30/7/2021

# POLÍTICA DA CLASSIFICAÇÃO DOS RISCOS RELATIVOS À PRIVACIDADE DOS DADOS

Lei Geral de Proteção de Dados Pessoais– LGPD

Lei nº13.709/2018

Coordenação da Região Metropolitana de Curitiba
**COMEC**

# Sumário

## INTRODUÇÃO

Essa Política de Classificação dos Riscos relativos à Privacidade dos Dados é um modelo holístico de abordagem à Segurança da Informação e Dados Pessoais, que servirá de guia na classificação do risco da violação.

Ela terá uma abordagem 360º à segurança, tendo como base:

**ABNT NBR ISO 31000:2018** - Informações Básicas, princípios e diretrizes para a implementação da gestão de riscos,
**ABNT NBR ISO/IEC 27001:2013** - Tecnologia da Informação – técnicas de segurança – sistemas de gestão da segurança da informação – requisitos e,
**ABNT NBR ISO 27701:2020** - Sistemas de Gestão de Segurança Privada.

A ISO 31000:2018[1] sugere que a gestão de risco eficaz é caracterizada por princípios, estrutura e processo. O propósito da gestão de riscos é a criação e proteção de valor.

Já a ISO 27001:2013[2] serve para que se opte por um modelo adequado de proteção a confidencialidade, integridade e disponibilidade da informação, identificando quais potenciais problemas podem ocorrer com a informação, e assim, definindo quais necessidades devem ser atendidas para prevenir tais problemas se ocorrerem, ou seja, descobrir onde os riscos estão, e então tratá-los sistematicamente.

Por fim, a ISO 27701:2020[3] especifica os requisitos e fornece diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de gestão de privacidade da informação.

[1] A ISO 31000 foi publicada originalmente em 2009 e uma versão atualizada foi publicado em fevereiro de 2018. No entanto, o objetivo geral da ISO 31000 continua o mesmo – integrando a gestão de risco em um sistema de gestão estratégica e operacional.
[2] A ISO 27001 teve sua primeira publicação em 2005 e atualizada em 2013, onde sua principal filosofia ainda está baseada na avaliação e tratamento de riscos.
[3] Versão original foi publicada em 2019 passando por correções em 2020.

## CAPÍTULO I – DOS OBJETIVOS

Art. 1. Esta Política de Classificação dos Riscos Relativos a Privacidade dos Dados tem por objetivo auxiliar na adequação à Lei Geral de Proteção dos Dados – LGPD junto a Coordenação Metropolitana de Curitiba – COMEC.

Art. 2. A presente política promove, por meio das ISO (31000:2018, 27001:2013 e 27701:2020) correta adequação, conformidade com as leis vigentes relacionadas ao tema e segurança jurídica.

Art. 3. Com esta Política, a COMEC determinará a Classificação dos Riscos relativos à Privacidade dos dados, para que a mesma possa auxiliar a gestão, enfrentamento e solução de possíveis condutas ilícitas ou não, que possam resultar na violação dos dados Pessoais dos titulares.

## CAPÍTULO II – DA FORMULAÇÃO DA CLASSIFICAÇÃO DOS RISCOS

Art. 4. Toda formulação dessa classificação se baseará nas informações prestadas pelos setores que formam a COMEC, as quais cuidadosamente devem ser coletadas.

Art. 5. Junto com o Grupo Multidisciplinar de Implantação da LGPD, será mapeado, encima das informações coletadas conforme art. 4º dessa Política, os riscos atuais e iminentes.

Art. 6. A tabela de Classificação dos Riscos Relativos à Privacidade dos Dados, como se trata de importante ferramenta no Tratamento Dos Dados, poderá sofrer atualizações sem prévia anuência do Gestor responsável, devendo logo em seguida informado sobre as mesmas.

**CAPÍTULO III – TABELA DE CLASSIFICAÇÃO DOS RISCOS RELATIVOS Á PRIVACIDADE DOS DADOS.**

Art. 7. A referência para tal classificação se baseará em:

I – Público: Informações que podem ser disponibilizadas e acessíveis a qualquer pessoa;

II – Interno: Informações que podem ser acessadas apenas por colaboradores da COMEC;

III – Confidencial – Informações acessíveis a apenas um grupo de pessoas autorizadas e;

IV – Restrito: Dados acessíveis apenas por pessoas pré-definidas.

Art. 8. Por ordem de gravidade (Baixo, Moderado e Alto) se classifica os Riscos Relativos à Privacidade dos Dados:

I – Baixo: classificação utilizada quando o incidente de segurança de dados ofertar apenas dados pessoais, não incluindo o número do CPF;

II – Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluindo o número do CPF, e/ou pelo menos um dado sensível, não incluindo raça, religião, nome social e dados de saúde;

III – Alto: classificação utilizada quando o incidente de segurança dos dados afetar dados pessoais, incluindo o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

Art. 9. Alguns fatores serão determinantes na definição da criticidade de um incidente:

I – Dados legíveis/ilegíveis: dados protegidos por algum sistema de pseudonimização (criptografia, por exemplo);

II – Volume de dados pessoais: expresso em quantidade de registros, arquivos, documentos e/ou em períodos de tempo (uma semana, um ano, etc.);

III – Facilidade de identificação de indivíduos: facilidade com que se pode deduzir a identidade das pessoas a partir dos dados envolvidos no incidente;

IV – Indivíduos com características especiais: se o incidente afeta pessoas com características ou necessidades especiais;

V – Número de indivíduos afetados: dentro de uma determinada escala, por exemplo, mais de 100 indivíduos.

**CAPÍTULO IV – CONTENÇÃO**

Art. 10. Após um incidente ser identificado como uma violação de segurança, o mesmo deverá ser contido, evitando, assim, que outros sistemas sejam afetados ou que ocasionem danos maiores.

Art. 11. Durante a contenção, deve haver o registro do incidente (conforme a Política de Tratamento de Incidentes à Privacidade de Dados) e as medidas de contenção que foram adotadas. O responsável pelo tratamento de dados da área afetada pelo incidente deve imediatamente informar o encarregado de dados para iniciar o processo de contenção.

Art. 12. Os envolvidos na contenção do incidente serão: O Operador daqueles dados, o Encarregado de Proteção de Dados, a Assessoria Jurídica, a Coordenadoria de Tecnologia da Informação e o Diretor Presidente.

Art. 13. O Encarregado de Proteção de Dados após ser alertado da ocorrência do incidente, avaliará a existência do plano de ação para tal incidente e inicia-lo, e identificando o caso concreto de vazamento de dados pessoais, preencherá o documento de Comunicação de Incidente de Segurança, para a notificação à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

Documento: **PoliticadeClassificacaodosriscosLGPDCOMEC.pdf**.

Assinatura Qualificada realizada por: **Gilson de Jesus dos Santos** em 04/08/2021 11:46.

Assinatura Avançada realizada por: **Ligia Damiani Riedel** em 04/08/2021 11:28.

Inserido ao protocolo **17.941.146-6** por: **Ligia Damiani Riedel** em: 04/08/2021 11:28.