PROJETO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

FICHA TÉCNICA

GOVERNO DO ESTADO DE MINAS GERAIS

Governador do Estado de Minas Gerais
Romeu Zema

Secretário de Estado de Planejamento e Gestão
Luisa Barreto

Controlador-Geral do Estado de Minas Gerais
Rodrigo Fontenelle de Araújo Miranda

Secretário de Estado de Fazenda
Gustavo de Oliveira Barbosa

Advogado-Geral do Estado de Minas Gerais
Sérgio Pessoa de Paula Castro

Diretor-Presidente da Companhia de Tecnologia da Informação de MG
Roberto Tostes Reis

PROGRAMA PROTEÇÃO DE DADOS PESSOAIS: SUGESTÕES PARA OS TRABALHOS - 2020

Elaboração
Grupo de Trabalho sobre a Lei Geral de Proteção de Dados

Contato:
gt-lgpd-governomg@prodemge.gov.br
https://lgpd.mg.gov.br/

GRUPO DE TRABALHO SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS:

Secretaria de Estado de Planejamento e Gestão
Rodrigo Diniz Lara
Fábrício de Barros Salum
Weslley Costa Nogueira
Daniel Machado Maia

Controladoria-Geral do Estado
André Luiz Guimarães Amorim
Beatriz Faria de Almeida Loureiro
Reginaldo Vieira Neres
Soraia Ferreira Quirino Dias

Secretaria de Estado de Fazenda
Aline Chevrand Campos
Anderson Aparecido Félix
Daniel de Oliveira Rezende
Gabriel Arbex Valle
Lindenberg Naffah Ferreira

Advocacia-Geral do Estado
Rafael Rezende Faria
Luisa Miranda Scalzo
Sandrelise Gonçalves Chaves

Prodemge
Alander Antônio Faustino
Bruno Moreira Camargos Belo
Filipe Rodrigues Costa

FASE 4

SUMÁRIO

1. Identificar pontos falhos na proteção aos dados pessoais (gap analysis) 5

2. Propor medidas para sanar as falhas referentes à proteção de dados pessoais 15

3. Analisar riscos de incidentes 17

4. Propor ações corretivas/mitigadoras dos riscos apontados 29

5. Elaborar e publicar política e diretrizes de privacidade e proteção de dados pessoais no site institucional 32

6. Política de Segurança da Informação e Requisitos em Contratações 67

7. Relatório de Impacto à Proteção de Dados Pessoais (RIPD) 81

1. IDENTIFICAR PONTOS FALHOS NA PROTEÇÃO AOS DADOS PESSOAIS (GAP ANALYSIS)

1.1. Diagnóstico diferencial

Para se identificar pontos falhos na proteção aos dados pessoais é necessário ter a visão completa do processo de tratamento de dados. Para isso, é recomendável a elaboração do Relatório de Impacto à Proteção de Dados (RIPD), cuja definição, estabelecida no art. 5º, XVII da Lei 13709/2018 (Lei Geral de Proteção de Dados), encontra-se abaixo transcrita:

"documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

É ponto pacífico entre os especialistas em Tecnologia da Informação, especialmente aqueles que orbitam a área do conhecimento denominada Segurança da Informação, que não é possível proteger (nesse contexto, vamos considerar a adoção de medidas, salvaguardas e mecanismos de mitigação de risco) aquilo que não é conhecido, inventariado, catalogado. Por isso, é mandatório que os agentes de tratamento de dados, em especial o controlador, realizem o inventário dos dados pessoais[1] sob sua custódia.
O ponto de partida para a criação do inventário de dados é o mapeamento dos processos que realizam operações de tratamento de dados pessoais. Nunca é demais relembrar que o conceito de tratamento é bastante amplo, conforme disposto no art. 5º, X, abaixo transcrito:

"toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Avançando na definição do RIPD nos termos da LGPD, chegamos ao termo: "que podem gerar riscos às liberdades civis e aos direitos fundamentais". De acordo com o Guia de Boas Práticas para a conformidade com a Lei Geral de Proteção de Dados elaborado pelo Governo Federal, para avaliar os riscos, é necessário levar-se em consideração quatro aspectos: a natureza, o escopo, o contexto e a finalidade do tratamento. A seguir detalharemos cada um deles.

1.2. Natureza

Representa como a instituição pretende tratar ou trata o dado pessoal. Importante descrever, dentre outros:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- meio utilizado para coleta dos dados pessoais (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.);
- com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;
- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
- medidas de segurança atualmente adotadas.

Nessa etapa, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

1.3. Escopo

Representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:

- os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis;
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento e abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala. Quanto maior o volume de dados tratados e a sensibilidade deles de acordo com a definição da lei, maiores os riscos de infringir diretos e liberdades fundamentais do titular. Consequentemente maior o cuidado que os agentes de tratamento deverão ter ao manipularem esses dados.

1.4. Contexto

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados. O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

1.5. Finalidade

É a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados. Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas nos artigos 7° e 11 da LGPD, no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiro;
- proteção do crédito; e
- garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos. Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto no art. 10 da LGPD.

Por fim, cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela mantém relacionamento.

A parte final do inciso que trata do RIPD nos traz outro aspecto extremamente importante e sob o qual é necessário um maior detalhamento, qual seja: “medidas, salvaguardas e mecanismos de mitigação de risco”.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

De acordo com a ISO 31000, o risco é o efeito da incerteza nos objetivos. Ainda conforme a referida norma:

- um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças.
- os objetivos podem possuir diferentes aspectos e categorias e podem ser aplicados em diferentes níveis.
- o risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais. Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

1.6. Definindo critérios de risco.

A Norma ISO 31000 que contempla as Diretrizes para a Gestão de Riscos recomenda:

- que a organização especifique a quantidade e o tipo de risco que pode ou não assumir em relação aos objetivos estabelecidos.
- que estabeleça critérios para avaliar a significância do risco para apoiar os processos de tomada de decisão.
- que os critérios de risco estejam alinhados à estrutura de gestão de riscos e sejam personalizados para o propósito específico e o escopo da atividade em consideração.
- que os critérios de risco reflitam os valores, objetivos e recursos da organização e sejam consistentes com as políticas e declarações sobre gestão de riscos.
- que os critérios de risco sejam estabelecidos levando em consideração as obrigações da organização e os pontos de vista das partes interessadas.

Embora convenha que os critérios sejam estabelecidos no início do processo de avaliação de riscos, eles são dinâmicos; e convém que sejam continuamente analisados criticamente e alterados, se necessário.

Para estabelecer os critérios de risco, convém considerar:

- a natureza e o tipo de incertezas que podem afetar resultados e objetivos (tanto tangíveis quanto intangíveis);
- como as consequências (tanto positivas quanto negativas) e as probabilidades serão definidas e medidas;
- fatores relacionados ao tempo;
- consistência no uso de medidas;
- como o nível de risco será determinado;
- como as combinações e sequências de múltiplos riscos serão levadas em consideração;
- a capacidade da organização.

O Guia de Boas Práticas do Governo Federal traz um modelo para identificação e avaliação de riscos. A seguir descreveremos o processo, que ressaltamos trata-se de uma dentre inúmeras possibilidades de processos para identificação e avaliação de riscos.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares desse exemplo são:

Tabela 1: Parâmetros Escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Tabela 1: Parâmetros Escalares

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Probabilidade	15	75	150	225
	10	50	100	150
	5	25	50	75
Impacto		5	10	15

Figura 1: Matriz Probabilidade X Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz representada pela Figura 1.

Risco enquadrado na região:
- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

Em resumo, a identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível do risco.

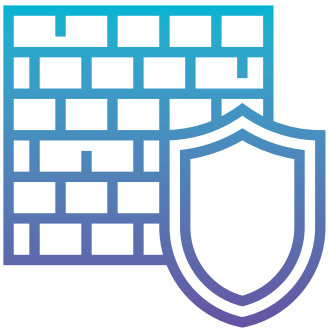
Para melhor entendimento, é destacada a seguir uma tabela com lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de risco indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros itens representam riscos de privacidade obtidos da seção 6.4.4 da norma ISO/IEC 29134:2017 que estabelece as Técnicas de segurança e as diretrizes para avaliação do impacto na privacidade.

Lembrando que deve ser identificado qualquer risco que afete o tratamento de dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade).

Tabela 2 Risco referente ao tratamento de dados pessoais

ID	Risco ao tratamento de dados pessoais	P1	I2	Nível de Risco (PxI)3
R01	Acesso não autorizado	10	15	150
R02	Modificação não autorizada	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada	5	15	75
R06	Coleção Excessiva	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.)	5	15	75
R14	Reidentificação de dados pseudonimizados	5	15	75

Legenda: P – Probabilidade; I – Impacto.



1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23)

Para finalizar, e importante destacar que o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição. Serve tanto para a análise quanto para a documentação. Por meio dele é possível ter uma visão detalhada de todos os processos da organização que tratam dados pessoais e identificar as inconformidades e riscos no tratamento e proteção dos dados pessoais.

2. PROPOR MEDIDAS PARA SANAR AS FALHAS REFERENTES À PROTEÇÃO DE DADOS PESSOAIS

Neste ponto, os agentes de tratamento de dados pessoais precisam propor e implementar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas. Abaixo apresentaremos um modelo contido no Guia de Boas Práticas do Governo Federal. A coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa de identificação e avaliação dos riscos.

Importante frisar que não existe segurança 100% e consequentemente não existem ações que garantirão 100% a proteção dos dados pessoais. Por esse motivo é importante ter em mente que o controlador não terá capacidade (técnica, administrativa e/ou financeira) de eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis, inclusive um de nível alto, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação (como custo, tempo, recursos técnicos e operacionais). No entanto, se houver um risco residual de nível alto, é recomendável consultar a Autoridade Nacional de Proteção de Dados antes de prosseguir com as operações de tratamento dos dados pessoais.

A seguir, são apresentados exemplos de medidas para lidar com os riscos:

RISCO	MEDIDA(S)	EFEITO SOBRE O RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S) APROVADA(S)[3]
			P	I	P x I	
R01 Acesso não autorizado	1. Controle de acesso Lógico.	Reduzir	5	10	50	SIM
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					

Legenda: P – Probabilidade; I – Impacto.

Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

Neste momento, e a critério do responsável pela elaboração do RIPD, a coluna "Medida(s)" também pode ser preenchida de forma mais detalhada, indicando os principais aspectos da medida segurança ou controles de segurança adotados para tratar o risco. Esse procedimento propicia mais visibilidade em relação ao tratamento do risco.

3. ANALISAR RISCOS DE INCIDENTES

Os riscos mapeados podem ou não se materializar, mas compete aos agentes de tratamento adotarem medidas para mitigá-los. Isso reduzirá a possibilidade da ocorrência de um incidente de segurança da informação, maculando princípios tutelados pela LGPD. É sempre importante reforçar que segurança 100% não existe. O que a lei visa assegurar é que o agente de tratamento adotou medidas preventivas (para evitar a ocorrência do incidente) e corretivas (minimizar o dano, caso o incidente aconteça) adequadas. As medidas preventivas foram tratadas anteriormente nesta etapa do Programa de Privacidade. O foco neste momento é abordar as ações corretivas. E para que elas sejam eficazes, é recomendável que a organização defina e implemente um processo de Gestão dos Incidentes de Segurança da Informação.

Primeiramente, vamos trazer o conceito de incidente de segurança da informação: "pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, levando à perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade".
O objetivo do processo de Gestão de Incidentes de Segurança da Informação, de acordo com a ISO 27002, é assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.

