UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ADMINISTRAÇÃO
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS

MARIA PAULA MILLÃO GRAEF

O GERENCIAMENTO DE RISCOS E O SEU PAPEL NA PROTEÇÃO DE DADOS

Porto Alegre, RS
2022

MARIA PAULA MILLÃO GRAEF

O GERENCIAMENTO DE RISCOS E O SEU PAPEL NA PROTEÇÃO DE DADOS

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientadora: Profª. Drª. Daniela Francisco Brauner

Porto Alegre, RS

2022

MARIA PAULA MILLÃO GRAEF

O GERENCIAMENTO DE RISCOS E O SEU PAPEL NA PROTEÇÃO DE DADOS

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientadora: Profª. Drª. Daniela Francisco Brauner

Conceito Final: A

Aprovado em: 05/10/2022

BANCA EXAMINADORA:

_____

Orientadora Profª. Dr.ª Daniela Francisco Brauner – Escola de Administração UFRGS

_____

Profª. Dr.ª Raquel Janissek-Muniz - Escola de Administração UFRGS

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus, pela minha vida, e por me permitir ultrapassar todos os obstáculos encontrados até o presente momento.

À Escola de Administração da UFRGS, responsável pelo meu processo de formação profissional, pelas portas abertas, e por tudo o que aprendi ao longo dos anos do curso.

À Profª. Drª. Daniela Francisco Brauner, por ter sido minha orientadora e ter desempenhado tal função com dedicação e excelência.

Às minhas queridas colegas e amigas Antonielle Braga da Cunha e Bruna Cristina Souza de Oliveira, pela amizade, companheirismo e apoio durante estes cinco anos de graduação.

Agradeço ao meu marido Juliano Corrêa Melo, por me incentivar nos momentos mais difíceis e acreditar em mim até mesmo quando eu não acreditei. Por compreender a minha ausência enquanto eu me dedicava à finalização da faculdade. Cada dia que passa tenho mais certeza que escolhi a pessoa certa para ter ao meu lado. Juliano, a vida contigo é muito mais bonita! O meu amor é, e sempre será teu!

E, principalmente, a minha mãe Luzia Fernandes Millão, por ter disposto dos seus conhecimentos acadêmicos para me ajudar na construção deste projeto, e de sua sabedoria para garantir que eu sempre seguisse em frente. Agradeço por ser minha maior incentivadora, por sempre ter me direcionado pelo caminho certo e por, sozinha, ter me proporcionado a melhor criação e as melhores oportunidades. Tudo o que conquistei até hoje foi por ela e graças a ela. Mãe, és o meu maior orgulho e minha maior inspiração, te amo muito e obrigada por tudo.

RESUMO

Com o desenvolvimento e disseminação das tecnologias de informação e comunicação, o uso de dados tornou-se essencial para apoio a tomada de decisão das organizações. Para proteger as pessoas do uso abusivo e não informado dos seus dados, o uso de dados pessoais passou regulado com a implantação recente de leis de proteção de dados. A Lei Geral de Proteção de Dados (LGPD) existe no Brasil desde 2018, e as organizações ainda estão passando pelo período de adequação. O gerenciamento de riscos é utilizado nas organizações para evitar que eventos disruptivos façam com que riscos se materializem, expondo a organização. Por esta razão, a aplicação do gerenciamento de riscos à adequação de processos para a proteção de dados nas organizações deve ser considerada. O objetivo do trabalho é analisar como as ferramentas de gerenciamento de riscos podem beneficiar o processo de proteção de dados em uma empresa de tecnologia especializada em meios de pagamento do Rio Grande do Sul. Na metodologia utilizou-se a revisão sistemática da literatura e uma pesquisa descritiva qualitativa com análise da aplicação das ferramentas de gerenciamento de riscos a proteção de dados em uma organização que já implementou o seu uso. A análise da empresa foi feita por meio de 4 entrevistas, a primeira com o gestor que fez a implantação e com colaboradores de três áreas, que tiveram seus processos impactados pela adoção das ferramentas de gerenciamento de riscos corporativos para proteção de dados. Como resultado da revisão sistemática foram selecionados 10 artigos, a respeito da aplicação do gerenciamento de risco a proteção de dados, principalmente, através de ferramentas de gerenciamento de riscos, que se destacaram no âmbito da proteção de dados. Três ferramentas destacaram-se como eficientes na revisão sistemática, o ROPA/DPIA, Matriz de Riscos e Controles e Análise de Vulnerabilidades. Em concordância, através das entrevistas foi possível verificar que a empresa analisada aplica as três ferramentas em seus processos. Assim, conclui-se que a utilização de sistemas de automatização torna as ferramentas de gerenciamento de riscos ainda mais eficientes no âmbito de proteção de dados.

Palavras-chave: Proteção de Dados. Gerenciamento de Riscos. LGPD. Informação.

ABSTRACT

With the development and spread of information and communication technologies, the use of data has become essential to support organizations' decision-making. To protect individuals from abusive and uninformed use of their data, the use of personal data has become regulated with the recent implementation of data protection laws. The General Data Protection Law (LGPD) has existed in Brazil since 2018, and organizations are still going through the compliance period. Risk management is used in organizations to prevent disruptive events from causing risks to materialize, exposing the organization. For this reason, the application of risk management to the adequacy of processes for data protection in organizations should be considered. The objective of this paper is to analyze how risk management tools can benefit the data protection process in a technology company specialized in means of payment in Rio Grande do Sul. The methodology used a systematic literature review and a qualitative descriptive research with analysis of the application of risk management tools to data protection in an organization that has already implemented its use. The analysis of the company was done through 4 interviews, the first with the manager who did the implementation and with employees from three areas, who had their processes impacted by the adoption of enterprise risk management tools for data protection. As a result of the systematic review, 10 articles were selected regarding the application of risk management to data protection, mainly through risk management tools, which stood out in the scope of data protection. Three tools stood out as efficient in the systematic review, ROPA/DPIA, Risk and Control Matrix and Vulnerability Analysis. In agreement, through the interviews it was possible to verify that the analyzed company applies the three tools in its processes. Thus, it is concluded that the use of automation systems makes the risk management tools even more efficient in the field of data protection.

Keywords: Data Protection. Risk Management. LGPD. Information.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ACPRM	*Automed Cyber and Privacy Risk Management*
ANDP	Agência Nacional de Proteção de Dados
BACEN	Banco Central do Brasil
CFA	Conselho Federal de Administração
CICA	*Canadian Institute of Chartered Accountants*
CMN	Conselho Monetário Nacional
CNIL	*Commission Nationale Informatique & Libertés*
COBIT	*Control Objectives for Information and related Technology*
CoCo	*Criteria of Control*
COSO	*Committee of Sponsoring Organizations*
CRO	*Chief Risk Officer*
DOAJ	*Directory of Open Acess Journal*
DPIA	*Data Protection Impact Assessment*
DPIAF	*Data Protection Impact Assessment Framework*
ENISA	*The European Union Agency for Cyber Security*
ERM	*Enterprise Risk Management*
EUA	Estados Unidos da América
GDPR	*General Data Protection Regulation*
IBGC	Instituto Brasileiro de Governança Corporativa
IIA	*Institute of Internal Auditors*
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
NBR	Norma Brasileira
PCAOB	*Public Company Accounting Oversight Board*
PIA	*Privacy Impact Assessment*
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*
RFID	*Radio-Frequency Identification*
ROPA	*Record of Processing Activities*
RS	*Rio Grande do Sul*
RSL	Revisão Sistemática da Literatura
SCFCJ	*Freedom Collection Journal*
SIAK	Sistema de Informação da Administração da População
SPRs	Entidade de Propósito Específico
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

Com o desenvolvimento e disseminação das tecnologias de informação e comunicação, o uso de dados tornou-se essencial para apoio a tomada de decisão (PROVOST; FAWCETT, 2013). Os dados sobre os clientes passaram a ser um ativo de grande valor para as organizações (ROGERS, 2019). A partir do conhecimento dos dados dos clientes é possível estabelecer comportamentos de consumo, saber sobre as necessidades de cada um, criar estratégias de mercado mais eficientes, entre várias outras informações privilegiadas, que muitas vezes não é de interesse do titular dos dados que sejam divulgadas, que normalmente são captadas através de redes sociais e cadastros realizados virtualmente (ROGERS, 2019).

A coleta de dados sobre clientes pelas organizações requer atenção especial, pois envolve dados pessoais e sensíveis. O uso de dados pessoais passou a ser regulado com a implantação das leis na Europa e Estados Unidos (EUA), em 2018, quando passou a vigorar o Regulamento Geral de Proteção de Dados, a GDPR (FERREIRA et al., 2018).

A legislação existente no Brasil, até então, ficou defasada por contemplar de forma geral o uso consciente da internet. Concomitante, com recente entrada em vigor da GDPR, se fez necessário a criação de uma legislação específica para controlar o uso e tratamento dos dados pessoais no Brasil, assim o Marco Cível da Internet foi alterado para a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que tem como principal objetivo “proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (BRASIL, 2018, p.1).

De acordo com o Conselho Federal de Administração (CFA), é uma organização sem fins lucrativos, que regulamenta os profissionais formados em Administração. Um dos casos mais famosos que antecede e que influenciou a criação da legislação foi a exposição do caso envolvendo a empresa Cambridge Analytica. Esta empresa dos Estados Unidos, em 2018, fez uso indevido dos dados de 50 milhões de pessoas com objetivo de influenciar as eleições americanas através do direcionamento de propagandas políticas (AHRENS, 2018). Em 2019, a Lei nº 13.709/2018 foi alterada pela Lei nº 13.853/2019, que estabeleceu a sigla LGPD e regulamentou a criação da Autoridade Nacional de Proteção de Dados, a ANPD (BRASIL, 2019).

Com a nova LGPD, o tema de proteção de dados necessita de mais atenção para o cumprimento das obrigações relacionadas à proteção de dados pessoais por parte das organizações. Especialmente aquelas que coletam e fazem de dados. O gerenciamento de riscos é apresentado como uma destas obrigações.

O gerenciamento de riscos é um conjunto de estruturas padronizadas que tem como objetivo realizar a identificação e a gestão dos riscos, assim como a mensuração, da probabilidade de ocorrência e do impacto que cada risco materializado pode gerar a organização (VESCO et al., 2014). Seus componentes visam construir os processos de controle, e objetiva detectar e gerir eventos que possam atingir negativamente a organização (ZONATTO; BEUREN, 2012).

