RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Tech Challenge - 5

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa a 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).

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Com base nos termos do art. 5º, inciso XVII da LGPD, o Relatório de Impacto deve conter "medidas, salvaguardas e mecanismos de mitigação de risco". Diante disso, os parâmetros escalares que serão adotados neste Relatório são os seguintes:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

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
		5	10	15
	Impacto			

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.

Ressalte-se, por oportuno, que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais pelo projeto do Tech Challenge 5 é realizado em consonância com o que preconiza a Política de Gestão de Riscos do órgão preconizada pela Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016 e boas práticas consolidadas e identificadas no mercado.

IDENTIFICAÇÃO E ANÁLISE DE RISCOS

Realizamos a identificação e análise de riscos baseada na Portaria CFQ nº 114, de 22 de dezembro de 2020, no qual foram considerados 14 riscos, conforme tabela a seguir:

ID	Risco	Descrição	Probabilidade	Impacto	Nível de Risco (P X I)
R01	Acesso não autorizado	Acesso indevido (permissões indevidas) a um ambiente físico ou lógico.	5	5	25
R02	Roubo	Dados roubados nas dependências internas do controlador/operador , falhas nos controles de segurança dos sistemas (a exemplo da ausência ou fraca criptografia, falha de sistema que permita escalação de privilégio ou tratamentos indevidos), entre outras.	5	15	75
R03	Coleção excessiva	Coleta de dados pessoais em quantidade superior ao mínimo necessário à finalidade do tratamento ou atividade que fará uso do dado pessoal.	5	5	25

MEDIDAS PARA TRATAR OS RISCOS

Conforme fixado pelo artigo 46 da LGPD, 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. Em razão disso, passa-se a relacionar os riscos e suas medidas:

Risco	Medida	Efeito sobre o Risco
Acesso não autorizado	S1 - Implementar um cadastro com senha para que o login exija a mesma junto com o CPF.	Reduzir
Roubo	S1 - Recuperar o registro do usuário através do CPF que estiver no token. S2 - Os dados pessoais do usuário retornados pelo endpoint deverão estar anonimizados.	Evitar
Coleção excessiva	S1 - Remover os dados de telefone e e-mail de nosso banco de dados enquanto não tivermos processos que os utilizem. S2 - Quando precisarmos dos dados de e-mail e telefone iremos solicitar aos usuários para que possamos coletar mediante aprovação dos mesmos.	Evitar