE, o inventário de dados pessoais foi iniciado, paralelamente a outras ações do Comitê.

Com os processos de trabalho mapeados, procedeu-se ao inventário de metadados, ou tipos de dados pessoais, referentes ao processo ou subprocesso, das unidades administrativas.

Como primeiro passo, o Comitê Temático da CGE realizou trabalhos sobre noções básicas em relação à adequação à LGPD junto aos agentes públicos vinculados à essa instituição. Em especial, foi dada ciência a todos sobre a necessidade de termos o IDP constando os parâmetros que facilitam a aplicação da LGPD em suas diversas aplicações.

Método

Inicialmente, a CGE realizou um piloto do inventário, com base no modelo proposto pelo Comitê Estadual. Partindo da planilha oferecida, foram identificados ajustes, para contemplar a realidade do órgão e as necessidades de registro que se apresentavam. Com a planilha ajustada, o grupo da CGE realizou inventários dos dados pessoais, contidos em processos específicos, juntamente com cada área finalística. O inventário foi registrado em planilhas, em que constavam:

- identificação da planilha: processo/subprocesso, área responsável (setor/unidade administrativa), responsável pelo preenchimento, versão da planilha;
- tipo de dado pessoal (nome completo, e-mail particular, endereço, dentre outros, formulário eletrônico de campo aberto);
- classificação (dado pessoal/funcional, dado pessoal sensível, dados de crianças/adolescentes);
- titular do dado;
- finalidade da coleta, meio da coleta, documento utilizado na coleta;
- armazenamento de dados: forma, local período de retenção previsto;
- descarte de dados: se há, forma de descarte;
- backup de dados: se há, local de armazenamento, período de retenção, se há descarte, forma de descarte;
- tratamento: tipos, responsáveis, controlador, operador;
- compartilhamento de dados: se há com terceiros, indicação de terceiros;
- respaldo legal: hipóteses legais para tratamento, justificativas das hipóteses, base legal, se há consentimento, forma de coleta do consentimento;
- controles: controles existentes/segurança.

Fluxo

O IDP tem sido desenvolvido a partir do mapeamento de processos, por meio das competências legais das unidades da CGE (processos e subprocessos), utilização de sistemas e bancos de dados diversos e verificação e ajustes pelos servidores ou gestores das unidades.

Principais desafios

No âmbito da CGE- MG, um dos grandes desafios está relacionado ao aprimoramento da cultura organizacional sobre a proteção de dados pessoais e a gestão de dados e informações, ao nivelamento do conhecimento entre os agentes públicos, com transparência, integridade e responsabilidade.

Outro ponto que causou grande impacto foi o fato de os membros do Comitê acumularem os trabalhos do inventário com outros projetos e atividades das respectivas unidades. Essa dificuldade reforça a importância de haver uma unidade integralmente dedicada (ou servidores dedicados) aos trabalhos que envolvem a gestão e proteção de dados.

Além disso, observa-se o desafio de manter o inventário constantemente atualizado.

Resultados alcançados

O processo de inventário de dados pessoais, embora não tenha sido totalmente concluído, trouxe alguns benefícios, como a atualização e consolidação do mapeamento de processos do órgão, assim como medidas de aprimoramento de segurança da informação. O encarregado pela proteção de dados vem trabalhando no sentido de buscar soluções automatizadas para concluir o inventário, o que também fortalece a segurança e acurácia do processo.

SECRETARIA DE ESTADO DE TRANSPARÊNCIA E CONTROLE DO MARANHÃO
STC/MA

Histórico – origem, contexto e motivações

A proteção de dados pessoais é dever de todos – inclusive da Administração Pública.

Em que pese fosse possível concluir que referido direito estava contemplado pela Lei Maior mesmo antes da Emenda Constitucional n.º 115/2022, buscando-se fundamento no direito individual à intimidade e vida privada, certo é que a sua positivação taxativa e específica acentua a sua importância no ordenamento vigente.