Mas como assegurar a efetividade dessa ação? A referida norma descreve um conjunto de recomendações sobre as quais discorreremos a seguir:

3.1. Responsabilidades e Procedimentos

Controle

Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

Diretrizes para implementação

Convém que as seguintes diretrizes para o gerenciamento de responsabilidades e procedimentos com relação à gestão de incidentes de segurança da informação sejam consideradas:

a) convém que responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização:

I. procedimentos para preparação e planejamento a resposta a incidente;

II. procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação;

III. procedimentos para registros das atividades de gerenciamento de incidentes;

IV. procedimentos para manuseio de evidências forenses;

V. procedimentos para avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação;

VI. procedimentos para resposta, incluindo aquelas relativas à escalação, recuperação controlada de um incidente e comunicação às pessoas ou organizações, internas e externas;

b) convém que os procedimentos estabelecidos assegurem que:
I. pessoal competente trate as questões relativas a incidentes de segurança dentro da organização;
II. um ponto de contato para notificação e detecção de incidentes de segurança seja definido;
III. contatos apropriados sejam mantidos com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação;

c) convém que procedimentos de notificação incluam:
I. preparação de formulários de notificação de evento de segurança da informação para apoiar as ações e ajudar a pessoa que está notificando, destacando todas as ações necessárias no caso de um evento de segurança da informação;
II. o procedimento a ser realizado no caso de um evento de segurança da informação, por exemplo, relatar todos os detalhes imediatamente, como tipo de não conformidade ou violação, ocorrências de mau funcionamento, mensagens na tela; e imediatamente notificar ao ponto de contato, de forma coordenada;
III. referência a um processo disciplinar formal estabelecido para tratar a situação de funcionários que cometam violações de segurança da informação;
IV. processo de realimentação adequado para assegurar que aquelas pessoas que notificaram um evento de segurança da informação sejam informadas acerca dos resultados após o assunto ter sido tratado e encerrado.

Convém que os objetivos para a gestão de incidentes de segurança da informação sejam acordados com a direção e garantam que as pessoas responsáveis pelo processo entendem as prioridades da organização para tratá-los.

Informações adicionais

Incidentes de segurança da informação podem transcender os limites organizacionais e nacionais. Para responder a tais incidentes, existe uma crescente necessidade de coordenar resposta e compartilhar informação sobre esses incidentes com organizações externas, quando apropriado.

3.2. Notificação de eventos de segurança da informação

Controle

Convém que os eventos de segurança da informação sejam relatados por meio dos canais de gestão, o mais rapidamente possível.

Diretrizes para implementação

Convém que todos os funcionários e partes externas sejam alertados sobre sua responsabilidade de notificar qualquer evento de segurança da informação o mais rapidamente possível. Convém que eles também estejam cientes do procedimento para notificar os eventos de segurança da informação e do ponto de contato, ao qual os eventos devem ser notificados.

Situações a serem consideradas para notificar um evento de segurança da informação incluem:

a) controle de segurança ineficaz;
b) violação da disponibilidade, confidencialidade e integridade da informação;
c) erros humanos;
d) não conformidade com políticas ou diretrizes;
e) violações de procedimentos de segurança física;
f) mudanças descontroladas de sistemas;
g) mau funcionamento de software ou hardware;
h) violação de acesso.

Informações adicionais

Mau funcionamento ou outro comportamento anômalo do sistema pode ser um indicador de um ataque de segurança ou violação na segurança atual e, portanto, convém que sempre seja reportado como um evento de segurança da informação.

3.3. Notificando fragilidades de segurança da informação

Controle

Convém que os funcionários e partes externas que usam os sistemas e serviços de informação da organização sejam instruídos a notificar e registrar quaisquer fragilidades de segurança da informação, observada ou suspeita, nos sistemas ou serviços.

Diretrizes para implementação

Convém que todos os funcionários e partes externas notifiquem essas questões para o ponto de contato, o mais rápido passivei, de forma a prevenir incidentes de segurança da informação. O mecanismo de notificação deve ser fácil, acessível e estar, sempre que possível, disponível.

Informações adicionais

Convém que funcionários e fornecedores sejam avisados a não tentar provar fragilidades de segurança da informação suspeitas. Testar fraquezas pode ser interpretado como potencial mau uso do sistema e pode também causar danos ao serviço ou sistema de informação e resultar em responsabilidade legal para o indivíduo que executou o teste.

3.4. Avaliação e decisão dos eventos de segurança da informação

Controle

Convém que os eventos de segurança da informação sejam avaliados e seja decidido se eles são classificados como incidentes de segurança da informação.

Diretrizes para implementação

Convém que o ponto de contato avalie cada evento de segurança da informação, usando a escala estabelecida de classificação de incidentes e eventos de segurança da informação, para decidir se é recomendado que o evento seja classificado como um incidente de segurança da informação. A priorização e a classificação de incidentes podem ajudar a identificar o impacto e a abrangência de um incidente.

Em casos em que a organização tenha uma equipe de resposta a incidentes de segurança da informação, a avaliação e decisão podem ser encaminhadas à equipe, para confirmação ou reavaliação.

Convém que os resultados da avaliação e decisão sejam registrados em detalhes, para verificação e referência futura.

3.5. Resposta aos incidentes de segurança da informação

Controle

Convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados.

Diretrizes para implementação

Convém que incidentes de segurança da informação sejam reportados para um ponto de contato definido e outras pessoas relevantes da organização, ou ainda, partes externas
Convém que a notificação inclua os seguintes itens:

a. coleta de evidências, tão rápido quanto possível, logo após a ocorrência;
b. condução de análise forense de segurança da informação, conforme requerido;
c. escalação, conforme requerido;
d. garantia de que todas as atividades de respostas envolvidas sejam adequadamente registradas para análise futura;
e. comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevante para pessoas internas ou externas, ou organizações que precisam tomar conhecimento;
f. tratamento com as fragilidades de segurança da informação encontradas que causem ou contribuam para o incidente;
g. uma vez que o incidente foi tratado de forma bem-sucedida, encerrá-lo e registrá-lo formalmente.
h. Convém que análises pós-incidente sejam realizadas, quando necessário, para identificar a fonte do incidente.

Informações adicionais

O primeiro objetivo de resposta a incidente é "voltar ao nível de segurança normal" e então iniciar a recuperação necessária.

3.6. Aprendendo com os incidentes de segurança da informação

Controle

Convém que os conhecimentos obtidos da análise e resolução dos incidentes de segurança da informação sejam usados para reduzir a probabilidade ou o impacto de incidentes futuros.

Diretrizes para implementação

Convém que haja mecanismos implementados para permitir monitorar e quantificar os tipos, volumes e custos de incidentes de segurança da informação. Convém que a informação resultante da análise de incidentes de segurança da informação seja usada para identificar incidentes recorrentes ou de alto impacto.

Informações adicionais

A avaliação de incidentes de segurança da informação pode indicar a necessidade de melhoria ou controles adicionais para diminuir a frequência, dano e custo de futuras ocorrências.

Com o devido cuidado aos aspectos de confidencialidade, incidentes atuais de segurança da informação podem ser usados em treinamentos de conscientizações de usuários como exemplos do que pode acontecer, como responder a tais incidentes e como evitá-los.

3.7. Coleta de evidências

Controle

Convém que a organização defina e aplique procedimentos para a identificação, coleta, aquisição e preservação das informações, que podem servir como evidências.

Diretrizes para implementação

Convém que procedimentos internos sejam desenvolvidos e seguidos quando lidando com evidência, para os propósitos de ação legal ou disciplinar.

Em geral, convém que esses procedimentos para evidência forneçam processos de identificação, coleta, aquisição e preservação de evidências, de acordo com diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados. Convém que os procedimentos levem em conta:

a. cadeia de custódia;
b. segurança da evidência;
c. segurança das pessoas;
d. papéis e responsabilidades das pessoas envolvidas;
e. competência do pessoal;
f. documentação;
g. resumo do incidente.

Convém que, sempre que disponível, certificação ou outros meios relevantes de qualificação de pessoal e ferramentas sejam buscados, para reforçar o valor da evidência preservada.

Evidência forense pode ir além dos limites da organização ou da jurisdição. Em tais casos, convém que seja assegurado que a organização tem direito de coletar as informações requeridas como evidência forense. Convém que os requisitos de diferentes jurisdições também sejam considerados para maximizar as chances de aceitação em jurisdições distintas.

Informações adicionais

Identificação é o processo envolvendo a busca, reconhecimento e documentação de potencial evidência.

Coleta é o processo de levantamento de itens físicos que podem conter potencial evidência.

Aquisição é o processo de criação de uma cópia dos dados dentro de um cenário definido.

Preservação é o processo para manter e proteger a integridade e condição original da evidência.

Logo quando um evento de segurança da informação é detectado, pode não ser óbvio se o evento resultará em uma ação judicial ou não. Portanto, existe o risco de que esta evidência necessária seja destruída intencionalmente ou acidentalmente antes que a gravidade do incidente seja percebida. É aconselhável envolver um advogado ou a polícia o quanto antes em qualquer ação legal e receber aconselhamento sobre a evidência requerida.

Outras recomendações importantes no processo de Gestão de Incidentes

- Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.

• Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.

• É recomendável que a segurança da informação seja considerada em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos sistemas existentes são oportunidades para as organizações atualizarem e melhorarem os controles de segurança, levando em conta os incidentes reais e os riscos de segurança da informação, projetados e atuais.

• Se os funcionários e fornecedores não forem conscientizados das suas responsabilidades em segurança da informação, eles podem causar danos consideráveis para uma organização. Pessoal motivado pode ser mais confiável e causar menos incidentes de segurança da informação.

• É recomendável que o programa de conscientização seja planejado levando em consideração os papéis a serem desempenhados na organização pelos funcionários e, quando relevante, as expectativas da organização quanto à conscientização das partes externas. Convém que as atividades do programa de conscientização sejam planejadas ao longo do tempo, preferencialmente de forma regular, de tal modo que as atividades sejam repetidas e contemplem novos funcionários e partes externas.

• É recomendável que o programa de conscientização também seja atualizado regularmente, de modo que ele permaneça alinhado com as políticas e os procedimentos da organização, e seja construído com base nas lições aprendidas dos incidentes de segurança da informação.

• É recomendável que um processo de gestão de vulnerabilidade técnica eficaz esteja alinhado com as atividades de gestão de incidentes, para comunicar dados sobre as vulnerabilidades às equipes de resposta a incidentes e fornecer procedimentos técnicos no caso em que ocorra um incidente.

- A instalação de software não controlada em dispositivos computadorizados pode introduzir vulnerabilidades e em seguida gerar o vazamento de informações, perda de integridade ou outros incidentes de segurança da informação além da violação de direitos de propriedade intelectual. Portanto a gestão adequada dos softwares homologados para uso dentro da organização é fundamental.

- É recomendável que os requisitos de segurança da informação sejam identificados usando vários métodos, como requisitos de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade. Convém que os resultados da identificação sejam documentados e analisados criticamente por todas as partes interessadas.

- É recomendável que a monitoração e a análise crítica dos serviços fornecidos garantam que os termos e condições dos acordos de segurança de informação sejam cumpridos e que os incidentes e problemas de segurança da informação sejam gerenciados de forma apropriada. Outro aspecto importante é o fornecimento de dados sobre incidentes de segurança de informação e analisá-los criticamente, conforme requerido pelos acordos e por quaisquer procedimentos e diretrizes que os apoiem;

- É recomendável que a organização mantenha controles gerais suficientes e visibilidade de todos os aspectos de segurança para as informações sensíveis ou críticas, ou para os recursos de processamento da informação acessados, processados ou gerenciados por um fornecedor.

- É recomendável que a organização mantenha visibilidade sobre as atividades de segurança, como o gerenciamento de mudanças, a identificação de vulnerabilidades, os relatórios e respostas de incidentes de segurança da informação, através de um processo definido de notificação.

Por fim, é importante destacar que a LGPD, em seu art. 48, estabelece que o controlador deverá comunicar, em prazo razoável, à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A lei estabelece as informações mínimas que devem ser repassadas pelo controlador:

I. a descrição da natureza dos dados pessoais afetados;
II. as informações sobre os titulares envolvidos;
III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
IV. os riscos relacionados ao incidente;
V. os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

A ANPD verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, como: ampla divulgação do fato em meios de comunicação; e medidas para reverter ou mitigar os efeitos do incidente. Por fim, no juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

4. PROPOR AÇÕES CORRETIVAS/ MITIGADORAS DOS RISCOS APONTADOS

Conforme dito anteriormente, a norma ISO 27001 apresentados os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

Por sua vez, a norma ISO 27005 trata especificamente da Gestão de Riscos de Segurança da Informação e estabelece processos para, dentre outras avaliar e tratar os riscos.

Por fim, a ISO 31000 traz recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto. A versão mais recente da norma apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

Anteriormente, a norma ISO/IEC 29134:2017 que estabelece as Técnicas de segurança e as diretrizes para avaliação do impacto na privacidade foi destacada. Na oportunidade foram elencados riscos que constam na norma e foram apresentadas, a título exemplificativo, controles que podem ser aplicados para minimizar os riscos.

