Guia Orientativo sobre a

INSTRUÇÃO NORMATIVA CGM/SP Nº 01/2022

para a Administração Pública do Município de São Paulo

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Guia Orientativo sobre a

INSTRUÇÃO NORMATIVA CGM/SP Nº 01/2022

para a Administração Pública do Município de São Paulo

Kelvin Peroli
Alexsandro Pereira de Almeida
Eden dos Santos Costa

São Paulo,
Janeiro de 2023

Prefeitura do Município de São Paulo

Prefeito

Ricardo Nunes

Controladoria Geral do Município

Controlador Geral do Município

Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município

Daniel Falcão

Chefe de Gabinete

Thalita Abdala Aris

Coordenadoria de Promoção da Integridade

Coordenador da Coordenadoria de Promoção da Integridade

José Maurício Linhares Barreto Neto

Autores

Kelvin Peroli

Alexsandro Pereira de Almeida

Eden dos Santos Costa

Diagramação

Marília Miquelin de Oliveira

Versão 1

Janeiro de 2023

Este Guia Orientativo foi elaborado em cumprimento aos termos do Decreto Municipal nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018, no âmbito do Poder Executivo do Município de São Paulo.

Controlador Geral do Município

Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município

Daniel Falcão

Lista de Abreviaturas e Siglas

AAAA – Ano

ABNT – Associação Brasileira de Normas Técnicas

ADI – Ação Direta de Inconstitucionalidade

ADPF – Arguição de Descumprimento de Preceito Fundamental

ANPD – Autoridade Nacional de Proteção de Dados

ANS – Acordo de Nível de Serviço

CD – "*Compact Disc*" (Disco Compacto)

CFTV – Circuito Fechado de TV

CGM/SP – Controladoria Geral do Município de São Paulo

CID-10 – "*International Classification of Diseases Version 10*" (10ª revisão da Classificação Estatística Internacional de Doenças e Problemas Relacionados à Saúde)

COBIT – "*Control Objectives for Information and Related Technologies*" (Controle de Objetivos para Informação e Tecnologias Relacionadas);

CORR – Corregedoria Geral do Município de São Paulo

CRFB/88 – Constituição da República Federativa do Brasil

DD – Dia

DVD – "*Digital Versatile Disc*" (Disco Digital Versátil)

EUA – Estados Unidos da América

HD – "*Hard Disk*" (Disco Rígido)

HH – Hora

HTTPS – "*Hyper Text Transfer Protocol Secure"* (Protocolo de Transferência de Hipertexto Seguro)

IEC – *"International Electrotechnical Commission*" (Comissão Internacional de Eletrotécnica)

IN – Instrução Normativa

ISO – "*International Organization for Standardization"* (Organização Internacional de Normatização)

ITIL – "*Information Technology Infrastructure Library*" (Biblioteca de Infraestrutura de Tecnologia da Informação);

JPEG – "*Joint Photographic Experts Group*"

LAI – Lei de Acesso à Informação

LGPD – Lei Geral de Proteção de Dados Pessoais

MCI – Marco Civil da Internet

MIN – Minuto

MM – Mês

MP3 – *"MPEG Audio Layer-3"*

MP4 – *"MPEG-4 Part 14"*

NBR – Norma Brasileira

PDF – "*Portable Document Format*" (Formato de Documento Portável)

PMSP – Prefeitura do Município de São Paulo

PRODAM – Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo

PSI – Política de Segurança da Informação

RGPD – Regulamento Geral de Proteção de Dados da União Europeia

RIPD – Relatório de Impacto à Proteção de Dados

SGSI – Sistema de Gestão de Segurança da Informação

SLA – "*Service Level Agreement*" (Acordo de Nível de Serviço)

SP – Município de São Paulo

SSD – *"Solid-State Drive*" (Unidade de Estado Sólido)

STF – Supremo Tribunal Federal

SWOT – ("*Strengths, Weaknesses, Opportunities and Threats*" (Forças, Fraquezas, Oportunidades e Ameaças)

TLS – "*Transport Layer Security"* (Segurança da Camada de Transporte)

UE – União Europeia

Lista de Tabelas

Sumário

Apresentação

Em complemento ao "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*", este Guia foi elaborado a fim de subsidiar especialmente os agentes públicos que serão responsáveis, no âmbito da Administração Pública Municipal direta e indireta, por implementar as disposições previstas pela Instrução Normativa CGM/SP nº 01/2022, que detalha algumas das ações necessárias do Programa de Governança em Privacidade e Proteção de Dados Pessoais do Poder Executivo do Município de São Paulo – denominado, conforme o art. 2º, inc. XIII, do Decreto Municipal nº 59.767/2020, de "*Plano de Adequação*"[1].

A Instrução Normativa CGM/SP nº 01/2022 estabeleceu, em seus anexos, padrões à realização de um "*Mapeamento 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.

Porém, estes documentos representam apenas o resultado de um conjunto estruturado de ações necessárias – cujo percurso é, por este Guia, orientado.

A fim de subsidiar a elaboração do Anexo I da Instrução Normativa CGM/SP nº 01/2022, "*Mapeamento de Dados Pessoais*", este Guia traz modelos à realização, por cada um dos órgãos e entidades, de: (i) Mapeamento de Processos, que consiste na identificação categorial de todas as ações existentes no órgão ou na entidade; e (ii) Questionário sobre a Privacidade e a Proteção de Dados Pessoais, que consiste em um conjunto de quesitos sobre a privacidade e a proteção de dados pessoais a ser aplicado em cada um dos processos do órgão ou entidade, conquanto identificados no Mapeamento de Processos.

A fim de subsidiar a elaboração do Anexo II da Instrução Normativa CGM/SP nº 01/2022, "*Relatório de Impacto à Proteção de Dados Pessoais*", este Guia traz, também, modelos à realização, por cada um dos órgãos ou entidades, de: (i) Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais.

Este Guia possui natureza orientativa em razão da necessidade de cada órgão e entidade ter em consideração, em sua estruturação do "*Mapeamento de Dados Pessoais*" e do "*Relatório de Impacto à Proteção de Dados Pessoais*", o *contexto* em que realiza o tratamento de dados pessoais, isto porque cada

[1] Conforme o art. 2º, inc. XIII, do Decreto Municipal nº 59.767/2020, o Plano de Adequação 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."*

contexto traz consigo, *e.g.*, diferentes riscos e diferentes gradações de riscos à segurança da informação, à privacidade e à proteção de dados pessoais.

Para a consecução das ações previstas na Instrução Normativa CGM/SP nº 01/2022 e, de modo geral, no Decreto Municipal nº 59.767/2020, é importante a designação de equipe de trabalho que proceda com as ações de todo o Plano de Adequação e seja um canal de comunicação do órgão ou entidade com o Encarregado pela Proteção de Dados Pessoais competente.

Conforme o art. 13, inc. III, da Instrução Normativa CGM/SP nº 01/2022, cada Pasta deverá criar um Plano de Adequação que descreva todas as ações desenvolvidas e a serem desenvolvidas para a implementação do sistema normativo de proteção de dados pessoais em vigor, observadas as disposições do Decreto Municipal n° 59.767/2020, da própria Instrução Normativa, de seu Anexo I – "*Mapeamento de Dados Pessoais*", de seu Anexo II – "*Relatório de Impacto à Proteção de Dados Pessoais*", do "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*" e deste *"Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022*".

Nesse sentido, como dispõe o art. 14, *caput*, também da Instrução Normativa CGM/SP nº 01/2022, cada Pasta deverá publicar e manter anualmente atualizado Relatório sobre o seu Plano de Adequação ao Decreto Municipal nº 59.767/2020. Para tanto, é possível que este Plano se estruture a partir de:

(i) Designação de equipe de trabalho;

(ii) Capacitação dos agentes públicos, nos termos do art. 13, inc. III, da Instrução Normativa CGM/SP nº 01/2022;

(iii) Mapeamento de Processos;

(iv) Mapeamento de Dados Pessoais;

(v) Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, que contenha:

   a. Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais;

   b. Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais;

   c. Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, com a descrição das medidas de segurança, técnicas e administrativas, implementadas e a serem implementadas;

(vi) Relatório de Impacto à Proteção de Dados Pessoais; e

(vii) Mapeamento do Fluxo de Dados Pessoais, nos termos do art. 2º da Instrução Normativa CGM/SP nº 01/2022.

Capítulo 1

Mapeamento de Processos

Capítulo I – Mapeamento de Processos

1. Mapeamento de Processos

O "*Mapeamento de Processos*" precede a realização de um "*Registro das Operações de Tratamento de Dados Pessoais*" (*"Inventário de Dados Pessoais"* ou *"Mapeamento de Dados Pessoais"*, conforme a terminologia do Decreto Municipal nº 59.767/2020 e da Instrução Normativa CGM/SP nº 01/2022), isto porque é necessária, justamente, a identificação categorial de todas as ações existentes ("*Mapeamento de Processos*") a fim de que possa haver a identificação das operações de tratamento de dados pessoais havidas em cada processo ("*Registro das Operações de Tratamento de Dados Pessoais*").

"Mas como realizar um Mapeamento de Processos adequado à realização de um Registro das Operações de Tratamento de Dados Pessoais?"

A Controladoria Geral do Município de São Paulo, por meio de seu Encarregado pela Proteção de Dados Pessoais, desenvolveu metodologia que objetiva padronizar a realização de um "*Mapeamento de Processos*" que possibilita a realização de um "*Registro das Operações de Tratamento de Dados Pessoais*" em conformidade ao que dispõe a Instrução Normativa CGM/SP nº 01/2022.
Esse "*Mapeamento de Processos*" dispõe da necessidade da identificação dos processos e das etapas de cada um dos processos, com a descrição, para cada etapa:

(i) de seu objetivo;
(ii) dos recursos humanos utilizados;
(iii) dos recursos físicos e tecnológicos utilizados;
(iv) do modo de comunicação entre os recursos humanos utilizados e o modo de compartilhamento das informações entre as etapas; e
(v) dos recursos informacionais utilizados.

Denominado de "*Contextualização dos Processos*", o modelo constante no Anexo I deste Guia pode ser distribuído para cada divisão de um órgão ou entidade, a fim de que os seus responsáveis procedam com o mapeamento de todos os processos existentes em sua área, em conformidade à metodologia do modelo.
Após isso, os documentos podem ser, pela equipe de trabalho, revisados e compilados em uma "*Contextualização dos Processos*" que se refira a todo o órgão ou entidade. Adicionalmente, poderá a "*Contextualização dos Processos*" estar acompanhado da entrega de um fluxograma relativo a cada processo existente na área.

O documento, então, servirá de subsídio à próxima etapa, "*Mapeamento de Dados Pessoais*".

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" >*.

Capítulo 2

Mapeamento de Dados Pessoais

Capítulo II – Mapeamento de Dados Pessoais

2. Mapeamento de Dados Pessoais

Realizado o "*Mapeamento de Processos*" do órgão ou entidade, é possível o início das atividades do "*Mapeamento de Dados Pessoais*".

O art. 14, inc. IV, da Instrução Normativa CGM/SP nº 01/2022, dispôs dos requisitos necessários à sua elaboração, observado, materialmente, o Anexo II da Instrução Normativa, "*Mapeamento de Dados Pessoais*":

(i) data de sua criação e de sua atualização, quando aplicável;

(ii) descrição sobre os processos do órgão ou entidade nos quais há o tratamento de dados pessoais;

(iii) identificação dos agentes de tratamento e do encarregado;

(iv) descrição do ciclo de vida do tratamento de dados pessoais;

(v) descrição da natureza e do escopo do tratamento de dados pessoais;

(vi) descrição da finalidade do tratamento de dados pessoais;

(vii) descrição das categorias de dados pessoais tratados, inclusive das categorias de dados pessoais sensíveis;

(viii) descrição do volume das operações de tratamento de dados pessoais e das categorias de dados pessoais tratados, inclusive o volume das categorias de dados pessoais sensíveis tratados;

(ix) descrição das categorias de titulares de dados pessoais;

(x) descrição do compartilhamento de dados pessoais, inclusive com a descrição dos agentes de tratamento com os quais os dados pessoais são compartilhados;

(xi) descrição dos contratos de serviços e de soluções de tecnologia da informação que tratam os dados pessoais do processo mapeado;

(xii) descrição das transferências internacionais de dados pessoais; e

(xiii) descrição das medidas, técnicas e administrativas, adotadas.

