PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

UMA PROPOSTA DE PROCESSO DE GERENCIAMENTO DE RISCOS BASEADO NA LGPD

GUILHERME BARBOSA ALVES

GOIÂNIA
2021

GUILHERME BARBOSA ALVES

UMA PROPOSTA DE PROCESSO DE GERENCIAMENTO DE RISCOS BASEADO NA LGPD

Trabalho para conclusão de curso apresentado à Escola Politécnica, da Pontifícia Universidade Católica de Goiás como requisito parcial para obtenção do título de Bacharel de Ciência da Computação.

Orientador: Profª: Ma. Adriana Silveira de Souza

GOIÂNIA

2021

GUILHERME BARBOSA ALVES

UMA PROPOSTA DE PROCESSO DE GERENCIAMENTO DE RISCOS BASEADO NA LGPD

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do título de Bacharel em Ciência da Computação, e aprovado em sua forma final pela escola Politécnica, da Pontifícia Universidade Católica de Goiás em _____/_____/_____.

_____

Profa. Ma. Ludmilla Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientadora: Profª. Ma. Adriana Silveira de Souza

_____

Prof. Me. André Luiz Alves

_____

Prof. Me. Joriver Rodrigues Canedo

GOIÂNIA

2021

Dedico este trabalho a minha mãe, meu pai, meus irmãos e meu filho, meus maiores exemplos de garra e determinação.

AGRADECIMENTOS

A todos os meus professores que eu tive a oportunidade de conhecer e aprender com eles.

A minha orientadora acadêmica, professora Adriana Silveira de Souza, pelo apoio e confiança no desenvolvimento deste trabalho.

Sou grato a todo o corpo docente, à direção e administração desta universidade.

A todos que direta ou indiretamente colaboraram para realização deste trabalho.

Sou grato a todos que participaram desta banca.

“Somos do tamanho de nossos sonhos.”

(Fernando Pessoa)

RESUMO

A proteção aos dados pessoais é um tema atual e muito discutido. É um direito fundamental para qualquer cidadão brasileiro, pois envolve a proteção da intimidade, da privacidade e da garantia de que os dados pessoais que geramos serão tratados de acordo com uma legislação adequada. Com a Lei Geral de Proteção de Dados Pessoais (LGPD) foi possível endurecer a legislação atual, que ainda era muito vaga. O gerenciamento de riscos apresenta-se como uma estratégia para auxiliar na mitigação dos riscos seguindo as normas estabelecidas pela LGPD, para evitar processos e multas. Este trabalho tem como objetivo apresentar uma proposta de processamento de riscos baseada na lei. Uma pesquisa bibliográfica sobre a LGPD e riscos foi realizada com objetivo de compreender e conceituar estes temas.

Palavra-chave: LGPD. Riscos. Gerenciamento de riscos.

ABSTRACT

The protection of personal data is a current and much discussed topic. It is a fundamental right for any Brazilian citizen, as it involves the protection of intimacy, privacy and the guarantee that the personal data we generate will be treated in accordance with appropriate legislation. With the General Personal Data Protection Law (GDPL) it was possible to tighten the current legislation, which was still very vague. Risk management is presented as a strategy to help mitigate risks following the standards established by the GDPL, to avoid lawsuits and fines. This work aims to present a proposal for processing risks based on the law. Bibliographical research on GDPL and risks was carried out in order to understand and conceptualize these themes.

Keywords: GDPL. Risk. Risk management.

LISTA DE ILUSTRAÇÔES

LISTA DE QUADRO

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados
CADE	Conselho Administrativo de Defesa Econômica
CPF	Cadastro de Pessoas Físicas
DP	Dados Pessoais
EAR	Estrutura Analítica dos Ricos
GDPR	*General Data Protection Regulation* ou Regulamento Geral de Proteção de Dados
GP	Gerente de Projeto
IDC	*International Data Corporation* ou Corporação de Dados Internacional
IEC	*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional
IP	*Internet Protocol* ou Protocolo de Internet
ISO	*International Organization for Standardization* ou Organização Internacional de Normalização
LGPD	Lei Geral de Proteção de Dados Pessoais
NBR	Norma Brasileira
RG	Registro Geral
SEBRAE	Serviço Brasileiro de Apoio às Micro e Pequenas Empresas
SENACON	Secretaria Nacional do Consumidor
ZB	*Zettabyte*

SUMÁRIO

1. INTRODUÇÃO

Com o desenvolvimento da tecnologia e intensificação dos fluxos de informação, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade, de modo que a informação que antes era dispersa, torna-se organizada. (FINKELSTEIN, 2020).

Segundo Pereira (2020) na última década, com as nossas vidas cada vez mais conectadas, percebemos uma explosão de dados. De acordo com a consultoria IDC, o que em 2018 foram 33 *zettabytes* gerados anualmente, em 2025, serão 175 ZB de dados criados, capturados e replicados, o que significa que cada pessoa conectada terá pelo menos uma interação com dados a cada 18 segundos.

A frase “dados são o novo petróleo”, foi criada por Clive Humby, um matemático britânico especializado em dados. Humby (2006) afirma que o dado é muito valioso, mas para ter um melhor uso precisa ser bem refinado e analisado.

Desta forma, permite que as empresas desenvolvam produtos personalizados para seus consumidores, criem soluções que atendam perfis únicos de clientes, entendam o comportamento de um determinado segmento da população para criar soluções inovadoras que atendam suas necessidades, consigam diagnosticar e avaliar potenciais riscos antes que se concretizem.

Pode-se dizer que os dados são um patrimônio da empresa. Em muitos casos, eles são até mais importantes do que o próprio patrimônio físico da companhia. Por isso, a proteção desses dados é fundamental. (NÉGOCIO SEGURO, 2021)

Diante desse cenário, iniciou-se uma discussão global acerca de como evitar “abusos”, por parte das empresas, na coleta e utilização desses dados. Como proposta de solução surgiu a ideia de regulamentação do uso de dados pessoais através de leis e regulamentos específicos em cada país, sendo que o Brasil não ficou de fora dessa discussão. (NASCIMENTO, 2021).

Inspirado no movimento global de privacidade e proteção de dados, bem como em leis já existentes em outros países, como a *General Data Protection Regulation* (GDPR), em 14 de agosto de 2018 foi sancionada a Lei n º 13.709 ou Lei Geral de Proteção de Dados Pessoais (LGPD), o que gerou discussões sobre como empresas e governos estão utilizando as nossas informações.

Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais.

Conforme a norma ABNT NBR 31000:2018 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018, p. 1) o risco é o efeito da incerteza nos objetivos. Tal efeito pode ser positivo, negativo ou ambos simultaneamente. Pode também criar oportunidades ou ameaças.

Gerenciamento de riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação.

Uma avaliação de riscos é essencial para garantir a segurança da informação em uma organização, assim a empresa pode garantir que todas as ações necessárias mitigar determinado risco. Logo, a LGPD prevê multas e penalidades graves para empresas que tratam dados pessoais e ocorra um incidente de segurança (SERVICE IT, 2020).

Esse tema foi escolhido porque é um tema atual e está sendo bastante discutido no mercado de trabalho, e é relevante pois é necessário um estudo aprofundado para compreender como o processo de gerenciamento de riscos e a LGPD podem atuar de forma conjunta, mostrando que a lei não prejudica e sim auxilia para que o processo seja realizado de uma maneira melhor.