Em concordância, Luiz, Beuren e Cortes (2020) definiram que o gerenciamento de riscos “envolve aplicação coordenada e econômica de recursos para mitigar a probabilidade ou o impacto de eventos negativos, ou para maximizar a realização de oportunidades” (LUIZ; BEUREN; CORTES, 2020, p. 4).

Gerenciar risco significa gerenciar a possibilidade de perdas e redução de lucros, e, como o risco é um fator adverso, deve ser controlado mediante análise dos objetivos da empresa, bem como sua propensão ao risco, sendo uma das premissas para a gestão baseada em risco (ZONATTO; BEUREN, 2012; FAÇANHA et al., 2020).

De acordo com o Tribunal de Contas da União (TCU, 2022), o gerenciamento de riscos é um processo essencial para as organizações que buscam realizar o controle e a mitigação de riscos. Com base na NBR ISO 31000:2009, Norma Brasileira de Gestão de Riscos – Princípio e Diretrizes, é possível definir risco como a combinação entre a possibilidade de um evento (acontecimento) ocorrer e as consequências (perdas ou ganhos) que podem resultar da sua ocorrência. O risco está sempre associado ao futuro e as suas incertezas, resultando na impossibilidade de avaliar ou prever a ocorrência de determinados fatos com certeza e segurança (ABNT, 2009).

O *Committee of Sponsoring Organizations of the Treadway Commission*, (COSO) é uma organização sem fins lucrativos criada nos EUA, com o objetivo de prevenir e evitar fraudes nos relatórios financeiros das instituições. O COSO é o modelo de referência mais utilizado no mundo para o gerenciamento de riscos e controles internos das organizações.

Para o COSO (2007), o gerenciamento de risco é definido como:

> [...] um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização e possibilitar garantia razoável do cumprimento dos seus objetivos. (COSO, 2007, p. 4)

De acordo com Marques, Muller e Silva (2019), com base na definição do COSO, é possível perceber que a gestão de riscos corporativa envolve a organização em todos os seus níveis, e na elaboração de toda a sua estratégia. Por possuir grande abrangência dentro da organização, o gerenciamento de riscos também precisa se fazer presente na gestão de proteção de dados, pois as estratégias das empresas precisam se adequar à nova realidade.

O gerenciamento de riscos é regulamentado no Brasil para empresas autorizadas a funcionar pelo Banco Central do Brasil (BACEN). O BACEN, na Resolução nº 4.557, de 2017, surgiu a fim de complementar a Circular nº 3.681, de 2013, a qual foi alterada pela Resolução BCB nº 25, de 22 de outubro de 2020, por fim, assim como já supracitado na Norma Brasileira de Gestão de Riscos – Princípios e Diretrizes, NBR ISO 31000:2009 (BRASIL, 2009).

Com o surgimento das leis de proteção de dados verifica-se que o gerenciamento de riscos se torna essencial na estratégia organizacional para apoiar a adequação à LGPD. O COSO (2007) apresenta os principais objetivos que gerenciamento de risco visa alcançar, são divididos em quatro categorias: estratégicos, operações, comunicação e conformidade. O último objetivo está relacionado a estar de acordo com ao cumprimento da legislação e regulamentação aplicável. Portanto, utilizar o gerenciamento de riscos aplicado a proteção de dados, com objetivo de deixar a organização aderente à LGPD, é uma estratégia inteligente.

Em concordância com o tema, o artigo 37, da LGPD, afirma que é obrigatória para organizações que controlam e operam com dados pessoais, a realização do gerenciamento de riscos, a fim de evitar e mitigar incidentes. De acordo com Kuner et al. (2015), o gerenciamento de riscos para a proteção de dados é uma disciplina chave a ser utilizada como ferramenta para a gestão de proteção de dados e, consequentemente, adequação das organizações à LGPD.

A LGPD apresenta em vários artigos a existência de riscos e a importância da sua avaliação para evitar possíveis consequências ao titular dos dados e a organização. Contudo, não existe uma definição de risco na legislação, pois, conforme Gomes (2020), foi uma decisão correta baseada no fato de que o conceito específico

de riscos na proteção de dados não é definido de forma concreta. Portanto, não é possível desassociar o risco em proteção de dados das ferramentas de gerenciamento de riscos já existentes.

Os temas gerenciamento de riscos e proteção de dados são relacionados também na literatura acadêmica. Marinho (2020) descreve oito itens para a melhor adequação das exigências da LGPD. No primeiro item, é de suma importância estabelecer uma estrutura de governança corporativa, e que é necessário incorporar a gestão de riscos de proteção de dados à estrutura de gerenciamento de riscos corporativos e controles internos da organização.

Os dois temas passaram a ser interligadas com a chegada da LGPD, em 2018. Para Gomes (2020), a capacidade de avaliação dos riscos, e, consequentemente, sua gestão, é imprescindível para que a organização esteja alinhada com a lei, e ainda afirma que existe certa dificuldade em compreender a noção de risco para LGPD. Já para Kuner et al. (2015) e Gellert (2017), a gestão de risco é uma ferramenta necessária no âmbito da proteção de dados. Por isso realizar uma revisão sistemática sobre esse tema, torna-se extremamente relevante para sistematizar o conhecimento nesta área (KUNER et al., 2015; GELLERT, 2017; GOMES, 2020).

A CNN Brasil (CORACCINI, 2021) apresentou uma pesquisa feita pela RD Station, empresa de tecnologia e marketing digital, realizada em agosto de 2021, mês em que iniciaram as sanções para o descumprimento das exigências da LGPD, apenas 15% das empresas analisadas estavam aderentes ou na finalização do processo de preparação para ficar de acordo com a lei. De acordo com a CNN Brasil, as multas que serão aplicadas podem atingir 2% das receitas da empresa com o limite de 50 milhões. Essa situação é ainda pior para as pequenas empresas, que ainda não tem conhecimento de todas as aplicações da lei.

Considerando que a legislação de proteção de dados enfatiza a necessidade da realização de gerenciamento de riscos e os relatos das dificuldades encontradas pelas empresas em ficarem aderentes a LGPD, torna-se interessante entender como as ferramentas de gerenciamento de riscos beneficiam os processos de proteção de dados nas organizações.

Assim, considerando as informações trazidas e a relevância do tema para as organizações que ainda estão se adaptando a nova realidade de proteção de dados, surge a seguinte questão de pesquisa: Como as ferramentas de gerenciamento de riscos beneficiam o processo de proteção de dados em uma empresa de tecnologia

de serviços financeiros?

1.1 OBJETIVO GERAL

Analisar como as ferramentas de gerenciamento de riscos podem beneficiar o processo de proteção de dados em uma empresa de tecnologia de serviços financeiros.

1.2 OBJETIVOS ESPECÍFICOS

1) Mapear as ferramentas existentes de gerenciamento de riscos aplicáveis a proteção de dados existentes na literatura.
2) Verificar como as ferramentas de gerenciamento de riscos aplicadas a proteção de dados são utilizadas em uma empresa de tecnologia de serviços financeiros.
3) Identificar os benefícios, facilidades e dificuldades trazidas na aplicação das ferramentas de gerenciamento riscos quando aplicados a proteção de dados.

1.3 JUSTIFICATIVA

O presente estudo pretende relacionar dois temas de extrema relevância para o mundo corporativo e acadêmico: o gerenciamento de riscos e a proteção de dados pessoais. Com o surgimento das leis e regulamentações sobre a coleta, tratamento e uso de dados pessoais, se fez necessário a maior atenção aos riscos inerentes ao processo de proteção de dados e como devem ser mitigados nas organizações. Saber a forma mais eficiente de realizar o gerenciamento dos riscos e suas adequações ao processo de proteção de dados pessoais se faz muito necessária tanto para as empresas quanto para academia, e o gerenciamento de riscos trata de etapas importantes deste processo.

O conhecimento obtido com esse estudo pretende contribuir como auxílio às organizações a implementarem a gerenciamento de riscos em sua área de proteção de dados de maneira eficiente, da mesma maneira que se pretende servir de base e incentivar os estudos futuros sobre o tema que ainda tem muito que ser explorado. A longo prazo, é possível vislumbrar uma sociedade em que os titulares e as organizações não sofrerão mais nenhum tipo de dano como mau uso, tratamento ou

até vazamento dos seus dados.

Deseja-se que os resultados obtidos neste trabalho sejam disseminados através de publicações no meio acadêmico e no meio corporativo, a autora almeja levar o estudo para a organização em que está inserida com o objetivo de incentivar a melhoria da gestão de proteção de dados.

A elaboração do presente estudo aspira incentivar a realização de mais estudos sobre o tema e demonstrar com maior clareza a aplicabilidade da gestão de riscos na proteção de dados para as empresas, para que as mesmas tratem com excelência seu processo de proteção de dados. Da mesma forma, trazida por Kuner et al. (2015), espera-se que este trabalho encoraje empresários, especialistas e acadêmicos a aprofundarem-se no tema para que futuramente tenhamos diversas análises, fazendo com que a gestão de riscos atinja seu potencial máximo na proteção de dados (KUNER et al., 2015).

2 REVISÃO TEÓRICA

2.1 PROTEÇÃO DE DADOS PESSOAIS

A necessidade de proteção dos dados pessoais de um indivíduo está intimamente ligada ao seu direito fundamental a privacidade. É possível identificar essa ligação através do histórico das definições do direito a privacidade. De acordo com Mendes (2014), durante o século XX houve uma evolução no direito à privacidade por conta da mudança na função do Estado em conjunto com a revolução tecnológica, “passou a ser considerado uma garantia de controle do indivíduo sobre as próprias informações e um pressuposto para qualquer regime democrático” (MENDES, 2014, p. 29).

A proteção aos dados pessoais passa a estar inserida no direito à privacidade a partir da sua exposição com a digitalização da sociedade, e dos riscos que esta exposição pode trazer ao seu titular, considerando que faz parte da sua personalidade individual, e por esta razão precisa ser tutelada pelo ordenamento jurídico. Com o intuito de proteger não apenas os seus dados, mas o individuo em si contra possíveis riscos oriundos do tratamento de dados pessoais (MENDES, 2014).

De acordo com Finkelstein e Finkelstein (2020), o direito fundamental a proteção de dados pessoais se faz necessária, pois:

> O aumento da eficiência nos métodos de monitoramento e investigação proporciona maior facilidade para manter, utilizar e coletar informações. E justamente o que ocorre na Internet. Nesse âmbito, a informação e coletada invisivelmente, eficientemente e sem inconvenientes para o usuário. A informação e mais facilmente obtida e as proteções legais contra essa busca desaparecem. (FINKELSTEIN; FINKELSTEIN, 2020, p. 288)

Em uma sociedade da informação, na qual as mesmas circulam por diversos ambientes virtuais que não possuem nenhum tipo de controle, os dados pessoais podem ser enviados para diversos lugares de maneira ágil e de difícil detecção. Por esta razão, as legislações de proteção de dados foram criadas para assegurar este direito básico aos cidadãos e apresentar regras e boas práticas para as organizações a respeito da realização do tratamento de dados pessoais (PINHEIRO et al., 2020).