No intuito de estruturar a elaboração do Anexo II da Instrução Normativa CGM/SP nº 01/2022, foram desenvolvidos os Anexos II e III deste Guia – respectivamente, "*Taxonomia de Dados Pessoais*" e "*Questionário sobre a Privacidade e a Proteção de Dados Pessoais*".

A "*Taxonomia de Dados Pessoais*" é utilizada para a classificação das categorias de dados pessoais tratados pelo Poder Executivo do Município de São Paulo e está metodologicamente presente no

Anexo I da Instrução Normativa CGM/SP nº 01/2022, "*Mapeamento de Dados Pessoais*", e no Anexo III deste Guia, "*Questionário sobre a Privacidade e a Proteção de Dados Pessoais*".

O "*Questionário sobre a Privacidade e a Proteção de Dados Pessoais*", por sua vez, traz, em forma de quesitos, as informações necessárias à elaboração do Anexo I da Instrução Normativa CGM/SP nº 01/2022, "*Mapeamento de Dados Pessoais*". O Questionário deve ser respondido no contexto de cada um dos processos mapeados na etapa anterior, "*Mapeamento de Processos*", isto a fim de identificar, em cada um dos processos, as questões relativas à privacidade e à proteção de dados pessoais em cada um dos processos.

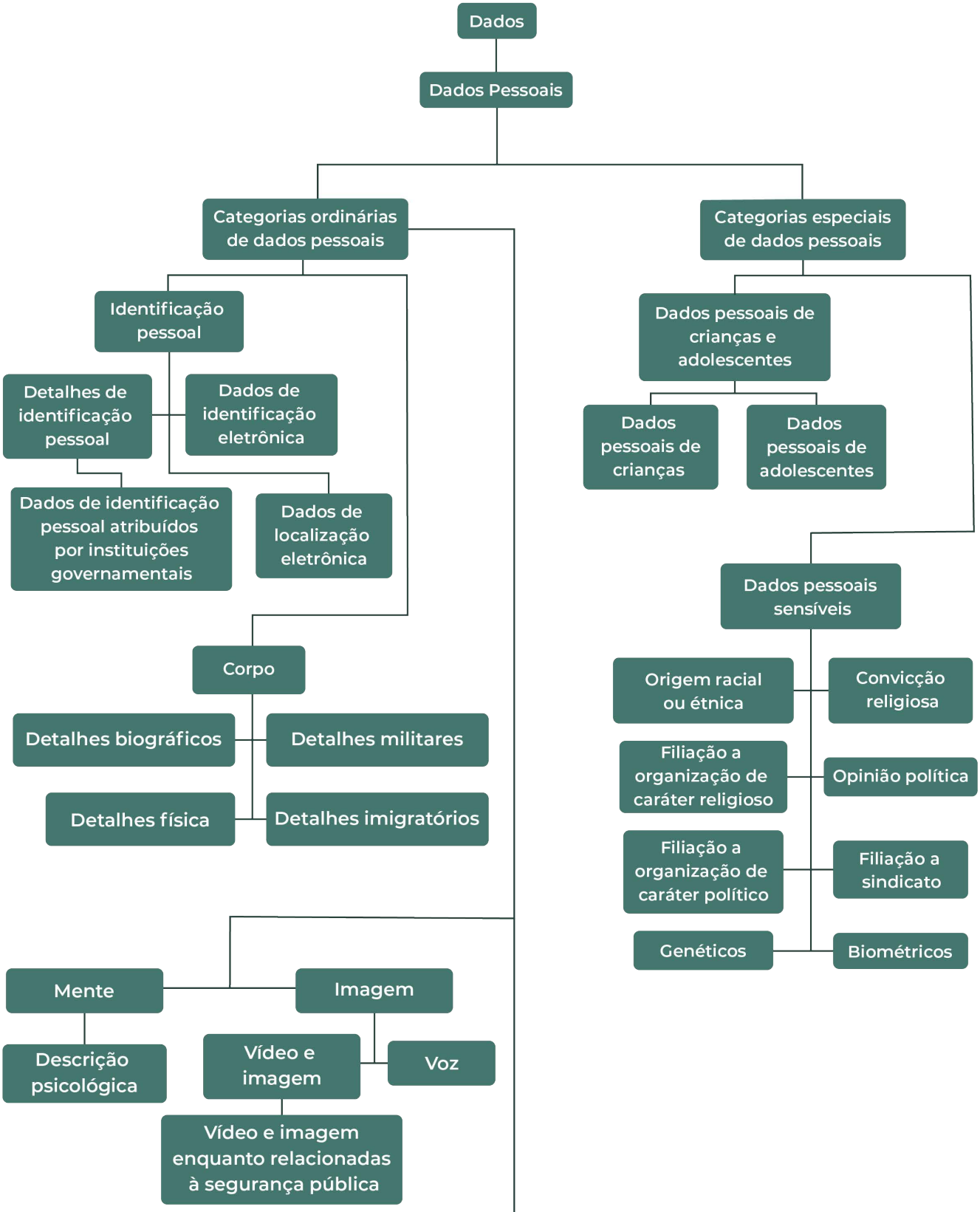
Anexo II – Taxonomia de Dados Pessoais

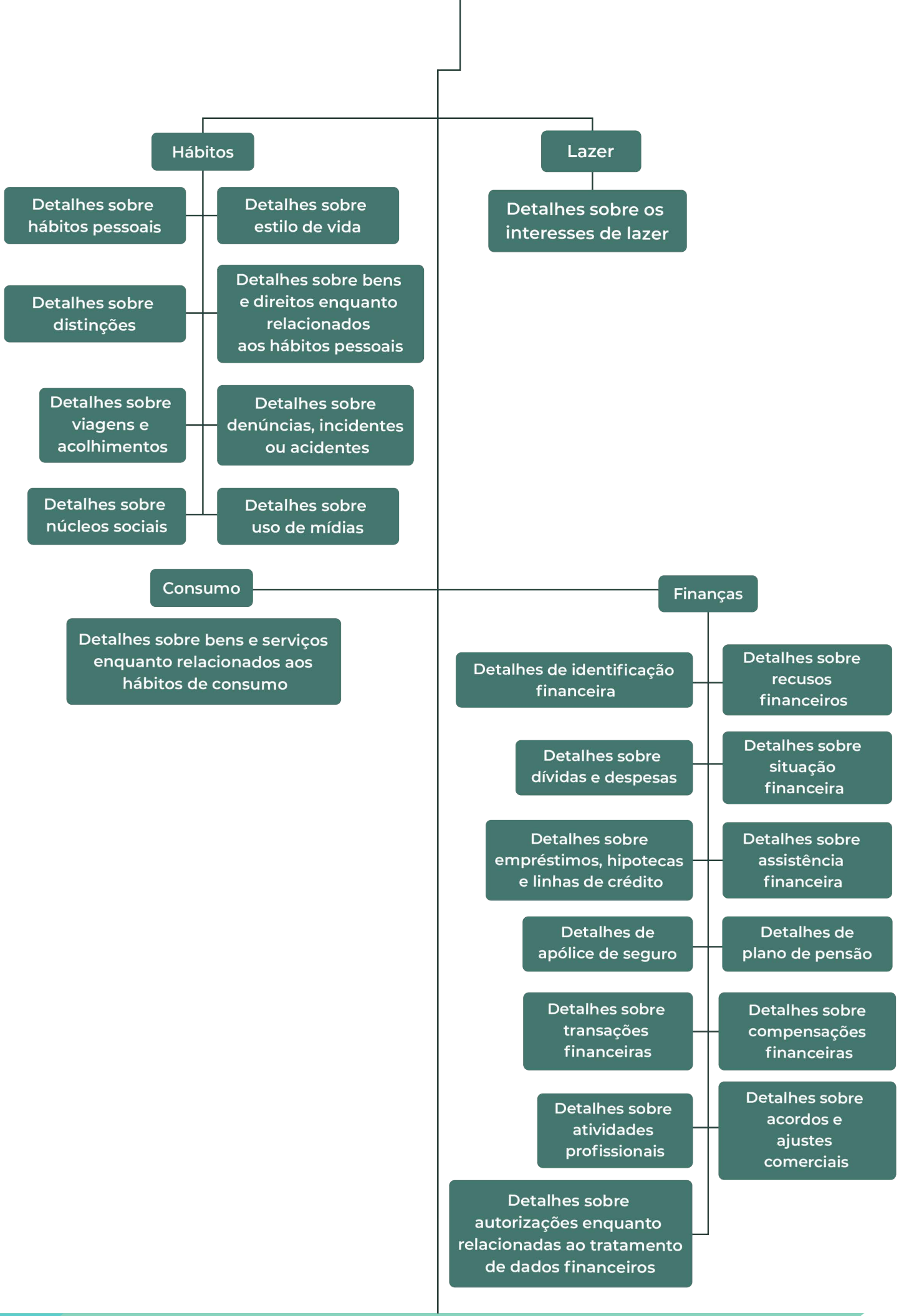
i. Categorias ordinárias de dados pessoais:
    1. Identificação pessoal:
        a. Detalhes de identificação pessoal;
            i. Dados de identificação pessoal atribuídos por instituições governamentais.
        b. Dados de identificação eletrônica; e
        c. Dados de localização eletrônica.
    2. Corpo:
        a. Detalhes biográficos;
        b. Detalhes militares;
        c. Descrição física; e
        d. Detalhes imigratórios.
    3. Mente:
        a. Descrição psicológica.
    4. Imagem:
        a. Voz; e
        b. Vídeo e imagem:
            i. Vídeo e imagem enquanto relacionadas à segurança pública.
    5. Hábitos:
        a. Detalhes sobre hábitos pessoais;
        b. Detalhes sobre estilo de vida;
        c. Detalhes sobre distinções;
        d. Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais;
        e. Detalhes sobre viagens e deslocamentos;
        f. Detalhes sobre denúncias, incidentes ou acidentes;
        g. Detalhes sobre núcleos sociais; e
        h. Detalhes sobre uso de mídias.
    6. Lazer:
        a. Detalhes sobre interesses de lazer.
    7. Consumo:
        a. Detalhes sobre bens e serviços enquanto relacionados aos hábitos de consumo.
    8. Finanças:
        a. Detalhes de identificação financeira;
        b. Detalhes sobre recursos financeiros;
        c. Detalhes sobre dívidas e despesas;
        d. Detalhes sobre situação financeira;
        e. Detalhes sobre empréstimos, hipotecas e linhas de crédito;
        f. Detalhes sobre assistência financeira;
        g. Detalhes de apólice de seguro;
        h. Detalhes de plano de pensão;
        i. Detalhes sore transações financeiras;
        j. Detalhes sobre compensações financeiras;
        k. Detalhes sobre atividades profissionais;
        l. Detalhes sobre acordos e ajustes comerciais; e
        m. Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros.