A definição dos riscos e as medidas a serem adotadas para mitigá-los dependerá da natureza, volume e especificidade dos dados tratados pelo controlador/operador. Adotar (ou não) processos de anonimização e pseudonimização dos dados. Compartilhar (ou não) dados pessoais com terceiros, públicos ou privados. Definir quais medidas, técnicas e administrativas serão adotadas para assegurar o cumprimento da LGPD. Essas definições estarão diretamente ligadas à finalidade do tratamento e às necessidades dos agentes de tratamento.

O fato é que esse tratamento precisa observar princípios estabelecidos no art. 6° da LGPD, como transparência e boa-fé. Outro princípio importante previsto na lei é o que consta no inciso III, do referido artigo, denominado de necessidade e que segue abaixo transcrito:

> *"limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados";*

Ele está intimamente relacionado ao princípio da adequação que estabelece que deve haver compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Combinando os dois princípios (adequação e finalidade) temos que a coleta de dados deve ser adequada à finalidade do tratamento e deve se ater ao mínimo de dados necessários ao objetivo buscado pelo agente de tratamento. Vivemos a era do conhecimento em que a informação se tornou um ativo valioso. Não por acaso, diversas das maiores empresas do mundo baseiam seus negócios em informação. Por esse motivo, os governos, visando regulamentar e criar regras em uma sociedade cada vez mais movida a dados, enxergaram e necessidade de criação de legislações voltas a assegurar a privacidade dos dados do titular. Nesse contexto, a informação não perdeu o seu valor, porém passou a ser um ativo que precisa receber cuidados especiais. Dito isso, se tivéssemos que apontar a "regra de ouro" no processo de tratamento de dados pessoais ela seria: coletar apenas os dados essenciais à finalidade pretendida. Essa frase, se aplicada no contexto das organizações, poderá poupá-las de diversos problemas futuros tangíveis e intangíveis. Os primeiros, encontram-se descritos no art. 52 da LGPD e são as seguintes:

I. advertência, com indicação de prazo para adoção de medidas corretivas;
II. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
Importante mencionar que a sanção de multa só é aplicável às pessoas jurídicas de direito privado.
III. multa diária, observado o limite total a que se refere o inciso II;
IV. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. eliminação dos dados pessoais a que se refere a infração;
VII. suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
VIII. suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
IX. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Em relação aos intangíveis está primordialmente o risco à imagem da organização, por ser de difícil mensuração, tanto em termos monetários, quanto da perda de credibilidade no mercado de atuação.

Por isso é importante repisar acerca da importância da implementação de um processo de análise e avaliação de riscos e da adoção de medidas, técnicas e administrativas adequadas à mitigação desses riscos.

5. ELABORAR E PUBLICAR POLÍTICA E DIRETRIZES DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO SITE INSTITUCIONAL

O Termo de Uso é um texto que deve ser elaborado visando esclarecer as regras e condições de uso de determinado serviço. Ao ser aceito pelo usuário, a utilização dos serviços estará vinculada às condições determinadas nele. Deve apresentar informações claras e precisas em relação aos serviços oferecidos aos usuários pela aplicação em questão e a forma de prestação deles, bem como requisitos para acessá-los e os locais e formas para o usuário apresentar eventual manifestação sobre a prestação do serviço.

Já na Política de Privacidade, o intuito é o prestador do serviço esclarecer como realiza o tratamento dos dados pessoais, como fornece privacidade, segurança, entre outros aspectos.

Desta forma, ambos documentos têm a ver com as responsabilidades dos agentes de tratamento em prover transparência sobre as atividades de tratamento de dados e como atendem os princípios dispostos na LGPD (art. 6º), compondo, portanto, deveres do controlador e direitos dos titulares.

Estes documentos devem estar constantemente atualizados de forma que reflitam, de maneira clara e precisa, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos usuários, que somente poderão ser utilizados caso se enquadrem nas hipóteses para tratamento de dados (art. 7º).

Os modelos apresentados são sugestivos, podendo ser adequados de forma que se enquadre para cada caso específico, conforme características e especificidades próprias de cada serviço.

Recomendamos também a utilização do "Questionário para elaboração de Termo de Uso para serviços públicos" elaborado pelo Ministério da Economia. Trata-se de uma ferramenta de fácil preenchimento que aborda os tópicos do presente material, gerando, a partir de um template, o Termo de Uso e a Política de Privacidade com as informações fornecidas.

Esta ferramenta está acessível por meio do link: https://limesurvey.sgd.nuvem.gov.br/index.php/759958?lang=pt-BR

Este documento poderá sofrer atualizações para se adequar a possíveis diretrizes que a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) possa promover ou outras novidades que possam surgir em relação à proteção de dados pessoais.

5.1. Termo de Uso

A seguir citamos os principais tópicos que necessitam estar presentes no Termo de Uso.

5.1.1. Aceitação dos Termos e Políticas

A aceitação dos termos e polícias visa informar ao usuário quanto a sua aplicação ao serviço em questão, além de alertar que o usuário concorda com os termos.

Em alguns casos poderá existir mais de uma política, por exemplo, ao responder uma enquete uma política específica poderá versar sobre quais são as regras relacionadas às respostas fornecidas.

As seguintes informações devem estar presentes neste tópico:
- Quais os termos e políticas aplicáveis;
- Informação de que o uso do serviço expressa acordo com os Termos apresentados.

Exemplo: Ao utilizar os serviços, o usuário confirma que leu e compreendeu os Termos e Políticas aplicáveis a ele e concorda em ficar vinculado a eles.

5.1.2. Definições (ou Glossário)

Conceitos importantes, como termos técnicos ou legais, precisam ser explicados para melhor entendimento. É fundamental que a forma de linguagem utilizada para esclarecer os significados das palavras seja simples e compreensível, evitando o uso de siglas, jargões e estrangeirismos.

Alguns termos já constam no artigo 5º da LGPD e podem ser usados no Termo de Uso:

> *"I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;*
>
> *II - dado pessoal sensível: 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;*
>
> *III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;*
>
> *IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;*

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - agentes de tratamento: o controlador e o operador;

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional."

As seguintes informações devem estar presentes neste tópico do Termo de Uso:

- Definições da Lei Geral de Proteção de dados aplicáveis ao documento;
- Definições necessárias sobre os termos utilizados no documento.

Exemplo de texto – Participa + Brasil[1]:

"Para os fins deste Termo de Uso e Política de Privacidade, consideram-se:

3.1. Agente Público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública, direta e indireta;

3.2. Códigos maliciosos: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

3.3. Cookies: são pequenos arquivos armazenados nos computadores ou dispositivos móveis que guardam informações relacionadas à página web acessada como, por exemplo, quantos acessos foram realizados àquela página, entre outras;

3.4. Internet: sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

[1] https://www.gov.br/participamaisbrasil/termo-de-uso-e-politica-de-privacidade

3.5. Sítios e aplicativos: instrumentos por meio dos quais o usuário acessa os serviços e conteúdos disponibilizados;

3.6. Terceiro: pessoa ou entidade que não participa diretamente em um contrato, em um ato jurídico ou em um negócio, ou que, para além das partes envolvidas, pode ter interesse num processo jurídico; [...]"

5.1.3. Arcabouço Legal

Alguns instrumentos legais podem embasar a utilização de sítios e sistemas por órgãos e entidades da Administração Pública. Dentre eles:

I. Lei nº 12.965, de 23 de abril de 2014: Marco Civil da Internet – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
II. Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação: Regula o acesso a informações previsto na Constituição Federal;
III. Lei nº 13.460, de 26 de junho de 2017: Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública;
IV. Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados: Dispõe sobre a proteção de dados pessoais;
V. Decreto nº 45.969, de 24 de maio de 2012: Regulamenta o acesso à informação no âmbito do Poder Executivo;
VI. Decreto nº 47.974/2020: Institui a Política de Tecnologia da Informação e Comunicação da Administração Pública e cria o Comitê de Tecnologia da Informação e Comunicação do Governo do Estado de Minas Gerais no âmbito da Administração Pública, e dá outras providências;
VII. Resolução Seplag n° 107/2018: Regulamenta a política da segurança da informação no que se refere à utilização da Tecnologia da Informação e Comunicação pelos usuários dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional;

VIII. Resolução Seplag nº 29, de 05 de julho de 2016: Estabelece diretrizes para estruturação, elaboração, manutenção e administração de sítios de informação de serviços públicos, na Internet dos Órgãos e entidades do Poder Executivo da Administração Pública Estadual Direta, autárquica e fundacional;

O principal conceito para a configuração do regime jurídico-administrativo é o princípio da legalidade. Desta forma, a administração pública só poderá ser exercida quando estiver em conformidade com a legislação. Dela não se pode afastar ou desviar, sob pena de praticar ato inválido e expor-se à responsabilidade disciplinar, civil e criminal, conforme o caso.

Sempre que o poder público realizar uma atividade de tratamento de dados pessoais, deverá informar de forma clara a previsão legal e a finalidade da política pública relacionada ao serviço prestado.

As informações a seguir devem estar presentes neste tópico:

- Leis e normativos que podem ser consultados pelo titular para esclarecimento de dúvidas relacionadas ao serviço e que envolvam: tratamento dos dados; transparência na administração pública; direitos dos titulares; competências legais do órgão ou entidade para tratamento dos dados; direito do consumidor etc.
- Arcabouço jurídico que respalda o tratamento de dados pessoais dos cidadãos; política pública, projeto, programa relacionado às competências legais relacionado ao serviço prestado

Exemplo:

"O Arcabouço legal aplicável ao serviço (citar o nome do serviço) compreende:

1. Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018;
2. Marco civil da internet - Lei nº 12.965, de 23 de abril de 2014;
3. Decreto da Governança no Compartilhamento de Dados - Decreto nº 10.046, de 9 de outubro de 2019;

4. Normas complementares do Gabinete de Segurança da Informação da Presidência (GSI/PR);
5. Decreto que institui a Estratégia de Governo Digital - Decreto nº 10.332, de 28 de abril de 2020."

Exemplo de texto – Participa + Brasil:

"A Secretaria de Governo da Presidência da República, considerando:

I. a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais, reafirma os seguintes fundamentos:

a) respeito à privacidade;
b) autodeterminação informativa;
c) liberdade de expressão, de informação, de comunicação e de opinião;
d) inviolabilidade da intimidade, da honra e da imagem;
e) desenvolvimento econômico e tecnológico e inovação;
f) livre iniciativa, livre concorrência e defesa do consumidor;
g) direitos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania pelas pessoas naturais;

II. a Lei nº 12.527, de 18 de novembro de 2011, intitulada Lei de Acesso à Informação (LAI);
III. a Lei nº 12.965, de 23 de abril de 2014, nominada como Marco Civil da Internet;
IV. o Decreto nº 10.046, de 9 de outubro de 2019, qualificado como Decreto da Governança no Compartilhamento de Dados;
V. a Portaria nº 93, de 26 de setembro de 2019, do Gabinete de Segurança Institucional da Presidência da República;
VI. o Decreto nº 10.332, de 28 de abril de 2020, que instituiu a Estratégia de Governo Digital para o período de 2020 a 2022;
VII. a Lei nº 13.444, de 11 de maio de 2017, que dispõe sobre a Identificação Civil Nacional (ICN); e
VIII. demais normativos vigentes no âmbito da Administração Pública Federal.

Compromete-se, tornando pública e acessível a seus usuários, demais partes interessadas e público em geral, a presente Declaração, que passa a vigorar."

5.1.4. Descrição do serviço

Neste tópico devemos informar aos titulares sobre a descrição do serviço a ser utilizado, incluindo suas formas de acesso, requisitos, documentos, etapas e prazos. As condições do serviço devem ser detalhadas de maneira transparente, é recomendado que contenha o detalhamento sobre compromissos e padrões de qualidade na prestação do serviço, como: prioridades de atendimento, previsão do tempo de espera e mecanismos de consulta acerca do andamento do serviço solicitado e de eventuais manifestações.

As seguintes informações devem estar presentes neste tópico:
- Quem é o responsável pela prestação do serviço;
- Descrição do escopo do serviço e sua finalidade;
- Forma de utilização do serviço e informações necessárias para o uso adequado do serviço.