Também anterior à referida Emenda foi o advento da Lei Geral de Proteção de Dados (LGPD), em 2018.

Nesse contexto, a Secretaria de Estado Transparência e Controle (STC/MA), em 2021, iniciou o processo de implantação da LGPD no órgão. Servidores envolvidos com o estudo da lei promoveram debates internos e realizaram reuniões com os gestores do órgão, sensibilizando quanto à necessidade de implantação da lei.

Após algumas reuniões com a alta administração, foram nomeados dois encarregados de dados, bem como foi criado um grupo de trabalho técnico para iniciar à implantação[8].

Com a mudança de gestão no órgão em 2022, foi publicada nova portaria, alterando os encarregados de dados. Em seguida, foi formado novo grupo de trabalho e realizada sensibilização de servidores acerca da temática da proteção de dados, em parceria com a Escola de Governo (EGMA).

Na sequência, foi realizada reunião com membros do Grupo Técnico de Trabalho, para apresentação do modelo de inventário de dados adotado, bem como para mapeamento dos processos de cada setor.

[8] https://www3.stc.ma.gov.br/2021/08/30/stc-realiza-reuniao-presencial-do-grupo-de-trabalho-que-atua-na-implementacao-da-lgpd/

Foi também elaborada uma planilha para estabelecer critérios para definir quais os processos cujos inventários de dados pessoais (IDP) deveriam ser priorizados.

A partir da formação dos inventários de dados pessoais, é possível ao órgão identificar as medidas de segurança existentes e promover a adequação ao que está previsto na LGPD.

Objetivo / escopo

Os responsáveis pela implantação da LGDP na STC/MA optaram por definir os processos cujas elaborações dos IDPs são prioritárias a partir do resultado de uma análise dos fatores: quantidade de indivíduos envolvidos no processo, tratamento de dados pessoais sensíveis, tratamento de dados de menores, compartilhamento de dados com terceiros.

O preenchimento do inventário de dados visa, além de prever o fluxo dos processos no órgão, indicar os setores envolvidos, as medidas de segurança aplicadas, os riscos associados, dentre outras informações entendidas como próprias para o documento.

Estrutura do órgão

A STC/MA é o órgão central de controle interno do Executivo estadual e conta com quatro unidades de atuação programática: Auditoria Geral, Corregedoria Geral, Ouvidoria Geral e Secretaria Adjunta de Transparência. Além disso, conta com a Secretaria Adjunta de Administração e Finanças, responsável pela atividade-meio.

O órgão conta com 179 servidores, entre comissionados e efetivos.

Para fins de adequação do órgão para a implantação da LGPD, foi instituído grupo de trabalho técnico (GTT), com 15 servidores de diversos setores do órgão, com o objetivo de abarcar as especificidades do tratamento de dados de cada setor, além de multiplicar as informações decorrentes dos debates havidos no GTT.

Governança

Conforme mencionado acima, em 24 de agosto de 2021 foi editada a Portaria n.º 45, que nomeou dois encarregados de dados para o órgão. Na mesma data, foi editada a Portaria n.º 46, que instituiu Grupo de Trabalho Técnico de caráter multidisciplinar para auxiliar os Encarregados no exercício de suas funções e demais atividades atinentes à implementação da LGPD no órgão.

Posteriormente, novas portarias vieram em substituição às supramencionadas – Portaria n. º 39, de 14 de junho de 2022, e Portaria n. º 41, de 15 de junho de 2022, alterando os servidores nomeados como encarregados de dados e participantes do GTT, respectivamente.

Capacitação – Treinamento

Ainda em 2021, houve reunião com os membros do Grupo Técnico de Trabalho com a alta administração para traçar planos da implantação da LGPD no órgão.

Em 2022, houve sensibilização promovida pela STC, após solicitação feita à Escola de Governo (EGMA), em que participaram servidores dos mais diversos setores, e que tratou do tema da proteção de dados, além de fazer um breve apanhado sobre a LGPD.