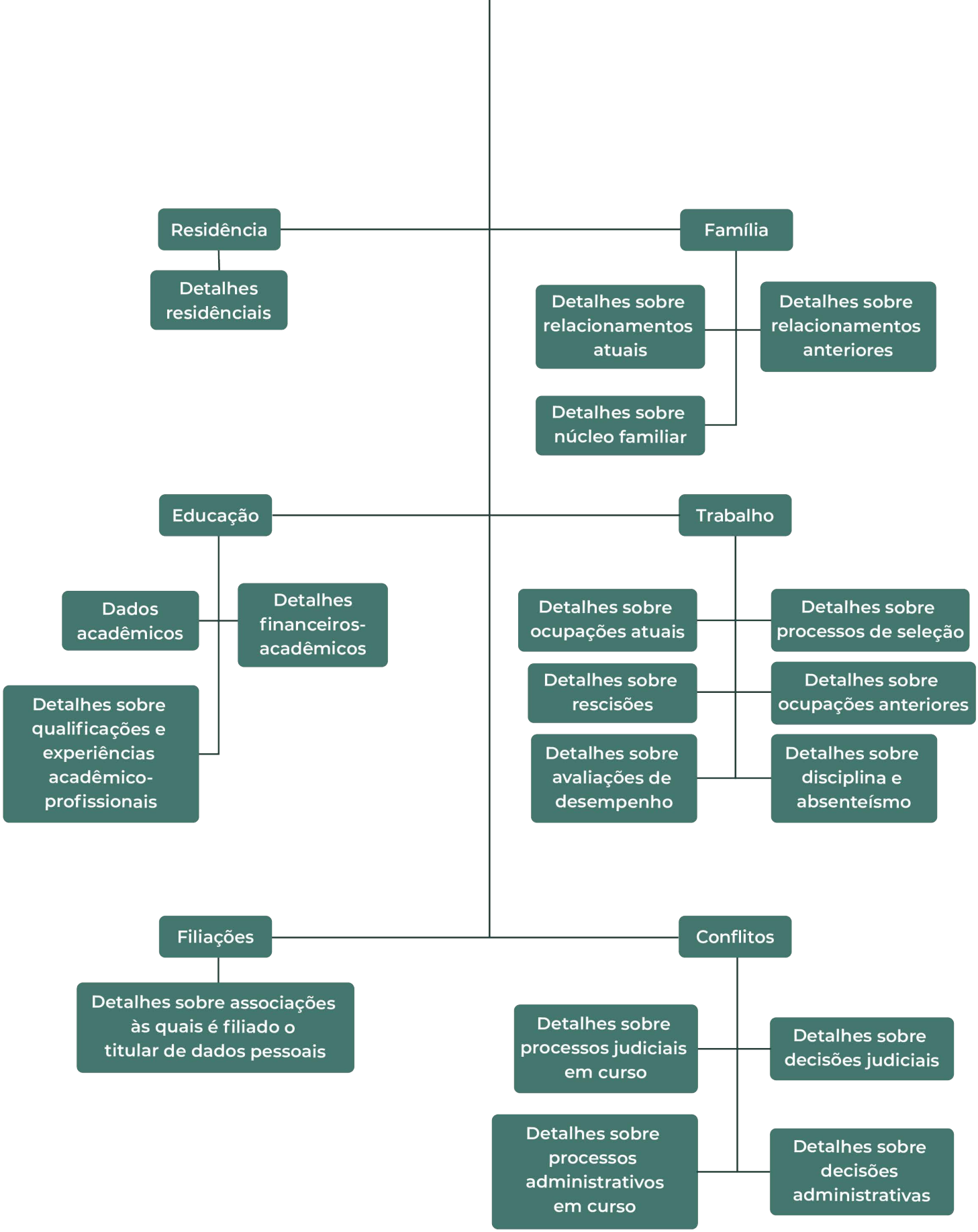
9. Residência:
    a. Detalhes residenciais.
10. Família:
    a. Detalhes sobre relacionamentos atuais;
    b. Detalhes sobre relacionamentos anteriores;
    c. Detalhes sobre núcleo familiar.
11. Educação:
    a. Dados acadêmicos;
    b. Detalhes financeiro-acadêmicos;
    c. Detalhes sobre qualificações e experiências acadêmico-profissionais.
12. Trabalho:
    a. Detalhes sobre ocupações atuais;
    b. Detalhes sobre processos de seleção;
    c. Detalhes sobre rescisões;
    d. Detalhes sobre ocupações anteriores;
    e. Detalhes sobre avaliações de desempenho; e
    f. Detalhes sobre disciplina e absenteísmo.
13. Filiações:
    a. Detalhes sobre associações as quais é filiado o titular de dados pessoais.
14. Conflitos:
    a. Detalhes sobre processos judiciais em curso;
    b. Detalhes sobre decisões judiciais;
    c. Detalhes sobre processos administrativos em curso; e
    d. Detalhes sobre decisões administrativas.

ii. Categorias especiais de dados pessoais:
1. Dados pessoais de crianças e adolescentes:
    a. Dados pessoais de crianças; e
    b. Dados pessoais de adolescentes.
2. Dados pessoais sensíveis:
    a. Origem racial ou étnica;
    b. Convicção religiosa;
    c. Filiação a organização de caráter religioso;
    d. Opinião política;
    e. Filiação a organização de caráter político;
    f. Filiação a sindicato;
    g. Filiação a organização de caráter filosófico;
    h. Saúde ou vida sexual;
    i. Genéticos; e
    j. Biométricos.

Tabela I – Organograma da Taxonomia de Dados Pessoais




Hábitos
Detalhes sobre hábitos pessoais
Detalhes sobre estilo de vida
Detalhes sobre distinções
Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais
Detalhes sobre viagens e acolhimentos
Detalhes sobre denúncias, incidentes ou acidentes
Detalhes sobre núcleos sociais
Detalhes sobre uso de mídias
Lazer
Detalhes sobre os interesses de lazer
Consumo
Detalhes sobre bens e serviços enquanto relacionados aos hábitos de consumo
Finanças
Detalhes de identificação financeira
Detalhes sobre recusos financeiros
Detalhes sobre dívidas e despesas
Detalhes sobre situação financeira
Detalhes sobre empréstimos, hipotecas e linhas de crédito
Detalhes sobre assistência financeira
Detalhes de apólice de seguro
Detalhes de plano de pensão
Detalhes sobre transações financeiras
Detalhes sobre compensações financeiras
Detalhes sobre atividades profissionais
Detalhes sobre acordos e ajustes comerciais
Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros


Residência
Detalhes residênciais
Família
Detalhes sobre relacionamentos atuais
Detalhes sobre relacionamentos anteriores
Detalhes sobre núcleo familiar
Educação
Dados acadêmicos
Detalhes financeiros-acadêmicos
Detalhes sobre qualificações e experiências acadêmico-profissionais
Trabalho
Detalhes sobre ocupações atuais
Detalhes sobre processos de seleção
Detalhes sobre rescisões
Detalhes sobre ocupações anteriores
Detalhes sobre avaliações de desempenho
Detalhes sobre disciplina e absenteísmo
Filiações
Detalhes sobre associações às quais é filiado o titular de dados pessoais
Conflitos
Detalhes sobre processos judiciais em curso
Detalhes sobre decisões judiciais
Detalhes sobre processos administrativos em curso
Detalhes sobre decisões administrativas

Anexo III – 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.>* *<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?

[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."

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:
   a. 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:

Capítulo 3

Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Capítulo III – Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

1. Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

O "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*", em seu Capítulo III, descreve os conceitos e as orientações gerais relativas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, em conformidade às disposições da norma ABNT NBR ISO nº 31000:2018.

Este Capítulo, por sua vez, traz metodologia, criada e adaptada a partir das normas ABNT NBR ISO nº 31000:2018, ABNT ISO/TR nº 31004:2015, ABNT NBR/IEC nº 31010:2021, ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022, ABNT NBR ISO/IEC nº 27701:2020, ABNT NBR ISO/IEC nº 29100:2020, ABNT NBR ISO/IEC nº 29134:2020, e ABNT NBR ISO/IEC nº 29151/2020, voltada, especialmente, a órgãos e entidades que estejam por iniciar a sua Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais. Vale destacar que a metodologia possui caráter orientativo aos órgãos e entidades da Administração Pública Municipal, podendo ser adaptada de acordo com as suas necessidades.

A fim de realizar a identificação dos riscos à segurança da informação, à privacidade e à proteção de dados pessoais, nos mais distintos processos da organização, foi concebida uma abordagem que atrela dois distintos pontos de vista: (i) o ponto de vista da equipe de gestão de riscos; e (ii) o ponto de vista da equipe dos setores objeto da avaliação de riscos.

A equipe de gestão de riscos, por meio de entrevistas ou por outras técnicas de identificação de riscos[5], deve ter como objetivos: (i) registrar informações coletadas juntamente aos membros da equipe dos setores; e (ii) identificar, a partir das informações coletadas e registradas, os riscos existentes.

Pelo ponto de vista da equipe de avaliação de riscos, não há, por essa técnica de identificação de riscos, o questionamento aos membros das equipes dos setores sobre tipos de riscos identificados, mas, sim, o questionamento sobre os processos previamente contextualizados (vide Capítulo I – Mapeamento de Processos e Capítulo II – Mapeamento de Dados Pessoais) ou o questionamento sobre a implementação de controles previstos nas normas ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022, ABNT NBR ISO/IEC nº 27701:2020, relativos à segurança

[5] Como, *e.g.*, pela técnica de análise de "*Brainstorming*" e pela técnica de análise "SWOT" ("*Strengths, Weaknesses, Opportunities and Threats*").

da informação, à privacidade e à proteção de dados pessoais, isto a fim de que a equipe de avaliação de riscos possa subsidiar-se do resultado dos questionamentos à sua identificação de riscos. Para a preparação, realização e documentação das entrevistas, este Guia inclui *layouts* em seu Anexo IV, *"Entrevistas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*.

A equipe dos setores objeto da avaliação de riscos, por sua vez, deve também, por meio de questionário ou por outras técnicas de identificação de riscos, trazer a sua percepção sobre os riscos que entende incorrer o setor quanto à segurança da informação, à privacidade e à proteção de dados pessoais. Para tanto, este Guia apresenta, em seu Anexo V, o *layout "Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*[6].

Na eventualidade de aplicação das técnicas de entrevistas, sob o ponto de vista da equipe de avaliação de riscos, e de questionário, sob o ponto de vista da equipe dos setores objeto da avaliação de riscos, recomenda-se que o questionário seja aplicado à equipe dos setores previamente à realização das entrevistas, isto a fim de que não haja a influência dos questionamentos da equipe de avaliação de riscos na percepção prévia de riscos da equipe dos setores.

Ainda que a equipe dos setores não tenha expertise relativa à gestão de riscos, este ponto de vista é imprescindível ao fim da percepção da equipe sobre o seu próprio contexto – isto de forma simples e orientada, em um intervalo de tempo razoavelmente prévio à realização de entrevistas ou outras técnicas conduzidas de identificação de riscos.

Essa abordagem, sobretudo àqueles órgãos que estejam no início de sua implementação de uma Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, desde que realizada por uma equipe de avaliação de riscos capacitada, poderá efetivamente permitir a identificação de vulnerabilidades, ameaças e riscos – inclusive, não percebidos pela equipe dos setores objeto de avaliação de riscos.

Para que as etapas seguintes possam ser eficientemente realizadas, é necessário que, pelas entrevistas, além dos questionamentos sobre os processos previamente contextualizados e dos questionamentos sobre a existência de controles previstos nas normas, sejam obtidas também informações adicionais, de acordo com cada contexto, que subsidiem não apenas a etapa de identificação dos riscos, mas também as etapas seguintes – ou seja, as etapas de análise, avaliação e tratamento de riscos.

Apesar das distinções entre os contextos, são informações que em todos devem ser colhidas: (i) informações sobre as vulnerabilidades; (ii) informações sobre as ameaças; (iii) informações o

[6] Este Questionário pode ser aplicado a partir de metodologia de "*Análise de Causa-Raiz*", orientada pelo *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP).
SÃO PAULO (Cidade). Controladoria Geral do Município. *Manual de Gestão de Riscos*. São Paulo, Controladoria Geral do Município, 2023.

histórico de registro de ameaças, caso existente; (iv) informações sobre a eficácia dos controles existentes, caso existentes; (v) informações sobre a percepção da equipe dos setores sobre a eficácia dos controles existentes, caso existentes; e (vi) informações sobre a relação do ativo com a confidencialidade, com a disponibilidade e com a integridade da informação.