De acordo com Pinheiro (2021):

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização. (PINHEIRO, 2021, p. 10).

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

O início dos debates sobre o tema ocorreu na União Europeia que resultou na publicação do Regulamento Geral de Proteção de Dados (GDPR), em 2016. O regulamento zela pela proteção das pessoas no que diz respeito ao tratamento de seus dados pessoais. A promulgação da GPDR gerou efeitos econômicos, sociais e políticos, fazendo com que demais países que tinham relação com a União Européia começassem a construir suas próprias legislações a respeito do tema (PINHEIRO, 2021). A LGPD possui diversas semelhanças com a GDPR, conforme o Quadro abaixo apresentado por Pinheiro (2021, p. 24):

Quadro 1. Comparação GDPR e LGPD. Porto Alegre, RS, 2022.

ITEM DE CONFORMIDADE	REGIME BRASILEIRO (LGPD)	REGIME EUROPEU (GDPR)
Definição e distinção do que são dados pessoais e dados sensíveis. Tal conceituação busca delimitar os direitos e as informações protegidas pelo ordenamento jurídico	Define que dado pessoal é qualquer informação que identifique ou torne identificável a pessoa natural; já dados sensíveis são dados pessoais sobre etnia, raça, crenças religiosas, opiniões políticas, dados genéticos/biométricos, além de informações sobre filiações a organizações quaisquer da pessoa natural.	Adota os mesmos princípios e conceitos para realizar a distinção e delimitação dos direitos relativos aos dados pessoais e dados sensíveis, e ainda pontua considerações acerca dos dados genéticos, biométricos e os relativos à saúde.
Obrigatoriedade do consentimento do usuário para a coleta de informações e limitação do tratamento do dado conforme finalidade	A coleta e o tratamento de dados só poderão ser realizados se o usuário (dono dos dados ou responsável legal no caso de menores legais) der consentimento. Todo agente deve apontar finalidade certa, garantida e justificável ao tratamento do dado. Além disso, deve garantir que ele será utilizado somente para tal finalidade.	Prevê a necessidade de uso do dado conforme a finalidade apontada. Traz exceções de tratamento por motivo de interesse público, segurança e saúde.
Distinção entre titularidade e responsabilidade sobre os dados, assim como delimitação das funções e responsabilidades assumidas no tratamento de dados	Titular é a pessoa natural a quem se referem os dados que são objeto de tratamento; por outro lado, o responsável é a pessoa física ou jurídica, de direito público ou privado, que realiza decisões sobre o tratamento de dados. São definidos dois agentes de tratamento: o responsável – cuja competência é decidir sobre o tratamento dos dados – e o operador – a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados. Ambos os agentes são juridicamente responsáveis pela segurança e privacidade dos dados.	Há a mesma distinção entre titularidade e agentes, mas os agentes são divididos em controlador e processador de dados. O controlador é quem realiza as decisões acerca do tratamento de dados; o processador, quem efetua o tratamento dos dados. Ambos são responsáveis pelo tratamento dos dados.
Indicação de um encarregado pela comunicação entre os agentes, titulares e órgãos competentes	Além dos agentes, aponta-se a necessidade da indicação de um encarregado – pessoa natural – pela comunicação de qualquer informação ou fato relevante em relação ao tratamento dos dados. Ele deve atuar como um canal entre os agentes, titulares e órgãos competentes e deve ser indicado pela organização responsável pelo tratamento (Agente de Proteção de Dados).	Aponta que o controlador deve ter uma pessoa responsável por tudo que seja relacionado à proteção de dados (DPO).
Aplicação de mecanismos e práticas pautadas no livre acesso à informação e na transparência entre os usuários e as organizações	Do consentimento ao fornecimento de dados ao término do tratamento dos dados, as informações acerca do processo devem ser claras, acessíveis e adequadas à linguagem e compreensão do usuário, de forma que o seu consentimento possa ser revogado a qualquer momento. O consentimento do usuário deve ser realizado por escrito ou de qualquer outro modo que demonstre a sua livre manifestação da vontade.	Os titulares também têm direito a informações claras e acessíveis do início ao fim do tratamento do dado, podendo revogar o consentimento a qualquer momento.
Aplicação de medidas de segurança e dever de reportar	Da mesma forma que as organizações são responsáveis no caso de incidentes – como vazamentos – no tratamento dos dados, devem aplicar medidas de prevenção e proteção à segurança dos dados que manuseiam, como anonimização e encriptação das informações. Ainda assim, no caso de qualquer incidente é obrigação da organização notificar as autoridades imediatamente.	Também aponta que as empresas devem criar medidas – como pseudoanonimização e encriptação de dados – para garantir a segurança de forma preventiva. No caso de qualquer incidente, a notificação às autoridades deve ser imediata.
Possibilidade de alteração e exclusão do dado pessoal	O titular do dado pode alterar ou excluir seu dado pessoal a qualquer momento,	Os titulares dos dados também podem alterar ou excluir seus dados.
Possibilidade de alteração e exclusão do dado pessoal	exceto nas hipóteses previstas na lei, como fins fiscais, por exemplo. Da mesma forma, assim que o tratamento de dados chegar ao final – seja porque cumpriu sua finalidade, seja porque o usuário revogou seu consentimento –, as informações devem ser eliminadas.	
Aplicação de sanções no caso do descumprimento das regras	As punições variam entre advertências, aplicação de multas, suspensão e até mesmo proibição das atividades relacionadas ao tratamento de dados. Essas punições variam de forma gradativa de acordo com cada caso, conforme a gravidade do dano, a condição econômica do infrator, a reincidência, a boa-fé do infrator etc., e devem ser investigadas por meio de um processo administrativo que assegura o contraditório, a ampla defesa e o direito de recurso. As multas podem ser simples ou diárias, com valor relativo a 2% do faturamento da organização privada, limitadas a um total de R$ 50 milhões por infração.	Também prevê a aplicação de sanções gradativas e multas administrativas, que podem chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa.
Criação de um órgão competente para fiscalizar e zelar pela proteção de dados pessoais e da privacidade	Criada a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).	Possui um Órgão de Controle e Fiscalização de Proteção de Dados Pessoais por Estado (28) e aplica o princípio do Balcão único.

Fonte: Pinheiro (2021, p. 24)

A LGPD descreve o conceito de dado pessoal sensível em linha com o regulamento europeu, definindo-o em seu artigo 5º, inciso II, como:

> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (BRASIL, 2018, p. 1)

A LGPD se tornou um instrumento de extrema relevância aos beneficiados por ela. A legislação permitiu que cada pessoa física tenha controle dos seus dados, e impôs deveres e responsabilidades para as organizações enquanto agentes de tratamento dos dados. Trouxe a necessidade do consentimento do titular dos dados para acesso e utilização dos seus dados. Para cumprir e orientar a respeito das normas exigidas pela LGPD, a ANDP foi criada (TEPEDINO, 2020).

A LGPD é aplicável a todas as empresas que prestam serviço no Brasil, que a coleta e tratamento de dados de pessoas localizadas no Brasil. Estes dados precisam ser coletados, tratados no Brasil, e com objetivo de oferecer bens e serviços no país. A lei não considera a forma de tratamento de dados, o país sede da empresa, a localização dos dados e a nacionalidade dos titulares dos dados. A LGPD prevê um protagonismo do titular de dados em todas as etapas do tratamento, por esta razão se faz necessária o consentimento do titular desde a coleta até a eliminação dos dados (PINHEIRO, 2020).

O tratamento abrange toda a operação realizada com os dados pessoais, e deve ser norteado pelos princípios elencados no artigo 6º da LGPD, os 10 princípios gerais da proteção de dados, são eles:

> Art. 6º - As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III- necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV- livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V- qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI- transparência: garantia, aos titulares, de informações claras, precisas e

> facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comerciais e industriais;
>
> VII- segurança: utilização de medidas 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 difusão;
>
> VIII- prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX- não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. (LGPD)

A LGPD lista uma série de direitos que possui o consumidor que fornece seus dados às empresas, devendo ficar atentas ao cumprimento destas obrigações, a fim de evitar eventuais sanções administrativas e ações de responsabilidade civil. Conforme a lei de proteção de dados, a qualquer momento o titular dos dados pode exigir das empresas o cumprimento à essas obrigações, com relação aos seus dados pessoais. Além disso, os direitos dos titulares dos dados previstos na lei são: a retificação, a eliminação, oposição, revogação, portabilidade, obrigação de notificação, limitação de tratamento e acesso a informação (LOURENÇO; TAQUES, 2020).

Para melhor entendimento da LGPD, é necessário compreender alguns conceitos trazidos por ela, em seu artigo 5º.

> Art. 5º - Para os fins desta Lei, considera-se:
>
> (...)
>
> V. Titular dos Dados: pessoa física a quem se referem os dados que são objetos de tratamento.
>
> VI. Controlador: Pessoa física ou jurídica, de direito Público ou Privado a quem competem às decisões referentes ao tratamento de dados pessoais.
>
> VII. Operador: Pessoa física ou jurídica, de direito publico ou privado que realiza o tratamento de dados pessoais em nome do controlador.
>
> VIII. Encarregado: Pessoa física indicada pelo controlador que atua como canal de comunicação entre o controlador, titulares de dados e autoridade nacional.
>
> (...)
>
> XIX. Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

A Autoridade Nacional de Proteção de Dados (ANPD) foi criada como órgão responsável pela adequação e aplicação da LGPD determinando as normas a respeito do tratamento de dados no Brasil, assim como tem a responsabilidade de fiscalizar e aplicar sanções e multas previstas na lei, quando necessário. (PINHEIRO, 2021). A

estrutura da ANPD foi publicada, em 2020, com o Decreto nº 10.474, de 26 de agosto de 2020, e publicou seu primeiro planejamento estratégico com vigência de 2021 a 2023. A partir deste momento, a ANPD passou a publicar guias orientativos para a adequação a LGPD, e a partir de agosto de 2021 a aplicar penalidades referentes ao não cumprimento da LGPD (ANPD, 2021).

