CAFÉ & COMPLIANCE

PLANO DE ADEQUAÇÃO – LGPD
PLANO DE INTEGRIDADE

CONCEITOS

DADOS – são informações;

TITULAR DOS DADOS – é aquele a quem a informação se refere.

DADOS PESSOAIS – são informações de uma pessoa identificada ou identificável;

DADOS PESSOAIS SENSÍVEIS – são informações que vão além da mera identificação, que indicam origem racial, opção sexual, convicções religiosas, opiniões políticas, etc.

DADOS PESSOAIS PSOUDONIMIZADOS – são informações a princípio anônimas, mas que pode ser revertido, permitindo a identificação do titular.

Titular dos dados

DADOS ANONIMIZADOS – são aqueles em que não se é possível identificar seu titular.

ADMINISTRAÇÃO PÚBLICA

Art. 7º O **tratamento de dados pessoais** somente poderá ser **realizado** nas seguintes hipóteses: (…)

II - para o cumprimento de **obrigação legal** ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de **políticas públicas previstas em leis** e regulamentos ou **respaldadas em contratos**, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

V - quando necessário para a **execução de contrato** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VIII - para a **tutela da saúde**, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

IX - quando necessário para **atender aos interesses legítimos** do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

TRATAMENTO

O tratamento de dados pela Administração Pública está regulamentado no capítulo IV, do art. 23 a 30 da LGPD, atribuindo ampla capacidade à Administração Pública de tratar dados pessoais sem o consentimento do titular

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, "b"
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, "c"
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, "d"
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, "e"
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, "f"
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, "g"

DEVERES DA ADMINISTRAÇÃO PÚBLICA

Art. 23 da LGPD:

a) Ao realizar o tratamento para atendimento de sua finalidade pública, com objetivo de executar competências legais ou cumprir atribuições do serviço público, **deve informar ao titular:**

I) as hipóteses em que realizam o tratamento de dados pessoais;

II) a base legal;

III) a finalidade;

IV) os procedimentos e as práticas para a execução dessas atividades.

b) **Indicar o encarregado** quando realizarem tratamento de dados pessoais.

c) **Manter os dados em formato interoperável e estruturado para o uso compartilhado**, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral;

d) **Comunicar à autoridade nacional os casos de transferências por convênio ou o uso compartilhado** de dados com pessoa jurídica de direito privado, conforme exceção da vedação prevista no § 1º do art. 26;

SANÇÕES NA ADMINISTRAÇÃO PÚBLICA

Estão previstas nos incisos I, IV, V, VI, X, XI e XII do artigo 52 da LGPD:

I - **advertência**, com indicação de prazo para adoção de medidas corretivas;

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;

X - **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;

XI - **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;

XII - **proibição parcial ou total do exercício** de atividades relacionadas a tratamento de dados.

O QUE FAZER?

PLANO DE ADEQUAÇÃO

Sumário

ETAPAS DE ADEQUAÇÃO

ETAPA 1 – Matriz de responsabilidade e nomeação do Encarregado;

ETAPA 2 – Elaboração do Guia LGPD – Guia de Orientação aos gestores;

ETAPA 3 – Mobilização das equipes, conscientização – Café & Compliance;

ETAPA 4 – Adequação das normas, definição da Política de Privacidade;