Anexo IV – Entrevistas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

1. Metodologia

Este *layout* de Entrevistas apresenta as ações necessárias ao planejamento e à execução de entrevistas com a equipe dos setores, isto com vistas à realização da primeira etapa da Gestão de Riscos – ou seja, da Identificação de Riscos.

Em primeiro lugar, necessário o destaque de que o órgão ou entidade deve considerar eventuais particularidades existentes em sua organização para que, uma vez compreendida a metodologia descrita, possa promover os ajustes que melhor se adequem ao contexto existente.

Previamente à comunicação à equipe dos setores e à realização das entrevistas, é necessário que haja o seu planejamento com detalhes, sobretudo, dos seguintes aspectos:

(i) Análise de contexto: trata-se da análise dos Mapeamentos dos Processos, conforme o Capítulo I deste Guia, entregues por cada setor, isto a fim de que haja uma percepção inicial da equipe sobre os riscos à segurança da informação, à privacidade e à proteção de dados pessoais, presente em cada processo, diante de suas informações elementares – que se exemplificam por aquelas informações contidas em cada uma das etapas dos processos.

(ii) Análise e seleção de controles de normas técnicas aplicáveis: trata-se da análise e compreensão do escopo dos controles relativos à segurança da informação, à privacidade e à proteção de dados pessoais existentes em normas técnicas aplicáveis, como as normas ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022 e ABNT NBR ISO/IEC nº 27701:2020 (vide o Anexo X deste Guia, "*Guia Orientativo para Entrevistas e Formulação de Pauta*"). A compreensão sobre os controles é fundamental para a preparação das entrevistas, ou seja, para a preparação dos temas e dos quesitos a serem abordados. Vale o destaque de que, a depender do nível de maturidade da organização com relação aos temas da segurança da informação, da privacidade e da proteção de dados pessoais, poderá decidir-se pela adoção de normas técnicas adicionais, como a norma ABNT NBR ISO/IEC nº 29151/2020, ou mesmo outras, em substituição àquelas acima elencadas – a exemplo dos "*frameworks*" *"Control Objectives for Information and Related Technologies*" (COBIT) e "*Information Technology Infrastructure Library"* (ITIL). Recomenda-se que a equipe de gestão de riscos detenha profissional com experiência prévia na utilização de normas técnicas relativas à

segurança da informação – o que pode otimizar o tempo de execução do processo, assim como o grau de acuracidade desta primeira etapa;

(iii) Definição das pautas das entrevistas: a partir da análise de contextos e da análise e da seleção de controles de normas técnicas, é necessário que haja a definição da pauta de entrevistas para cada um dos setores a serem entrevistados – que pode se utilizar do *layout* presente no item 3 do Anexo IV deste Guia, *"Layout de Pauta de Entrevistas"*.

A pauta pode ser formulada a partir das diretrizes de implementação de controles presentes no Anexo VII deste Guia, *"Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*, externo a este documento, e pode ser definida por tema ou por processo:

a. no caso de ser definida por temas, poderá se referir aos controles, a partir dos quais os quesitos seriam direcionados, como, a título exemplificativo: *"Como são descartadas as mídias removíveis?"*. Esse quesito relaciona-se ao controle *"gerenciamento de mídias removíveis"*, presente na norma ABNT NBR ISO/IEC nº 27001:2013, que possui, entre as suas diretrizes de implementação, o descarte seguro de mídias removíveis. A partir desse quesito, e a depender do uso ou não de mídias removíveis, os entrevistados poderão detalhar sobre o processo de utilização das mídias (vide o Anexo X deste Guia, "*Guia Orientativo para Entrevistas e Formulação de Pauta*").

b. no caso de ser definida por processos, poderá se referir aos documentos resultantes do mapeamento de processos (vide Capítulo I, "*Mapeamento de Processos*"). Nesta hipótese, o mesmo assunto do item anterior poderia ser iniciado com o seguinte quesito: *"Neste processo, como os dados pessoais são inicialmente coletados?"* Esse quesito remete-se à coleta de dados pessoais e traz respostas que ensejam novos quesitos relacionados a todo o fluxo de dados pessoais existente no processo, isto de modo a se obter, ao final, um questionamento sobre todo o ciclo de vida dos dados pessoais no processo objeto da entrevista. A partir dessa exposição, o entrevistador, ciente dos controles das normas técnicas selecionados, poderá, então, realizar quesitos relacionados aos controles, isto a fim de entender o quão seguros ou não estão os dados pessoais tratados no referido processo. A título exemplificativo: *"Os dados estão criptografados?"*; "*Como é feito o descarte das mídias?*"; e *"Onde as mídias estão guardadas?"*; e *"Quem tem acesso?"*.

Ambas as abordagens, de acordo com a experiência obtida na Controladoria Geral do Município de São Paulo (CGM/SP), adaptam-se às necessidades dos diferentes

contextos presentes na organização – mas possuem, cada qual, os seus pontos de atenção:

a. no caso de ser definida por temas, traz a desafio de alocação de entrevistados que tenham ciência do tema em questão; e
b. no caso de ser definida por processos, traz o desafio da condução de entrevistas pautadas pela síntese e não pela prolação.

(iv) Definição de agenda de "*kickoff*" e de entrevistas: após a análise de contextos, a análise e a seleção de controles de normas técnicas e a definição das pautas, necessário a definição de:

a. agenda de "*kickoff*", a ser realizado entre a equipe de gestão de riscos e aqueles que serão entrevistados, que preveja uma contextualização prévia de todo o processo de entrevistas para os entrevistados; e
b. agenda de entrevistas, que seja realizada com o planejamento:
    i. da quantidade de entrevistas;
    ii. da duração das entrevistas;
    iii. das datas das entrevistas;
    iv. da identificação dos entrevistados, a partir de escolha conjunta com o chefe de cada setor objeto da gestão de riscos;
    v. do tempo de preparação da equipe de gestão de riscos à condução das entrevistas;
    vi. do tempo de análise das entrevistas pela equipe de gestão de riscos; e
    vii. do tempo de "*feedback*" do conteúdo das entrevistas pelos entrevistados, seja ratificando-as ou retificando-as.

(v) Realização de "*kickoff*": reunião preparatória, entre a equipe de gestão de riscos e aqueles que serão entrevistados, a fim de que possuam uma contextualização prévia de todo o processo de entrevistas, especialmente sobre:

a. agenda de entrevistas;
b. pauta das entrevistas;
c. método de condução das entrevistas;
d. consentimento às gravações das entrevistas, se necessário, a fim de subsidiarem a documentação das entrevistas;
e. documentação das entrevistas em atas; e
f. próximos passos após a realização das entrevistas, como "*feedback*" dos entrevistados sobre a acuracidade das documentações das entrevistas em atas.

(vi) Recolhimento do "*Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*": previamente à realização das entrevistas, recomenda-se o recolhimento deste Questionário, que será objeto de descrição a seguir, que contém a percepção prévia de riscos à segurança da informação, à privacidade e à proteção de dados pessoais da equipe objeto da gestão de riscos, isto apenas a partir de seu conhecimento específico sobre os seus respectivos setores e sobre os seus respectivos processos; e

(vii) Documentação das entrevistas: as entrevistas precisam ser adequadamente documentadas e encaminhadas aos entrevistados, isto a fim de que validem todo o seu conteúdo. Como citado anteriormente, as entrevistas podem ser gravadas, a partir do consentimento dos entrevistados, para que esta etapa de documentação seja mais acurada e a entrevista flua como um diálogo – sem a necessidade de que a as entrevistas sejam transcritas ao vivo.

2. Terminologia

(i) Medida: medida de segurança presente na norma técnica que é objeto de avaliação para implementação;

(ii) Subtema: conjunto temático de medidas de segurança; e

(iii) Objetivo: objetivo de uma medida de segurança.

3. *Layout* de Pauta de Entrevista

Pauta de Entrevista		
<"Nome do órgão/entidade"/ "Nome da divisão">		
Número: *<"Número sequencial da Entrevista">*		
Data: *<DD/MM/AAAA>*		
Hora: *<HH;MIN>*		
Local: <*"Se presencial, inserir endereço. Se online, indicar aplicativo utilizado e 'link'">*		
Entrevistadores	**Setor**	***Status***
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Entrevistados	**Setor**	***Status***
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Medida	**Subtema**	**Objetivo**
<"Medida de segurança presente na norma técnica que é objeto de avaliação para implementação.">	*<"Conjunto temático de medidas de segurança.>"*	*<"Objetivo de uma medida de segurança.">*
<"Medida de segurança presente na norma técnica que é objeto de avaliação para implementação.">	*<"Conjunto temático de medidas de segurança.>"*	*<"Objetivo de uma medida de segurança.">*

4. ***Layout*** **da Ata de Entrevista à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais**[7]

Ata de Entrevista		
<"Nome do órgão/entidade"/ "Nome da divisão">		
Número: *<"Número sequencial da Entrevista">*		
Data: *<DD/MM/AAAA>*		
Hora: *<HH;MIN>*		
Local: <*"Se presencial, inserir endereço. Se online, indicar aplicativo utilizado e 'link'">*		
Entrevistadores	**Setor**	***Status***
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Entrevistados	**Setor**	***Status***
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Quesitos e Respostas		

[7] Como mencionado, este Questionário pode ser aplicado a partir de metodologia de "*Entrevistas*", orientada pelo *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP).
SÃO PAULO (Cidade). Controladoria Geral do Município. *Manual de Gestão de Riscos*. São Paulo, Controladoria Geral do Município, 2023.

<"Controles relacionados devem sempre ser citados pelo(s) Entrevistador(es) no início de cada série de Quesitos. Os controles podem ser encontrados no Anexo VI do Guia, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'."> *<"Exemplo">* *<"Controles relacionados a esta série de Quesitos são: (i) [....]; e (ii) [...], disponíveis no Anexo VI do 'Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo', 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'">* *<"**Existem Políticas, no setor, relativas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais**?>* *<"Respondeu [Nome], [Cargo/Função], que [...]">* ***<Já houve algum incidente de segurança da informação?>*** *<"Respondeu [Nome], [Cargo/Função], que [...]">*
Informações adicionais
<"Comentários adicionais a critério do(s) Entrevistador(es) ou mesmo por solicitação do(s) Entrevistado(s).">
Próximos passos

Responsável	Ação	Data
<"Inserir nome do agente público.">	*<"Inserir ação a ser realizada pelo agente público">*	*<DD/MM/AAAA>*
<"Inserir nome do agente público.">	*<"Inserir ação a ser realizada pelo agente público">*	*<DD/MM/AAAA>*

5. *Layout* de Comunicado da Equipe de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais sobre "*Kickoff*" e sobre as Entrevistas

<"Prezados Chefes dos setores da ZZ/SP,

Conforme alinhado com a Chefia de Gabinete, a partir do dia DD/MM/AAAA, dando continuidade às ações deste Programa de Governança em Privacidade e Proteção de Dados Pessoais da XX/SP, iniciaremos a realização de Entrevistas e respostas ao denominado 'Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'.

Abaixo, segue, para maiores esclarecimentos, as principais informações que serão abordados durante 'Kickoff', a ser realizado em DD/MM/AAAA, às HH, online, via 'XX'.