O objetivo principal é estabelecer uma proposta de processo de gerenciamento de riscos baseado na LGPD.

Este trabalho está organizado da seguinte forma: No capítulo 2 apresenta uma abordagem sobre a LGPD. No capítulo 3 apresenta uma abordagem sobre riscos e gerenciamento de riscos. No capítulo 4 apresenta uma proposta de gerenciamento de riscos baseado na LGPD. No capítulo 5, apresenta as principais conclusões e sugestões de trabalhos futuros.

2. Lei Geral de Proteção de Dados Pessoais (LGPD)

A LGPD estabelece diretrizes importantes e obrigatórias para a coleta, processamento e armazenamento de dados pessoais. Ela foi inspirada na GDPR (*General Data Protection Regulation*), que entrou em vigência em 2018 na União Europeia, trazendo grandes impactos para empresas e consumidores. (SEBRAE, 2020).

Antes de mais nada, é preciso entender que a legislação se aplica no meio físico e eletrônico, mas que o assunto se tornou iminente em face da maior facilidade de captação de dados no meio eletrônico.

No Brasil, a lei entrou em vigor em 18 de setembro de 2020, representando um passo importante para o Brasil. Com isso, passamos a fazer parte de um grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos. Diante dos atuais casos de uso indevido, comercialização e vazamento de dados, as novas regras garantem a privacidade dos brasileiros, além de evitar entraves comerciais com outros países. (SEBRAE, 2020).

Segundo Nascimento (2021) a lei regula o tratamento de dados pessoais, por pessoa jurídica ou por pessoa natural, com o objetivo de proteger os direitos fundamentais e a privacidade dos indivíduos. Dessa forma, ela traz uma transformação cultural e organizacional para as empresas, exigindo uma série de medidas e procedimentos para garantia de conformidade**.**

A LGPD exige que as empresas que tratam dados garantam um nível de segurança adequado ao risco envolvido em projetos e atividades específicos. Na qual podem cumprir esse requisito identificando primeiro o risco, antes de implementar o nível apropriado de medidas técnicas e organizacionais para mitigá-lo.

Esta lei dispõe do tratamento de três tipos de dados, que são muito importantes. O dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável, ou seja, são as informações básicas de um determinado individuo: Nome e sobrenome, data e local de nascimento, RG, CPF, retrato em fotografia, endereço residencial, endereço de e-mail, número de cartão bancário, renda, histórico de pagamentos, hábitos de consumo, dados de localização, como por exemplo, a função de dados de localização no celular, endereço de IP (protocolo de internet), testemunhos de conexão (*cookies*), número de telefone.

Da mesma forma, fragmentos de informação que, juntos, permitam identificar uma pessoa física também são considerados dados pessoais.

Dentre os dados pessoais, há aqueles que exigem maior atenção no tratamento, aqueles relacionados a crianças e adolescentes, e os sensíveis, que são os que revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde ou a vida sexual de uma pessoa.

Quando o dado corresponder a menores de idade, é imprescindível obter o consentimento específico e em destaque dado por pelo menos um dos pais ou responsável legal e se limitar a pedir apenas o conteúdo estritamente necessário, sem repasse a terceiros.

Sobre os dados sensíveis, o tratamento depende do consentimento explícito do(a) titular dos dados e para um fim definido. De acordo com Brasil (2021) caso o titular dos dados ou seu responsável não dê o consentimento, o tratamento poderá ser realizado nas hipóteses em que for indispensável:

- A empresa controladora cumprir alguma obrigação disposta em lei ou regulação;
- Execução pela administração pública de políticas públicas previstas em leis ou regulamentos;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiros.
- Tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;
- Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Os dados anonimizados já se difere um pouco em relação aos anteriores, são aqueles que não permitem a identificação, direta ou indireta, de seu titular e, portanto,

estão fora do escopo de proteção da LGPD. Contudo se o processo de anonimização de dados puder ser revertido, a lei será sim aplicável.

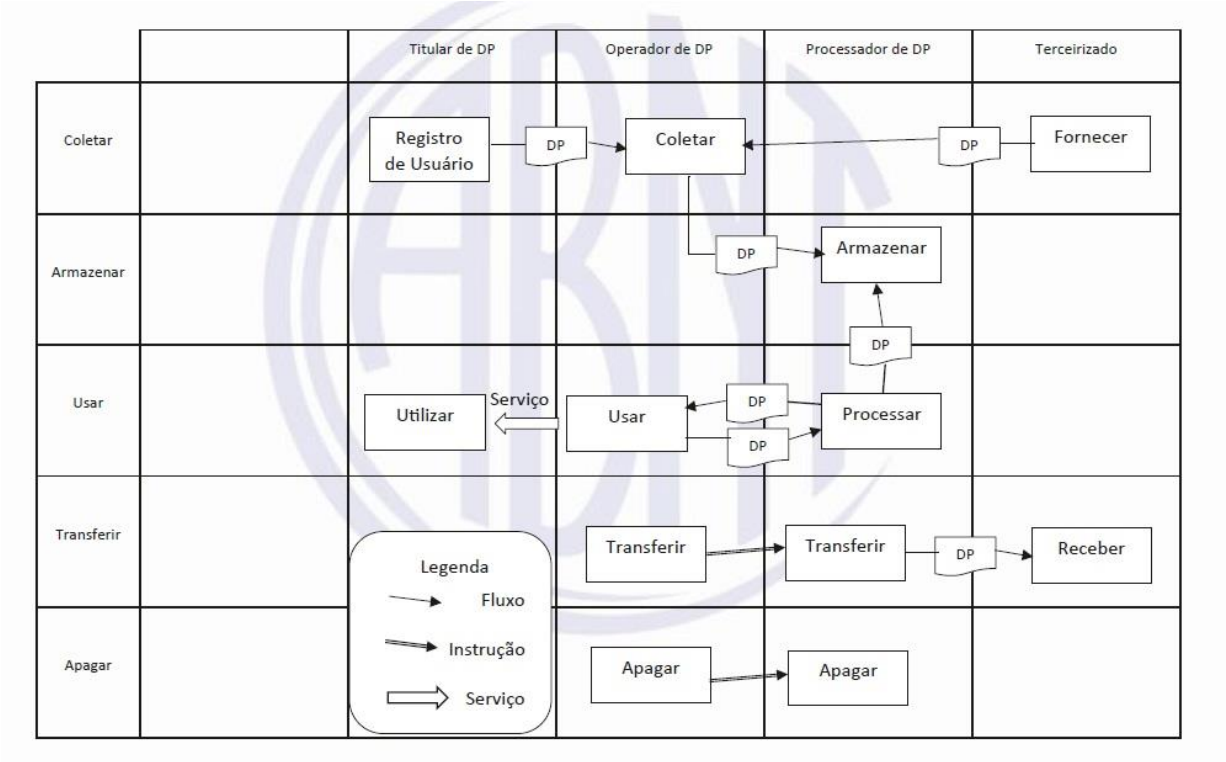
O tratamento de dados pessoais na LGPD são todas as operações realizadas com informações de pessoas naturais, inclusive nos meios digitais, por outras pessoas naturais ou pessoas jurídicas, tanto de direito privado quanto de direito público.

Mas para saber tudo sobre o que é tratamento de dados, é importante compreender quem é o “dono” desses dados. O titular de dados “é toda pessoa natural a quem se referem os dados que são objeto de tratamento”.