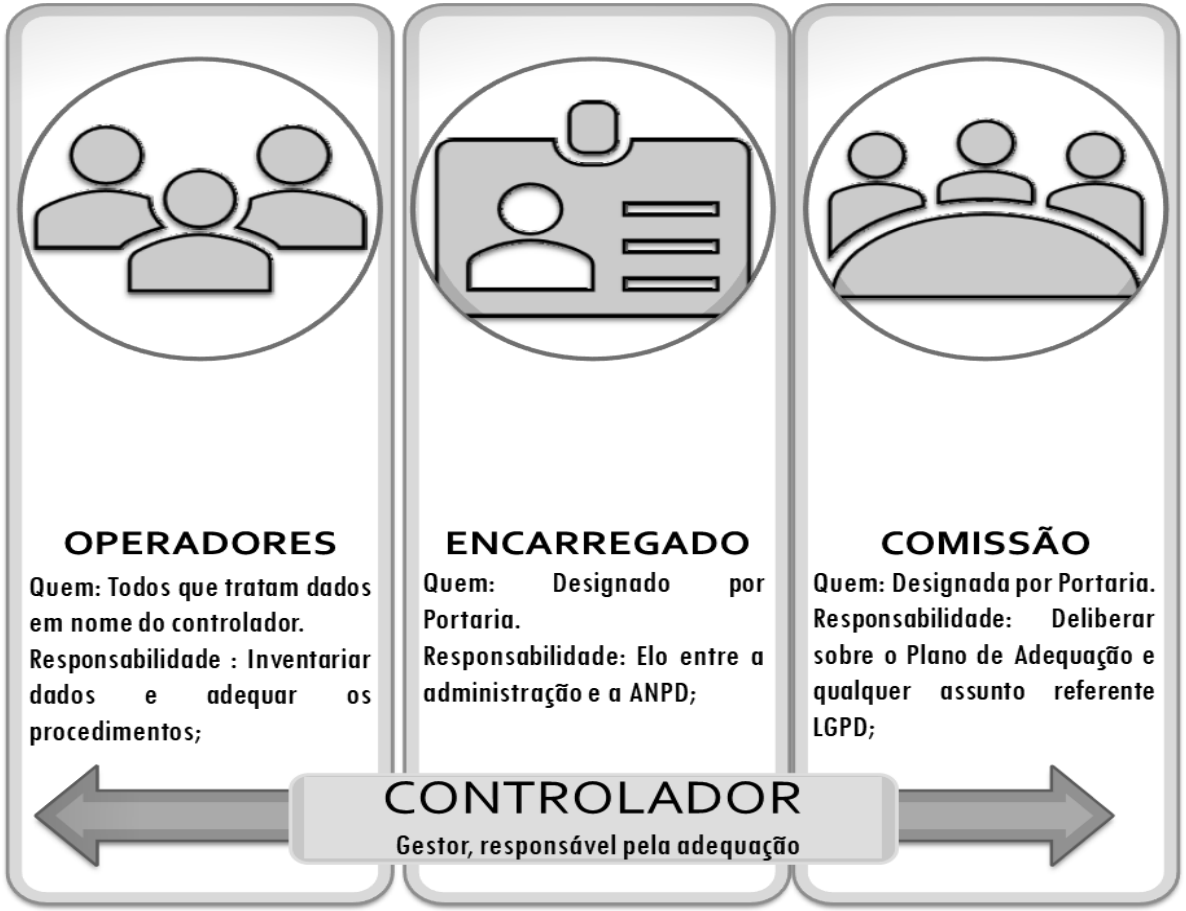
ETAPA 5 – Instituição da Comissão Mista de Reavaliação de Informações (CMRI);

ETAPA 6 – Inventário de dados: mapeamento dos dados pessoais, os fluxos de dados e a análise de risco;

ETAPA 7 – Modelo de relatório de impacto à proteção de dados pessoais.

ETAPA 1

Matriz de responsabilidade



ETAPA 1
Matriz de responsabilidade

A Os agentes envolvidos no armazenamento, tratamento e operação de dados, previstos na LGPD, são:

a) **controlador:** pessoal natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
b) **operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
c) **encarregado:** pessoa indicada pelo controlador e operador como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
d) **agentes de tratamento:** o controlador e o operador;
e) **titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

ETAPA 2

Elaboração do Guia LGPD

ETAPA 3
Mobilização das equipes conscientização

O QUE	PARA QUE	QUANDO
PROGRAMA DE INTEGRIDADE	Instituir o Programa de Integridade – Lei 1.807/2020 Conscientizar sobre as ações necessárias	1º e 2º Semestre
CÓDIGO DE ÉTICA	Compreender as regras e difundir no ambiente de trabalho, na relação com terceirizados, fornecedores e cidadãos.	1º Semestre
LEI GERAL DE PROTEÇÃO DE DADOS	Implementar a LGPD	1º e 2º Semestre
FISCALIZAÇÃO E GESTÃO DE CONTRATOS	Compreender a aplicação do Manual de Gestão de Contratos e os reflexos da Lei de Integridade.	2º Semestre
TRANSPARÊNCIA E PARTICIPAÇÃO – OUVIDORIA	Compreender o Sistema de Ouvidoria	2º Semestre
ANÁLISE DE RISCO NA ADMINISTRAÇÃO MUNICIPAL	Implementar a análise de risco nas Unidades Executoras.	2º Semestre
SICI WEB	Implementar o Sistema de Auditoria	2º Semestre