1. *Serão agendadas até XX Entrevistas para cada setor, com até XX horas de duração, às XXh, conforme Anexo deste Comunicado, 'Agenda de Entrevistas por setor';*

2. *Eventuais informações adicionais, descobertas com as Entrevistas, que possam depender de nova Entrevista, poderão, portanto, suscitar o agendamento de nova(s) Entrevista(s);*

3. *Os Chefes dos setores estão a receber, anexo, as Pautas das Entrevistas, as quais serão abordadas no 'Kickoff' para maiores esclarecimentos;*

4. *Os Chefes dos setores deverão encaminhar, até o dia DD/MM/AAA, a confirmação dos nomes e e-mail dos agentes públicos que participarão das Entrevistas, para o e-mail XXXX@prefeitura.sp.gov.br;*

5. *Serão considerados, durante as Entrevistas, os documentos já entregues pelos setores até as datas das respectivas Entrevistas;*

6. *Eventualmente, poderão ser repetidos quesitos sobre pontos eventualmente já respondidos em documentos ou em Entrevista pregressas;*

7. *Eventualmente, poderá haver Entrevistas conjugadas entre setores no caso em que se perceba haver alguma relação entre ambos quanto ao subtema tratado;*

8. *Serão levantadas, previamente às Entrevistas, informações sobre os sistemas utilizados pelos setores, restando os esclarecimentos sobre questões tecnológicas, para esta equipe de gestão de riscos, a cargo da equipe de TI e/ou do fornecedor desta Pasta;*

9. *As Entrevistas poderão/serão gravadas;*

10. *Serão consideradas, em ata das Entrevistas, a redação dos quesitos realizados pelos entrevistadores e as respostas dadas pelos entrevistados e consolidadas por esta equipe de gestão de riscos;*

11. *Poderão ser emitidas Notas Técnicas por esta equipe de gestão de riscos no decorrer da execução da agenda de Entrevistas, isto de acordo com a avaliação da própria equipe de gestão de riscos, assim como de acordo com a avaliação dos setores entrevistados, com vistas à implementação de controles, quando oportuno;*

12. *As respostas documentadas serão analisadas a fim de que subsidiem esta equipe em seu processo de identificação dos riscos à segurança da informação, à privacidade e à proteção de dados pessoais presentes em cada setor;*

13. *Os Chefes dos setores estão a receber, anexo, o denominado 'Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais', o qual cada setor deverá responder, a partir de avaliação de sua equipe, e encaminhar à equipe de gestão de riscos previamente à realização da primeira Entrevista relativa ao seu respectivo setor.*

Anexo

Agenda de Entrevistas por setor:

DD/MM/AAAA: XXX/ZZ/SP;
DD/MM/AAAA: XXX/ZZ/SP;
DD/MM/AAAA: XXX/ZZ/SP;
DD/MM/AAAA: XXX/ZZ/SP;
DD/MM/AAAA: YYY/ZZ/SP;
DD/MM/AAAA: YYY/ZZ/SP;
DD/MM/AAAA: YYY/ZZ/SP; e
DD/MM/AAAA: YYY/ZZ/SP.

Cordialmente,

Equipe de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais da ZZ/SP.">

Anexo V – Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

1. Metodologia

Solicitação de resposta, para os responsáveis de cada divisão do "*órgão/entidade*", à "*Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", constante no tópico 3 deste Anexo, que diz respeito à sua percepção de riscos à segurança da informação, à privacidade e à proteção de dados pessoais em sua respectiva área, isto com o subsídio das informações contidas nas Tabelas II e III, respectivamente, "*Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", e "*Quesitos à Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

2. Terminologia

(i) Probabilidade (P): probabilidade é a chance da ocorrência de um evento;

(ii) Impacto (I): impacto é o resultado de um evento que traz o efeito da incerteza nos objetivos;

(iii) Risco (R): risco é o *"efeito da incerteza nos objetivos"*[8];

(iv) Risco inerente (RI): risco inerente é o risco intrínseco à natureza de um processo;

(v) Risco residual (RR): risco residual é o risco remanescente após a adoção de controles.

[8] Item 3.1, "*risco*", da norma ABNT NBR ISO nº 31000:2018.

3. *Layout* do Questionário sobre Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Risco	Risco Inerente		Controles propostos	Efeito sobre o risco	Risco residual	
	(P)	(I)			(P)	(I)
R"*x*" – <*"Descrição do risco, com o subsídio da Tabela 'Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*> Processos: "*xx*"; "*xy*"; e "xz".	<*"Muito alta, alta, média, baixa ou muito baixa"*>	<*"Muito alto, alto, médio, baixo ou muito baixo"*>	<*"Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'"*>	<*"Reduzir, evitar, Compartilhar, aceitar ou potencializar"*>	<*"Muito alta, alta, média, baixa ou muito baixa"*>	<*"Muito alto, alto, médio, baixo ou muito baixo"*>
			<*"Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais.'"*>	<*"Reduzir, evitar, Compartilhar, aceitar ou potencializar"*>		
R"*x*" – <*"Descrição do risco, com o subsídio da Tabela 'Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*> Processos: "*xx*"; "*xy*"; e "xz".	<*"Muito alta, alta, média, baixa ou muito baixa"*>	<*"Muito alto, alto, médio, baixo ou muito baixo"*>	<*"Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'"*>	<*"Reduzir, evitar, Compartilhar, aceitar ou potencializar"*>	<*"Muito alta, alta, média, baixa ou muito baixa"*>	<*"Muito alto, alto, médio, baixo ou muito baixo"*>
			<*"Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'"*>	<*"Reduzir, evitar, Compartilhar, aceitar ou potencializar"*>		

Tabela II – Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Identificação	Risco	Escopo
1	Acesso não autorizado	Acesso indevido (permissão indevida) a um ambiente físico ou lógico.
2	Modificação não autorizada	Usuário sem permissão de alteração para um determinado registro realiza modificação não autorizada.
3	Perda	Perdas provocadas tanto por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, quanto por ações não intencionais, como falhas em sistemas e sobrescrita de dados.
4	Roubo	Dados roubados nas dependências internas do controlador/operador, como falhas nos controles de segurança dos sistemas, a exemplo da ausência ou fraca criptografia e falha de sistema que permita escalação de privilégio.
5	Remoção não autorizada	Usuário sem permissão para retirar ou copiar dados pessoais para outro local.
6	Coleta excessiva	Coleta de dados pessoais em quantidade superior ao necessário à finalidade da atividade a qual terá o tratamento de dados pessoais.
7	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais deve atender a uma finalidade específica a ser informada de forma transparente ao titular de dados pessoais.

8	Tratamento sem consentimento do titular de dados pessoais na hipótese em que o tratamento não esteja previsto em normas aplicáveis	Controlador de dados pessoais não obtém o consentimento do titular de dados pessoais para realizar um tratamento de dados sem norma que lhe diga respeito.
9	Falha em considerar os direitos do titular de dados pessoais	Falha na garantia de atendimento dos direitos do titular, conforme descritos, sobretudo, entre os arts. 9º e 17 a 23 da LGPD.
10	Compartilhar dados pessoais com terceiros sem o consentimento do titular na hipótese em que o consentimento esteja previsto em normas aplicáveis	Organização compartilha os dados pessoais sem hipótese de tratamento de dados que lhe autoriza.
11	Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro dos dados pessoais.
12	Associação indevida, direta ou indireta, de dados pessoais ao titular	A realização de todo tratamento de dados pessoais deve estar em conformidade com as normas aplicáveis. Qualquer tratamento que não atenda esse requisito pode produzir dados pessoais e informações pessoais com associações indevidas.
13	Erro de processamento	Dados de entrada que não são corretamente validados e operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado, a exemplo de execução de *script* de banco de

		dados que atualiza dado pessoal com dado equivocado e ausência de validação dos dados de entrada.
14	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento de dados pessoais.
15	Exposição a vulnerabilidades diversas	Existência de vulnerabilidade que, uma vez explorada, pode gerar outras vulnerabilidades ou mesmo outros riscos

Tabela III – Quesitos à Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais[9]

Quesitos
<"Apenas para referência."> *<"Não é necessário o preenchimento.">*
Quais são os processos que tratam dados pessoais e que, portanto, podem apresentar riscos à privacidade e à proteção de dados pessoais?
Quais são os objetivos desses processos?
Quais são os atores (a exemplo de fraquezas, ameaças e falhas) que podem afetar o alcance dos objetivos?
Quais são os riscos que podem se originar da ocorrência desses fatores e quais são as consequências caso o risco ocorra?
Quais são as medidas de mitigação já adotadas e quais são os controles internos já estabelecidos a fim de se evitar a ocorrência desses riscos? Qual a eficácia dessas medidas e desses controles?
Quais outras medidas de mitigação e controles internos podem ser adotados para adequar os níveis de risco identificados nesses processos?
Qual é a probabilidade e o impacto esperado da ocorrência desses riscos mesmo após a realização de uma avaliação de eficácia e de adequação das medidas de mitigação dos riscos e da adoção de controles internos?

A equipe de gestão de riscos deve, então, analisar a integralidade do Mapeamento de Processos (orientado pelo Capítulo I deste Guia, "*Mapeamento de Processos*") e do Mapeamento de Dados Pessoais (orientado pelo Capítulo II deste Guia, "*Mapeamento de Dados Pessoais*") em conjunto com as respostas aos quesitos presentes nas "*Entrevistas à Identificação de Riscos à Segurança da Informação, à*

[9] Adaptado do seguinte referencial bibliográfico: BRASIL. Tribunal de Contas da União. *Referencial Básico de Gestão de Riscos*. Brasília, Tribunal de Contas da União, abril de 2018.

Privacidade e à Proteção de Dados Pessoais" e em conjunto com as respostas aos quesitos dos "*Questionários à Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", isto a fim de que sejam identificadas: (i) as vulnerabilidades[10] existentes; (ii) as ameaças[11] que podem vir a explorar as vulnerabilidades existentes; e (iii) os riscos[12] existentes a partir da identificação das vulnerabilidades e das ameaças.

2. Análise de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Após a "*identificação*" dos riscos à segurança da informação, à privacidade e à proteção de dados pessoais existentes nos distintos processos da organização, é necessária uma "*análise*" sobre a "*natureza*" dos riscos e de suas respectivas "*características*".

Entre as "*características*" a serem analisadas, é possível a classificação dos riscos com base:

(i) no "*contexto*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[13], e o Anexo VI deste Guia, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", externo a este documento;

(ii) na "*análise dos controles existentes*", conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[14], e a norma ABNT NBR ISO nº 31000:2018[15];

---

[10] Rol exemplificativo de vulnerabilidades encontra-se presente no Guia Orientativo sobre Privacidade e Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, em suas Tabelas I e II – respectivamente, "*Exemplos de Vulnerabilidades e de Ameaças aos Recursos Humanos em uma Organização*" e "*Exemplos de Vulnerabilidades e de Ameaças aos Recursos Físicos, Tecnológicos e Informacionais em uma Organização*".

[11] Rol exemplificativo de ameaças encontra-se presente no Guia Orientativo sobre Privacidade e Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo, em suas Tabelas I e II – respectivamente, "*Exemplos de Vulnerabilidades e de Ameaças aos Recursos Humanos em uma Organização*" e "*Exemplos de Vulnerabilidades e de Ameaças aos Recursos Físicos, Tecnológicos e Informacionais em uma Organização*".

[12] Rol exemplificativo de riscos à segurança da informação, à privacidade e à proteção de dados pessoais encontra-se presente neste Guia, em sua Tabela II, "*Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[13] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*", e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[14] O *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP) dispõe dos seguintes critérios com relação ao nível de confiança sobre os controles existentes: (i) inexistente; (ii) fraco; (iii) mediano; (iv) satisfatório; e (v) forte. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[15] Item 6.4.3, "*análise de riscos*", da norma ABNT NBR ISO nº 31000:2018.