Assim, compreende-se como atividades pertinentes ao tratamento dessas informações:

- Coleta: incluindo coleta, produção e recepção;
- Retenção: armazenamento e arquivamento;
- Processamento: utilização, classificação, reprodução, controle, avaliação, modificação e extração;
- Compartilhamento: comunicação, distribuição, transmissão, difusão e transferência;
- Eliminação: finalização do tratamento de dados.

Figura 1 – Diagrama de Fluxo do tratamento de DP



Fonte: ABNT NBR ISO/IEC 29134, 2020.

A figura acima mostra um exemplo de acordo com a ABNT NBR ISO/IEC 29134, de como o fluxo de informações de DP ou dados pessoais pode ser visualizado, em um tratamento de dados pessoais. O seu uso, pode incluir fluxos aprovados de compartilhamento para outras partes, a organização descreverá o fluxo de informações da maneira mais detalhada possível para ajudar a identificar os possíveis riscos de privacidade.

Para resguardar o tratamento dos dados pessoais dos titulares, a Lei traz em seu Capítulo III seus direitos e garantias. Esses direitos trazem o “empoderamento” ao titular sobre seus dados, por meio de uma série de garantias que buscam resguardar o livre acesso e decisão sobre os dados pessoais.

Além disso, a lei deixa clara que os dados pertencem ao indivíduo, e não à empresa que controla ou opera esses dados.

Conforme o art. 18 da LGPD, ao(à) titular estão garantidos os direitos de (BRASIL, 2021):

- Confirmação da existência de tratamento;
- Acesso aos dados;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da Autoridade Nacional, observados os segredos comercial e industrial;
- Eliminação dos dados pessoais tratados com o consentimento do(a) titular, exceto nas hipóteses previstas no art. 16 da Lei;
- Informação das entidades públicas e privadas com as quais o Controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento e sobre consequências da negativa;
- Revogação do consentimento.

Para que o controle dos tratamentos seja feito de forma adequada, as empresas precisam contar com a figura do controlador e o operador. Os quais podem ser pessoas naturais ou jurídicas, de direito público ou privado.

O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais (BRASIL, 2021).

O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada.

Ou seja, o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador (BRASIL, 2021).

Com o objetivo de criar um canal de comunicação entre o controlador, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados, bem como um responsável direto pelo tema da privacidade e proteção de dados pessoais, a LGPD criou a figura do Encarregado, o qual terá como atividades:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

A fiscalização e a regulação da LGPD ficarão a cargo da ANPD. Essas são tarefas essenciais para que a autoridade nacional atue como um órgão a serviço do cidadão. A autoridade será ainda um elo entre sociedade e governo, permitindo que as pessoas enviem dúvidas, sugestões, denúncias ligadas à LGPD para apuração. (SERPRO, 2020).

Também tem a função de informar e fazer com que a população tenha conhecimento das políticas de proteção aos dados, das práticas e dos direitos sobre

os dados, bem como estimular o entendimento das normas pelas empresas que fazem uso dos dados e informações pessoais.

Contudo, esta lei não se aplica quando se trata da coleta de dados realizada por pessoa natural para fins particulares. Também não se aplica a fins exclusivos, como (BRASIL, 2018):

- Jornalísticos e artísticos;
- Segurança pública;
- Defesa nacional;
- Segurança do Estado;
- Investigação e repressão de infrações penais;
- Particulares sem fins econômicos;
- Dados de fora do Brasil e que não sejam objeto de transferência internacional.

A LGPD está em vigor desde o final de 2020, entretanto, as sanções administrativas entraram em vigor em 01 de agosto de 2021**.** Os artigos 52, 53 e 54 da lei são os que tratam destas sanções, sendo assim, os que passam a valer integralmente a partir de agora. (BRASIL, 2021).

A aplicação das sanções irá depender de cada caso, pois será validado se a empresa em questão tem uma política de boas práticas e governança em relação ao vazamento de dados, se as medidas corretivas foram adotadas, além de levar em consideração a gravidade das infrações, condições econômicas e grau do dano, por exemplo.

A ANPD é o único órgão com autorização para aplicar as sanções administrativas da LGPD, embora já estejam agindo em parceria com outras entidades e órgãos da administração pública para exercer a fiscalização, como a Secretaria Nacional do Consumidor – SENACON e o Conselho Administrativo de Defesa Econômica – CADE. (SOFTWALL, 2021).

Conforme o art. 52 da LGPD, a ANPD pode aplicar as seguintes sanções administrativas. (BRASIL, 2021):

- Advertência, com indicação de prazo para adoção de medidas corretivas;
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício,

excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;

- Multa diária, observado o limite total a que se refere o inciso II;
- Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;
- 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;
- 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;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

As sanções administrativas mais graves, como proibição total do exercício das atividades da empresa, serão aplicadas apenas depois de penalizações menos intensas, como multas diárias ou divulgação pública da infração.

As sanções e multas só serão aplicadas depois do procedimento administrativo que permita uma ampla defesa e irá considerar os seguintes parâmetros e critérios de gravidade:

- A natureza das infrações e dos direitos pessoais afetados;
- A boa-fé;
- A vantagem auferida ou pretendida;
- A condição econômica do infrator;
- A reincidência;
- O grau do dano;
- A cooperação do infrator e adoção reiterada;
- A demonstração de mecanismos e procedimentos internos capazes de minimizar o dano e de medidas corretivas;
- A adoção de política de boas práticas e governança;
- A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

3. RISCOS

Um risco é a combinação das consequências que podem seguir após a ocorrência de um evento indesejado e da probabilidade da ocorrência deste. O processo de avaliação de riscos quantifica ou descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos. (ABNT NBR 27005).

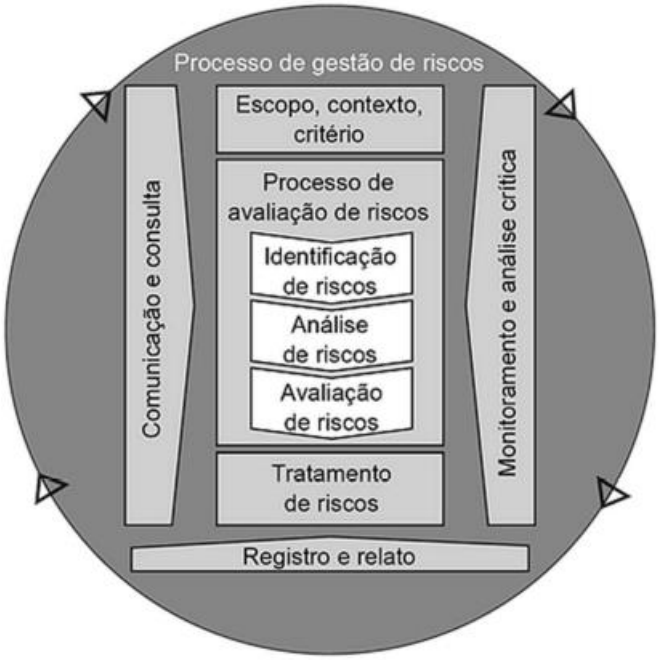
Identificar esses riscos tem por propósito determinar o que possa causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer.

As avaliações de risco é um componente central. O Art. 50º da LGPD estabelece que as organizações devem “levar em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos”. (BRASIL, 2018).