Especificamente quanto aos membros do GTT, foram indicados cursos da Escola Nacional da Administração Pública para que os mesmos pudessem se familiarizar ainda mais com a referida lei.

Além das iniciativas acima, está em curso o desenvolvimento de campanhas sobre cultura de proteção de dados para veiculação por meio das redes sociais do órgão, além de curso cíclico sobre proteção de dados, a ser ministrado anualmente no órgão.

Metodologia

O processo para elaboração do Inventário de Dados Pessoais teve como etapas as seguintes:

- Definição de “template” a ser seguido: Houve reuniões entre os encarregados de dados analisando modelos utilizados nos mais diversos órgãos, tendo sido escolhido o Guia de Elaboração de Inventário de Dados Pessoais, disponibilizado pela Secretaria de Governo Digital, disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd;
- Realização de reuniões com os membros do Grupo Técnico de Trabalho, nas quais se esclareceu sobre o preenchimento do “template”, sobre a necessidade e preenchimento de planilha que identificasse a quantidade e natureza dos dados tratados;
- Definição de processos cuja elaboração de inventário é prioritária, em vista da quantidade e qualidade dos dados tratados dentro de cada setor;
- Entrega dos inventários de dados.

Principais desafios

Por se tratar de norma que exige uma ruptura de comportamento a LGPD carrega consigo o desafio de se implantar uma cultura de proteção de dados.

Esse fato não se altera quando se fala da elaboração do inventário de dados.

Para a referida elaboração, é preciso não apenas conscientização e treinamento dos servidores sobre proteção de dados, categorização de dados, mapeamento de processos e identificação de bases legais, mas também sobre a utilidade e alcance do referido documento.

Conforme o grau de maturidade do órgão, no que se refere à segurança da informação e à proteção de dados, é possível determinar qual o modelo adequado de inventário de dados a ser adotado.

Há dificuldade também na identificação e no mapeamento do fluxo de dados pessoais. Não havia, até o início dos trabalhos, fluxo dos processos havidos dentro do órgão, e, por conseguinte, fluxo dos dados pessoais inerentes a esses processos.

Além disso, ainda há pouca regulamentação sobre a aplicação da lei por parte da Autoridade Nacional de Proteção de Dados (ANPD). Assim, há pouco respaldo acerca de algumas definições sobre a implementação da lei por parte do órgão.

Também impacta negativamente a pouca disponibilização de capacitação aos membros do GTT. Os cursos e vídeos gratuitos ajudam – mas por se tratar de tarefa de alta especialização, que demanda conhecimentos jurídicos, de gestão e de segurança da informação, mostra-se mais adequada uma capacitação voltada para o tema de forma mais aprofundada.

Houve também dificuldade na identificação de tabelas de temporalidade, o que, por sua vez, dificultou a identificação do período pelo qual se faz necessário manter determinados documentos, e, por conseguinte, os dados pessoais neles contidos.

Por último, a cumulação de funções. É correto afirmar que o fato de os servidores componentes do Grupo de Trabalho Técnico não estarem dedicados exclusivamente à adequação do órgão à LGPD – ou ainda, não terem reduzida sua carga de trabalho ordinária – implica em sobrecarga de trabalho e não permitem a sua condução de maneira célere.

Resultados alcançados

Como afirmado acima, o processo de elaboração de inventário de dados não foi concluído. A STC/MA elaborou inventários de dados relativos a poucos processos.

Não obstante, como etapa necessária para a própria elaboração do inventário, fez-se necessário capacitar minimamente os servidores a respeito da cultura da proteção de dados que deve existir no órgão. Assim, é possível notar a mudança de determinados comportamentos decorrente dessa sensibilização.

Além disso, fez-se necessário mapear processos existentes no órgão, coisa que não existia anteriormente ao processo de elaboração do IDP.


Conaci
CONSELHO NACIONAL DE CONTROLE INTERNO