Mobilização é a construção inicial das ações para adequação dos órgãos à LGPD. Para tanto, optou-se por incluir na programação de treinamentos do projeto Café & Compliance, onde será explanado os passos iniciais da implementação.

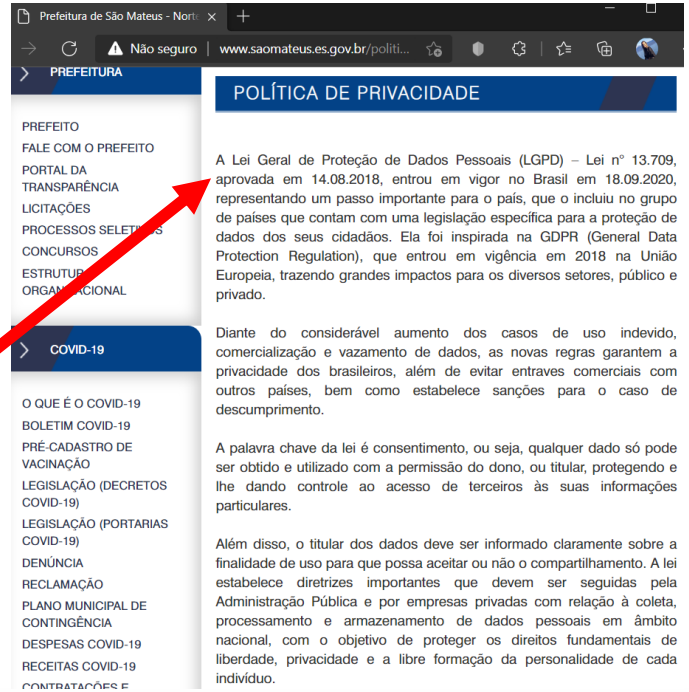
A definição do projeto Café & Compliance como estratégia inicial de mobilização e conscientização não tira a responsabilidade dos controladores de mobilizar seu setor/órgão, bem como, de planejar e executar estratégias de conscientização.

