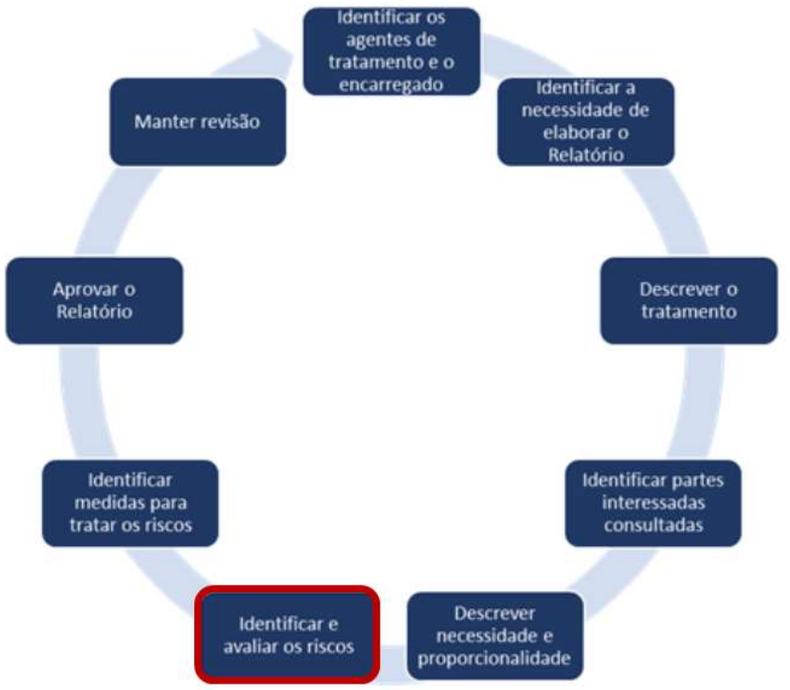
LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Relatório de Impacto à Proteção de Dados Pessoais – Identificação e avaliação de riscos

Prezados colegas e colaboradores, hoje daremos continuidade à análise da etapa de identificação e avaliação de riscos no tratamento de dados pessoais:



Na publicação anterior foram apresentados critérios e parâmetros que podem ser estabelecidos para identificar e mensurar riscos passíveis de gerar impacto sobre o titular dos dados pessoais a serem tratados:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

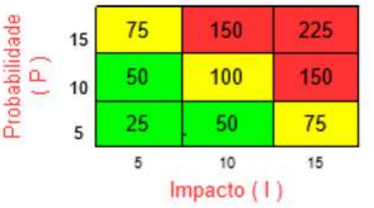


Figura 2 Matriz Probabilidade x Impacto

Assim, a título de exemplo, apresenta-se a seguir uma tabela com lista não exaustiva de riscos de privacidade e de segurança da informação relacionados à 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 norma ISO/IEC 29134:2017 seção 6.4.4.

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).

LGPD
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Relatório de Impacto à Proteção de Dados Pessoais – Identificação e avaliação de riscos

Tabela: Risco referente ao tratamento de dados pessoais

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).

Por hoje é só, até a próxima publicação!