Informações gerais sobre os serviços como os benefícios trazidos ao cidadão e previsão de redução de gastos também ser informado neste tópico.

Exemplo de texto – Participa + Brasil:

"4. O QUE É O PARTICIPA + BRASIL?

A plataforma Participa + Brasil é uma ferramenta, desenvolvida no âmbito da Secretaria de Governo da Presidência da República, que visa simplificar a comunicação e a aproximação entre o Governo e os cidadãos em prol da participação social e do exercício da cidadania.

Para o cidadão, esta ferramenta representa a possibilidade de participar ativamente do processo de elaboração de políticas públicas; para o gestor, representa um meio de aprimoramento, acompanhamento e escolha de políticas públicas efetivas.

A navegação e as consultas disponibilizadas nesta Plataforma estão condicionadas ao aceite expresso do presente Termo de Uso e Política de Privacidade, bem como à realização de cadastro no site, com a criação de perfil de acesso (login e senha), além da confirmação de ciência de cadastro restrito a maiores de 18 anos.

Para o cadastramento, serão solicitadas informações pessoais do usuário, que tem o dever de prestá-las de acordo com o ordenamento jurídico, resguardado o sigilo dos dados."

5.1.5. Direitos do usuário

Os cidadãos têm o direito à adequada prestação dos serviços públicos, que devem ser ofertados de acordo com diretrizes como respeito; igualdade no tratamento aos usuários, sem qualquer tipo de discriminação; acessibilidade; cumprimento de prazos e normas; e adequação entre meios e fins – sem a imposição de exigências, obrigações, restrições e sanções não previstas na legislação.

O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. O titular do dado tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

I - finalidade específica do tratamento;
II - forma e duração do tratamento, observados os segredos comercial e industrial;
III - identificação do controlador;
IV - informações de contato do controlador;
V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
VI - responsabilidades dos agentes que realizarão o tratamento; e
VII - direitos do titular

É um direito do titular ter acesso a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

Abaixo, resume-se quais informações devem estar presentes neste tópico:

- Quais os direitos do titular que utiliza o serviço;
- Descrição detalhada dos direitos.

Exemplo de texto – Netflix[2]:

"Seus dados e direitos
Você pode solicitar confirmação de que processamos seus dados pessoais, bem como solicitar acesso aos seus dados pessoais e corrigir ou atualizar dados pessoais desatualizados ou incorretos que temos sobre você. Você também pode solicitar que a Netflix exclua seus dados pessoais.

Ao acessar a seção "Conta" no nosso site, onde você pode ver e atualizar diversos dados sobre sua conta, inclusive seus dados de contato, de pagamento e diversas outras relacionadas à sua conta (como o conteúdo a que você assistiu e classificou). Para acessar a seção "Conta" você precisa estar registrado.

Você pode se opor ao uso de seus dados pessoais, solicitar que a Netflix restrinja o uso de seus dados pessoais ou solicitar a portabilidade deles; se a Netflix coletou e processou seus dados pessoais com o seu consentimento, você pode retirar esse consentimento a qualquer momento; a retirada do seu consentimento não afeta a legalidade do uso que fizemos desses dados antes da retirada do seu consentimento nem afeta o uso dos seus dados pessoais tratados com outra base legal além do consentimento; você pode solicitar que a Netflix informe se usou seus dados pessoais de forma compartilhada (consulte a seção "Divulgação de dados" acima); você tem o direito de reclamar à Autoridade Nacional de Proteção de Dados se não conseguir resolver qualquer preocupação com a Netflix.

[2] https://help.netflix.com/pt/legal/privacy

Se você for o titular da conta, para baixar uma cópia dos seus dados pessoais, acesse: www.netflix.com/account/getmyinfo (é preciso estar conectado para acessar a seção "Conta") e siga as instruções.

Para outras solicitações ou caso você tenha uma dúvida sobre nossas práticas de privacidade, escreva para o Encarregado de Proteção de Dados/Divisão de Privacidade por email no endereço privacy@netflix.com. Para saber mais sobre o acesso aos seus dados, incluindo nosso processo de verificação, consulte este artigo: help.netflix.com/node/100624. Para saber mais sobre a exclusão, remoção e retenção de dados, consulte este artigo: help.netflix.com/node/100625. Respondemos a todas as solicitações que recebemos de indivíduos que queiram exercer os seus direitos de proteção de dados em conformidade com as respectivas leis de proteção de dados. Consulte também a seção "Suas opções" desta Declaração de privacidade para ver quais são suas outras opções relativas aos seus dados pessoais.

A Netflix pode rejeitar solicitações que sejam desarrazoadas ou não exigidas por lei, como aquelas que sejam extremamente impraticáveis, capazes de exigir um esforço técnico desproporcional ou que possa nos expor a riscos operacionais, como fraude em relação ao período de utilização gratuita. A Netflix pode reter dados conforme exigência ou permissão prevista em leis e regulamentos aplicáveis, inclusive para honrar suas escolhas, para fins de cobrança ou registros e para atender às finalidades descritas nesta Declaração de privacidade. A Netflix toma medidas razoáveis para destruir ou anonimizar dados pessoais de forma segura quando deixam de ser necessários."

5.1.6. Responsabilidades do usuário e da Administração Pública

Necessário esclarecer as responsabilidades das partes envolvidas no processo, desta forma o titular e a Administração compreenderão as obrigações no provimento e uso do serviço, e em quais situações se configuram necessidades de reparação de danos.

No caso da Adminsitração Pública, como provedora do serviço, deve garantir o cumprimento das legislações pertinentes ao coreto uso dos dados pessoais do titular, preservando o sigilo e privacidade dos dados tratados e demais direitos e garantias legais dos titulares.

Além disso, a Administração Pública poderá, quanto às ordens judiciais de pedido das informações, compartilhar informações necessárias para investigações ou tomar medidas relacionadas a atividades ilegais, suspeitas de fraude ou ameaças potenciais contra pessoas, bens ou sistemas que sustentam o Serviço ou de outra forma necessária para cumprir com as obrigações legais. Caso ocorra, a Administração Pública deve notificar os titulares dos dados, salvo quando o processo estiver em segredo de justiça.

O usuário de serviços públicos deve utilizar adequadamente os serviços, procedendo com urbanidade e boa-fé; prestar as informações pertinentes ao serviço utilizado quando solicitadas; colaborar para a adequada prestação do serviço; e preservar as condições dos bens públicos por meio dos quais lhe são prestados os serviços.

Também é dever do usuário do serviço: apresentar informações verdadeiras e se responsabilizar pelas possíveis consequências de erros e omissões; obedecer às regras estabelecidas nos Termos e Políticas; manter o sigilo da senha, que deve ser pessoal e intransferível; responsabilizar-se por possíveis aplicativos de terceiros que possam fazer o uso de dados pessoais em seus dispositivos; responsabilizar-se pela segurança do dispositivo pelo qual é realizado o acesso ao serviço; reparar danos diretos e indiretos que sejam causados à Administração Pública e a terceiros pelo mal uso do serviço; dentre outros.

Por fim, é importante esclarecer o que é considerado culpa exclusiva do titular dos dados ou de Terceiros que sejam atores diretos na prestação dos serviços e determinar exemplos de isenção de responsabilidade por parte da Administração Pública.

Logo, as seguintes informações devem estar presentes neste tópico:

- Limitação da responsabilidade da administração e excludentes de responsabilidade;
- Responsabilidades do usuário ao utilizar o serviço.

Exemplo de texto – Participa + Brasil:

"6. RESPONSABILIDADES

6.1. Usuário

O Usuário se responsabiliza pela precisão e veracidade dos dados informados no cadastro e reconhece que a inconsistência destes poderá implicar a impossibilidade de utilizar serviços públicos do Governo Federal.

A visualização e o envio de contribuições nos documentos disponibilizados nesta plataforma, condicionam-se ao aceite expresso do presente Termo de Uso e Política de Privacidade, bem como à realização de cadastro no site, com a criação de perfil de acesso (login e senha), além da confirmação de ciência de cadastro restrito a maiores de 18 anos.

Para o cadastramento serão solicitadas informações pessoais do usuário, que tem o dever de prestá-las idoneamente, sob pena de responsabilização.

O login e senha só poderão ser utilizados pelo usuário cadastrado. Este deve manter o sigilo da senha, que é pessoal e intransferível, não sendo possível, em qualquer hipótese, a alegação de uso indevido, após o ato de compartilhamento.

O Usuário da Plataforma é responsável pela atualização das suas informações pessoais e consequências na omissão ou erros nas informações pessoais cadastradas.

O Usuário é responsável pela reparação de todos e quaisquer danos, diretos ou indiretos (inclusive decorrentes de violação de quaisquer direitos de outros usuários, de terceiros, inclusive direitos de propriedade intelectual, de sigilo e de personalidade), que sejam causados à Administração Pública Federal (APF), a qualquer outro Usuário, ou, ainda, a qualquer terceiro, inclusive em virtude do descumprimento do disposto nestes Termo de Uso e Política de Privacidade ou de qualquer ato praticado a partir de seu acesso à Internet, ao sítio e/ou aplicativo.

6.2 Administração Pública

O Órgão não poderá ser responsabilizado pelos seguintes fatos:

a. Equipamento infectado ou invadido por hackers;
b. Equipamento avariado no momento do consumo de serviços;
c. Proteção do computador;
d. Proteção das informações baseadas nos computadores dos usuários;
e. Abuso de uso dos computadores dos usuários;
f. Monitoração clandestina do computador dos usuários;
g. Vulnerabilidades ou instabilidades existentes nos sistemas dos usuários; e
h. Perímetro inseguro.

A Administração Pública, no papel de detentora da custódia das informações pessoais dos Usuários, deve cumprir todas as legislações inerentes ao uso correto dos dados pessoais do cidadão de forma a preservar a privacidade dos dados utilizados na plataforma.

Em nenhuma hipótese a Administração Pública Federal será responsável pela instalação no equipamento do Usuário ou de terceiros, de códigos maliciosos (vírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros que venham a ser criados), em decorrência da navegação na Internet pelo Usuário."

5.1.7. Mudanças no Termo de Uso

As possibilidades de futuras mudanças nos Termos de Uso precisam ser informadas, informando como serão comunicadas aos usuários, como por meio de e-mail ou diretamente ao acessar o serviço, ou alertando para que revisem os Termos com frequência.

As seguintes informações devem estar presentes neste tópico:

- Como as alterações no Termo de Uso serão comunicadas;
- Caso não sejam comunicadas diretamente ao titular (por e-mail, por exemplo), alertar sobre a responsabilidade dele em acessar o Termo de Uso frequentemente.

Exemplo de texto – Netflix:

"7.5. Alterações dos termos de uso e cessão. A Netflix poderá alterar estes Termos de uso periodicamente. Notificaremos você com pelo menos 30 dias de antecedência antes que as alterações se apliquem a você. A qualquer momento, a Netflix poderá ceder ou transferir o nosso contrato com você, inclusive nossos direitos e obrigações associados. Você concorda em cooperar com a Netflix nessas cessões ou transferências."

5.1.8. Informações para contato

As informações para contato são essenciais, por onde o titular poderá sanar eventuais dúvidas. O controlador deve informar o canal, como telefone, e-mail e/ou link, e se existem procedimentos necessários para o contato quando for o caso.

As seguintes informações devem estar presentes neste tópico:
- Quais são os canais para esclarecimento de dúvidas;
- Detalhes sobre o funcionamento dos canais, como horário de funcionamento, conforme o caso.

Exemplo – Netflix:

"Como contatar a Netflix
Caso tenha dúvidas gerais sobre sua conta ou queira saber como entrar contato com o atendimento ao cliente, acesse nosso Centro de ajuda online em help.netflix.com. Para questões específicas sobre esta Declaração de privacidade, incluindo a utilização de dados pessoais, cookies e outras tecnologias semelhantes, entre em contato com o nosso Encarregado de Proteção de Dados/Divisão de Privacidade por email no endereço privacy@netflix.com."

Exemplo – Participa + Brasil:

"10. COMUNICAÇÃO

Demais informações sobre este Termo de Uso e Política de Privacidade poderão ser obtidas com a equipe do Portal Participa + Brasil e encaminhadas para o endereço eletrônico: participacaosocial@presidencia.gov.br."