ETAPA 4

Adequação das normas

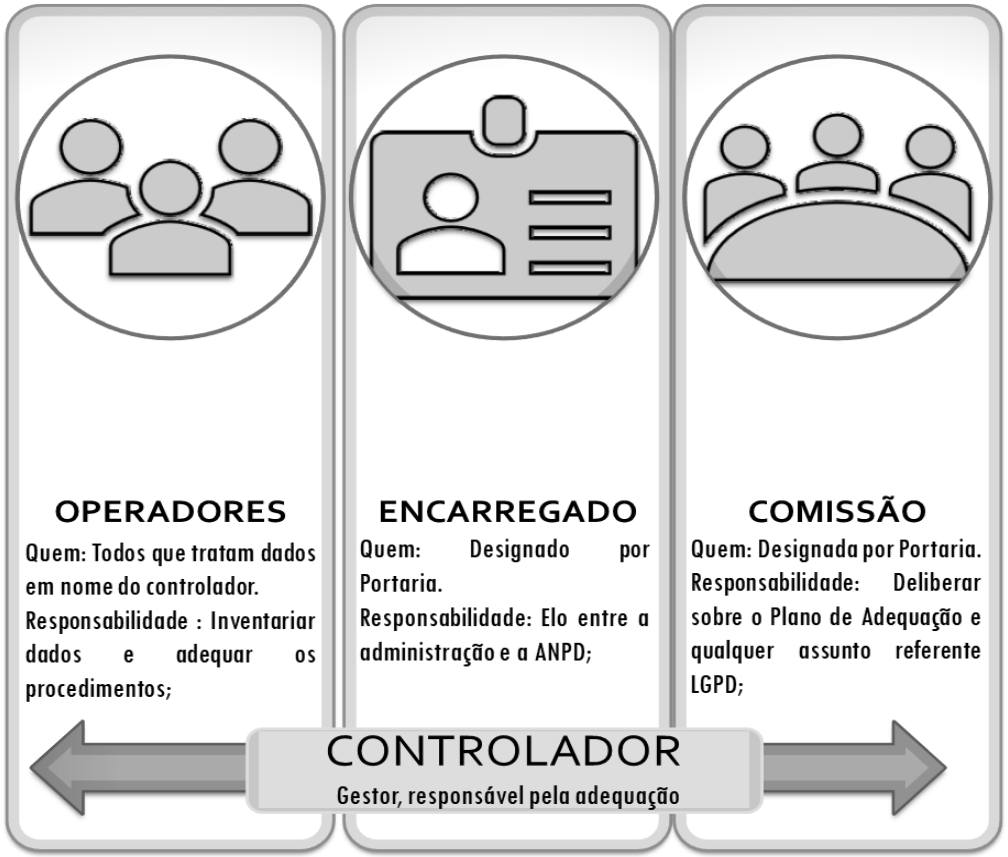
Política de Privacidade

A Secretaria de Ciência e Tecnologia atualizará norma de segurança da informação, estabelecendo regras de procedimentos para adequação à LGPD.



Os controladores e operadores, no âmbito de suas competências pelo tratamento de dados pessoais, poderão formular regras.

ETAPA 5
COMISSÃO MISTA



Art. 9º Cabe à Comissão Mista de Reavaliação de Informações (CMRI), por solicitação do encarregado da proteção de dados:

I - deliberar sobre proposta de diretrizes para elaboração dos planos de adequação, nos termos do art. 4º, parágrafo único deste decreto;

II - deliberar sobre qualquer assunto relacionado à aplicação da Lei Federal nº 13.709, de 2018, e do presente decreto pelos órgãos do Poder Executivo.

ETAPA 6
Inventário de dados análise de risco

Inventário de Dados Pessoais					
Essa guia é um modelo de um formulário operacional a ser reproduzido, adaptado e preenchido de acordo com a sua atividade de tratamento de dados pessoais. São fornecidos comentários adicionais como notas para auxiliar no preenchimento do formulário (Nota em vermelho na célula).					
1 - Identificação dos serviços/ processos que tratam dados pessoais					
1.1 - Nome do serviço / Processo					
1.2 - Data de Criação do Inventário					
1.4 - Data Atualização do Inventário					
2 - Agentes de Tratamento e Encarregado	Nome	Cargo/Setor	Telefone	E-mail	
2.1 - Controlador					
2.2 - Encarregado					
2.3 - Operador					
3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processamento	Compartilhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					
4 - De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados					
4.1 - Descrição do Fluxo do tratamento dos dados pessoais					
5 - Escopo e Natureza dos Dados Pessoais					
5.1 - Abrangência da área geográfica do tratamento					
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais					
6 - Finalidade do Tratamento de Dados Pessoais					
6.1 - Hipótese de Tratamento					
6.2 - Finalidade					
6.3 - Previsão legal					
6.4 - Resultados pretendidos para o titular de dados					
6.5 - Benefícios esperados para o órgão, entidade ou					
7 - Categoria de Dados Pessoais					
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos Dados	Fonte Retenção	Nome Base de Dados	
7.1.1 - Informações de identificação pessoal					
7.1.2 - Informações de identificação atribuídas por instituições governamentais					

Inventário de dados *(data flow, data mapping)* deverá identificar:

I - Serviços e processos que tratam dados;

II - Os agentes de tratamento;

III - Fases do Ciclo de Vida do Tratamento Dados Pessoais;

IV - Fluxo do tratamento dos dados pessoais;

V - Escopo e Natureza dos Dados Pessoais;

VI - Finalidade do Tratamento;

VII - Categoria de dados pessoais;

VIII - Categoria de dados pessoais sensíveis;

IX - Frequência e quantidade de dados pessoais tratados;

XI – Medidas de segurança de privacidade.

ETAPA 6
Inventário de dados análise de risco

MATRIZ = PxI			IMPACTO		
			LEVE	MODERADO	ALTO
			5	10	15
PROBABILIDADE	LEVE	5	25	50	75
	MODERADO	10	50	100	150
	ALTO	15	75	150	225

Parâmetros escalares para avaliar o nível potencial de risco para cada evento considerou a multiplicação entre os níveis de Probabilidade e Impacto, que resultam nos níveis de risco escalares, assim, disposto:

a) leve – 5
b) moderado – 10
c) alto – 15

ETAPA 6

PREFEITURA MUNICIPAL DE SÃO MATEUS
ESTADO DO ESPÍRITO SANTO
MAPA DE GESTÃO DE RISCO

Secretaria/Órgão: **DATA:**

Os riscos serão avaliados nos processos que tratam dados do órgão/secretaria.
Risco = Probabilidade x Impacto

MAPEAMENTO DE RISCO

Critérios: **Risco baixo** **Risco médio** **Risco alto**

ID	RISCO DE TRATAMENTO DE DADOS	P	I	RISCO (PXI)
R1	Acesso não autorizado	10	15	**150**
R2	Modificação não autorizada.	5	15	**75**
R3	Perda	10	15	**150**
R4	Roubo	5	15	**75**
R5	Remoção não autorizada	5	15	**75**
R6	Coleção excessiva	5	5	**25**
R7	Informação insuficiente sobre a finalidade do tratamento.	5	5	**25**
R8	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	10	**100**
R9	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 municipal sem o consentimento do titular dos dados pessoais.	10	15	**150**
R11	Retenção prolongada de dados pessoais sem necessidade.	5	15	**75**
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	15	15	**225**

ETAPA 6

PREFEITURA MUNICIPAL DE SÃO MATEUS

ESTADO DO ESPÍRITO SANTO

MAPA DE GESTÃO DE RISCO

Controles e tratamento serão definidos conforme escala de classificação do risco .
Risco = Probabilidade x Consequência

PLANO DE RESPOSTA

Critérios: **Risco baixo** **Risco médio** **Risco alto**

ID	TRATAMENTO/PRAZO	MEDIDAS	RISCO RESIDUAL		
			P	I	RISCO (PxI)
R1	Acesso não autorizado				**0**
R2	Modificação não autorizada.				**0**
R3	Perda				**0**
R4	Roubo				**0**
R5	Remoção não autorizada				**0**
R6	Coleção excessiva				**0**
R7	Informação insuficiente sobre a finalidade do tratamento.				**0**
R8	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).				**0**
R9	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).				**0**
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública municipal sem o consentimento do titular dos dados pessoais.				**0**
R11	Retenção prolongada de dados pessoais sem necessidade.				**0**
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.				**0**
R14	Reidentificação de dados pseudonimizados				**0**

ETAPA 7
RELATÓRIO DE IMPACTO A PROTEÇÃO DE DADOS
RIPD

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.

ETAPA 7

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	
Operador	
Encarregado	
E-mail Encarregado	**Telefone Encarregado**

2. NECESSIDADE DE ELABORAR O RELATÓRIO

3. DESCRIÇÃO DO TRATAMENTO

- 3.1 NATUREZA DO TRATAMENTO
- 3.2 ESCOPO DO TRATAMENTO
- 3.3 CONTEXTO DO TRATAMENTO
- 3.4 FINALIDADE DO TRATAMENTO

4. PARTES INTERESSADAS CONSULTADAS

5. NECESSIDADE E PROPORCIONALIDADE

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]

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).

7. MEDIDAS PARA TRATAR OS RISCOS

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S)[3] APROVADA(S)
			P	I	(P X I)	

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.

8. APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
<Nome do responsável> **Matrícula** <Local>, <dia> de <mês> de <ano>	<Nome do responsável> **Matrícula** <Local>, <dia> de <mês> de <ano>
AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
<Nome do responsável> **Matrícula**. <Local>, <dia> de <mês> de <ano>	<Nome do responsável> **Matrícula**. <Local>, <dia> de <mês> de <ano>

Modelo de Relatório CCGD da Secretaria do Governo Digital.