Após a classificação dos riscos a partir dessas "*características*", é possível a diferenciação de sua "*natureza*" entre:

(i) "*risco inerente*", que é um risco intrínseco à natureza de um processo, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[16], e o Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(ii) "*risco residual*", que é um risco remanescente após a adoção dos controles existentes, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[17], e o Anexo VI deste Guia, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

Posteriormente à distinção dos riscos entre "*riscos inerentes*" e "*riscos residuais*", é possível a classificação dos riscos com base nas seguintes "*características*":

(i) na "*probabilidade*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[18], e o Anexo VI deste Guia, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(ii) no "*impacto*" de sua ocorrência, conforme o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP)[19], e o Anexo VI deste Guia, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

---

[16] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

[18] Por "*contexto*", é possível entender a classificação, realizada pelo "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), que objetiva a categorização dos riscos em: (i) operacionais; (ii) orçamentários; (iii) de imagem; (iv) de conformidade; (v) social; e (vi) de integridade.
Os conceitos relativos a cada categoria contextual de risco podem ser encontrados no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".
[18] O *"Manual de Gestão de Riscos"* da Controladoria Geral do Município de São Paulo (CGM/SP), dispõe dos seguintes critérios com relação à análise da probabilidade: (i) muito baixa; (ii) baixa; (iii) média; (iv) alta; e (v) muito alta. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".
[19] O *"Manual de Gestão de Riscos"*, da Controladoria Geral do Município de São Paulo (CGM/SP), dispõe dos seguintes critérios com relação à análise de impacto: (i) muito baixo; (ii) baixo; (iii) médio; (iv) alto; e (v) muito alto. A descrição sobre cada nível pode ser encontrada no próprio "*Manual de Gestão de Riscos*" e no Anexo VI deste Guia, "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*".

A fim de mensurar, objetivamente, a análise dos "*riscos inerentes*" e dos "*riscos residuais*", é possível o uso de uma "*matriz de riscos*", que considere a "*probabilidade*" e o "*impacto*"[20] de suas respectivas ocorrências.

Para tanto, o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), traz metodologia que pode ser utilizada e que se encontra já instrumentalizada e adaptada ao contexto da segurança da informação, da privacidade e da proteção de dados pessoais, no Anexo VI deste Guia, "*Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*" e no Anexo VII, também deste Guia, "*Registro dos Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", externo a este documento.

3. Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

A "*mensuração*" dos riscos, como referida na etapa precedente, "*Análise de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", é importante para tornar possível à organização a sua "*Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", ou seja, a sua tomada de decisão frente aos riscos identificados.

A norma ABNT NBR ISO nº 31000:2018 entende, *e.g.*, ser possível as seguintes tomadas de decisão quanto aos riscos identificados:

(i) "*fazer mais nada*";
(ii) "*considerar as opções de tratamento de riscos*";
(iii) "*realizar análises adicionais para melhor compreender o risco*";
(iv) "*manter os controles existentes*"; e
(v) "*reconsiderar os objetivos*".

O "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), por sua vez, exemplificou as seguintes tomadas de decisão:

(i) *"evitar"*;
(ii) *"reduzir"*;
(iii) *"compartilhar"*;

[20] Apesar de o "*Manual de Gestão de Riscos*", da Controladoria Geral do Município de São Paulo (CGM/SP), dispor sobre diferentes tipos de impactos (operacionais, orçamentários, sociais, de imagem, de integridade e de conformidade), a metodologia trazida por este Guia utiliza-se apenas do tipo "*impacto de conformidade*", isto por entender que este possibilita o acoplamento dos demais tipos de impactos em si.

(iv) *"aceitar"*; e

(v) *"potencializar"*.

Nesse sentido, a partir da "*análise de riscos*", é possível, então, diferentes "*avaliações*" com relação aos riscos identificados.

"Mas por que aceitá-lo e não fazer mais nada?"

Muitas vezes, apesar de ser possível, por "*controles*", manter ou tratar os riscos identificados e analisados, a organização pode avaliar não valer a pena implementá-los, tendo em vista, *e.g.*, a possibilidade da incidência de novos riscos, inclusive não relacionados à segurança da informação, à privacidade e à proteção de dados pessoais, ou a expansão de aqueles já existentes.

4. Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Conforme a norma ABNT NBR ISO/IEC nº 27002:2022, um "*controle*" é uma medida apta a manter ou modificar um risco[21]. Assim, um "*controle*" pode reduzir ou eliminar a probabilidade e/ou o impacto de um risco identificado, analisado e avaliado.

Nesse sentido, pode um "*controle*" dizer respeito a todo o contexto de incidência da privacidade e da proteção de dados pessoais no âmbito da organização, ou mesmo ser aplicado a contextos específicos de incidência, a partir dos contextos internos e externos que influenciam nos distintos processos da organização.

Assim, a implementação de "*controles*" depende da especificidade dos riscos identificados, analisados e avaliados no contexto da salvaguarda à segurança da informação, da privacidade e da proteção de dados pessoais de uma organização.

Apesar disso, algumas normas técnicas e guias orientativos trazem exemplos que podem servir de parâmetro à análise dos controles existentes e como parâmetro à implementação de novos controles. Nesse sentido encontram-se os controles presentes na norma ABNT ISO/IEC nº 27001:2013, que trata de controles de segurança da informação, e na norma ABNT ISO/IEC nº 29151:2020, que trata de controles para a salvaguarda da privacidade e da proteção de dados pessoais.

No intuito de sistematizar os controles presentes na norma ABNT ISO/IEC nº 27001:2013 e na e na norma ABNT ISO/IEC nº 29151:2020, o Anexo VII deste Guia, externo a este documento,

[21] Item 0.3, "*controles*", da norma ABNT NBR ISO/IEC nº 27002:2022.

"*Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", os apresenta como rol exemplificativo de controles aptos ao tratamento dos riscos, assim como inclui diretrizes para as suas respectivas implementações.

A fim de auxiliar a documentação de todas as ações deste Capítulo, "*Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*", apresenta-se, neste Guia, o Anexo VI, *"Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*, cujo objetivo é dispor de metodologia à realização de parte do processo de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, e do Anexo VII, *"Registro dos Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*, cujo objetivo é dispor de *layout* à sua elaboração.

Anexo VI – Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

1. Metodologia

Como subsídio à realização da Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, este Anexo objetiva disponibilizar à equipe de gestão de riscos metodologia para documentar a realização das etapas presentes neste Capítulo: (i) Identificação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais; (ii) Análise de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais; (iii) Avaliação de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais; e (iv) Tratamento de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais. Como mencionado, por sua vez, o Anexo VII deste Guia, externo a este documento, traz *layout* à realização do Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais.

Utilizando-se do *layout* descrito, pode o Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais ser elaborado a partir das seguintes etapas:

(i) Registro das informações coletadas sobre as origens possíveis de riscos à segurança da informação, à privacidade e à proteção de dados pessoais: as primeiras informações a serem documentadas são, justamente, as relativas aquelas que trazem possíveis origens de riscos. Este registro diz respeito tanto às informações contidas no Mapeamento de Processos e no Mapeamento de Dados Pessoais, quanto às informações presentes nas Entrevistas e nos Questionários à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, de modo a tornar rastreável as possíveis origens dos riscos e a tornar mais acurado o "*feedback*" dos setores com relação às ações da equipe de gestão de riscos. Tome como exemplo a seguinte possível origem de risco, extraída de uma fictícia ata de entrevista: "*Os arquivos contendo os dados pessoais dos solicitantes são armazenados em sala fechada e com acesso restrito? Resposta: Não. Os arquivos são armazenados em armários ao longo dos corredores, no próprio setor e também em setores vizinhos e não são trancados.*"

(ii) Registro das vulnerabilidades: em seguida, necessária a documentação sobre as vulnerabilidades identificadas nas possíveis origens de riscos. Tendo em vista a possível origem de risco exemplificada pelo item anterior, a partir de sua análise e da análise do rol exemplificativo de vulnerabilidades existente nas Tabelas I e II do *"Guia Orientativo sobre Privacidade e Proteção de Dados Pessoais para a Administração Pública*

do Município de São Paulo", é possível a identificação de vulnerabilidade que pode ser redigida da seguinte forma: *"Armazenamento de documentos físicos contendo dados pessoais, em local sem confinamento e acesso exclusivo aos integrantes do setor"*.

(iii) Registro das ameaças: identificadas as vulnerabilidades, necessária a identificação das ameaças às vulnerabilidades relacionadas. Para a vulnerabilidade descrita no item anterior, é possível a identificação da seguinte ameaça: "*Acesso a dados pessoais por visitantes ou agentes estranhos ao setor custodiante dos documentos*". Em síntese, a análise tem como objetos o sujeito, a causa e a consequência adveniente relativa às vulnerabilidades identificadas.

(iv) Registro da identificação do risco: identificadas as vulnerabilidades e as ameaças a partir dos fatos contidos e documentados, o passo seguinte é o de identificar os riscos relacionados a essas vulnerabilidades e a essas ameaças, enquanto relativos à segurança da informação, à privacidade e à proteção de dados pessoais. Para tanto, poderá ser utilizada a Tabela II deste Guia, presente no Anexo VI, *"Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*;

(v) Registro da identificação da natureza do risco: como mencionado na etapa *"Análise de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*, a partir da identificação de um risco, é possível, pela análise de suas "*características*" ("*contexto*" e "*controles atuais*"), classificá-lo entre um "*risco inerente*" e um "*risco residual*";

(vi) Registro da probabilidade e do impacto de cada risco inerente: identificados os riscos inerentes, com a consideração sobre os controles eventualmente já existentes à sua mitigação, é necessária a definição sobre a probabilidade e sobre o impacto de cada um dos riscos inerentes. Para tanto, poderão ser utilizados os parâmetros escalares contidos nas Tabelas V e VI deste Guia, *"Parâmetros Escalares de Probabilidade para Riscos" e "Parâmetros Escalares de Impactos para Riscos"*. Ressalta-se que, apesar da existência de critérios quantitativos para essa definição, como a quantidade de ocorrências de um risco em determinado período de tempo, muitas das vezes as informações necessárias ao uso desses critérios não estão disponíveis ou não são confiáveis. Por essa razão, é necessário que a equipe de gestão de riscos, quando do pedido de "*feedback*" aos setores sobre o resultado destas ações (documentadas a partir do *layout* presente no Anexo VII deste Guia, externo a este documento), enfatizem a importância da análise, pelas equipes dos setores, da probabilidade da ocorrência e dos impactos dos riscos, enquanto definidos pela

equipe de gestão de riscos, isto a fim de que tragam considerações sobre a acuracidade dessa definição;

(vii) Registro do nível de risco inerente: o nível de risco inerente é calculado a partir da multiplicação entre o peso relativo ao parâmetro de probabilidade e o peso relativo ao parâmetro de impacto de conformidade de um risco;

(viii) Registro da identificação, da análise e da avaliação dos controles atualmente existentes com relação aos riscos: recomenda-se que a identificação, a análise e a avaliação dos controles atuais, relacionados a cada um dos riscos, sejam documentadas a partir do *layout* presente no Anexo VII deste Guia, externo a este documento. Para tanto, é possível a utilização da Tabela IV deste Guia, "*Parâmetros de Avaliação de Controles*" – que contempla, justamente, os parâmetros de avaliação ("*inexistente*", "*fraco*", "*mediano*", "*satisfatório*" e "*forte*") para a definição de parâmetro relativo ao conjunto de controles atualmente existentes. Para cada parâmetro, há a atribuição de um peso, que, ao final deste processo, será multiplicado pelo nível do risco inerente, que será objeto de análise a seguir, a fim de que seja encontrado o nível do risco residual – ou seja, o risco ainda presente apesar da existência de controles já implementados pela organização. A avaliação dos controles deve ser documentalmente justificada a partir do *layout* presente no Anexo VII deste Guia, externo a este documento, isto a fim de permitir as possíveis contestações, advindas das equipes dos setores, quando de seus respectivos "*feedbacks*" do resultado deste processo;

(ix) Registro da probabilidade e do impacto de cada risco residual: após a definição da probabilidade e do impacto de conformidade de cada risco inerente, é necessária, também, a definição da probabilidade e do impacto de conformidade de cada risco residual, ou seja, os riscos tendo em consideração os controles já existentes e aptos a mitigá-los. A análise dos controles atuais ocorre no momento da análise das características dos riscos, conforme mencionado;

(x) Registro de cada nível de risco residual: o nível de risco residual é calculado a partir da multiplicação do nível de risco inerente e o peso relativo ao(s) eventual(is) controle(s) já implementado(s) pela organização. Inexistindo-se controle(s) já implementado(s), por óbvio, o atual nível de um risco será aquele a si inerente.