5.1.9. Foro

Neste tópico, devemos indicar a eleição do foro relativo às hipóteses em que reivindiquem eventuais direitos em determinado órgão jurisdicional, no caso de uma das partes veja violação de questões presentes no Termo de Uso.

Interessante também indicar a possibilidade do titular dos dados em registrar reclamação à Autoridade Nacional de Proteção de Dados conforme previsto pelo art. 18 § 1º da LGPD.

As seguintes informações devem estar presentes neste tópico:
- Quem será responsável por receber eventuais litígios;
- O direito do titular em reclamar à Autoridade Nacional de Proteção de Dados.

Exemplo de texto – Consumidor.gov.br[3]:

"Fica eleito o Foro da Justiça Federal, Seção Judiciária do Distrito Federal, para dirimir quaisquer controvérsias decorrentes deste Instrumento que porventura não tenham sido resolvidas administrativamente."

5.2. Política de Privacidade

A Política e Diretrizes de Privacidade e Proteção de Dados Pessoais tem por objetivo esclarecer aos titulares sobre os processos e procedimentos adotados pelo tratamento de dados pessoais em um determinado serviço. Deve estar facilmente disponível, em linguagem clara e precisa, demonstrando seu compromisso com a transparência no tratamento de dados pessoais.

Deve também orientar quanto ao atendimento dos direitos do titular, indicando como pode exercer seus direitos previstos na LGPD (como acesso, retificação, exclusão, transferência, etc) quando for o caso, expondo as motivações quando não couber.

[3] https://www.consumidor.gov.br/pages/principal/termos-de-uso-consumidor

O art. 6° da Lei 13.709/2018 versa sobre os princípios que devem ser observados nas atividades de tratamentos de dados[4]. A política de privacidade deve demonstrar como os mesmos estão sendo atendidos. São eles:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

---

4 Tratamento de dados - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração

A seguir, elaboramos sobre os principais tópicos que necessitam estar presentes na Política de Privacidade.

5.2.1. Controlador

O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, da Lei 13.709/2018).

O inciso III do Art. 9º da LGPD determina que o titular tem direito de acesso às informações de contato do controlador, que deverão ser disponibilizadas de forma clara, adequada e ostensiva.

Desta forma, a recomendação é de que as informações abaixo estejam presentes neste tópico:

- Identificação do controlador;
- Informações de contato com o controlador.

5.2.2. Operador

O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, da Lei 13.709/2018).

O princípio da transparência, conforme disposto no art. 6º da LGPD, visa assegurar a garantia aos titulares do fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

No inciso VI do Art. 9º, a LGPD também estabelece a necessidade de disponibilizar informações sobre as responsabilidades dos agentes que realizarão o tratamento. Portanto, é importante fornecer informações ao titular também sobre o operador.

Logo, algumas informações sobre o operador são interessantes serem informadas neste tópico, como:

- Identificação do operador.

5.2.3. Encarregado

O encarregado é aquela pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (art. 5°, VIII, da Lei 13.709/2018).

O controlador deverá indicar um encarregado pelo tratamento de dados e divulgar publicamente a identidade e as informações de contato do encarregado (art. 41 § 1° da Lei 13.709/2018). Recomendamos verificar as instruções sobre sua indicação na Atividade 5 da Fase 1 deste Projeto de Adequação.

Desta forma, as seguintes informações devem estar presentes neste tópico:

- Identificação do encarregado;
- Informações de como entrar em contato com o encarregado.

5.2.4. Quais dados tratados

O tratamento dos dados pessoais também deve respeitar os princípios anteriormente citados, em especial ao princípio da necessidade, devendo limitar o tratamento ao mínimo necessário para a realização das respectivas finalidades, de forma proporcional e não excessiva.

Deve-se dar destaque para as informações sobre o tratamento de dados pessoais de crianças e adolescentes, que requerem maiores cuidados. Além disso, não podemos esquecer que alguns dados pessoais tratados podem ser coletados automaticamente, sem ser manualmente fornecidos pelo titular, como endereço IP e informações sobre o dispositivo, estes também devem ser informados.

Em resumo, as seguintes informações devem estar presentes neste tópico:

- Dados pessoais do titular tratados pelo serviço;
- Destaque para dados de crianças e adolescentes, caso sejam tratados;
- Incluir dados pessoais do titular que são coletados automaticamente.

Exemplo – Participa + Brasil:

"Para diversos serviços, coletamos dados indispensáveis ao funcionamento das aplicações, como nome e CPF (ou Razão Social e CNPJ, no caso de Pessoas Jurídicas), endereço, e-mail, telefones para contato, entre outros. O titular pode optar por não conceder alguma dessas informações. Nessa situação, a aplicação avisará sobre as consequências da não-autorização, tanto em termos de limitações de serviço, como de negação de acesso à aplicação, informando os motivos. Ressalta-se que, nos termos do artigo 26 da Lei nº 13.709/2018, o uso compartilhado de dados pessoais pelo Poder Público atenderá às finalidades específicas de execução de políticas públicas e consoante às atribuições legais dos órgãos e das entidades públicas, respeitados os princípios de proteção de dados pessoais, elencados no art. 6º da referida lei."

Exemplo – Governo do Reino Unido[5]:

"Coletamos, armazenamos e usamos determinadas categorias de informações pessoais sobre você, como:
1. detalhes de contato pessoal, como nome, cargo, endereços, números de telefone e endereços de e-mail pessoais.
2. gênero.
3. estado civil e dependentes.
4. número de seguro Nacional.
5. detalhes da conta bancária.
6. informações sobre sua renda.
7. informações sobre o seu emprego
8. informações sobre suas atividades de negócios.
9. informações sobre suas propriedades domésticas e comerciais.
10. informações sobre passaporte e carteira de motorista.

Também coletamos, armazenamos e usamos determinadas categorias especiais de informações pessoais mais sensíveis, como:
1. dados biométricos, como dados de reconhecimento de voz.
2. Informações sobre condenações criminais, alegações e ofensas, quando relevantes em relação às nossas funções."

5 https://www.gov.uk/government/publications/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you/data-protection-act-dpa-information-hm-revenue-and-customs-hold-about-you

5.2.5. Como os dados são obtidos

Neste tópico é preciso descrever a forma de coleta dos dados pessoais. Pode ser que o serviço utilize uma base de dados que já exista, ou coletar os dados durante o uso do site ou aplicativo, seja digitado pelo usuário ou por meio de funcionalidades do dispositivo, como câmera e/ou leitor biométrico.

Importante destacar que o princípio da necessidade deve ser respeitado, ou seja, o tratamento deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Além disso, determinados recursos utilizados nos dispositivos para coleta de informações possuem maiores riscos de segurança associados. Portanto, deve-se identificar e avaliar os riscos envolvidos com cada recurso utilizado para coleta de dados. Para mais informações sobre identificação e avaliação de riscos, consultar a seção 2.5.2.6 Guia de Boas Práticas LGPD (CCGD, 2020).

5.2.6. Tratamento realizado e finalidade

Outra informação que a Administração Pública precisa esclarecer ao titular é qual o tratamento realizado com os dados pessoais e para qual finalidade.

Desta forma, a sugestão é que as seguintes informações devem estar presentes neste tópico:

- Quais as operações de tratamento são realizadas para cada dado pessoal utilizado;
- Qual a finalidade da operação realizada.

Exemplo de texto – Netflix:

"A Netflix utiliza os dados para oferecer, analisar, administrar, aprimorar e personalizar nossos serviços e esforços de marketing, para gerenciar encaminhamentos de assinantes, para processar sua inscrição, seus pedidos e pagamentos, e para nos comunicarmos com você sobre esses e outros assuntos. Por exemplo, a Netflix utiliza esses dados para:

• determinar sua localização geográfica aproximada, oferecer conteúdo localizado, oferecer recomendações personalizadas e customizadas de filmes e séries que, na nossa avaliação, poderiam ser do seu interesse, determinar o seu provedor de Internet para auxiliar na resolução de problemas de rede para você (também usamos dados agregados do ISP para fins operacionais e comerciais) e ajudar nossa equipe a responder de forma rápida e eficiente às suas dúvidas e solicitações;

• coordenar com os Parceiros a disponibilização do serviço Netflix para os assinantes e fornecer aos não assinantes dados sobre a disponibilidade do serviço Netflix de acordo com a relação específica que você mantém com o Parceiro;

• proteger nossos sistemas, prevenir fraudes e nos ajudar a manter seguras as contas Netflix;

• prevenir, detectar e investigar atividades possivelmente proibidas ou ilegais, incluindo atividades fraudulentas, e aplicar nossos termos (tais como determinar se você está qualificado para ofertas de inscrição na Netflix e a quais ofertas essa qualificação se aplica e determinar se um aparelho em particular pode ser usado com a conta segundo os nossos Termos de uso);

• analisar e entender nosso público, melhorar o serviço (inclusive a interface do usuário e o desempenho do serviço) e otimizar a seleção de conteúdo, os algoritmos de recomendação e a transmissão;

• comunicar-se com você sobre o serviço para que possamos enviar novidades sobre a Netflix, detalhes sobre novas funcionalidades, conteúdos disponíveis na Netflix, ofertas especiais, anúncios sobre promoções, pesquisas de mercado, e para prestar ajuda com pedidos de natureza operacional, como pedidos de redefinição de senha. Essas comunicações podem ser feitas por vários métodos, tais como email, notificações push, mensagens de texto, canais de mensagens online e comunicações de identificadores correspondentes (descritas abaixo). Consulte a seção "Suas Opções" desta Declaração de privacidade para saber como configurar e modificar suas preferências de comunicação."

5.2.7. Dados compartilhados

O compartilhamento de dados deve ser buscado como uma forma de facilitar o acesso aos serviços públicos, visando o aproveitamento dos dados pessoais que já estão presentes nas bases de dados do governo.

Almejando os princípios apresentados pela LGPD, o serviço deverá informar ao titular do dado sobre o uso compartilhado de dados pelo controlador e a finalidade de seu compartilhamento, conforme previsto no art. 9º da LGPD. Além disso, deve atender o disposto no artigo 26 da LGPD, que trata do uso compartilhado de dados pessoais pelo Poder Público.

Desta forma, recomenda-se que as seguintes informações devem estar presentes neste tópico:

- Quais dados são compartilhados;
- Com quem os dados são compartilhados;
- Qual a finalidade do compartilhamento.

Exemplo de texto – Netflix:

"A Netflix divulgará seus dados para fins específicos e a terceiros, conforme descrição abaixo:

• Família Netflix de empresas: poderemos compartilhar seus dados com a família Netflix de empresas (help.netflix.com/legal/corpinfo) conforme necessário, para: proporcionar acesso a nossos serviços; proporcionar serviço de atendimento ao cliente; tomar decisões sobre melhorias ao serviço, desenvolvimento de conteúdo e outros fins descritos na seção "Uso de dados" da presente Declaração de privacidade.

• Prestadores de Serviços: a Netflix poderá contratar outras empresas, agentes ou terceirizados (os "Prestadores de Serviços") para fornecer serviços em nome da Netflix ou ajudar a Netflix no fornecimento de serviços destinados a você. Por exemplo, a Netflix contrata Prestadores de Serviços para prestar serviços de marketing, publicidade, comunicação, segurança, infraestrutura e serviços de TI para personalizar e otimizar o serviço Netflix, fornecer dados de conta bancária ou de saldo, processar transações por cartão de crédito e outras formas de pagamento, prestar serviços de atendimento ao cliente, analisar e aprimorar dados (inclusive dados de interação com o serviço Netflix) e conduzir pesquisas de mercado. No decorrer da prestação desses serviços, esses Prestadores de Serviços podem ter acesso a seus dados pessoais ou de outra natureza. Não autorizamos estas empresas a usar ou divulgar seus dados pessoais, a não ser com a finalidade de fornecer os serviços contratados pela Netflix (que incluem a manutenção e o aprimoramento de seus serviços).