> Segundo Bezerra: “A gestão de riscos contribui para a realização demonstrável dos objetivos e para a melhoria do desempenho, referente à segurança e saúde das pessoas, à conformidade legal e regulatória, à aceitação pública, à proteção do meio ambiente, à qualidade do produto, ao gerenciamento de projetos, à eficiência nas operações, à governança e à reputação” (BEZERRA, 2013).

O processo de gestão de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes, identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e os ordena de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

Figura 2 - Processo de gestão de riscos



Fonte: ABNT NBR ISO/IEC 3100, 2018.

Na Figura 2 é demonstrado como é feito a gestão de risco de acordo com a ABNT NBR ISSO/IEC 3100, logo é um processo cíclico e continuo.

O processo começa com a comunicação e consulta, que visa auxiliar as partes interessadas pertinentes na compreensão do risco, na base sobre a qual decisões são tomadas e nas razões pelas quais ações específicas são requeridas.

Um dos princípios da gestão de riscos é que o processo de gerenciamento de riscos deve ser parte integrante de todos os processos organizacionais, para que isso possa ser concretizado. Um bom plano de comunicação deve ser planejado nas etapas iniciais.

A comunicação busca promover a conscientização e o entendimento do risco, enquanto a consulta envolve obter retorno e informação para auxiliar a tomada de decisão.

A identificação de riscos é definida como um processo para determinar o que, onde, quando, porque e como algo poderia ocorrer. A sua abordagem dependerá da natureza das atividades analisadas, dos tipos de riscos, do contexto e a sua finalidade no gerenciamento de riscos.

Um conjunto de riscos devem ser identificados, com o objetivo é gerar uma lista abrangente de riscos que possam criar, aumentar, evitar, reduzir, acelerar ou atrasar a realização dos objetivos. Um risco não identificado nesta fase, obviamente não será incluído em análises posteriores.

A tendência é que as organizações, com o tempo, passem a incrementar essa lista com novas fontes de risco, o processo deve melhorar continuamente.

A análise de riscos fornece uma compreensão sobre os riscos da organização. Tem como propósito compreender a natureza do risco e suas características, incluindo o nível de risco, onde apropriado. Envolve a consideração detalhada de incertezas, fontes de risco, consequências, probabilidade, eventos, cenários, controles e sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

Nessa etapa a organização deverá analisar todos os riscos identificados na etapa anterior, verificando quais são as consequências e probabilidade dos riscos, isso será insumo para a etapa posterior.

A Tabela a seguir, apresenta parâmetros escalares para se classificar os riscos identificados.

Quadro 1 – Parâmetros escalares

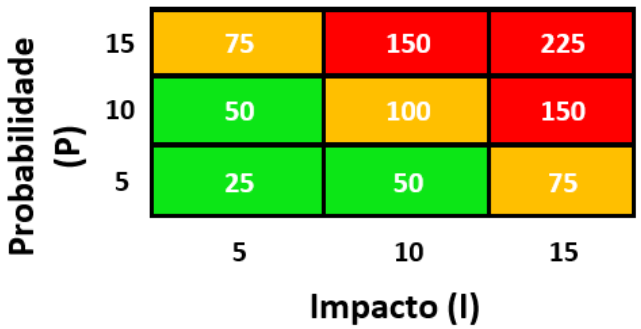
CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

Fonte: BRASIL (2020).

Esses parâmetros são utilizados para classificar o risco, atribuindo um valor gradual para cada faixa (Baixo, Moderado e Alto). Dessa forma, representam os níveis de probabilidade e impacto que, ao ser multiplicado tem como resultado o nível de risco que auxiliará na aplicação de medidas de segurança. (BRASIL, 2020).

Depois de cada risco ser classificado, é feito uma matriz que relaciona a probabilidade ou chance de algo acontecer com o impacto que possa causar. Ao multiplicar esses dois valores, obtém-se o nível de risco. (BRASIL, 2020).

Quadro 2 – Matriz de probabilidade X Impacto



Fonte: BRASIL (2020).

Sendo que verde é considerado baixo, amarelo de nível moderado e vermelho considerado alto. Dessa forma iremos para a próxima etapa.

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado. Essa é a hora de dizer, por exemplo, se um risco deve ou não ser tratado e como será a prioridade.

Segundo a ABNT NBR 31000 "O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes"

Aqui são implementados os planos de ação para tratamento dos riscos que em geral, podem ser:

- Redução da probabilidade de ocorrer;
- Evitados, não realizar a atividade;
- Remoção da fonte de risco;
- Aumentados, quando eles forem uma oportunidade (risco positivo);
- Compartilhados com terceiros (seguros por exemplo);
- Redução da consequência;
- Retidos por uma decisão bem consciente e embasada.

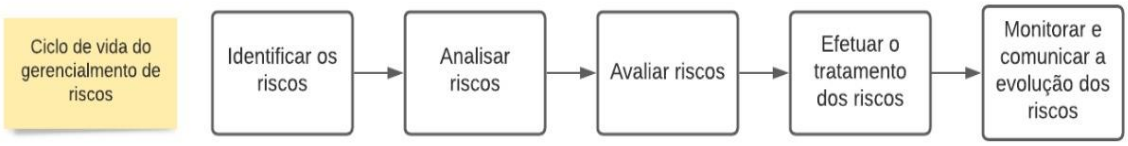
A melhoria contínua deverá acontecer ao longo do processo de gestão de riscos. Ao utilizar a metodologia os critérios de riscos poderão ser alterados, novas ocorrências poderão incrementar as listas de riscos e oportunidades poderão ser consideradas. O contexto interno e externo pode sofrer alterações e a organização aprender com seus sucessos e falhas.

4. PROPOSTA DE GERENCIAMENTO DE RISCO

Um processo de gerenciamento de riscos tem a finalidade de construir uma estrutura capaz de mitigar potenciais problemas. Dessa forma as organizações adquirem melhor capacidade para identificar eventos em potencial e estabelecer respostas, reduzindo surpresas e custos ou prejuízos associados, na qual demandam soluções rápidas para que suas consequências não prejudiquem o bom andamento da empresa. Com o advento da LGPD, o gerenciamento de riscos tornou-se fundamental para demonstrar *compliance* com a lei.

Esse capítulo apresenta uma proposta de um processo de gerenciamento de riscos que pode ser aplicado à LGPD. Este processo é composto por cinco atividades: Identificar os riscos, analisar riscos, avaliar riscos, efetuar tratamento dos riscos e monitorar e comunicar a evolução dos riscos.

Figura 3 – Ciclo de vida do Gerenciamentos de Riscos



Fonte: Autoria própria.

A seguir são apresentadas as atividades que compõem o processo de gerenciamento de risco.

4.1. IDENTIFICAR OS RISCOS

Identificação dos riscos mediante critérios, dentro do escopo e limites organizacionais. Os riscos devem ser identificados, quantificados e qualificados.

Diretrizes:

- Um risco é a combinação das consequências que podem seguir após a ocorrência de um evento indesejado e da probabilidade da ocorrência deste;
- O processo de risco deve apoiar os donos dos processos a avaliar os riscos de forma quantificadas ou descrever o risco qualitativamente e capacita os

gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

- Um ativo é algo que tem valor para a organização e que requer proteção.