A digitalização da sociedade afeta todos os setores da economia mundial, até mesmo setores tradicionais como agricultura. Nesse contexto, a preocupação em torno do tratamento dos dados pessoais se faz presente na rotina das organizações (GUTIERREZ, 2021).

De acordo com Pinheiro et al. (2020), esta preocupação se tornou ainda maior com a chegada da LGPD, e com as dificuldades apresentadas pelas organizações, de todos os portes, públicas e privadas, de ficar em conformidade com as novas regras sobre proteção de dados impostas pela legislação. Ainda, segundos os autores, tais dificuldades giram em torno de dois pontos principais, “instabilidade regulatória do país frente ao tema e a falta de direcionamento por parte da ANPD” (PINHEIRO et al., 2020, p. 31).

Para estar em conformidade com a LGPD, as organizações, que são agentes de tratamento de dados pessoais, devem apresentar alguns exercícios de controle do tratamento de dados pessoais. Em seu artigo 37, a LGPD determina que o controlador e operador dos dados pessoais devem manter o registro das operações de tratamento dos dados pessoais que realizarem (BRASIL, 2018). O registro das operações de tratamento dos dados pessoais é conhecido pela sigla ROPA, abreviação de *Record Of Processing Activities* especificado no artigo 30 da GDPR. O ROPA deve mapear todos os processos realizados na organização sob a ótica do dado, sabendo todo o fluxo da informação desde a sua origem até seu processo de eliminação, que também está previsto como obrigatório na LGPD (VEIGA, 2021).

Após a realização do ROPA o artigo 38 da LGPD afirma que a ANPD pode determinar que o controlador elabore um relatório de impacto á proteção de dados pessoais. No parágrafo único do artigo 38 da LGPD está descrito que neste relatório deve conter:

> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.

O relatório de impacto também teve influência da legislação europeia que exige o *Data Protection Impact Assessment* (DPIA), ficando também conhecido pela sigla em inglês.

De acordo com Gomes (2019, p. 4), o DPIA, que serviu de fonte inspiradora para a criação da ferramenta do relatório de impacto na LGPD, tem como objetivo a identificação, mitigação e prevenção de riscos e altos riscos aos titulares de dados.

O documento é fruto da avaliação de impacto e se realizado de maneira correta, o DPIA pode ser um instrumento balizador nas atividades de tratamento de dados nas organizações, trazendo muitos benefícios na realização da governança de dados e na aderência a legislação. Por esta razão não deve ser visto como uma documentação que é obrigatória pela lei, e que deve ser feita apenas para cumprir as obrigações (GOMES, 2019).

Visto que o DPIA é um documento que considera os riscos aos titulares dos dados, se faz necessária o entendimento do gerenciamento de riscos corporativos nas organizações.

2.3 GERENCIAMENTO DE RISCOS: PERSPECTIVA HISTÓRICA

A definição de risco, tendo por base o IBGC (2007), COSO (2007) e Assi (2012), está relacionada com a probabilidade de um evento ocorrer de forma inesperada, podendo gerar perda as organizações. O gerenciamento de riscos refere-se a um processo que engloba riscos e oportunidades que afetam o valor das organizações (VIEIRA et al., 2019).

O gerenciamento de riscos corporativos iniciou no campo acadêmico, em 1921, com a publicação da obra *Risk, Uncertainty and Profit*, de Frank Knight. A produção de Knight passou a ser a maior referência sobre o tema, principalmente, no que tangia a sistematização, conceitos e diretrizes do gerenciamento de riscos. Já sob a perspectiva corporativa, o estudo do gerenciamento de risco teve seu relativamente há pouco tempo, somente no início do século XX. A publicação do artigo *The Risk Manage Revolution*, na revista Fortune, foi um marco importante que ocorreu em 1975, estabelecendo as principais funções de riscos nas organizações e como a alta administração deveria realizar a aceitação ou não e a gestão de tais riscos. O gerenciamento de riscos surgiu no Brasil por volta de 1980 no mercado de logística, e tinha como objetivo prevenir intercorrências nas operações do processo. Já o

surgimento das discussões sobre os dados pessoais é anterior, foi iniciada na década de 1960 (FRASER; SIMKINS, 2009).

Em 1992, ocorre a primeira publicação do *Committee of Sponsoring Organizations of the Treadway Commission,* o COSO, de um framework de controles internos o *Internal Control – integrated framework* (COSO-IC ou COSO I). Esta publicação tem como objetivo apresentar as melhores práticas e princípios de controles internos, e, consequentemente, gerenciamento de riscos, a serem seguidas pelas organizações (COSO, 1992). Concomitante a publicação do COSO I, ocorre no Reino Unido a publicação que trata a respeito do tema do Comitê Cadbury, comitê criado pelo banco da Inglaterra que objetivava escrever um código de melhores práticas de governança corporativa. Neste código é atribuído aos governantes da organização a responsabilidade de realizar as políticas de gerenciamento de riscos e garantir que a organização esteja ciente dos seus riscos, assim como realizar o gerenciamento de riscos corporativos (CADBURY, 1992).

No ano de 2001, o escândalo da empresa Enron fez com que os estudos sobre gerenciamento de riscos e controles internos se fizessem ainda mais necessários. Enron Corporation foi uma empresa norte-americana de energia, sendo uma das empresas líderes no mundo em energia e comunicações até 2001. Nos anos 2000, as empresas concorrentes da Enron estavam em queda, enquanto a Enron continuava apresentando lucro, o que levantou uma suspeita ao mercado. Em outubro de 2001, a empresa publicou seu balanço demonstrando um prejuízo de US$ 604 milhões, e escondendo dívidas de cerca de US$ 25 bilhões. As ações da Enron passaram de US$ 90,56 em agosto de 2000 para US$ 0,06 em dezembro de 2002. Isso foi possível, pois ocorreu uma manobra contábil, de forma que as despesas da Enron eram repassadas à Entidade de Propósito Específico (SPRs) que não eram consolidadas. Desta forma, o balanço da Enron demonstrava sempre lucro. A razão para o ocorrido era que os executivos da Enron recebiam parte de seu bônus através de ações da empresa, sendo o lucro da empresa uma das métricas para pagamento das ações. Desta forma, conhecendo a fragilidade de controles sobre a consolidação da empresa, o diretor financeiro manipulou o resultado da empresa, para assim suas ações valorizarem, enquanto recebia mais ações como parte do pagamento pelo bom resultado (HERRERA, 2002).

Buscando por justiça pela fraude bilionária ocorrida na Enron, diversos tribunais americanos iniciaram investigações para descobrir as causas da fraude. Após a

descoberta de como os executivos haviam realizado a fraude, em resposta a isso, em 2002, os congressistas Paul Sarbanes e Michael Oxley, criaram a Lei 107-204: Sarbanes-Oxley, que ficou popularmente conhecida como a Lei SOx. A nova lei estabeleceu diretrizes a respeito de governança corporativa, instituiu o órgão governamental *Public Company Auditing Oversight Board* (PCAOB), que passou a reger regras a serem seguidas pelos auditores, regulamentou diversos temas sobre auditoria, como a rotação dos sócios de auditoria, tornando-os auditores independentes e estabeleceu a melhoria nas demonstrações financeiras, impondo que os relatórios 10-K, para empresas americanas listadas na bolsa e o relatórios 20-F, para empresas estrangeiras listadas nas bolsas americanas, possuíssem mais informações, como as transações de ações dos executivos (ALVES, 2009).

Após o estabelecimento da Lei SOx, em 2004, o COSO publica o Enterprise Risk Management - *integrated framework* (COSO-ERM ou COSO II), que apresenta maior foco em gerenciamento de riscos corporativos quando comparado ao COSO I. Ainda em 2004 é publicado o Acordo de Basileia II, que complementa o Acordo de Basiléia I, um tratado que tem como objetivo regular o funcionamento de bancos e instituições financeiras, firmado em 1988, na cidade de Basileia na Suíça, com a participação de mais de 100 países, com requisitos específicos relacionados ao gerenciamento de riscos operacionais (SILVA, 2007).

No Brasil, em 2009, a ABNT publica a norma técnica ISO 31.000: Gestão de Riscos – Princípios e diretrizes. A norma apresenta as melhores práticas de gerenciamento de riscos corporativos para todas as organizações (ABNT, 2009).

2.4 GERENCIAMENTO DE RISCOS: MODELOS DE REFERÊNCIA E REGULAMENTAÇÕES

Existem outros modelos de gerenciamento de riscos corporativos além do COSO, que apresentam objetivos específicos e não são tão conhecidos no mercado, vamos elencar os principais em seguida.

O *Guidance on Assessing Control – The CoCo Principles (CoCo*) foi desenvolvido, em 1997, no Canadá, *pelo Canadian Institute of Chartered Accountants(CICA).* O modelo também objetiva demonstrar como a administração das organizações deve implementar seu ambiente de controle, visando atingir seus objetivos estratégicos. Sua principal diferença em relação ao COSO é que específica

o responsável pela prestação de contas (VESCO et al., 2014).

De acordo com Tenório (2007, p. 49), o modelo CoCo “concentra-se nos valores comportamentais como a base fundamental para os controles internos de uma companhia, e não na estrutura e nos procedimentos de controle em si”.

Em 1999, a Austrália e a Nova Zelândia também apresentaram um modelo de referência de gerenciamento de risco. Por meio de um Comitê de Gestão de Riscos a Standards Austrália e Standards New Zealand publicaram a AS/NZS 4360. Assim como os outros, fornecem diretrizes e orientações sobre gerenciamento de riscos para as organizações (VESCO et al., 2014).

Outro modelo de referência de gerenciamento de riscos é o *Control Objectives for Information and related Technology* (COBIT), foi desenvolvido pela *Information Systems Audit and Control Association* (ISACA). O COBIT é mais direcionado ao gerenciamento de riscos na tecnologia da informação (TI), por isso apresenta uma estrutura de governança de TI. Surgiu como iniciativa aos ambientes mais automatizados que eram encontrados pelas auditorias nas organizações. Contudo, em sua versão mais recente publicou o RISKIT, focado para gerenciamento de riscos (SILVA, 2020).

No Brasil, em 2009, a ABNT publica a ISO 31.000: Gestão de Riscos – Princípios e Diretrizes, que também propôs um framework de boas práticas para um processo de gerenciamento de riscos em todas as organizações que gerenciem riscos em algum grau. A norma estabelece princípios que precisam ser atendidos para um gerenciamento de riscos eficaz (ABNT, 2009).