(xi) Registro do controle a ser implementado para cada risco: obtidos os níveis de riscos inerentes e residuais, é possível a análise sobre quais controles podem ser implementados a fim de que esses riscos possam ser tratados. Para tanto, esta

metodologia pauta-se pelos controles indicados nas normas técnicas ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022 e ABNT NBR ISO/IEC nº 27701:2020, adaptados sob a forma de rol exemplificativo e presentes no *layout* do Anexo VII deste Guia, externo a este documento. Dessa forma, após a identificação, a análise e avaliação de determinado risco, e em consideração de suas características ("*contexto*" e "*controles atuais*"), é necessária uma tomada de decisão com relação a cada risco: se será aceito, nos termos nos quais se encontra, ou se será implementado algum controle com vistas a reduzi-lo, a eliminá-lo ou mesmo, em tese, a explorá-lo.

2. Terminologia

(i) Probabilidade (P): probabilidade é a chance da ocorrência de um evento;

(ii) Impacto (I): impacto é o resultado de um evento que traz o efeito da incerteza nos objetivos;

(iii) Risco (R): risco é o *"efeito da incerteza nos objetivos"*[22];

(iv) Risco inerente (RI): risco inerente é o risco intrínseco à natureza de um processo;

(v) Risco residual (RR): risco residual é o risco remanescente após a adoção de controles.

(vi) Parâmetro de Avaliação de Controles de um Risco (PAVALC): é o método de cálculo da avaliação de controles de um risco, conforme a Tabela IV deste Guia, "*Parâmetros de Avaliação dos Controles de um Risco*";

(vii) Média do Parâmetro de Avaliação de Controles de um Risco (mPAVALC): é a média aritmética consolidada da avaliação de controles de um risco observado em um órgão ou entidade, obtido pela média aritmética entre todos os Parâmetros de Avaliação de Controles de um risco observado;

(viii) Parâmetro de Probabilidade de um Risco (PPROB): é o método de cálculo da probabilidade de um risco, conforme a Tabela V deste Guia, "*Parâmetros Escalares de Probabilidade para Riscos*";

(ix) Parâmetro de Impacto de um Risco (PIMP): é o método de cálculo do impacto de um risco, conforme a Tabela VI deste Guia, "*Parâmetros Escalares de Impacto de Conformidade para Riscos*";

[22] Item 3.1, "*risco*", da norma ABNT NBR ISO nº 31000:2018.

(x) Nível de Risco Inerente (NRI): é o nível de um risco inerente observado, calculado a partir da multiplicação entre um dado Parâmetro de Probabilidade de um Risco (PPROB) e um dado Parâmetro de Impacto de um Risco (PIMP);

(xi) Nível de Risco Residual (NRR): é o nível de um risco residual observado, calculado a partir da multiplicação entre um dado Nível de Risco Inerente (NRI) e um dado Parâmetro de Avaliação de Controles de um Risco (PAVALC);

(xii) Média do Nível de Risco Inerente (mNRI): é a média aritmética consolidada do Nível de Risco Inerente de um dado risco em um órgão ou entidade, obtido pela média aritmética entre todos os Níveis de Risco Inerentes (NRIs) relativos a um dado risco;

(xiii) Média do Nível de Risco Residual (mNRR): é a média aritmética consolidada do Nível de Risco Residual de um dado risco em um órgão ou entidade, obtido pela multiplicação entre a média do Nível de Risco Inerente (mNRI) e a média do Parâmetro de Avaliação de Controles de um Risco (mPAVALC) relativos a um dado risco.

Tabela IV - Parâmetros de Avaliação dos Controles de um Risco

Descrição de Controle(s)	Parâmetro
Inexistente(s)	1
Fraco(s)	0,8
Mediano(s)	0,6
Satisfatório(s)	0,4
Forte(s)	0,2

Tabela V – Parâmetros Escalares de Probabilidade para Riscos

Probabilidade	Descrição	Frequência	Parâmetro
Muito baixa	**Improvável:** evento nunca ocorreu e, em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	<= 20%	1
Baixa	**Rara:** evento nunca ocorreu, mas de forma inesperada ou casual, o evento poderá até ocorrer, mas as circunstâncias pouco indicam essa possibilidade	> 20% e <=40%	2

Média	**Possível:** evento já ocorreu no passado e, de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	>40% e <=60%	5
Alta	**Provável:** evento já ocorreu no passado e, de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade	> 60% e <= 80%	8
Muito alta	**Praticamente certa:** de forma inequívoca, o evento está ocorrendo ou já ocorreu e as circunstâncias indicam claramente que poderá ser recorrente em um curto espaço de tempo	>80%	10

Tabela VI – Parâmetros Escalares de Impacto de Conformidade para Riscos

Impacto	Impacto de Conformidade	Parâmetro
Muito baixo	Descumprimento de políticas e processos internos de maneira reversível	1
Baixo	Descumprimento de políticas e processos internos de maneira irreversível	2
Médio	Descumprimento de atos normativos municipais de maneira reversível	5
Alto	Descumprimento de atos normativos municipais de maneira irreversível	8
Muito alto	Descumprimento de atos normativos estaduais e federais	10

3. *Layout* do Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

O *layout* do Registro de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais está disponível de forma externa a este documento, em formato de planilha, como Anexo VII deste Guia.

A fim de auxiliar a consecução do Registro, encontram-se, a seguir, instruções relativas a alguns de seus campos de preenchimento:

(i) "*Origem*": trata-se de cópia de trechos de entrevistas ou de outras informações coletadas que revelem origens possíveis de riscos à segurança da informação, à privacidade e à proteção de dados pessoais;

(ii) "*Código de Identificação*": trata-se da aposição de sigla do setor no qual foi identificado possíveis origens de riscos à segurança da informação, à privacidade e à proteção de dados pessoais, em conjunto com algum número sequencial distintivo das diferentes possíveis origens de riscos relacionadas ao setor. A título exemplificativo, a Corregedoria Geral do Município de São Paulo (CORR) pode ser identificada a partir de sua sigla juntamente com diferentes números que distinguem as diferentes possíveis origens de riscos identificadas, como CORR-01 e CORR-02;

(iii) "*Vulnerabilidade*": após a aposição de possível origem de riscos relacionada a determinado setor (preenchimento de "*Origem*" e de "*Código de Identificação*"), é possível o início da identificação de riscos a partir da identificação e aposição de vulnerabilidade relacionada a cada possível origem de risco. Observe que, a partir desta metodologia, é possível que ocorra a reincidência de uma mesma vulnerabilidade em diferentes possíveis origens de risco, inclusive em diferentes setores da organização – de modo que um mesmo tipo de risco, em consequência, também possa ser identificado diversas vezes. Por essa razão, para que possa ser obtida a mensuração única de um risco inerente, é necessária a realização de cálculo da média aritmética dos Níveis de Risco Inerente (NRIs) de um dado risco, identificado diversas vezes. O resultado é a média do Nível de Risco Inerente (mNRI) do risco considerado. Após a identificação de todas as vulnerabilidades relacionadas às possíveis origens de risco, é recomendável a criação de um rol exemplificativo de vulnerabilidades que afetam o órgão ou a entidade – que pode se utilizar das Tabelas I e II, presentes no "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*";

(iv) "*Ameaça*": após a identificação das vulnerabilidades, é necessário que sejam identificadas as ameaças. Como observado anteriormente, as ameaças podem ser de natureza humana ou de ordem natural e se classificam de acordo com a sua natureza acidental ou intencional. Após a identificação de todas as ameaças relacionadas às possíveis origens de risco, é recomendável a criação de um rol exemplificativo de ameaças que afetam o órgão ou a entidade – que pode se utilizar das Tabelas I e II, presentes no "*Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo*";

(v) "*Risco (R)*": neste campo, deve ser aposto o risco identificado, que podem ser aqueles listados na Tabela II deste Guia, presente no Anexo VI, *"Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais"*;

(vi) "*Parâmetro de Probabilidade de um Risco (PPROB)*": neste campo, deve ser aposto o parâmetro relativo à probabilidade do risco identificado, conforme a Tabela V deste Guia, "*Parâmetros Escalares de Probabilidade para Riscos*";

(vii) "*Probabilidade (P)*": neste campo, deverá ser aposta a descrição de chance da ocorrência do risco observado de acordo com o parâmetro de probabilidade utilizado. Como antevisto, é possível a aposição das seguintes descrições, alternativamente, a depender do parâmetro selecionado: "*muito baixa*"; "*baixa*"; "*média*"; "*alta*"; e "*muito alta*";

(viii) "*Parâmetro de Impacto de um Risco (PIMP)*": neste campo, deve ser aposto o parâmetro do impacto do risco identificado, conforme a Tabela VI deste Guia, "*Parâmetros Escalares de Impacto de Conformidade para Riscos*";

(ix) "*Impacto (I)*": neste campo, deverá ser aposto o parâmetro adequado de impacto de conformidade do risco. Como antevisto, é possível a aposição das seguintes descrições, alternativamente: "*muito baixo*"; "*baixo*"; "*médio*"; "*alto*"; e "*muito alto*";

(x) "*Justificativa da Probabilidade (P) e do Impacto (I)*": neste campo, deverá ser justificada a aposição dos parâmetros de probabilidade e de impacto para o risco identificado;

(xiv) "*Nível de Risco Inerente (NRI)*": neste campo, deverá ser aposto o resultado do cálculo relativo à multiplicação entre o parâmetro de probabilidade e o parâmetro de impacto definidos e selecionados para o risco identificado;

(xi) "*Controles Atuais*": neste campo, deverão ser indicados os controles atualmente implementados;

(xv) "*Parâmetro de Avaliação de Controles de um Risco (PAVALC)*": neste campo, deverá ser aposto o parâmetro que mais se adequa à avaliação sobre a efetividade dos controles já

implementados, conforme a Tabela IV deste Guia, "*Parâmetros de Avaliação dos Controles de um Risco*";

(xii) "*Avaliação de Controles Atuais*": neste campo, deverá ser aposta a descrição do parâmetro selecionado previamente. Como antevisto, é possível a aposição das seguintes descrições, alternativamente: "*Inexistente(s)*"; "*Fraco(s)*"; "*Mediano(s)*"; "*Satisfatório(s)*"; e "*Forte(s)*".