Quadro 3 – Identifica os riscos

Objetivos:	• Identificar os riscos que podem causar uma perda potencial ou prejuízo em relação a dados pessoais. Devem ser incluídos os riscos que estão sob controle da organização ou não.
Tarefas:	• Identificar e ou revisar os processos, determinando o valor dos ativos de informação, ameaças e vulnerabilidades aplicáveis existentes; • Deve-se fazer uma análise detalhada que forneça informações suficientes para o processo de avaliação de riscos; • Para isso pode ser feito mais de uma iteração de análise dos processos; • Deve-se identificar o responsável pelo ativo. O responsável pelo ativo não precisa ser o dono, mas deve ser responsável ou pela sua produção, ou desenvolvimento, ou manutenção, utilização e segurança. Geralmente o dono do ativo é a pessoa mais habilitada para determinar o valor para a organização; • Identificar as ameaças aos ativos; • Identificação das consequências que a perda da confidencialidade, integridade e de disponibilidade possam ter sobre os ativos; • Definir os riscos a partir das tarefas anteriores.
Entradas:	**Critérios:** • Processos analisados com os respectivos ativos de dados pessoais.

<table>
<tr><td></td><td colspan="2">Produtos:
Mapeamento dos processos;
Identificação dos ativos de dados.</td></tr>
<tr><td rowspan="2">Saídas:</td><td colspan="2">Critérios:
Identificação dos ativos;
Identificação das consequências;
Lista de riscos aprovada.</td></tr>
<tr><td colspan="2">Produtos:
Identificação dos ativos;
Identificação das consequências dos riscos;
Lista de risco com o respectivo dono.</td></tr>
<tr><td rowspan="2">Participantes:</td><td>Responsável:
Dono do processo.</td><td>Aprovação:
DPO – Data Protection Officer.</td></tr>
<tr><td>Consultados:
Comitê LGPD.</td><td>Informados:
Todos os membros da Organização.</td></tr>
</table>

Fonte: Autoria própria.

4.2. ANALISAR RISCOS

Descreve a forma como o risco pode impactar a organização. Para isso é realizada uma análise qualitativa, quantitativa, avaliação das consequências, avaliação da probabilidade e pôr fim a determinação do nível do risco.

Quadro 4 – Analisa riscos

Objetivos:	• Analisar os riscos de forma a identificar as diferentes nuances que um risco pode ter quando se torna um problema. Para isso deve-se identificar a nível de criticidade dos ativos, a extensão das vulnerabilidades conhecidas e dos incidentes anteriores envolvendo a organização.
Tarefas:	• Fazer uma análise qualitativa do risco, com a finalidade de obter uma indicação geral do nível de risco e também para revelar os grandes riscos. Avaliar a magnitude potencial do risco; • Fazer uma avaliação quantitativa para dimensionar os grandes riscos. Nesse sentido verifica-se o impacto e a probabilidade de ocorrência do risco. Prioriza-se dados históricos de incidentes anteriores para se estabelecer os valores quantitativos; • Avaliar as consequências significa fazer uma valorização do ativo pela sua criticidade e sua importância para cumprimento dos objetivos para a organização; • Gerar a lista das consequências referentes ao cenário de risco estabelecido; • Avaliar a probabilidade dos incidentes. Deve-se identificar a ocorrência da percepção do nível de ameaça, da vulnerabilidade, controles existentes; • Definir o nível de risco, com a respectiva probabilidade de ocorrência, e impacto; • Priorizar os riscos conforme a avaliação da probabilidade e impacto.
Entradas:	**Critérios:** • Riscos identificados e lista de ativos aprovados.

<table>
<tr><td></td><td colspan="2">Produtos:
Lista de riscos.</td></tr>
<tr><td>Saídas:</td><td colspan="2">Critérios:
Riscos quantificados e qualificados;
Lista de riscos analisados com probabilidade e impacto identificados.</td></tr>
<tr><td rowspan="2">Participantes:</td><td>Responsável:
Dono do processo.</td><td>Aprovação:
Comitê LGPD.</td></tr>
<tr><td>Consultados:
Executores dos processos.</td><td>Informados:
Colaboradores.</td></tr>
</table>

Fonte: Autoria própria.

4.3. AVALIAR RISCOS

A avaliação de risco preocupa-se em definir, com base nos critérios de avaliação de riscos, as ações para tomada de decisão sobre os riscos.

Quadro 5 – Avalia riscos

Objetivos:	• Definir decisões sobre os riscos com base na avaliação do contexto apresentado na atividade análise de risco. As decisões tomadas durante a atividade de avaliação de riscos são baseadas principalmente no nível de risco aceitável;

<table>
<tr><td>Tarefas:</td><td colspan="2">Avaliar o nível de confiabilidade dos critérios utilizados para calcular a probabilidade de ocorrência do risco e consequências;
Analisar e agregar pequenos riscos que juntos podem resultar em um risco total bem mais significativo;
Avaliar a importância do processo de negócio ou da atividade suportada por um determinado ativo;
Classificar a importância dos riscos mediante sua probabilidade e impacto;
Definir lista de riscos com a priorização.</td></tr>
<tr><td rowspan="2">Entrada:</td><td colspan="2">Critérios:
Lista de riscos identificada, com probabilidade de ocorrência e impacto.</td></tr>
<tr><td colspan="2">Produtos:
Lista de riscos.</td></tr>
<tr><td rowspan="2">Saídas:</td><td colspan="2">Critérios:
Lista de riscos avaliada mediante critérios de impacto, criticidade e probabilidade de ocorrência.</td></tr>
<tr><td colspan="2">Produtos:
Lista de riscos priorizados.</td></tr>
<tr><td rowspan="2">Participantes:</td><td>Responsável:
Dono do processo.</td><td>Aprovação:
Comitê LGPD.</td></tr>
<tr><td>Consultados:
Executores dos processos.</td><td>Informados:
Colaboradores.</td></tr>
</table>

Fonte: Autoria própria.

4.4. EFETUAR TRATAMENTO DOS RISCOS

Consiste em efetuar ações para tratamento dos riscos. Consiste desde tomar ações que evitem a ocorrência do risco até o compartilhamento do risco com outros agentes.

Diretrizes:

Há quatro opções disponíveis para o tratamento de risco: modificação do risco, retenção do risco, ação de evitar o risco e compartilhamento do risco.

Quadro 6 – Efetua o tratamento dos riscos

Objetivos:	• Essa atividade tem por finalidade construir ações que causem grande modificação do risco com um pequeno nível de esforço. Com isso, proporcionando que as consequências adversas do risco sejam reduzidas ao mínimo possível.
Tarefas:	• Para cada risco identificado, definir as ações para eliminar o risco ou diminuir sua probabilidade de ocorrência; • Classificar as ações em: modificação do risco, retenção do risco, ação de evitar o risco e compartilhamento do risco. Essas ações não são mutuamente exclusivas; • Identificar as ações e os controles indicados para o tratamento dos riscos; • Modificar o risco. O nível de risco deve ser gerenciado por meio da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável; • Decidir sobre a Retenção do risco. Isso ocorre quando o nível do risco atende aos critérios para aceitação do risco. Quando isso ocorre não há necessidade de se implementar controles adicionais e pode haver a retenção

	do risco; • Efetuar ação de evitar o risco. Essa medida é tomada quando os cursos da implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja pela eliminação de uma atividade planejada ou existente, ou por mudanças nas condições em que a operação da atividade ocorre; • Compartilhamento do risco envolve a decisão de se compartilhar certos riscos com entidades externas. Pode ser feito mediante um seguro que cubra as consequências ou a subcontratação de um parceiro; • Aceitação dos riscos deve ser adotada, quando o risco pode ser acolhido pela organização; • Efetuar o planejamento do tratamento do risco; • Os riscos residuais precisam ser considerados até que ele seja considerado aceitável.
Entrada:	**Critérios:** • Lista de riscos priorizados de acordo com os critérios de avaliação de riscos.
	Produtos: • Lista de riscos.
Saídas:	**Critérios:** • Plano de gerenciamento de risco aprovado.
	Produtos: • Plano de gerenciamento de risco.