• Parceiros: como descrito acima, você pode ter um relacionamento com um ou mais de nossos Parceiros. Nesse caso, poderemos compartilhar determinados dados com esses Parceiros para coordenar com eles a prestação do serviço Netflix aos assinantes e fornecer dados sobre a disponibilidade do serviço Netflix. Por exemplo, dependendo de quais serviços de Parceiros você usa, poderemos compartilhar dados:

- para facilitar as promoções pré-pagas do Parceiro ou o recebimento do pagamento do serviço Netflix pelo Parceiro e o repasse desse pagamento para a Netflix;

- com Parceiros que operam plataformas de assistente de voz que permitem interagir com o nosso serviço por meio de comandos de voz;

- para que seja possível sugerir a você, na interface de usuário do Parceiro, o conteúdo e os recursos disponíveis no serviço Netflix. Para os assinantes, essas sugestões fazem parte do serviço Netflix e podem incluir recomendações personalizadas de conteúdo a ser assistido.

• Ofertas promocionais: a Netflix poderá oferecer programas ou promoções conjuntas que, para efeitos de participação, exijam que dados pessoais sejam compartilhados com terceiros. Para realizar estes tipos de promoção, a Netflix poderá compartilhar seu nome e outros dados pessoais referentes ao benefício que estamos oferecendo. Por favor, observe que estes terceiros são responsáveis por suas próprias políticas de privacidade.
• Proteção da Netflix e outros: a Netflix e seus Prestadores de Serviços poderão divulgar ou, de outra forma, utilizar seus dados pessoais quando a Netflix ou tais empresas tiverem motivos razoáveis para acreditar que tal divulgação é necessária para (a) atender a alguma lei ou norma aplicável, processo legal ou solicitação governamental, (b) fazer cumprir os termos de uso aplicáveis, incluindo a investigação de potenciais infrações destes, (c) detectar, prevenir ou endereçar atividades ilegais ou suspeitas (inclusive fraude de pagamentos), problemas técnicos ou de segurança ou (d) proteger-se contra infrações aos direitos, propriedade ou segurança da Netflix, de seus usuários ou do público, conforme requerido ou permitido por lei."

5.2.8. Segurança

O art. 46 da LGPD dispões que "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito." Faz-se necessário informar quais as medidas de segurança que foram implementadas no serviço que tratam dados pessoais.

Ademais, deve informar que será feita a comunicação em caso de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

Um canal de comunicação com o titular também deve estar disponível para relatar possíveis violações, falhas e vulnerabilidades do serviço para o tratamento de possíveis incidentes.

Desta forma, as seguintes informações deverão estar presentes neste tópico:

- Medidas de segurança implementadas;
- Informar o titular que incidentes de segurança que possam acarretar risco ou dano relevante aos titulares serão comunicados.

Exemplo de texto – Globo.com[6]:

"Adotamos práticas alinhadas aos padrões técnicos e regulatórios de mercado para segurança e privacidade de Dados, com ações abrangentes em tecnologia e nos processos organizacionais.
Nossas medidas para preservar seus Dados contra acesso, uso, alteração, divulgação ou destruição não autorizados incluem a proteção física e lógica dos ativos, comunicações criptografadas, gestão sobre os acessos, adesão ao desenvolvimento seguro de software e políticas internas de conformidade que inserem a segurança no ciclo de vida dos nossos Serviços.
Todos esses controles são continuamente revisados para acompanhar e reagir ao contexto de ameaças na Internet. Ainda assim, não é possível garantir que os nossos Serviços sejam completamente invioláveis. Mas fique tranquilo: contamos com equipes preparadas para detectar e responder prontamente, no caso da ocorrência de algum evento ou incidente que comprometa a segurança dos seus Dados ou de nossos Serviços."

Exemplo de texto – Participa + Brasil:

"7.9 Princípio da Segurança: a Presidência da República mantém uma das maiores e mais preparadas equipes de segurança da informação e de segurança física em atividade e atualização constantes, como atua na contínua integração de normas e políticas, revisão de procedimentos e harmonização do nível de gestão em SI e do nível de Gestão de Privacidade com o nível de Governança Corporativa;"

6 https://privacidade.globo.com/privacy-policy/

5.2.9. Cookies

Cookies são pequenos arquivos criados ao visitar um sítio da internet, armazenados no computador do usuário pelo navegador. Estes arquivos podem conter informações para identificação do visitante, seja para personalizar a página conforme o perfil ou para facilitar o transporte de dados entre os sítios do controlador.

Como alguns serviços podem utilizar cookies para armazenar dados do usuário, como histórico de navegação, logins e senhas, estes também são considerados tratamentos de dados pessoais e, caso seja utilizado, o usuário deve ser informado sobre quais dados são coletados, armazenados e suas funcionalidades. Além disso, as medidas de segurança implementadas em seu uso também devem ser informadas (como o uso de criptografia).

Caso faça uso de cookies de terceiros, como de rede sociais ou Google Analytics, também deve informar sobre os dados coletados, o tratamento e a finalidade do uso.

As seguintes informações devem estar presentes neste tópico:

- Cookies que são utilizados (cookies próprios e/ou de terceiros);
- Dados são coletados pelos cookies;
- Finalidade do uso de cookies;
- Como o usuário pode obter mais informações sobre os cookies de terceiros utilizados no serviço, quando for o caso.

Exemplo de texto – Globo.com:

*"**O que são cookies e qual sua utilidade***
Cookies são pequenos arquivos de texto enviados e armazenados no seu computador. Estes pequenos arquivos servem para reconhecer, acompanhar e armazenar a sua navegação como usuário na Internet.

Qual a utilidade dos cookies

O uso de cookies para acompanhar e armazenar informações possibilitará à Globo oferecer um serviço mais personalizado, de acordo com as características e interesses de seus usuários, possibilitando, inclusive, a oferta de conteúdo e publicidade específicos para cada pessoa, beneficiando a experiência do usuário na Internet.

Em geral, os cookies são utilizados para:

· Proporcionar serviços diferenciados, lembrando quem você é e quais são os seus hábitos de navegação, além de acessar as informações do seu cadastro na Globo;

· Calcular a dimensão da audiência da Globo;

· Acompanhar o andamento de promoções. Quando uma promoção organizada pela Globo usa cookies, as informações gravadas no cookie indicam a pontuação do usuário;

· Medir certos padrões de navegação, mapeando quais áreas dos portais dos Serviços você visitou e seus hábitos de visita como um todo. Usamos essa informação para verificar a rotina de navegação dos nossos usuários, e assim oferecer conteúdo e/ou serviços cada vez mais personalizados; e

· Facilitar e agilizar o preenchimento de formulários. As informações contidas nos cookies de cada usuário podem ser utilizadas para preencher previamente os formulários de coleta de dados existentes na Internet.

Categorias de cookies

Estritamente necessária

Necessários para o funcionamento do site. Eles permitem que você navegue em nossos sites e use os serviços e recursos (por exemplo, cookies de segurança para autenticar usuários, evitar a utilização fraudulenta de credenciais de login e proteger os dados do usuário de terceiros não autorizados).

Desempenho

Esses cookies normalmente coletam informações de forma anônima e permitem determinar informações, como o número de visitantes de uma página, como os visitantes chegaram ao site e as páginas acessadas.

Funcionalidade

Os cookies desta categoria permitem que a Globo se lembre de informações sobre o comportamento e preferências do usuário, como, por exemplo, uma cidade escolhida.
A perda das informações armazenadas em um cookie de preferência pode tornar a experiência no website menos funcional, mas não o impede de funcionar.

Publicidade e direcionamento

A Globo utiliza alguns cookies com o fim publicitário. Isto se faz para entregar anúncios e fazer campanhas publicitárias de acordo com um determinado público. Através desses é possível entregar anúncios de acordo com o seu perfil de consumo no site.

Utilização de cookies de terceiros

Prestadores de serviços de tecnologia poderão utilizar seus próprios cookies nos Serviços, com a nossa autorização, para prestação de serviços à Globo. Tais cookies coletarão os seus Dados nas nossas propriedades para as finalidades previstas nesta política.

Como alterar ou bloquear cookies

A maioria dos navegadores é configurada para aceitar automaticamente os cookies. Você pode, contudo, alterar as configurações para bloquear cookies ou alertá-lo quando um cookie estiver sendo enviado ao seu dispositivo. Existem várias formas de gerenciar cookies, sendo possível criar um bloqueio geral para cookies, bloquear cookies de um site específico e até mesmo bloquear cookies de terceiros em relação a um site. Bloquear todos os cookies vai afetar o funcionamento da sua experiência, pois não será possível identificar suas preferências e recomendar conteúdo e publicidade relevantes.

Consulte as instruções do seu navegador para saber mais sobre como ajustar ou alterar suas configurações, lembrando que a configuração desejada deve ser replicada em todos os dispositivos utilizados para acessar os Serviços (como computadores, smartphones, tablets). Se desejar, consulte aqui os links para alterar a configuração de cookies nos principais navegadores."

5.2.10. Tratamento posterior para outras finalidades

O § 7º do art. 7º da LGPD dispões que "O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei." Assim, alguns dados pessoais podem ser utilizadas para outras finalidades além daquelas relacionadas ao serviço. Por exemplo, informações sobre o dispositivo, da conexão ou características de segurança podem ser utilizados para a constante melhoria dos serviços e aprimoramento da experiência do usuário. Órgãos de pesquisa também podem utilizar para fins de pesquisa, desde que os dados sejam anonimizados. Desta forma, quaisquer tratamentos posteriores dos dados para outras finalidades devem ser informados aos titulares.

As seguintes informações devem estar presentes neste tópico:

- Quais dados poderão ser utilizados para tratamentos posteriores;
- As finalidades do tratamento posterior.

Exemplo de texto – Login Único[7]:

"Quanto à plataforma, o Órgão poderá efetuar a coleta de informações, como modelo do hardware, sistema operacional (entre elas configuração, navegadores) e identificadores do dispositivo (localização, dentre outros). Tais informações visam realizar a melhoria contínua dos processos e serviços prestados.
O Órgão poderá, a qualquer tempo, fornecer dados ou informações relativas aos usuários da Plataforma de Autenticação a outros serviços públicos digitais cuja finalidade seja a efetiva prestação de serviço público pelo compartilhamento de dados ou informações ou atender demanda judicial ou policial ou por requisição do Ministério Público, conforme a LGPD.
A transparência será proporcionada nos termos da Lei de Acesso à Informação – Lei nº 12.527, de 18 de novembro de 2011 e do Decreto nº 7.724, de 16 de maio de 2012."

5.2.11. Transferência internacional de dados

A LGPD trata em seu capítulo V de condições específicas sobre o tratamento internacional de dados. Por esta razão é preciso deixar claro para o titular dos dados quando ela ocorre, quais os dados serão transferidos internacionalmente, para qual finalidade, quais são os países envolvidos e qual o grau de proteção e privacidade presentes.

Assim, as seguintes informações devem estar presentes neste tópico:

- Quais são os dados que ocorre a transferência internacional;
- Finalidade da transferência;
- Quais países envolvidos e o grau de proteção de dados pessoais.

[7] https://cadastro.acesso.gov.br/nova-conta/cpf

Exemplo de texto – Deezer[8]:

"Observe que alguns desses destinatários se encontram localizados em países fora da União Europeia/Espaço Econômico Europeu e não garantem um nível de proteção de dados pessoais considerado equivalente ao nível de proteção de dados pessoais garantido pelo Regulamento 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativamente à proteção das pessoas físicas no que se refere ao tratamento de dados pessoais (RGPD).

A maioria desses destinatários fora da União Europeia/Espaço Econômico Europeu está localizada nos Estados Unidos e certificou sua conformidade com os EUA. O Escudo de Proteção da Privacidade, criado pelo Departamento de Comércio dos EUA e pela Comissão Europeia, para fornecer às empresas de ambos os lados do Atlântico um mecanismo para atender aos requisitos de proteção de dados ao transferir dados pessoais da União Europeia e da Suíça para os Estados Unidos, em apoio ao comércio transatlântico.

Para destinatários que não estariam localizados na União Europeia/Espaço Econômico Europeu, ou não estariam localizados em um país com nível adequado de proteção de dados pessoais (Artigo 45 do RGPD), ou que não cumprem com o Escudo de Proteção da Privacidade UE-EUA, tomaremos todas as medidas necessárias para verificar se fornecem salvaguardas apropriadas, como a implementação de cláusulas padrão de proteção de dados adotadas pela Comissão Europeia (Artigo 46.2 do RGDP).

Para obter mais informações sobre transferências de dados entre fronteiras, contate nosso Responsável de Proteção de Dados."

8 https://www.deezer.com/legal/personal-datas

6. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E REQUISITOS EM CONTRATAÇÕES

6.1. Política de Segurança da Informação Estadual

A informação está presente em todos os processos de trabalho desenvolvidos pelos diversos profissionais da Administração Pública Estadual, independente do cargo ou função que ocupam.

Por meio da escrita, da fala, da comunicação eletrônica, por telefone, memorandos, ofícios, formulários, projetos, contratos, sistemas informacionais, diálogos, nas atividades mais complexas e nas mais simples.

Pensar em Segurança da Informação na Administração Pública Estadual é observar as normas e dicas que orientam as condutas dos servidores. Essas normas referem-se à secretaria como um todo e a cada unidade administrativa em particular.

A SEPLAG estabeleceu uma política da segurança da informação no que se refere à utilização da Tecnologia da Informação e Comunicação pelos usuários dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional. Esta política, dentre outros documentos orientativos, estão disponíveis para consulta no endereço: http://planejamento.mg.gov.br/pagina/gestao-governamental/gestao-de-ti/seguranca-da-informacao

É importante ressaltar que a política da Seplag pode ser utilizada como modelo podendo realizar possíveis ajustes de acordo com a necessidade de cada órgão.

A relação entre segurança da informação e a LGPD diz respeito à privacidade e à proteção de dados pessoais. Dispondo que em seu art. 47 que "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

6.2. Requisitos e Obrigações quanto a Segurança da Informação e Privacidade em Contratações de Soluções de Tecnologia da Informação (TIC)

O objetivo deste tópico é fornecer orientações básicas às instituições públicas para a especificação de requisitos mínimos necessários de Segurança da Informação e Privacidade em contratações de Soluções de Tecnologia da Informação (TIC).

Destaca-se que aspectos inerentes à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709 de 14 de agosto de 2018, foram abordados, em especial os que abrangem a implantação de mecanismos de gerenciamento de riscos e análise de impacto na privacidade dos dados pessoais, bem como diversos mecanismo de controle de privacidade.
Cabe ressaltar que fica a cargo da equipe de planejamento da contratação identificar os requisitos aplicáveis às especificidades do objeto a ser contratado. Por este motivo, os requisitos, presentes neste guia, não possuem caráter obrigatório tampouco exaustivos.

6.2.1. Requisitos Gerais de Estruturação de Segurança e Privacidade

6.2.1.1. Política de Segurança da Informação (POSIN)

A empresa contratada deverá possuir uma Política de Segurança da Informação (POSIN), ou equivalente, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas, com processo de revisão periódico formalizado e institucionalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança da informação para assegurar não apenas a disponibilidade, a integridade, a confidencialidade e a autenticidade, mas também a consistência, a privacidade e a confiabilidade dos dados e informações tratados pela Solução de TIC ;

6.2.1.2. Análise de Impacto na Privacidade de Dados Pessoais

Realizar, em conjunto com a contratante, análise de impacto na privacidade dos dados pessoais relacionada à Solução de TIC, considerando o descrito pelo relatório de impacto à proteção de dados pessoais, conforme previsto na Lei nº 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço;

6.2.1.3. Análise e Avaliação de Riscos

Realizar e apresentar à contratante periodicamente uma análise/avaliação de riscos da arquitetura de Solução de TIC, indicando os eventos de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia indicada pela contratante;

6.2.1.4. Arquitetura, Controles de Segurança e Matriz de Responsabilidades

Apresentar, em tempo determinado pela contratante:
a) Documentação que descreve a arquitetura física e lógica da Solução de TIC;
b) Uma descrição dos controles de segurança da informação e privacidade implementados em cada componente descrito na arquitetura física e lógica; e
c) Matriz de responsabilidades descrevendo a atribuição das responsabilidades pela segurança da informação na organização, pela privacidade (encarregado), identificação dos gestores de serviços com dados pessoais, operador(es) de tratamento de dados, relacionada ao objeto da contratação e com relação aos itens aqui descritos.

6.2.1.5. Continuidade Operacional e Contingência

Possuir e implementar um Plano de Continuidade Operacional e um Plano de Contingência relacionados ao objeto contratado, que garantam o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

6.2.1.6. Gestão de Incidentes

Possuir um processo de Gestão de Incidentes que registre os incidentes de segurança da informação e privacidade ocorridos e que contemple: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares de dados pessoais envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário; além de implementar e manter controles e procedimentos específicos para detecção, tratamento e resposta a incidentes de segurança da informação e de privacidade, de forma a reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;

6.2.1.7. Coleta e preservação de evidências

Implementar os controles necessários para coleta e preservação de evidências de incidentes de segurança da informação e privacidade;

6.2.1.8. Gestão de Mudanças

Possuir e implementar processo de gestão de mudanças adequado para que mudanças na organização, nos processos de negócio e nos recursos de processamento da informação sejam controlados e não afetem a segurança da informação e privacidade, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante. No caso de contratação de sistemas de informação, se aplicável, considerar ainda na gestão de mudanças o processo referente a migração dos dados do sistema legado para o novo sistema;

6.2.1.9. Gestão de Capacidade

Dispor possuir e implementar processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos relacionados ao objeto do contrato, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade relacionado ao objeto contratado, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

6.2.1.10. Desenvolvimento Seguro

Possuir e manter trilhas de qualidade e teste de software, e realizar desenvolvimento seguro;

1.1.1.1. Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) devem passar por um processo de anonimização;

1.1.1.2. A utilização dos dados pessoais em ambiente de TDH (teste, desenvolvimento e homologação), não anonimizados, deve ser autorizada pelo proprietário do ativo de informação;

1.1.1.3. A Contratada deve utilizar técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação no processo;

1.1.1.4. A aplicação desenvolvida pela Contratada deve ter funcionalidade para, ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais sejam anonimizados ou pseudoanonimizados;

1.1.1.5. A Contratada deve possuir e implementar política de privacidade que atenda aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), a ser homologada pelo órgão contratante, assegurando o adequado tratamento dos dados pessoais e principalmente sua classificação em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde e informações pessoais financeiras;

1.1.1.6. O Contratante e a Contratada realizarão a análise de impacto na proteção dos dados pessoais relacionada à Solução de TIC, devendo considerar as informações levantadas pelo relatório de impacto da Contratada.

6.2.1.11. Segurança das Redes Corporativas

Implementar e manter controles e procedimentos específicos para assegurar o nível adequado de segurança da informação às redes corporativas da Contratante e da Contratada, de forma a reduzir o nível de risco ao qual a Solução de TIC e a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante;

1.1.2. Implementar e manter controles e procedimentos específicos de Segurança Web, nos servidores da aplicação, ou na própria aplicação, para garantir o nível adequado de segurança da informação e privacidade.

6.2.1.12. Política de Backup

Possuir e implementar política de backup das informações e dos registros de log da solução contratada, em conformidade com os dispositivos legais aplicáveis, a ser homologada pela contratante, que assegure a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica, os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha ou por solicitação da contratante, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

6.2.2. Requisitos de Segurança sa Informação e Privacidade

6.2.2.1.Controles Criptográficos

Implementar e manter controles criptográficos para armazenamento, tráfego e tratamento da informação, de acordo com o nível de criticidade e grau de sigilo da informação definido pela contratante, observando a periodicidade e tempo de guarda legalmente estabelecidos ou definidos pela contratante.

6.2.2.2. Controle de Acesso

Implementar controles de acesso baseados em uma política de controle de acesso para o objeto contratado, elaborada pela contratante em conjunto com a contratada, tendo em vista o princípio do menor privilégio, a segurança da informação e a privacidade, de forma a reduzir o nível de risco ao qual o objeto e a contratante estão expostos, considerando

os critérios de aceitabilidade de riscos definidos pela contratante. A política deve estabelecer, dentre outros critérios, que se deve conceder autorizações de acesso apenas quando realmente sejam necessárias para o desempenho de uma atividade específica, definindo também protocolos para cadastramento, mecanismo de controle de acesso (como, por exemplo, validação de formulário), habilitação, inabilitação, atualização de direitos de acesso e exclusão de usuário, além de revisões periódicas da política. A política também deve definir situações e protocolos para acesso à informações sensíveis, necessidades de não repúdio, situações que requerem autenticação via duplo fator e acesso via certificado digital, nos casos em que a contratante julgar necessário.

6.2.2.3. Registro de Eventos e Incidentes de Segurança

Implementar os controles necessários para o registro de eventos e incidentes de segurança da informação e privacidade.

6.2.2.4. Registro de Eventos e Rastreabilidade

Implementar e manter controles específicos para registro de eventos e rastreabilidade de forma a manter trilha de auditoria de segurança da informação e privacidade, de forma a assegurar a rastreabilidade das ações de usuário por meio de logs de transações e de acesso aos sistemas, conforme especificação de requisitos, e gerá-los e disponibilizá-los à contratante para fins de auditorias e inspeções.

6.2.2.5. Salvaguarda de Logs

Implementar medidas de salvaguarda para os logs descritos no item anterior, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto do contrato, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

6.2.2.6. Compartilhamento, uso e proteção da Informação
Contemplar procedimentos e controles adequados para compartilhamento, uso e proteção da informação e os casos de compartilhamento de informações com terceiro devem ser avaliados pela contratante, por intermédio da autoridade competente, a qual caberá autorizar a divulgação do mínimo de informações necessárias para cada compartilhamento, caso julgue apropriado, preservados os casos de sigilo previstos na legislação aplicável e de proteção de dados pessoais disposto pela Lei nº 13.709/2018.

6.2.2.7. Análise de Vulnerabilidades
Executar periodicamente análise de vulnerabilidades na Solução de TIC, para detecção de vulnerabilidades técnicas e execução de medidas para seu saneamento ou contenção.

6.2.2.8. Internet das Coisas (IoT)
Implementar mecanismos de segurança da informação e privacidade relativos à Internet das Coisas (IoT).

6.2.3. Ações de Responsabilidade da Contratada

6.2.3.1. Recursos em Versões Comprovadamente Seguras e Atualizadas
Utilizar recursos de segurança da informação e de tecnologia da informação de qualidade, eficiência e eficácia reconhecidas e em versões comprovadamente seguras e atualizadas, de forma reduzir o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

6.2.3.2. Reportar Incidentes

Reportar de imediato à contratante incidentes que envolvam vazamento de dados, indisponibilidade ou comprometimento da informação relacionados à Solução de TIC.

6.2.3.3. Termo de Compromisso e Ciência

Implementar e manter controles e procedimentos específicos para assegurar completo e absoluto sigilo quanto a todos os dados e informações de que o preposto ou os demais empregados da contratada venham a tomar conhecimento em razão da execução do contrato, de forma a assegurar que seus empregados e outros profissionais sob sua direção e/ou controle respeitem o uso dos dados somente para as finalidades previstas em contrato e as restrições de uso dos ativos utilizado para desenvolvimento e/ou operação da Solução de TIC, cumprindo e fazendo cumprir o disposto nos Termo de Compromisso e Termo(s) de Ciência firmados respectivamente, pelo representante legal e pelo(s) empregado(s) da contratada.

6.2.3.4. Descarte Seguro

Definir e executar procedimento de descarte seguro dos dados pessoais ou sigilosos da contratante ao encerrar a execução do contrato.

6.2.3.5. Revogação de Privilégios

Comunicar à contratante, de imediato, a ocorrência de transferência, remanejamento ou demissão de funcionário, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da contratante, porventura colocados à disposição para realização dos serviços contratados.

6.2.3.6. Utilização de Serviços de Terceiros

Informar e obter a anuência do órgão contratante sobre a utilização de serviços de terceiros (como Content Delivery Network, Youtube, Flicker etc.) para sustentar ou viabilizar o funcionamento da Solução de TIC.

6.2.3.7. Segurança Física e do Ambiente

Implementar e manter, em conjunto com a contratante, controles e procedimentos específicos para assegurar a segurança física e do ambiente de acesso às bases, informações, sistemas e demais ativos que compõem a Solução de TIC, de forma a prevenir qualquer tipo de ocorrência de evento de efeitos danosos ou prejudiciais ao funcionamento dos recursos de processamento das informações relacionadas à Solução de TIC, reduzindo assim o nível de risco ao qual o objeto do contrato e/ou a contratante estão expostos, considerando os critérios de aceitabilidade de riscos definidos pela contratante.