De acordo com Silva (2020), após uma revisão sobre a implementação do gerenciamento de riscos, é possível perceber que a integração dos frameworks do COSO e da ISO 31.000 é amplamente utilizada pelas organizações, provando a eficiência de ambas as normas. Apesar de parecidas, os modelos de referência se complementam em determinados pontos, fazendo com que o seu uso de forma integrada também traga bons resultados no gerenciamento de riscos das organizações (SILVA, 2020).

Apesar da existência de outros modelos de referência que tratem do tema de gerenciamento de riscos, o COSO é o mais utilizado. O framework do COSO é muito utilizado por conta de ser um modelo americano e endereçar diretamente diversas exigências da SOx. Desta forma, passou-se a utilizar o framework em larga escala para endereçar os controles internos (ZONATTO; BEUREN, 2012).

O framework do COSO apresenta cinco diretrizes principais, são elas: ambiente de controle, avaliação de risco, atividades de controle, informação e comunicação e monitoramento de atividades (COSO, 2013).

O ambiente de controle apresenta cinco princípios relacionados ao conceito *top of top*, nos quais são abordadas a integridade e o comprometimento com os valores éticos. Já a avaliação de riscos possui quatro princípios que determinam que a administração deve realizar avaliações de riscos em linha com os objetivos das operações. As atividades de controle determinam três princípios em que a administração se responsabiliza por estabelecer controles que mitiguem os riscos que foram identificados. A diretriz de informação e comunicação traz três princípios acerca da relevância das informações que devem ser comunicadas interna e externamente. Por fim, o monitoramento de atividades apresenta dois princípios relacionados às atividades realizadas pela administração para garantir que o ambiente de controle esteja *in place* e funcionando adequadamente (COSO, 2013).

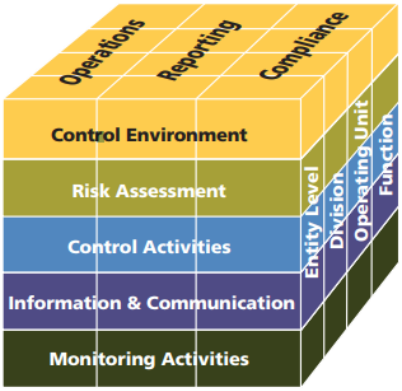

Figura 1. Cubo do COSO.

Fonte: COSO (2013)

Em 2004, o COSO publicou um framework complementar ao de 1992, no qual divide a diretriz de Avaliação de Risco em outras três: identificação de eventos, avaliação de riscos e resposta aos riscos. Tornando assim o modelo do COSO I mais direcionado a controles internos e o COSO II mais direcionado para riscos empresariais. O COSO I foi atualizado em 2013 e é o mais utilizado por estar inserido também no escopo da Lei SOx.

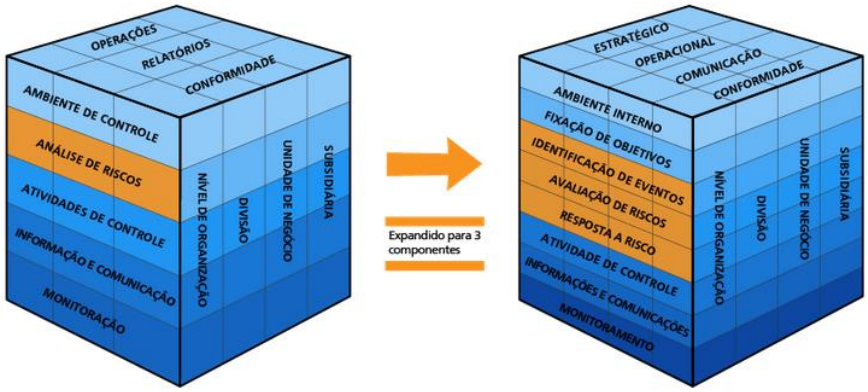

Figura 2. Comparação COSO I (1992) e COSO II (2004).
Fonte: TCU (2019)

O gerenciamento de riscos é regulamentado no Brasil para empresas autorizadas a funcionar pelo Banco Central do Brasil, o BACEN, na Resolução nº 4.557 de 2017, que surgiu a fim de complementar a Circular nº 3.681, de 2013, a qual foi alterada pela Resolução BCB nº 25, de 22 de outubro de 2020.

A Resolução nº 4.557 foi criada pelo Conselho Monetário Nacional (CMN) e publicada através do Banco Central do Brasil (BACEN), e exige que instituições financeiras implementem uma estrutura de gerenciamento de risco. A Resolução trouxe muitos avanços no gerenciamento de riscos, como a obrigatoriedade de demonstração de apetite ao risco, assim como torna obrigatório o estabelecimento de um comitê interno de riscos (BACEN, 2017).

As regulamentações determinam a existência do gerenciamento de riscos e como deve ser a sua estrutura. Segundo a determinação da Circular nº 3.681 do BACEN, a estrutura de gestão de riscos deve realizar a gerência dos riscos operacionais, riscos de liquidez e riscos de crédito. Neste estudo nos direcionaremos para a gestão de riscos operacionais, pois é nela que a gestão de proteção de dados está inserida. De acordo com a Resolução nº 4.557, em seu artigo 32, risco operacional define-se “como a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas” (BACEN, 2017, p. 41). Em complemento, o primeiro evento citado na Circular nº 3.681, refere-se à falha na segurança de dados sensíveis. (BACEN, 2013).

2.5 GERENCIAMENTO DE RISCOS APLICADO À PROTEÇÃO DE DADOS

Após o entendimento dos dois temas de forma separada, é possível identificar alguns pontos em comum entre o gerenciamento de riscos corporativos e a adequação das empresas à nova legislação de proteção de dados. Entre os objetivos estabelecidos pelo gerenciamento de riscos corporativos está a mitigação de possíveis riscos, o estabelecimento de controles para estes e também preconizam a conformidade com as legislações vigentes. Por esta razão, pode-se afirmar que a LGPD e tudo que ela abrange passa a fazer parte do gerenciamento de riscos corporativos como uma nova disciplina, que precisa ter seus riscos envolvidos tratados, monitorados e mitigados (OLIVEIRA, 2021).

Na aplicação da metodologia de aplicação de um gerenciamento de riscos corporativos eficiente apresentada pelo *The Institute of Internal Auditors* (IIA), organização que desenvolve padrões e orientações a respeito dos processos de autoria interna, se faz presente a definição das três linhas de defesa. A primeira linha de defesa é composta pelo operacional na organização, o que tem contato com o cliente. Os gerentes operacionais precisam ter propriedade sobre os riscos existentes em seus processos e gerenciá-los da maneira correta. A segunda linha de defesa é composta pelo setor de gerenciamento de riscos corporativos da organização, que é responsável por conscientizar os colaboradores e estabelecer as funções que a primeira linha precisa executar para manter a organização segura. Por fim, a terceira linha de defesa é composta pela auditoria interna, que consegue perceber algum problema que não tenha sido contido pela primeira e segunda linha de defesa (IIA, 2013).

A adequação a LGPD precisa passar pelas três linhas de defesa. A primeira linha precisa ter consciência do processo de tratamento de dados, como realizar a coleta da maneira correta, assim como a eliminação. A segunda linha de defesa precisa garantir que o tratamento de dados esteja ocorrendo da maneira correta, assim como criar estratégias para a identificação dos riscos, prevenção de incidentes, de vazamento de dados e estratégia para resolver e mitigar os riscos quando aparecerem. Portanto, o amadurecimento nas práticas de gerenciamento de riscos fará com que as empresas tenham mais agilidade para ficarem aderentes a LGPD (OLIVEIRA, 2021).

Em concordância com o tema, Silva (2020) ao propor um framework de

utilização do gerenciamento de riscos aplicados a proteção de dados, destaca a semelhança com as prerrogativas de tratamento de dados pessoais existentes no COBIT e na LGPD. A semelhança se faz presente por conta da relação do COBIT com segurança da informação e de seus fundamentos a respeito de direito dos titulares dos dados e práticas de governança corporativa (SILVA, 2020).

O exercício da execução dos relatórios de impacto previstos na LGPD precisa ser realizado pela ótica do risco. Por ser uma avaliação de impacto, precisa considerar todos os riscos relacionados ao tratamento de dados envolvidos no processo que está sendo avaliado. Deve estar relacionado à prevenção e mitigação dos riscos envolvendo os titulares dos dados. Com isso, os exercícios de proteção de dados, o ROPA e DPIA, precisam estar inseridos no cronograma de exercícios da área de gerenciamento de riscos corporativos, pois assim como os demais também faz parte da função principal da segunda linha de defesa que é controlar e mitigar os riscos existentes nos processos das organizações (GOMES, 2019).

3 PROCEDIMENTOS METODOLÓGICOS

Visando atingir os objetivos determinados e para responder à questão de pesquisa foram realizados uma revisão sistemática da literatura e uma pesquisa descritiva qualitativa.

3.1 REVISÃO SISTEMÁTICA DA LITERATURA

Foi realizado uma revisão sistemática da literatura, para embasar teoricamente os conceitos e o estado da arte das áreas de gerenciamento de riscos e proteção de dados, buscando uma relação conceitual e prática entre elas. Uma revisão sistemática da literatura “consiste em investigar o conhecimento produzido em determinada área através de uma metodologia rigorosa e formal” (SOUZA; JERÔNIMO, 2020, p.152). A utilização de revisão sistemática da literatura como método de pesquisa tem como objetivo buscar uma coerência na documentação acadêmica sobre o tema escolhido. Ainda evita a duplicidade de pesquisas e possibilita a utilização das existentes como base de conhecimento e referência sobre o tema (GALVÃO; RICARTE, 2019).

Para realizar a revisão sistemática de forma eficiente foi utilizado o método PRISMA - *Preferred Reporting Items for Systematic Reviews and Meta-Analy*ses. A recomendação PRISMA objetiva ajudar os autores de revisões sistemáticas a melhorarem seus relatos e análises dos estudos realizados. Consiste em um checklist de itens que não podem deixar de serem contemplados em uma revisão sistemática, somado de um fluxograma que definirá o fluxo da informação nas fases da revisão sistemática (MOHER et al., 2015).

De acordo com Gomes e Caminha (2014), as 7 etapas necessárias para a confecção de uma revisão sistemática da literatura, desenvolvidas pelo Instituto Cochrane (instituto dedicado a estudos sobre revisões sistemáticas), são: formulação da pergunta, localização e seleção dos estudos, avaliação crítica dos estudos, coleta, análise e apresentação e interpretação dos dados obtidos e o aprimoramento e atualização da revisão. O decorrer da execução do método será detalhado a seguir.