Participantes:	**Responsável:** Dono do processo.	**Aprovação:** Comitê LGPD.
	Consultados: Executores dos processos.	**Informados:** Colaboradores.

Fonte: Autoria própria.

4.5. MONITORAR E COMUNICAR A EVOLUÇÃO DOS RISCOS

Essa atividade consiste em monitorar os riscos identificados, atualizando sua probabilidade e impacto ao longo do ciclo de vida do risco. Também nessa atividade preocupa-se em manter as partes interessadas informadas sobre o nível desempenho dos riscos.

Quadro 7 – Monitora e comunica a evolução dos riscos

Objetivos:	• Essa atividade tem por finalidade comunicar as partes interessadas sobre o desempenho do risco. Desta forma o tomador de decisão se manterá informado sobre a evolução ou involução dos riscos.
Tarefas:	• Coletar informações sobre os riscos, identificando informações sobre os valores dos ativos, impactos, ameaças, vulnerabilidades, evolução do processo de probabilidade de ocorrência; • O monitoramento deve incluir: novos ativos, modificações necessárias sobre os valores dos ativos, novas ameaças, vulnerabilidades e/ou incidentes;

<table>
<tr><td></td><td colspan="2">Compartilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento do risco;
Evitar ou reduzir tanto a ocorrência quanto as consequências das violações da segurança e privacidade da informação que acontecem devido à falta de entendimento mútuo e os tomadores de decisão;
Fornecer informações e dar conhecimento para suportar o processo de tomada de decisão;
Informar a todos os colaboradores sobre o desempenho dos riscos a fim de ampliar o nível de conscientização;
Definir um plano de comunicação sobre os riscos.</td></tr>
<tr><td rowspan="2">Entrada:</td><td colspan="2">Critérios:
Lista de riscos com o respectivo impacto, probabilidade. prioridade e tratamento estabelecidos.</td></tr>
<tr><td colspan="2">Produtos:
Plano de riscos.</td></tr>
<tr><td rowspan="2">Saídas:</td><td colspan="2">Critérios:
Monitoramento e comunicação do desempenho dos riscos.</td></tr>
<tr><td colspan="2">Produtos:
Plano de comunicação
Relatório de monitoramento de riscos.</td></tr>
<tr><td>Participantes:</td><td>Responsável:
Dono do processo.</td><td>Aprovação:
Comitê LGPD.</td></tr>
</table>

	Consultados: Executores dos processos.	**Informados:** Colaboradores.

Fonte: Autoria própria.

O processo aqui proposto possui quatro papéis. Esses papéis participam das atividades do processo de gerenciamento de riscos. O quadro abaixo resume os principais aspectos relacionados a esses papéis e as respectivas responsabilidades.

Quadro 8 – Papéis e suas responsabilidades

Papel:	Composto por:	Responsabilidade:	Quando Acionar:
Dono do processo.	Executor do processo.	Definir, avaliar e monitorar os riscos.	Sempre.
Comitê LGPD.	Composto por pelo menos uma pessoa de cada departamento mais um elemento da diretoria.	Definir ações para mitigar os riscos.	Quando a gravidade do risco for classificada como Alta.
Encarregado pelo Tratamento de Dados Pessoais (DPO)	Profissional externo a organização.	Responsável por encaminhar comunicações formais, fomentar a cultura e a disseminação e conhecimento do programa ou processo de segurança de informação	Sempre que ocorrer uma elevação do nível de risco.
Diretor.	Diretores da Decisão.	Responsável pela tomada de decisão, alocação de recursos	Conforme a classificação do risco.

Fonte: Autoria própria.

5. CONCLUSÕES E TRABALHOS FUTUROS

Este trabalho apresenta uma proposta de processo de gerenciamento de riscos com base na LGPD, em que se utilizou técnicas e um modelo de gerenciamento de riscos, que combinadas podem afirmar o compromisso com a privacidade e proteção dos dados pessoais.

O gerenciamento de riscos, é uma estratégia que age, de forma preventiva, quando se antecipa a uma série de situações negativas. Essa prevenção faz com que os eventos sejam anulados ou minimizados, para que as organizações estejam preparadas para lidar com as possíveis adversidades da melhor forma possível.

A concretização do risco pode causar prejuízo direto aos titulares de dados pessoais e indiretos à própria organização quando for responsabilizada pelos danos causados. Um dos pontos abordados pela lei, e também um dos pontos de maior importância, é a segurança e privacidade do titular desses dados.

Pois são a identidade de uma pessoa e não existe bem maior do que a nossa identidade. Ela é intransferível e, sobretudo, inestimável. Em razão disso, os dados pessoais são o maior bem de um indivíduo.

Entre as contribuições deste trabalho estão o estudo da Lei Geral de Proteção de Dados Pessoais e uma proposta de gerenciamento de riscos, além da abertura de novos caminhos para futuras pesquisas a serem aplicadas.

Conclui-se a importância do gerenciamento de riscos para todas as áreas das empresas, principalmente se tratando de dados pessoais. Cada empresa precisa tentar mensurar como poderá extrair ao máximo de benefícios do gerenciamento de riscos.

É importante que as empresas façam um estudo e o devido planejamento para a implantação dos itens necessários para se fortalecer e manter-se competitivo no novo cenário que a LGPD está trazendo, que é essencial para a construção do respeito à identidade e privacidade dos indivíduos.

Uma organização que não garanta a privacidade dos dados pessoais pode sofrer prejuízos muito maiores do que o financeiro. Pode perder sua credibilidade no mercado, a confiança dos consumidores e a força da sua marca.

5.1. TRABALHOS FUTUROS

Sugestões para trabalhos futuros incluem a aplicação do processo em situações reais de empresas para ver sua efetividade, desenvolver uma ferramenta que auxilie no processo gerenciamento de riscos e na realização de um estudo completo dos dados pessoais.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 31000 - Gestão de riscos — Diretrizes. Rio de Janeiro. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR 29134 - Tecnologia da informação — Avaliação de impacto de privacidade — Diretrizes. Rio de Janeiro, 2020.

ABEINFO. Brasil sofre mais de 16,2 bilhões de tentativas de ataques cibernéticos na primeira metade de 2021. Disponível em: <https://abeinfobrasil.com.br/brasil-sofre-mais-de-162-bilhoes-de-tentativas-de-ataques-ciberneticos-na-primeira-metade-de-2021/> Acesso em: 29 set. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. GUIA ORIENTATIVO PARA DEFINIÇÕES DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS E DO ENCARREGADO, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf>. Acesso em: 03 jun. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. Sanções Administrativas: o que muda após 1º de agosto de 2021?, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 01 nov. 2021.

BRASIL. Autoridade Nacional de Proteção de Dados. Sanções Administrativas: o que muda após 1º de agosto de 2021?. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 01 ago. 2021.

BEZERRA, Edson Kowask. ABNT NBR 27005 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. Rio de Janeiro: RNP/ESP, 2013.