6.2.3.8. Ambientes Tecnológicos

Assegurar que os ambientes tecnológicos de desenvolvimento, teste, homologação e produção estejam segregados e possuam controles de segurança da informação adequados a cada ambiente, de forma a reduzir o nível de riscos de acessos ou modificações não autorizadas.

6.2.3.9. Auditabilidade

Apresentar à contratante, sempre que solicitado, toda e qualquer informação e documentação que comprovem a implementação dos requisitos de segurança da informação e privacidade especificados na contratação, de forma a assegurar a auditabilidade do objeto contratado, bem como demais dispositivos legais aplicáveis.

6.2.3.10. Auditoria de segurança da informação e privacidade

Disponibilizar todos os recursos necessários para que a contratante, ou outra entidade por ela indicada, realize atividade continuada de auditoria de segurança da informação e privacidade relacionadas ao objeto do contrato.

6.2.3.11. Tratamento de incidentes de segurança da informação e privacidade

Realizar em conjunto com a contratante, ou com outros órgãos por ela indicados, ações de tratamento de incidentes de segurança da informação e privacidade relacionados ao objeto do contrato, bem como apoiar essas ações com o monitoramento e o envio de informações tempestivos.

6.2.4. Gestão do Contrato

6.2.4.1. Escala, natureza e finalidade do processamento
O Modelo de Gestão do Contrato, para contratos firmados com os operadores de dados pessoais, deve incluir cláusulas que contemplem, não se limitando a: uma declaração adequada sobre a escala, natureza e finalidade do processamento contratado; relatar casos de violação de dados, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais; medidas aplicáveis na rescisão do contrato, especialmente no que diz respeito à exclusão segura de dados pessoais; impedimento de tratamento de dados pessoais por subcontratados, exceto por aprovação do controlador; conforme previsto pela Lei Geral de Proteção de Dados, Lei nº 13.709/2018.

6.2.4.2. Norma de proteção de dados pessoais
Dispositivo que garanta uma política ou norma de proteção de dados pessoais que aborde a finalidade da contratada perante o processamento de dados; a transparência com relação à coleta e processamento; a estrutura estabelecida para a proteção; regras para tomar decisões relacionadas a dados pessoais; critérios de aceitação de risco e compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade.

6.2.4.3. Monitorar e auditar dados pessoais
Dispositivo para controle de proteção de dados pessoais que devem ser monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis.

6.2.4.4. Treinamento e concientização
Dispositivo para implementação e manutenção de estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos entendam suas responsabilidades e os procedimentos de proteção de dados pessoais.

6.2.4.5. Requisitos de conformidade
Dispositivo para o monitoramento contínuo das ações de proteção de dados pessoais, a fim de determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, comparando o desempenho em todo processo e também da organização, capaz de identificar vulnerabilidades e lacunas na política e na implementação e capaz de identificar modelos de sucesso.

6.2.4.6. Atendimento de finalidade pública
Dispositivo para que o tratamento de dados pessoais seja realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (embasamento legal).

6.2.4.7. Dados limitados ao mínimo para tratamento
Dispositivo para que os dados coletados e seu processamento sejam limitados ao mínimo necessário para atendimento da finalidade do tratamento.

6.2.4.8. Notificar violação
Dispositivo que defina a obrigação do operador de dados pessoais notificar o Controlador em caso de ocorrência de violação de dados pessoais.

6.2.4.9. Precisão dos dados
Dispositivo que define que a contratada implemente medidas que garantam e maximizem a precisão dos dados pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais.

6.2.4.10. Controle de Integridade
Dispositivo que defina que os dados pessoais armazenados/retidos possuam controles de integridade permitindo identificar se os dados foram alterados sem permissão

6.2.4.11. Identificar operação
Dispositivo que defina que que as operações de processamento realizadas com dados pessoais sejam registradas de modo a identificar a operação realizada, quem realizou, data e hora.

6.2.4.12. Canal de comunicação
Dispositivo que defina um canal de comunicação ativo, seguro e autenticado para o recebimento de reclamações e manter um ponto de contato para receber e responder a reclamações, preocupações ou perguntas dos titulares sobre o tratamento de dados pessoais realizados pela Contratada.

6.2.4.13. Sanções administrativas
Dispositivo que estipule sanções administrativas pelo descumprimento de cada um dos requisitos de segurança da informação e de privacidade especificados.
No Anexo A deste guia são relacionadas as possíveis sanções que devem ser aplicadas em caso de descumprimento de cláusulas contratuais.

7. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

"XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;"

A LGPD define em seu art. 38 sobre a determinação do controlador elaborar o relatório de impacto à proteção de dados (RIPD). Hoje este assunto ainda está pendente de maiores definições por parte da ANPD, entretanto é importante já nos prepararmos para esta determinação que está por vir, conforme disposto na LGPD:

> *"Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.*
> ***Parágrafo único.*** *Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados."*

Além do art.38 que define que a ANPD poderá determinar a qualquer momento a elaboração do RIPD, também está previsto nos seguintes casos:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados).

Além destes casos específicos previstos pela LGPD relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
- rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);
- tratamento de 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" (LGPD, art. 5º, II);
- processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);

- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
- tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4°, § 3°);
- tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3°);
- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
- reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, deve(m) ser explicitado(s) qual(is) dos itens expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

O RIPD deve ser revisto e atualizado anualmente, amparado pelas necessidades listadas acima, ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição. De uma forma geral, essa mudança pode ser motivada por alteração:

- significativa na finalidade do tratamento de dados pessoais;
- que impacte no processo de como esses dados são tratados;
- expressiva na quantidade de dados pessoais coletados; e
- no contexto do tratamento de dados resultantes de identificação de falha de segurança, uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

A seguir, apresentaremos um modelo de relatório de impacto comentado, de acordo com o template elaborado pelo Ministério da Economia. Este modelo pode ser atualizado futuramente.

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Histórico de Revisões

Data	Versão	Descrição	Autor
XX/XX/20XX	1.0	Conclusão da primeira versão do relatório	XXXX
XX/XX/20XX	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	XXXX

ATENÇÃO!

Os trechos marcados em azul neste template são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário.

Template Versão 1.0 – Atualizado em 17/09/2021

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO	
Controlador	
Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (LGPD, art. 5º, VI).	
Operador	
Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (LGPD, art. 5º, VII).	
Encarregado	
Nome da pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD (LGPD, art. 5º, VIII).	
E-mail Encarregado	Telefone Encarregado
xxxx.xxxx.gov.br	(99)9999-9999

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado são:
• para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
• quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
• a qualquer momento sob determinação da ANPD (art. 38).>

Quando for necessária a elaboração do RIPD, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

A elaboração de um único RIPD para todas as operações de tratamento de dados pessoais ou de um RIPD para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um RIPD único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único RIPD não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

Além dos casos específicos previstos pela LGPD no início desta seção 2 relativas à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
• rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (LGPD, art. 12 § 2º);
• tratamento de 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" (LGPD, art. 5º, II);
• processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
• tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
• tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
• tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
• tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o RIPD ser elaborado ou atualizado pela instituição.

3 – DESCRIÇÃO DO TRATAMENTO

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da natureza, escopo, contexto e finalidade do tratamento.

A LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

3.1 – NATUREZA DO TRATAMENTO

A natureza representa como a instituição pretende tratar ou trata o dado pessoal.

Importante descrever, por exemplo:

• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

• fonte de dados (ex: titular de dados, planilha eletrônica, arquivo xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;

• com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;

• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
• medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

3.2 – ESCOPO DO TRATAMENTO

O escopo representa a abrangência do tratamento de dados. Nesse sentido, considerar destacar:
• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
• o volume dos dados pessoais a serem coletados e tratados;
• a extensão e frequência em que os dados são tratados;
• o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
• o número de titulares de dados afetados pelo tratamento; e
• a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

3.3 – CONTEXTO DO TRATAMENTO

Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:
• natureza do relacionamento da organização com os indivíduos;
• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de dados;
• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
• destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

3.4 – FINALIDADE DO TRATAMENTO

A finalidade é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.>

Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo arts. 7 ° e 11 da LGPD), no que for aplicável:

• cumprimento de obrigação legal ou regulatória pelo controlador;
• execução de políticas públicas;
• alguma espécie de estudo realizado por órgão de pesquisa;
• execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
• exercício regular de direitos em processo judicial, administrativo ou arbitral;
• proteção da vida ou da incolumidade física do titular ou de terceiro;
• tutela da saúde;
• atender aos interesses legítimos do controlador ou de terceiro;
• proteção do crédito; e
• garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:
• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a finalidade ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os
dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento
de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

4 – PARTES INTERESSADAS CONSULTADAS

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nessa seção, é importante identificar:
• quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e
• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

< Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.>

5 – NECESSIDADE E PROPORCIONALIDADE

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6°, III).

Nesse sentido, destacar:
• A fundamentação legal para o tratamento dos dados pessoais.
• Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:
- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.
• Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
• Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5°, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5°, VI).
• Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
• Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
• Quais são as salvaguardas para as transferências internacionais de dados.

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever "medidas, salvaguardas e mecanismos de mitigação de risco".

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Tabela 1: Parâmetros Escalares

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

Probabilidade	15	75	150	225
	10	50	100	150
	5	25	50	75
Impacto		5	10	15

Figura 1: Matriz Probabilidade X Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:
- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.>

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.

Id	Risco referente ao tratamento de dados pessoais	P1	I2	Nível de Risco (P x I) 3
R01	<Risco 1>			
R02	<Risco 2>			
R03	<Risco N>			

Legenda: P – Probabilidade; I – Impacto.

1 Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

2 Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
3 Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

A título de informação, é destacada a seguir uma lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os doze primeiros riscos representam riscos de privacidade obtidos da norma ISO/IEC 29134:2017 seção 6.4.4.

ID	Risco ao tratamento de dados pessoais	P1	I2	Nível de Risco (PxI)3
R01	Acesso não autorizado	10	15	150
R02	Modificação não autorizada	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada	5	15	75
R06	Coleção Excessiva	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente)	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso)	5	15	75

ID	Risco ao tratamento de dados pessoais	P1	I2	Nível de Risco (PxI)3
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.)	5	15	75
R14	Reidentificação de dados pseudonimizados	5	15	75

7 – MEDIDAS PARA TRATAR OS RISCOS

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46.).

<Importante reforçar que as medidas para tratar os riscos podem ser: de segurança; técnicas ou administrativas.

A coluna “Medida(s)” pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto-, devidos aos benefícios do processamento dos dados pessoais e as dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.

RISCO	MEDIDA(S)	EFEITO SOBRE O RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S) APROVADA(S)[3]
			P	I	P x I	
R01	Medida 1; Medida 2; Medida N					
	Medida 1; Medida 2; Medida N					
	Medida 1; Medida 2; Medida N					

Legenda: P – Probabilidade; I – Impacto.
Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.
3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

A seguir são apresentados exemplos de medidas para tratar os riscos a fim de demonstrar o preenchimento da tabela apresentada na página anterior.

RISCO	MEDIDA(S)	EFEITO SOBRE O RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S) APROVADA(S)[3]
			P	I	P x I	
R01 Acesso não autorizado	1. Controle de acesso Lógico.	Reduzir	5	10	50	SIM
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					
R04 Roubo.	1. controle de acesso lógico	Reduzir	5	5	25	Sim
	2. controles criptográficos					
	3. proteção física e do ambiente					
R06 Coleção excessiva	1. Limitação da coleta.	Reduzir	5	10	50	Sim

8 – APROVAÇÃO

Esta seção visa formalizar a aprovação do RIPD por meio da obtenção das assinaturas do Responsável pela elaboração do RIPD, pelo encarregado e pelas autoridades que representam o controlador e operador. O responsável pela elaboração do Relatório pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
_____ Nome do responsável Matrícula/SIAPE: xxxxx Local / dia / mês / ano	_____ Nome do responsável Matrícula/SIAPE: xxxxx Local / dia / mês / ano

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
_____ Nome do responsável Matrícula/SIAPE: xxxxx Local / dia / mês / ano	_____ Nome do responsável Matrícula/SIAPE: xxxxx Local / dia / mês / ano

Fontes

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd
https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_requisitos_obrigacoes.pdf
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/templates-e-ferramentas/estudo_template_preenchido_ripd.pdf

MINAS GERAIS

GOVERNO DIFERENTE.
ESTADO EFICIENTE.