(xiii) "*Justificativa da Avaliação dos Controles Atuais"*: neste campo, deverá ser justificada a aposição do parâmetro de avaliação dos controles atuais relativo ao risco identificado;

(xiv) "*Nível de Risco Residual (NRR)*": neste campo, deverá ser aposto o resultado do cálculo relativo à multiplicação entre o Nível de Risco Inerente (NRI), definido previamente, e o parâmetro de avaliação de controles atuais selecionado;

(xv) "*Dado Pessoal (DP)*": neste campo, deverá ser indicado se o risco identificado se relaciona ao tratamento de dados pessoais – isto de acordo com o conceito de dado pessoal previsto pelo art. 5º, inc. I, da LGPD;

(xvi) "*Dado Não Pessoal (DNP)*": neste campo, deverá ser indicado se o risco identificado se relaciona a outros dados que não aqueles conceituados como dados pessoais;

(xvii) "*Suporte*": neste campo, deverá ser indicado o suporte do ativo objeto da avaliação de riscos – ou seja, o suporte pelo qual flui a informação e que pode deter vulnerabilidades e ser objeto de ameaças, a exemplo das fontes tangíveis e intangíveis de retenção (citadas no Anexo III deste Guia, *"Questionário sobre a Privacidade e a Proteção de Dados Pessoais"*);

(xviii) "*Controle(s) a implementar*": após a análise e avaliação dos riscos, neste campo, deverão ser apostos os controles selecionados que visem a tratar os riscos identificados. Os controles relacionados nesta metodologia, de modo exemplificativo, são os constantes nas normas técnicas ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022 e ABNT NBR ISO/IEC nº 27701:2020. No Anexo VII deste Guia, externo a este documento, é possível encontrar o rol exemplificativo de controles, que poderão ser utilizados;

(xix) *"Diretriz de implementação"*: neste campo, poderão os controles indicados no campo "*Controle(s) a implementar*" ser complementados com diretrizes que sejam entendidas como pertinentes;

(xx) "*Confidencialidade*": neste campo, deverá ser indicado se a ocorrência do risco poderá afetar a confidencialidade das informações tratadas pela Prefeitura do Município de São Paulo;

(xxi) "*Disponibilidade*": neste campo, deverá ser indicado se a ocorrência do risco poderá afetar a disponibilidade das informações tratadas pela Prefeitura do Município de São Paulo;

(xxii) "*Integridade*": neste campo, deverá ser indicado se a ocorrência do risco poderá afetar a integridade das informações tratadas pela Prefeitura do Município de São Paulo;

(xxiii) "*Responsável*": neste campo, poderá ser indicado a divisão do setor no qual originou-se o risco identificado;

(xxiv) *"De Acordo?"*: após o preenchimento de todo o Registro pela equipe de gestão de riscos, seu rascunho deverá ser enviado à equipe de cada setor a fim de avaliar a sua concordância com todas as atividades relacionada à gestão de riscos até então realizadas. Neste campo, a equipe do setor poderá responder "*sim*" ou "*não*";

(xxv) *"Justificativa da Equipe do Setor"*: neste campo, poderá a equipe de cada setor relacionada ao risco identificado manifestar-se a respeito das atividades desenvolvidas pela equipe de gestão de riscos. Em caso de concordância com as atividades até então realizadas (conforme aposição de "*sim*" no campo "*De Acordo?*"), não é obrigatória a manifestação da equipe. Porém, em caso de discordância (conforme aposição de "*não*" no campo "*De Acordo?*"), obrigatória a justificativa, isto a fim de que sejam esclarecidas, à equipe de gestão de riscos, as razões detalhadas pelas quais a equipe do setor entende pertinente uma revisão;

(xxvi) *"Data da Manifestação da Equipe do Setor"*: neste campo, a equipe do setor deverá apor a data de suas manifestações presentes nos campos *"De Acordo?"* e *"Justificativa da Equipe do Setor"*;

(xxvii) *"Justificativa da Equipe de Gestão de Riscos"*: neste campo, a equipe de gestão de riscos poderá emitir justificativa diante da manifestação da equipe do setor, de modo a acatá-la ou não; e

(xxviii) *"Mantém ou Exclui?"*: neste campo, a equipe de gestão de riscos deverá indicar a resposta que mais se aproxima daquela emitida no campo anterior, *"Justificativa da Equipe de Gestão de Riscos"*, isto a partir das possibilidades de resposta "*sim*", "*não*" e "*retifica*".

Após a realização do Registro dos Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, a fim de prosseguir com o processo de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, necessário que os controles a serem implementados, conforme a avaliação da equipe de gestão de riscos e com a ciência da equipe dos

setores, sejam, então, levados à Chefia do órgão ou da entidade, isto a fim de que possam ser previstos em plano de ação que objetive as suas respectivas implementações.

Todos os processos objeto deste Guia, como é de se concluir, devem periodicamente ser revisitados e atualizados – no mínimo, anualmente, quanto aos órgãos da Administração Municipal, como estabelece a Instrução Normativa CGM/SP nº 01/2022, com relação ao "*Mapeamento de Dados Pessoais*" e ao "*Relatório de Impacto à Proteção de Dados Pessoais*".

Essas contínuas revisitações e atualizações dos processos orientados por este Guia são necessárias justamente em razão de constituírem-se como um instrumento apto a permitir a mensuração da maturidade dos órgãos e das entidades com relação à sua conformidade às normas referentes à privacidade e à proteção de dados pessoais, além de permitirem o registro histórico dessa conformidade a partir de metodologia específica.

5. Relatório de Impacto à Proteção de Dados Pessoais

Conforme o art. 5º, inc. XVII, da LGPD, o "*Relatório de Impacto à Proteção de Dados Pessoais*" é a documentação do controlador que contém a descrição dos *"Registros das Operações de Tratamento de Dados Pessoais"* que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoas, bem como a descrição dos controles implementados ou que serão implementados a fim de mitigar esses riscos.

Como se pode interpretar, a descrição sobre os controles já implementados ou que serão objeto de implementação diz respeito à descrição sobre a integralidade do processo de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais realizado.

Como dispõe o art. 32 da LGPD, a ANPD, a qualquer momento, pode solicitar ao Poder Público a publicação de Relatório e sugerir a adoção de boas práticas para o tratamento de dados pessoais. Visando a padronizá-lo no âmbito do Poder Executivo Municipal, a Controladoria Geral do Município, por meio de sua Instrução Normativa CGM/SP nº 01/2022, também estabeleceu requisitos para a sua elaboração e disponibilizou, em seu Anexo II, *layout* à realização do "*Relatório de Impacto à Proteção de Dados Pessoais*".

Como aduziu o art. 14, inc. V, da Instrução Normativa CGM/SP nº 01/2022, o Relatório de Impacto à Proteção de Dados Pessoais deve contemplar:

(i) data de sua criação e de sua atualização, quando aplicável;

(ii) identificação dos agentes de tratamento e do encarregado;

(iii) descrição sobre a necessidade de sua elaboração ou de sua atualização;

(iv) descrição do tratamento de dados pessoais, com base no "*Mapeamento de Dados Pessoais*";

(v) descrição sobre a natureza e sobre o escopo do tratamento de dados pessoais;

(vi) descrição sobre o contexto e sobre a necessidade do tratamento de dados pessoais;

(vii) descrição sobre a finalidade do tratamento de dados pessoais;

(viii) descrição sobre a "*Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais*"; e

(ix) descrição sobre as partes consultadas durante a sua elaboração.

No intuito da consecução de "*Relatório de Impacto à Proteção de Dados Pessoais*" por cada órgão ou entidade, a Controladoria Geral do Município também desenvolveu, como antevisto, metodologia que busca a padronização da realização de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, que pode ser encontrada neste Guia e complementada pelo "*Manual de Gestão de Riscos*", do mesmo órgão.

Conforme atribuição conferida pelo art. 6º, inc. VIII, do Decreto Municipal nº 59.767/2020, o Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município deverá publicar os Relatórios de Impacto à Proteção de Dados Pessoais de cada órgão da Administração Pública Municipal, isto quando assim solicitado pela ANPD, nos termos do art. 32 da LGPD: *"A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público."*

Referências bibliográficas

ABNT. Associação Brasileira de Normas Técnicas. ABNT ISO/TR nº 31004:2015. *Gestão de riscos* – guia para implementação da ABNT NBR ISO 31000. Rio de Janeiro: ABNT, 2015.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO nº 31000:2018. *Gestão de riscos* – diretrizes. Rio de Janeiro: ABNT, 2018.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27001:2013. *Tecnologia da informação* – técnicas de segurança – sistemas de gestão da segurança da informação – requisitos. Rio de Janeiro: ABNT, 2013.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27002:2022. *Segurança da informação, segurança cibernética e proteção à privacidade* – controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27701:2020. *Técnicas de segurança* – extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – requisitos e diretrizes. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 29100:2020. *Tecnologia da informação* – técnicas de segurança – estrutura de privacidade. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC nº 27018:2021. Tecnologia da informação – técnicas de segurança – código de prática para proteção de dados pessoais em nuvens públicas que atuam como operadores de dados pessoais. Rio de Janeiro: ABNT, 2021.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR ISSO/IEC nº 29151/2020. *Tecnologia da informação* – técnicas de segurança – código de prática para proteção de dados pessoais. Rio de Janeiro: ABNT, 2020.

ABNT. Associação Brasileira de Normas Técnicas. ABNT NBR/IEC nº 31010:2021. *Gestão de riscos* – técnicas para o processo de avaliação de riscos. Rio de Janeiro: ABNT, 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. Estudo Preliminar. *Hipóteses legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/participamaisbrasil/blob/baixar/17636>. Acesso em: 04 out. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. Guia Orientativo. *Tratamento de dados pessoais pelo Poder Público*. Brasília, Autoridade Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 04 out. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, *Diário Oficial da União*, Brasília, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, *Diário Oficial da União*, 11 de janeiro de 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, *Diário Oficial da União*, 18 de novembro de 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, *Diário Oficial da União*, 24 de abril de 2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17 nov. 2022.

BRASIL. Lei Federal nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, *Diário Oficial da União*, 15 de agosto de 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 04 out. 2022.

BRASIL. Lei Federal nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, *Diário Oficial da União*, 16 de julho de 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 17 nov. 2022.

BRASIL. Tribunal de Contas da União. *Referencial Básico de Gestão de Riscos*. Brasília, Tribunal de Contas da União, 2018.

FALCÃO, Daniel; PEROLI, Kelvin. As novas abordagens da privacidade: contextos, tipos e dimensões. *Migalhas*, Migalhas de Proteção de Dados Pessoais, 30 dez. 2021. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/357252/as-novas-abordagens-da-privacidade-contextos-tipos-e-dimensoes>. Acesso em: 04 out. 2022.

FALCÃO, Daniel; PEROLI, Kelvin. Imagem, dado pessoal sensível? *Consultor Jurídico*, Observatório Constitucional, 28 maio 2022. Disponível em: <https://www.conjur.com.br/2022-mai-28/observatorio-constitucional-imagem-dado-pessoal-sensivel>. Acesso em: 17 nov. 2022.

NISSENBAUM, Helen. *Privacy in Context*. Technology, Policy, and the Integrity of Social Life. Stanford, EUA: Stanford University Press, 2010.

PEROLI, Kelvin; FALEIROS JÚNIOR, José Luiz de Moura. Comentários aos arts. 50 e 51 da LGPD. *In:* MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (orgs.). *Comentários à Lei Geral de Proteção de Dados Pessoais.* Indaiatuba: Foco, 2022, pp. 461-479.

SÃO PAULO (Cidade). Decreto Municipal nº 59.767, de 15 de setembro de 2020. Regulamenta 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 Municipal direta e indireta. São Paulo, *Diário*

Oficial da Cidade de São Paulo, 15 de setembro de 2020. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/decreto-59767-de-15-de-setembro-de-2020>. Acesso em: 04 out. 2022.

SÃO PAULO (Cidade). Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022. Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Administração Pública Municipal de São Paulo. São Paulo, *Diário Oficial da Cidade*, 22 de julho de 2022. Disponível em: <https://legislacao.prefeitura.sp.gov.br/leis/instrucao-normativa-controladoria-geral-do-municipio-cgm-1-de-21-de-julho-de-2022>. Acesso em: 04 out. 2022.

SÃO PAULO (Cidade). Lei Municipal nº 8.989, de 29 de outubro de 1979. Dispõe sobre o estatuto dos funcionários públicos do município de São Paulo, e dá providências correlatas. São Paulo*, Diário Oficial da Cidade de São Paulo*, 29 de outubro de 1979. Disponível em: < http://legislacao.prefeitura.sp.gov.br/leis/lei-8989-de-29-de-outubro-de-1979>. Acesso em: 04 out. 2022.

SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, jan. 2006, vol. 154, n. 3, pp. 477–560. Disponível em: <https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1/>. Acesso em: 17 nov. 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Bruxelas, *Jornal Oficial da União Europeia*, 27 abril 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 17 nov. 2022.

XAVIER, Fábio Correa. *Recomendações de Segurança da Informação para Municípios de Pequeno Porte na jornada de adequação à LGPD*. São Paulo: Tribunal de Contas do Estado de São Paulo, 21 out. 2021. Disponível em: <https://www.tce.sp.gov.br/6524-artigo-recomendacoes-seguranca-adequacao-lgpd-por-fabio-xavier>. Acesso em: 03 nov. 2022.

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO