Modelo de Plano de Análise de Riscos

Escopo, premissas e resultados esperados:

Escopo:

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) 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. Por este motivo, sugere-se a elaboração de um **Plano de Análise de Riscos**, com a metodologia sugerida no presente documento. 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. Para fins da presente análise, **apenas os riscos ao cumprimento das legislações e melhores práticas da proteção de dados pessoais são considerados**. Não serão considerados todos os possíveis riscos de segurança da informação incidentes - até porque a análise deverá incluir o tratamento de dados pessoais que ocorra em documentos físicos e digitais, independentemente do meio em que se encontrem.

Premissas:

A identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco, considerando a realidade especifica de cada agente de tratamento. A título de ilustração, é destacada a seguir uma sugestão de análise dos 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.

Tabela 4 Parâmetros Escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Fonte: Guia de Avaliação de Riscos de Segurança e Privacidade do Governo Federal. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf

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

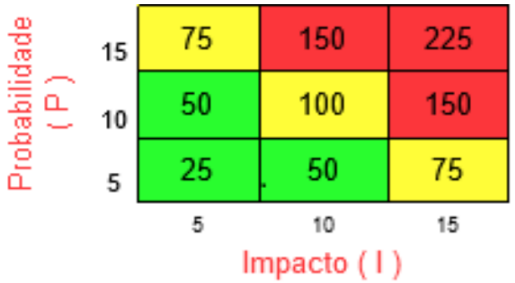

Figura 2 Matriz Probabilidade x Impacto

Risco enquadrado na região:

• verde, é entendido como baixo, sendo a ele atribuída pontuação 5;
• amarelo, representa risco moderado, sendo a ele atribuído pontuação 10;
• vermelho, indica risco alto, sendo a ele atribuído pontuação 15;

A classificação (de uma probabilidade de ocorrência de determinado risco ou o impacto do resultado de um evento) como alto, médio e baixo é de competência dos responsáveis pela elaboração da análise de risco, devendo levar em conta os aspectos especificos da realidade institucional do seu órgão/entidade, além das questões pertinentes ao tratamento de dados pessoais realizadas pelos agentes de tratamento.

A título de ilustração, 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, retirada do Guia de Boas Práticas de LGPD do governo federal. O nível de probabilidade, impacto e nível de risco indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. 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). Alguns dos riscos à privacidade que sugere-se que devem ser elencados nesta análise:

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[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 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

A proposta constante na aba "modelo" traz uma **lista não-exausitva de riscos identificados no tratamento de dados pessoais**, de modo que essa lista pode ser modificada, analisada e aperfeiçoada pelos agentes de tratamento de dados pessoais da Prefeitura Além do levantamento dos potenciais riscos, devem ser calculados, para cada um dos riscos identificados, a sua probabilidade de impacto e o seu nível de risco, que devem ser ao final classificados como alto, médio e baixo risco, permitindo a hierarquização dos riscos identificados. Além disso, devem ser apresentadas também as medidas que devem ser adotadas para tratamento dos riscos, apontando, ao final, a identificação do risco residual esperado após a implementação da medida tratamento.

A proposta de metodologia elaborada trata-se de uma adaptação das melhores práticas sugeridas pelo governo federal, além da adequação de algumas premissas da metodologia COSO, da ISO/IEC 29134:2017 e de entidades de referência na área de privacidade de dados pessoais. Os riscos sugeridos neste modelo e as medidas sugeridas para tratá-las não são exausitvas e podem (e devem) ser revisadas e discutidas considerando a realidade de cada órgão/entidade (agente de tratamento).		
Resultados esperados: Espera-se, após a análise de tratamento de riscos à proteção de dados pessoais, que o órgão/entidade seja capaz de identificar com clareza as medidas necessárias para o cumprimento das legislações relativas à proteção de dados pessoais, além de ter subsídios para elaboração do RIPD.		

Modelo de Plano de Análise de Riscos

DESCRIÇÃO DO RISCO	FUNDAMENTAÇÃO DO RISCO	PROBABILIDADE DO RISCO	IMPACTO DO RISCO	NÍVEL DE RISCO (P x I)	CLASSIFICAÇÃO DO RISCO	AÇÕES PARA MITIGAÇÃO DO RISCO	RISCO RESIDUAL
Detalhar o risco relativo ao cumprimento d	*Mencionar a norma legal ou boa prática (l*	*Elencar a probabilidad*	*Elencar o impacto de ocorrência do r*		Alto / Médio / Baixo	*Indicar ações sugeridas para tratar o risco*	*Alto / Médio / Baixo*
Ausência de indicação de encarregado	Art. 41, LGPD	15	15	225	Alto	incidicar encarregado pelo tratamento dos dados pessoais, disponibilizar o contato com o encarregado	Baixo
Acesso não autorizado	princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017	15	15	225	Alto	política de credenciais; controle de acesso lógico; política de segurança em redes; restrição de acesso aos arquivos físicos	Médio
Modificação não autorizada	princípio da segurança (art. 6, VII e art. 46, LGPD) + ISO / IEC 29134:2017	10	15	150	Alto	política de credenciais; controle de acesso lógico; política de segurança em redes; termo de responsabilidade	Médio
Tratamento sem consentimento do titular dos dados pessoais (Caso a base legal seja consentimento)	Art 5, inciso XII e art. 7, inciso I, LGPD	10	15	150	Alto	termo de consentimento; mapeamento de dados pessoais	Baixo
Compartilhar ou distribuir dados pessoais com terceiros fora das hipóteses de compartilhamento	Art. 26 e 27 da LGPD	10	15	150	Alto	termo de uso; contratos com claúsulas destacadas acerca da transferência de dados pessoais, especificando a base legal	Baixo
Perda	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de inicidente de segurança de dados pessoais	Baixo
Roubo	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de inicidente de segurança de dados pessoais	Baixo
Remoção não autorizada	princípio da segurança (art. 6, VII e art. 46, LGPD) + princípio da responsabilização (art. 6, X, LGPD)	10	10	100	Médio	política de resposta de incidentes de proteção de dados; política de segurança da informação; modelo de relatório de inicidente de segurança de dados pessoais	Baixo
Utilização de dados em excesso	princípio da necessidade (art. 6, II e III, LGPD)	10	10	100	Médio	Limitação da coleta/minização dos dados; governança de dados; segmentação dos dados; mapeamento de dados	Médio
Não especificação de quais as medidas de segurança adotadas	princípio da segurança (art. 6, VII e art. 46, LGPD)	5	15	75	Médio	Elevar os níveis de segurança, com política de segurança da informação implementada e atualizada; mapeamento de dados	Baixo
Execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.	princípio da qualidade dos dados (art. 6, V, LGPD)	5	15	75	Médio	mapeamento de dados realizado com precisão e qualidade (assegurar que os dados coletados são exatos e relevantes para o cumprimento da finaldiade do tratamento).	Baixo
Tratamento de dados pessoais de crianças e adolescentes sem o consentimento de pais ou responsáveis	princípio da segurança (art. 6, VII e art. 46) e princípio da responsabilização (art 6, X) e regras para tratamento de dados de crianças (art. 14, LGPD)	15	15	225	Alto	Anonimização dos dados; termos de uso; controle de acesso; política de segurança da informação; treinamento e orientação para os funcionários; coleta do consentimento dos pais e responsáveis; termo de consentimento	Médio
Retenção prolongada de dados pessoais sem necessidade.	Art. 5, inc. XIV, LGPD + Art. 18, IV e VI, LGPD	15	5	75	Médio	Controle do tempo de guarda [clico de vida]; controles de segurança em redes; política interna; governança de dados; mapeamento de dados pessoais	Baixo
O órgão/entidade não apresenta uma política de privacidade informando o tratamento realizado e dados pessoais tratados	Art. 50, § 3º, LGPD + Princípio da transparência	15	15	225	Alto	Elaborar política de segurança da informação, monitorar e auditar a privacidade; disponibilização no site do órgão	Baixo
Compartilhamento de dados excessivos com órgãos públicos	Art. 18, VII, LGPD + princípio da necessidade	10	5	50	Baixo	acordos de cooperação com entidades externas à Prefeitura para compartilhamento para fins de politicas publicas; informação de compartilhamento nos termos de uso; publicar no site do órgão a dispensa de consentimento; auditorias constantes para identificar novas necessidades de compartilhamento	Baixo

Modelo de Plano de Análise de Riscos

DESCRIÇÃO DO RISCO	FUNDAMENTAÇÃO DO RISCO	PROBABILIDADE DO RISCO	IMPACTO DO RISCO	NÍVEL DE RISCO (P x I)	CLASSIFICAÇÃO DO RISCO	AÇÕES PARA MITIGAÇÃO DO RISCO	RISCO RESIDUAL
Detalhar o risco relativo ao cumprimento d	*Mencionar a norma legal ou boa prática (l*	*Elencar a probabilidad*	*Elencar o impacto de ocorrência do r*		Alto / Médio / Baixo	*Indicar ações sugeridas para tratar o risco*	*Alto / Médio / Baixo*
Informação insuficiente sobre a finalidade do tratamento	Art. 6º, I; art. 9º, I; art. 23, LGPD	10	15	150	Alto	Atualização dos termos de uso; atualização das políticas de compartilhamento; treinamento e orientação para os funcionários; atualização dos contratos, convenios, acordos de cooperação e instrumentos jurídicos congeneres; mapeamento de dados pessoais	Alto
Falha em considerar os direitos do titular dos dados pessoais (Ex.: não possibilitar remooção do consentimento)	Art. 9º; art. 18º, LGPD	10	10	100	Médio	Atualização dos termos de uso; modificação dos sistemas para permitir eliminação do dado, caso o titular revogue o consentimento; termos de uso; treinamento e orientação para os funcionários; termo de consentimento; plano de adequação à proteção de dados	Baixo
Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular	Art 5º, I; art. 13, §4º, LGPD	5	5	25	Baixo	ue estejam publicamente disponíveis de modo a permitir que a	Baixo
Reidentificação de dados pseudonimizados	Art 5º, I; art. 13, §4º, LGPD	5	15	75	Médio	ologias mais atualizadas para realizar a anonimização dos dad	Baixo