O primeiro passo foi o (1) estabelecimento da pergunta de pesquisa. (2) Após foi realizado a definição do string de busca em plataformas de periódicos acadêmicos e definição das fontes de busca. (3) Após esta primeira pesquisa, foram estabelecidos os filtros necessários para a escolha de estudos mais relevantes para o que está

sendo pesquisado. Posteriormente, (4) foi realizado a leitura e análise dos trabalhos escolhidos. Por fim, (5) a interpretação as principais dos resultados encontradas, e (6) análise crítica e debate sobre os dados obtidos.

A primeira etapa foi a formulação da pergunta de pesquisa, a qual este trabalho tem por objetivo responder: “Como as ferramentas de gerenciamento de riscos beneficiam o processo de proteção de dados em uma organização financeira de meios de pagamento do Rio Grande do Sul?” Foi definida a *string* de busca, palavras-chave que poderiam resultar em trabalhos científicos já realizados relacionados ao tema pesquisado. Foram realizados alguns testes para verificar os retornos obtidos com cada string utilizado. No Quadro 2 estão apresentados os resultados obtidos na primeira etapa. Com base nos resultados encontrados nos testes de definição das strings, foram escolhidas as fontes de busca: Oxford Journals Current, Computers & Applied Science Complete, DOAJ Directory of Open Acess Journal e Freedom Collection Journal (SCFCJ).

Quadro 1. Strings de busca e quantidade obtida. Porto Alegre, RS, 2022.

Teste	***String***	**Oxford**	**Computer & Applied**	**DOAJ**	**SCFCJ**
1	“risk management” + “data protection”	68	660	1320	100
2	“risk assessment” + “data protection”	165	394	3292	362
3	“gdpr” + “risk management”	18	56	321	17
4	"compliance" “gdpr" "risk management"	15	42	177	5

Fonte: Elaborada pela autora.

A string selecionada foi “risk management” + “data protection”, pois, resultou em maiores resultados quantitativos de retorno, e mais qualificado em função do tema em pesquisa.

Foi realizada a criação de filtros para seleção dos artigos que trariam informações mais relevantes ao estudo (Quadro 3). Excluiu-se inicialmente os artigos anteriores a 2015, pois percebeu-se que os trabalhos anteriores eram muito distantes da realidade atual, visto que se trata de um tema recente. Contudo, escolheu-se 2015 como ano de corte por conta das publicações do autor que tratou com pioneirismo o tema de gerenciamento de riscos a proteção de dados, Raphael Gellert. O segundo filtro foi a seleção por idioma (inglês) e o terceiro, por produção literária. Foram selecionados apenas artigos científicos, revisado por pares, capítulos de livros e

outras formas textuais foram desconsideradas. O quarto filtro foi a análise dos títulos dos artigos, foi aplicado uma busca avançada para encontrar artigos que obtivessem a expressão “data protection” no título, a fim de objetivar mais a busca.

Quadro 3. Filtros Utilizados para a seleção dos artigos da RSL e justificativa. Porto Alegre, RS, 2022.

Ordem	Filtro	Justificativa
1	Data da Publicação	O tema de proteção a dados pessoais e as legislações existentes sobre o tema são recentes. Publicações anteriores a 2015 sobre o tema são difíceis de serem encontradas, e os que existem não poderiam ser comparados com a realidade atual.
2º	Idioma	As strings foram direcionadas em inglês, pois antes de defíni-las não foram encontradas publicações relevantes sobre o assunto investigado em português, apenas em inglês.
3º	Seleção por produção literária	Foram selecionados apenas artigos científicos revisados por pares. Capítulos de livros, livros e publicações de sites foram excluídos.
4º	Análise do título	Na análise do título, foram selecionados apenas os artigos que apresentassem a expressão “data protection” no título. Filtro aplicado através da ferramenta de busca avançada.
5º	Análise dos resumos	Na leitura dos resumos, foram escolhidos o que possuíam a expressão “risk management”, após buscamos os que apresentavam relação com a aplicação ao tema de proteção de dados.
6º	Leitura dos artigos	Ao final do processo restaram 12 artigos, os quais foram lidos por inteiro e selecionados apenas os que versavam especificamente sobre os temas gerenciamento de riscos e proteção de dados.

Fonte: Elaborada pela autora

O quinto filtro foi a seleção dos artigos. Os critérios de elegibilidade foram (i) a identificação da expressão *risk management* explícita no resumo e (ii) termos que remetessem ao universo que abrange ao universo de proteção de dados e sua legislação como “data protection”, “privacy”, “GDPR” e “personal data protection”. Vale ressaltar que além dos artigos obtidos ao final da aplicação de todos os filtros foi incluído na revisão mais um artigo que não esteve presente nos resultados das buscas, por não apresentar as palavras “data protection” no título, contudo é de extrema relevância para a discussão do tema. O artigo incluído propõe um conjunto de ferramentas de gerenciamento de riscos e proteção de dados. As referências do artigo são *Automated Cyber and Privacy Risk Management Toolkit* dos autores Granadillo et al. (2021), no periódico Sensores.

Na etapa 6, conforme Figura 3, restaram 12 artigos, os quais foram lidos para verificar se abrangiam o tema escolhido: Gerenciamento de riscos e Proteção de dados. Destes, restaram 10 artigos para análise, 9 resultado da string de busca e 1

incluído por critério de inclusão. As etapas 4, 5 e 6 – coleta de dados, análise e apresentação dos dados, interpretação dos dados e análise crítica, respectivamente – serão apresentadas e discutidas no capítulo de análise dos resultados.

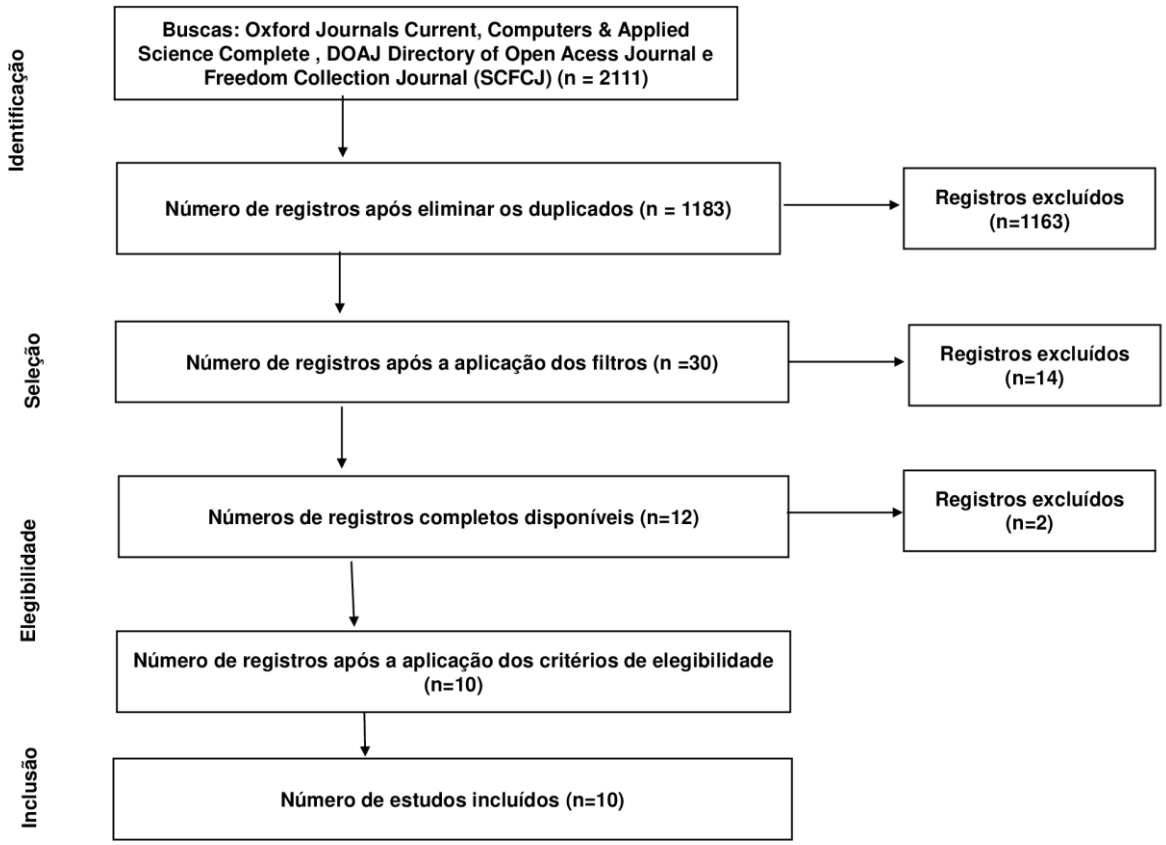

Figura 2. Fluxograma do processo de seleção.

Fonte: Moher et al. (2015).

3.2 PESQUISA QUALITATIVA

Após realização da revisão sistemática em que foram analisadas as ferramentas de gerenciamento de riscos e sintetizadas as ferramentas-chave de gerenciamento de riscos para proteção de dados foi realizada uma pesquisa descritiva com análise qualitativa, com o intuito de entender dos benefícios da aplicação das ferramentas de gerenciamento de riscos para proteção de dados.

De acordo com Gil (2010), a pesquisa descritiva pode ser definida como qualquer estudo que objetiva “descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis” (p. 3).

Para Godoy (1995), a pesquisa qualitativa:

> [...] tem como preocupação fundamental o estudo e a análise do mundo empírico em seu ambiente natural. Nessa abordagem valoriza-se o contato direto e prolongado do pesquisador com o ambiente e a situação que está sendo estudada. (GODOY, 1995, p. 62)

Godoy (1995) ainda complementa que todos os estudos descritivos devem ser acompanhados de uma análise qualitativa, pois o que está sendo buscado é o entendimento de um fenômeno e sua complexidade como um todo.

O local da pesquisa foi uma empresa de tecnologia voltada para meios de pagamento, físico e digital, da região sul do Brasil. A organização financeira solicitou que não fosse identificada, por essa razão iremos denominá-la empresa TX. Fundada, em 2003, em uma cidade de interior; em 2014 passou a fazer parte de um grupo empresarial multinacional, passando a operar em toda a América Latina, após a fusão, em 2016, a TX passou a ser regulamentada pelo BACEN. Por esta razão, iniciou-se a implementação da área de gerenciamento de riscos operacionais e controles internos, com a contratação de um gerente específico para a área, juntamente com riscos financeiros, que já eram acompanhados há mais tempo pela organização.

Com o crescimento da empresa, se fez necessário uma maior atenção a área de gerenciamento de riscos operacionais e controles internos, assim, em 2018, a empresa contratou um *Chief Risk Officer* (CRO), estabelecendo uma vice-presidência inteira para a gestão de riscos. Em 2019, houve a separação das áreas de gestão de riscos financeiros e riscos operacionais e controles internos, na qual a segunda passou a responder diretamente para o CRO. Por fim, em 2020, com início das sanções da LGPD, a empresa contratou um especialista em proteção de dados e LGPD para realizar a adequação da TX a nova lei. O especialista integrou a equipe de riscos operacionais (não financeiros) e controles internos e passou a realizar a gestão de proteção de dados e aplicar as recomendações de gerenciamento de riscos. Em 2021, a área passou a ser chamada de Riscos Não Financeiros e Controles Internos.

Como a TX usa o gerenciamento de riscos aplicado à proteção de dados, permitindo um levantamento de dados contextualizado para posterior cruzamento com a teoria e a identificação de benefícios de uso destas práticas para uma organização.

Os instrumentos de coleta utilizado foram entrevistas com base em questionários com perguntas de respostas abertas que podem ser consultadas nos apêndices (APÊNDICE A). A amostra foi intencional e os participantes convidados por email. Foram realizadas 4 entrevistas com funcionários da empresa analisada, sendo

eles: um gestor responsável pela implementação da área de proteção de dados na organização, denominado G1, e mais três colaboradores das áreas comercial, administração de pessoal e controladoria, denominados E1, E2 e E3. Essas áreas foram escolhidas porque tiveram implementados em seus processos algumas ferramentas de gerenciamento de riscos para proteção de dados.

A partir das respostas, foram definidos os perfis dos respondentes. E1 é colaborador da empresa há dois anos e já participou de dois exercícios (exercício é a denominação utilizada pela empresa para aplicação anual das ferramentas de gerenciamento de riscos aplicadas à proteção de dados) realizados pela área de proteção de dados. E2 é funcionário da área de administração de pessoal, de gestão de pessoas, está na empresa há cinco anos e participou dos 3 exercícios de proteção de dados realizados. Por fim E3, trabalha na área de controladoria, está na empresa há três anos, e participou de dois exercícios de proteção de dados. Com isso, é perceptível que todos os entrevistados já participaram de mais de um exercício e estão no mínimo há dois anos na empresa.

Os dados obtidos nas entrevistas foram analisados à luz da Análise de Conteúdo proposto por Bardin (2011) e os resultados serão apresentados no capítulo de análises de resultados. Análise de Conteúdo constitui uma metodologia de pesquisa usada para descrever e interpretar o conteúdo das comunicações, constituída por três etapas:

a) Pré-análise: leitura do material coletado visando a compreensão das idéias e significados;
b) Exploração do material: seleção das unidades de análise por meio de categorização. Uma categoria é um conjunto de dados com semelhanças que aparecem em diferentes contextos ou situações;
c) Interpretação dos dados: é realizado o tratamento dos resultados, a inferência e a interpretação, em que os dados construídos são tratados de maneira a se tornar significativos.

4ANÁLISE DOS RESULTADOS

4.1 REVISÃO SISTEMÁTICA DA LITERATURA

A fim de cumprir o objetivo proposto por este trabalho, foi realizada uma revisão sistemática da literatura para entender o papel desenvolvido pelo gerenciamento de riscos na proteção de dados. Vale ressaltar que as legislações sobre o tema são recentes e em razão disso, ainda não existem muitos estudos de caso aplicados. A pesquisa encontrou, nos artigos selecionados, inicialmente uma discussão jurídica sobre o tema, a respeito de sua aplicação nas empresas, e, posteriormente, foi possível identificar a relação entre o gerenciamento de risco e proteção de dados, principalmente, através de ferramentas de gerenciamento de riscos que se destacaram no âmbito da proteção de dados.

As reflexões jurídicas são apresentadas por Raphael Gellert (2015), afirmando que “a proteção de dados é um quadro legal para a regulação de riscos decorrentes da implantação de Tecnologias da Informação e Comunicação na sociedade” (GELLERT, 2015, p. 3, *tradução nossa*). O autor argumenta que o tema de proteção de dados apresenta os três elementos constitutivos de regulações de risco, que são estabelecimento de padrões, recolha de informação e modificação de comportamento, ressaltando que proteção de dados se enquadra em uma regulação de riscos, pois trata os novos riscos vindos de novas tecnologias (GELLERT, 2015).

Gellert (2017) começa sua análise buscando a compreensão conceitual de risco, e, posteriormente, sua noção no Regulamento Geral de Proteção de Dados (GDPR), legislação europeia. O autor começa trazendo os objetivos que circundam o conceito de risco. O risco no mundo corporativo resume-se em prever eventos futuros, podendo ser bons ou ruins, e tomar a decisão sobre o que fazer a respeito. Contudo, por ser ainda um conceito muito abstrato, o autor traz a análise de risco como solução. O objetivo da avaliação de risco é medir a probabilidade do risco ocorrer e qual seria sua gravidade se ocorresse e após essa avaliação, é papel do gerenciamento de riscos decidir se a organização irá assumir o risco em questão ou não. Ao analisar a legislação, Gellert (2017) afirma que o entendimento de risco, presente no artigo 35, está voltado para eventos de riscos relacionados a processamentos, novas tecnologias e tipos de dados e traz o titular dos dados como vítima das consequências dos riscos (GELLERT, 2017).

Kuner et al. (2015) afirmam que a utilização do gerenciamento de riscos na proteção de dados pode trazer benefícios como priorizar investimentos, reduzir custos e no cumprimento das obrigações. Aponta também que todas as legislações de proteção de dados trazem o gerenciamento de riscos em sua composição, e apresenta relatórios governamentais que interligam os dois temas. Vale destacar que os autores enfatizam as ferramentas de gerenciamento de riscos de proteção de dados:

> É também importante que as ferramentas de gerenciamento de risco de proteção de dados se enquadrem nas metodologias e programas de gerenciamento de risco existentes. Isto é necessário por muitas razões, incluindo permitir que o gerenciamento de risco de proteção de dados se beneficie da experiência desenvolvida em outras áreas, assegurando que o gerenciamento de risco de proteção de dados aproveite os recursos consideráveis já dedicados pelas organizações ao gerenciamento de risco em outras áreas, e aumentando a eficiência (e reduzindo o custo) da gestão de risco da proteção de dados. (KUNER et al., 2015, p. 5)

Os autores Kuner *et al.* (2015) e Gellert (2017) concordam em relação à aplicação das ferramentas de gerenciamento de riscos em proteção de dados. Ambos destacam a Avaliação de Impacto de Proteção de Dados (DPIA, sigla em inglês). Gellert (2017) aponta como a principal ferramenta de gestão de riscos utilizada em proteção de dados. Enquanto Kuner *et al*. (2015) afirmam que a DPIA precisa estar de acordo com as normas e metodologias de gerenciamento de risco.

Nos artigos analisados na revisão sistemática, a ferramenta DPIA apareceu diversas vezes como aplicação dos temas analisados, por esta razão é necessário entender sua origem e funcionamento. As avaliações de impacto de privacidade e proteção de dados (PIA/DPIA) são ferramentas utilizadas pelas organizações para realizar a gestão dos riscos de privacidade e proteção de dados (BINNS, 2017).

A forma conceitual dos PIA/DPIA foi originada para entender os riscos de impacto de áreas mais amplas como política e direito ambiental na década de 1990, nos países Canadá, Austrália e Nova Zelândia. Em 2000, foi adotada pela área de proteção de dados, tornando-se uma ferramenta essencial, em que várias autoridades nacionais de proteção de dados passaram a produzir orientações a respeito (BINNS, 2017).

Dijk, Gellert e Rommetveit (2015) apresentam os modelos de realização destas avaliações que foram elaborados no decorrer do tempo, são eles:

a) *Privacy Impact Assessment* e *Data Protection Impact Assessment Framework* (DPIAF), proposto pela indústria em 2010 para organizações que fazem uso da tecnologia RFID (*Radio Frequency Identification*), utilizada para

verificação de informações e comandos;

b) DPIA para redes e sistemas de medição inteligente, apresentado pelo grupo de especialistas (EG2) da Força-Tarefa de Redes Inteligentes da Comunidade Europeia em 2013;
c) Documento de elaboração do DPIA, publicado pela Agência Europeia para a Segurança das Redes e da Informação (ENISA);
d) *Privacy Impact Assessment* – methodology CNIL (*Commission Nationale Informatique & Libertés*), a agência de proteção de dados francesa.

A avaliação de impacto exigida na legislação europeia se assemelha em alguns pontos com os modelos apresentados, mas traz especificidades para a realidade de proteção de dados da união europeia (DIJK; GELLET; ROMMETVEIT, 2015).

É importante ressaltar que não existe um modelo padrão a ser seguido, os frameworks de realização da DPIA são escolhidos de acordo com a realidade da organização e do que é solicitado pela legislação. Nos casos analisados nesta revisão foram utilizados modelos diferentes para a execução do exercício.

De acordo com Wolford (2020), a avaliação de impacto a proteção de dados está estabelecida no artigo 35 da GDPR como obrigatória para operações que, provavelmente, podem acarretar um alto risco para as informações dos titulares dos dados. Contudo, elenca diversos aspectos que se estiverem na operação, o DPIA se torna necessário, seguem abaixo:

a) Utilização de novas tecnologias;
b) Rastreamento de localização ou o comportamento de pessoas;
c) Monitoramento sistemático de locais públicos;
d) Processamento de dados pessoais sensíveis;
e) Processamento de dados infantis;
f) Se o processamento for utilizado na tomada de decisões sobre pessoas que possam ter efeitos legais;
g) Se os dados processados vazarem puderem acarretar danos físicos aos titulares.

Ainda no artigo 35, a GDPR informa que é necessário conter no DPIA os seguintes elementos:

> [...] uma descrição sistemática das operações de tratamento previstas e as finalidades do tratamento, incluindo, quando aplicável, o interesse legítimo prosseguido pelo responsável pelo tratamento.
>
> Uma avaliação da necessidade e proporcionalidade das operações de

> tratamento em relação às finalidades.
>
> Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados.
>
> As medidas previstas para lidar com os riscos, incluindo salvaguardas, medidas de segurança e mecanismos para garantir a proteção de dados pessoais e demonstrar a conformidade com o GDPR, levando em consideração os direitos e interesses legítimos dos titulares dos dados e outras pessoas envolvidas. (UNIÃO EUROPEIA, 2018)

Atualmente existem diversas ferramentas para a execução do DPIA disponíveis, cada uma com sua particularidade, como já mencionado anteriormente não existe apenas um modelo a ser seguido. A da ENISA é uma plataforma online que consiste em seis etapas para calcular o risco. Já a plataforma da CNIL considera responsável os profissionais que realizam o tratamento dos dados. O DPIA, independente do modelo escolhido, é realizado através de um questionário que deve ser respondido pelo responsável pelo processo analisado (GRANADILLO et al., 2021).