BRASIL. Governo Digital. Guia de Avaliação de Riscos de Segurança e Privacidade. Disponível em:<https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf>. Acesso em: 01 jun. 2021.

BRASIL. Ministério da Cidadania. Classificação dos Dados, 2021. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados>. Acesso em: 05 maio 2021.

BRASIL. Ministério da Cidadania. Direitos do(a) Titular, 2021. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/direitos-do-titular>. Acesso em: 05 maio 2021.

BRASIL. Ministério da Cidadania. Encarregado da LGPD, 2021. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/encarregado-da-lgpd>. Acesso em: 05 maio 2021

BRASIL. Presidência da República. Secretária-geral. Subchefia para Assuntos Jurídicos. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018., 2018. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato20152018/2018/lei/L13709compilado.htm>. Acesso em: 01 maio 2021.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. Revista de Direito Brasileira, [S.l.], v. 23, n. 9, p. 284-301, fev. 2020. ISSN 2358-1352. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343>. Acesso em: 09 nov. 2021.

NASCIMENTO, Arthur Braga. Principais Desafios da LGPD, 2021. Disponível em: <https://valorinveste.globo.com/blogs/seu-negocio/post/2021/12/principais-desafios-da-lgpd.ghtml>. Acesso em: 07 dez. 2021.

NASCIMENTO, Arthur Braga. A Era de Dados e o impacto da LGPD nos negócios, 2021. Disponível em: <https://valorinveste.globo.com/blogs/seu-negocio/post/2021/10/a-era-de-dados-e-o-impacto-da-lgpd-nos-negocios.ghtml>. Acesso em: 11 dez. 2021.

SERPRO. OBJETIVO E ABRANGÊNCIA DA LGPD, 2020. Disponível em: <https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd>. Acesso em: 01 nov. 2021.

NÉGOCIO SEGURO. SEGURO CIBERNÉTICO: O QUE É E COMO SE PROTEGER DESSES RISCOS?. Disponível em: <https://www.negocioseguroaig.com.br/industria/de-olho/seguro-cibernetico/>. Acesso em: 10 dez. 2021.

PEREIRA, Olimpo. A LGPD e a alfabetização em dados. Disponível em: <https://www.oconsumerista.com.br/2020/01/lgpd-alfabetizacao-dados/>. Acesso em: 15 jul. 2021.

PMI. Um guia do conhecimento em gerenciamento de projetos. Guia PMBOK, 6ª. Ed. EUA: Project Management Institute, 2017.

SERVICE IT. A importância da avaliação de riscos no processo de adequação à LGPD. Disponível em: <https://www.service.com.br/a-importancia-da-avaliacao-de-riscos-no-processo-de-adequacao-a-lgpd/>. Acesso em: 03 set. 2021.

SERPRO. QUEM VAI REGULAR A LGPD?, 2020. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 03 set. 2021.

SOFTWALL. Sanções administrativas da LGPD entram em vigor; entenda o que muda, 2021. Disponível em: <https://www.softwall.com.br/blog/sancoes-administrativas-da-lgpd/>. Acesso em: 01 set. 2021.

TEXEIRA, Alvaro. O que é ANPD? [Autoridade Nacional de Proteção de Dados], 2020. Disponível em: <https://tecnoblog.net/409033/o-que-e-anpd-autoridade-nacional-de-protecao-de-dados/>. Acesso em: 03 set. 2021.

ANEXO A - TEMPLATE PLANO DE GERENCIAMENTO DOS RISCOS

Controle de Versões			
Versão	**Data**	**Autor**	**Notas da Revisão**

- Objetivo do Plano de Gerenciamento dos Riscos

[Descreva o objetivo do Plano de gerenciamento dos riscos.]

Gerenciar os riscos do projeto requer um Plano de gerenciamento dos riscos descrevendo como os processos de riscos serão estruturados e executados iniciando pela identificação dos riscos, análise de risco, avaliação dos riscos, tratamento dos riscos, monitorar e comunicar evolução dos riscos.

O Plano de gerenciamento dos riscos é desenvolvido e aprovado durante a fase de planejamento do projeto e é um plano auxiliar do Plano de gerenciamento do projeto.

Tem como objetivo aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto e orientar a equipe do projeto sobre como os processos de riscos serão executados.

- Gerenciamento dos Riscos

[Use as seções seguintes para identificar os componentes do Plano de gerenciamento dos riscos ou modifique-as para encontrar suas necessidades.]

- Processos de Riscos

[Descreva os Processos de Gerenciamento dos riscos a serem adotados no projeto.]

- Identificar os riscos

Determinar quais riscos podem afetar o projeto e documentar suas características.

- Analisar os riscos

Avaliar a exposição ao risco para priorizar os riscos que serão objetos de análise ou ação adicional.

Efetuar a análise numérica do efeito dos riscos identificados nos objetivos gerais do projeto.

- Avaliar os riscos

Definir, com base nos critérios de avaliação de riscos, as ações para tomada de decisão sobre os riscos.

- Efetuar o Tratamento dos Riscos

Implementar as respostas planejadas em Planejar as respostas aos riscos

- Monitorar e Comunicar os Riscos

Monitorar e manter as partes interessadas informadas sobre o nível desempenho dos riscos,

durante o ciclo de vida do projeto.

- Documentos Padronizados de Risco

[Descreva os documentos padronizados a serem usadas nos processos dos riscos. Indique onde estão armazenados, como serão usados, e os responsáveis envolvidos.]
[Exemplo:

Documento	Descrição	Template
Plano de gerenciamento dos riscos	O Plano de Gerenciamento dos riscos tem como objetivo aumentar a probabilidade e o impacto dos eventos	Plano de gerenciamento

	positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto e orientar a equipe do projeto sobre como os processos de riscos serão executados.	dos riscos.docx
Registro dos riscos	O registro dos riscos é iniciado no processo identificar os riscos e é atualizado conforme os outros processos de gerenciamento dos riscos (análise qualitativa, quantitativa, planejar as respostas aos riscos e monitorar e controlar os riscos) são conduzidos, resultando em um aumento no nível e no tipo de informações contidas no registro dos riscos ao longo do tempo.	Registro dos riscos.xlsx

- Responsabilidades dos Riscos da Equipe do Projeto

[Descreva as responsabilidades referentes aos processos dos riscos de cada membro do projeto, mesmo que já citados em outros tópicos do documento. Ressaltar as divisões de responsabilidade entre compras, projetos e jurídico.]
[Exemplo:

Membro da Equipe	Responsabilidades
GP	Certificar que os riscos foram identificados e tratados de modo a aumentar a probabilidade e o impacto dos eventos positivos, reduzir a probabilidade e o impacto dos eventos negativos no projeto. Monitorar os riscos conforme descrito neste plano. Divulgar informações pertinentes aos riscos do projeto
Advogado	Assessorar juridicamente o GP em relação às decisões contratuais relacionadas aos riscos

Patrocinador/Comitê do Projeto	Aprovar o plano de gerenciamento de riscos e suas reservas de contingências. Aprovar o uso das reservas de contingência.

Membro da Equipe	Responsabilidades

- Ferramentas Usadas

[Lista as ferramentas que o projeto empregará. Descreve como serão usadas e o responsável por isso. Saiba mais em Ferramentas de Riscos do Guia PMBOK®.]
[Exemplo:

Ferramenta	Descrição da aplicação	Quando aplicar	Responsável
Brainstorming	Será usado para identificar riscos	No início do projeto e sempre que for necessário revisar os riscos identificados	Gerente do Projeto

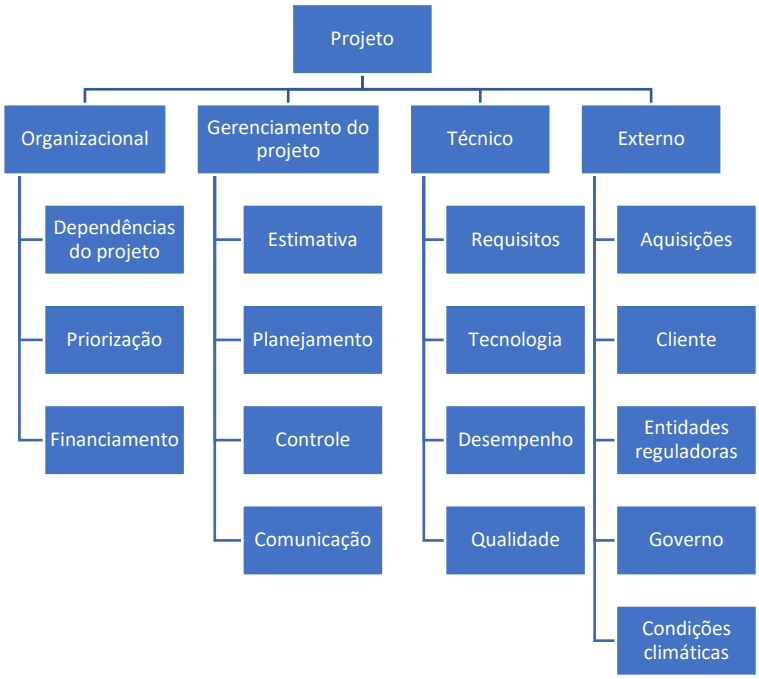
- Identificar os Riscos

[Descreva como os riscos serão determinados e documentados. Saiba mais em Identificar os riscos.]
[Exemplo:
- Será usado o Brainstorming para identificar os riscos do projeto.

O Gerente de projetos deverá compor uma equipe multidisciplinar para participar do brainstorming de modo que todas as áreas estejam bem representadas e que os riscos principais do projeto sejam identificados.

- EAR (Estrutura Analítica dos Riscos)

[Determinar as categorias e subcategorias de riscos e melhor forma de agrupá-las de modo a facilitar seu gerenciamento.]
Exemplo:



- Riscos

[Riscos identificados e como serão tratados (Tipos de Contrato, Cláusulas, Requisitos de bônus de desempenho, seguros, ...).]
[Exemplo:
Os riscos estão detalhados no Registro dos riscos.]

- Realizar a Análise dos Riscos

[Descreva como será feita a análise qualitativa dos riscos.]

- Definições de Probabilidade e Impacto dos Riscos

[Definir como será feio a Avaliação de probabilidade e impacto dos riscos.]

Probabilidade	% de certeza
1-Muito baixa	0 a 20%
2-Baixa	20 a 40%
3-Média	40 a 60%
4-Alta	60 a 80%
5-Muito Alta	> 80%

Impacto
1-Muito baixo
2-Baixo
3-Médio
4-Alto
5-Muito Alto

O impacto varia de acordo com a área impactada. Veja o quadro abaixo orientando como classificar o impacto.

Quando um risco impactar mais de uma área, deverá ser usada a área mais impactada.

	Muito baixo (Nota = 1)	**Baixo (Nota = 2)**	**Médio (Nota = 3)**	**Alto (Nota = 4)**	**Muito alto (Nota = 5)**

Custo	Até 2% no orçamento	De 2 a 5% no orçamento	De 5 a 8% no orçamento	De 8 a 10% no orçamento	Acima de 10% no orçamento
Tempo	Até 2% no prazo total	De 2 a 5% no prazo	De 5 a 8% no prazo	De 8 a 10% no prazo	Acima de 10% no prazo
Escopo		Mudança impactará no custo	Mudança impactará no custo e no tempo	Mudança impactará no custo, tempo e qualidade	

O grau do risco (G = I * P) está definido na matriz de probabilidade x impacto demonstrada abaixo.

Matriz de Probabilidade X Impacto

Probabilidade					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Impacto	1	2	3	4	5

Os graus de riscos serão priorizados da seguinte forma:

- Vermelho: risco elevado;
- Amarelo: risco médio;
- Verde: risco baixo.

- Avaliar os Riscos

[Descreva como será feita a avaliação dos riscos.]

- Efetuar o tratamento dos riscos

[Descreva como os riscos serão tratados e como serão determinadas as respostas aos riscos. Saiba mais em Planejar as respostas aos riscos.]

- Estratégias para Riscos Negativos ou Ameaças

[Identificar as Estratégias para riscos negativos ou ameaças.]

Estratégia	Descrição	Exemplo
Eliminar	Remover em 100% a probabilidade que a ameaça ocorra.	Cancelar o projeto;
Transferir	Transferir total ou parcial o impacto em relação a uma ameaça para um terceiro.	Fazer um seguro;
Mitigar	Reduzir a probabilidade e/ou impacto de um risco.	Redundância de recursos;
Aceitar	De forma ativa, estabelecendo plano de contingência caso o evento ocorra; ou de forma passiva, o risco será tratado quando ocorrer.	

- Estratégias para Riscos Positivos ou Oportunidades

[Identificar as Estratégias para riscos positivos ou oportunidades.]

Estratégia	Descrição
Explorar	Garantir que a oportunidade ocorra para explorar seus benefícios;
Compartilhar	Transferir total ou parcial a propriedade da oportunidade para um terceiro que tem maior capacidade de explorá-la;
Melhorar	Aumentar probabilidade e/ou impacto de uma oportunidade;
Aceitar	Tirar proveito caso a oportunidade ocorra.

- Monitorar e Comunicar Evolução dos Riscos

[Descreva como os riscos serão monitorados e controlados. Saiba mais em Controlar os riscos.]
[Exemplo:

O GP e os responsáveis definidos na matriz de responsabilidade devem acompanhar os riscos identificados, monitorar os riscos residuais, identificar novos riscos, executar os planos de respostas a riscos e avaliar sua eficácia durante todo o ciclo de vida do projeto.

O gerente de projeto executa o que foi planejado na análise de riscos e controla os riscos novos identificados durante a execução do projeto.

Este processo consiste de:

- Identificar, analisar, e planejar para riscos novos;
- Monitorar os riscos identificados;
- Analisar novamente os riscos existentes de acordo com as mudanças de contexto;
- Monitorar condições para ativar planos de contingência;
- Monitorar riscos residuais;
- Rever a execução do plano de respostas aos riscos para avaliar sua eficácia;
- Determina se as premissas do projeto ainda são válidas;
- Determinar se as políticas e os procedimentos de gestão de risco estão sendo seguidas;
- Determinar se as reservas de contingência de custo e prazo devem ser modificadas com os riscos do projeto.

CheckList

Implementar a análise de risco aprovada.

Identificar novos riscos e gerenciá-los adequadamente.

Atualizar o plano de resposta de riscos com os riscos novos.

Incluir um sumário dos riscos nas reuniões de status.

Revisar todos os documentos impactados.

Conduzir sessões para avaliar os riscos se necessário.

Aprovações		
Participante	**Assinatura**	**Data**
Patrocinador do Projeto		
Gerente do Projeto		