De acordo com Granadillo et al. (2021), ainda existem outras ferramentas mais direcionadas a cumprir o que é solicitado pela legislação:

> A ferramenta GDPR DPIA (Ferramenta DPIA) é uma ferramenta baseada na Web para ajudar as organizações a avaliar os riscos de proteção de dados em relação ao GDPR. A ferramenta foi desenvolvida para apoiar a implementação do DPIA e fornece uma abordagem estruturada e orientada para o risco para identificação e avaliação de potenciais riscos de proteção de dados. A estrutura da ferramenta DPIA é baseada em um questionário e, portanto, oferece uma automação bastante limitada da avaliação das atividades de processamento de dados pessoais dentro da organização. Por último, a ferramenta Compliance-Kit 2.0 segue a norma britânica, GDPR e ISO 29100, e baseia-se na obrigação legal de cumprir os requisitos do GDPR e das estratégias de gestão decisão de implementar esses regulamentos com o objetivo de estabelecer, manter e desenvolver o Gerenciamento de Proteção de Dados prático e orientado a processos. (GRANADILLO *et al.*, 2021, p. 5)

Granadillo et al. (2021), em seu trabalho, propõem um kit de ferramentas de gerenciamento de riscos cibernéticos e de privacidade, chamada AMBIENT (*Automed Cyber and Privacy Risk Management*), que integra *softwares* e ferramentas que auxiliam na avaliação de riscos e impactos de forma automatizada, com recursos que auxiliam no suporte a tomada de decisão, a ferramenta foi criada para ser utilizada em ambientes de saúde. Os autores dividem a ferramenta em três módulos: o módulo 1 de segurança cibernética, o módulo 2 de avaliação dos riscos de privacidade e o módulo 3 de mitigação de riscos. O módulo 2 irá considerar as informações relevantes obtidas no módulo 1 e realizará ao mapeamento de operações de processamento de dados, para encontrar os riscos de proteção de dados existentes. Por fim, o módulo 3 irá criar formas de mitigação para os riscos encontrados (GRANADILLO et al., 2021).

Em razão do foco deste estudo estar em gerenciamento de riscos aplicado à proteção de dados, vamos manter o foco no módulo 2 do kit de ferramentas voltado para avaliação de riscos de proteção de dados.

Os autores apostam em uma forma de automatizar a realização do DPIA, que ocasionalmente é realizado de maneira mais manual, apenas direcionando o questionário para o responsável por respondê-las, e os modelos já supracitados auxiliam na elaboração das perguntas e na avaliação das respostas do questionário DPIA. Na AMBIENT, o DPIA será realizado de forma automática, considerando evidências obtidas através de sensores de infraestrutura implantados e ações de processamento dos dados que já são documentadas nas organizações (GRANADILLO et al., 2021). Os autores ainda especificam:

> Avaliação de Risco de Privacidade considera as inter-relações que existem entre os ativos de infraestrutura de Tecnologia da Informação e Comunicação (TIC) que suportam atividades de processamento de dados, fontes de dados, titulares de dados e informações de identificação pessoal (PII) e infere os riscos de privacidade que uma organização pode enfrentar devido a vulnerabilidades e ameaças direcionadas a ela. (GRANADILLO *et al.,* 2021, p. 11)

Ao analisar o trecho acima, é possível entender que o modelo proposto pelos autores, vai ao encontro do proposto por Gellert (2015), relacionando o tema de proteção de dados a infraestrutura de Tecnologia da Informação e Comunicação. Com o resultado da avaliação de impacto de privacidade, a AMBIENT gera uma lista de riscos encontrados e possíveis formas de mitigação, que podem auxiliar os gestores na tomada de decisão (GRANADILLO et al., 2021).

Além da avaliação de impacto (DPIA), o módulo conta com outros componentes que auxiliam a realizar a avaliação dos riscos de privacidade. Os autores apresentam que os dois pilares do módulo são um sistema de pontuação para quantificar os riscos de privacidade ocasionados por vulnerabilidades e ameaças identificadas. Já o segundo pilar está voltado a auxiliar os administradores a estarem em conformidade com a GDPR e demais agências reguladoras. (GRANADILLO et al., 2021). Aqui vale destacar a utilização de outra ferramenta de gerenciamento de riscos aplica à proteção de dados, o mapeamento de vulnerabilidades.

Análise de Vulnerabilidade é o processo de identificação das falhas e fragilidades presentes no ambiente e que pode expor a organização a ameaças. Pode se entender também como incapacidade de impedir que o risco vire realidade. (GAZOLA, 2020). De acordo com Instrução Normativa Conjunta MP/CGU nº 01/2016,

que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal, elenca o mapeamento e análise das vulnerabilidades dos processos das organizações, como um princípio básico a ser seguido pela gestão de riscos da organização (BRASIL, 2016).

Georgiou e Lambrinoudakis (2021) apresentaram um estudo de caso a respeito da realização de um DPIA, seguindo o modelo de avaliação de impacto proposto pela CNIL, em uma organização de saúde. Contudo apresentaram somente as duas primeiras etapas do exercício, a finalidade do tratamento de dados e as categorias de dados envolvidos nos processos analisados, ao final realizam uma análise de lacunas para verificar o nível de conformidade a GDPR. Os autores concluem que a realização de DPIA é uma excelente forma de avaliar os riscos existentes nos processos (GEORGIOU; LAMBRINOUDAKIS, 2021).

> O estudo de Avaliação de Impacto na Proteção de Dados é uma ferramenta útil, com o objetivo de avaliar os riscos de privacidade envolvidos nas operações de processamento. Um DPIA ajuda as organizações a atender às expectativas de privacidade e proteção de dados de seus clientes, funcionários e outras partes interessadas. (GEORGIOU; LAMBRINOUDAKIS, 2021, p. 11)

A respeito das avaliações de impacto conhecidas, Gonçalves (2017) alerta para que não sejam realizadas pelas empresas apenas a fim de estar em conformidade com a legislação. A realização do DPIA é de caráter obrigatório de acordo com a GDPR apenas em processos que acarretem altos riscos aos titulares de dados, no entanto, é recomendado que se faça em todos os processos que envolvam tratamento de dados. A autora ainda ressalta que a falta de padronização e incertezas a respeito do DPIA pode depreciar sua eficiência enquanto ferramenta de gerenciamento de riscos de proteção de dados. De acordo com Gonçalves (2017), o framework elaborado para as empresas RFID está na direção correta de uma padronização ideal das avaliações de impacto.

Cha e Yeh (2021), em seu trabalho, propõem uma avaliação de riscos baseada em dados para a proteção de dados pessoais. Esta avaliação é difere das avaliações de impacto conhecidas até aqui, pois não é baseada em processos, mas mantém o objetivo semelhante de avaliar os riscos para proteção de dados nas operações. Os autores afirmam que a avaliação de riscos baseada em dados tem o objetivo de alertar as organizações para os riscos existentes em dados confidenciais que não são utilizados. A principal crítica que os autores trazem ao DPIA tradicional é que busca

garantir que as organizações estejam de acordo com os princípios de proteção de dados, do que garantir que os riscos envolvidos não se materializem. O esquema proposto é composto pelas seguintes etapas:

1) Identificação dos dados pessoais envolvidos e os predispostos legais aplicáveis;
2) Identificar as fontes dos dados pessoais e os destinos do compartilhamento dos dados;
3) Mapeamento dos fluxos dos dados pessoais;
4) Identificação da possibilidade de incidentes envolvendo os dados pessoais;
5) Avaliação dos riscos identificados.

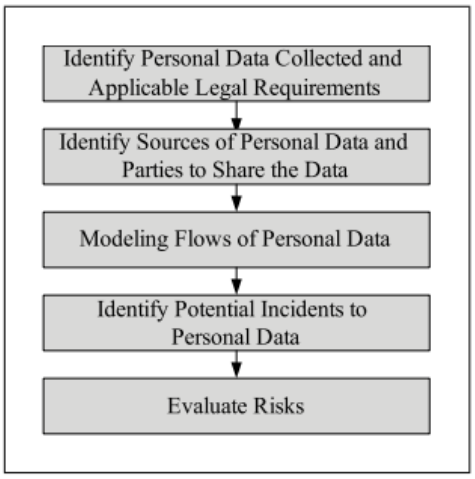

Figura 3. Etapas do esquema proposto.

Fonte: CHA e YEH (2021, p.3)

Ao analisar os trabalhos de Gonçalves (2017) e de Cha e Yeh (2021), nos deparamos com uma crítica à aplicação do DPIA nas empresas com objetivo de cumprir somente o estabelecido na legislação. Ambos afirmam que os resultados obtidos com o DPIA devem ser considerados pelo gerenciamento de riscos das organizações.

Santosa e Yusvinindya (2019) propõem a utilização de análise de risco e controle para o processo de proteção de dados pessoais das aplicações Sistema de Informação da Administração da População (SIAK), utilizada no gerenciamento de dados pessoais de residentes da Indonésia.

As análises de riscos foram baseadas no modelo de referência de gerenciamento de riscos ISO 31000:2018, que consiste, de acordo com os autores, nas seguintes etapas: “definição do escopo, contexto e critérios; avaliação de risco

que inclui identificação, análise e avaliação de risco; e, finalmente, tratamento de risco” (SANTOSA; YUSVININDYA, 2019, p. 499).

A definição do escopo, contexto e critérios consiste em avaliar os processos de proteção de dados pessoais, a fim de descobrir quais dos seus ativos possuem riscos e se possuem, ou não, controles mapeados para mitigá-los. Já na segunda etapa, se faz necessário antes de iniciá-la, a definição dos critérios de avaliação dos riscos, no trabalho analisado são escolhidos a taxa de ocorrência e impacto causado pelo risco, após os riscos serão classificados como baixo, médio e elevado, estas informações serão inseridas da Matriz de Riscos. Após os critérios definidos deve-se seguir para a identificação dos riscos existentes nos processos de proteção de dados, também devem ser descritos na matriz. Em sequência os riscos descritos serão avaliados conforme os critérios definidos anteriormente. Por fim, são apresentados os controles existentes para os riscos mapeados, caso não exista controle mapeado, o risco pode ter sua avaliação modificada, e definem os controles em preventivo, sucessivo e corretivo, podendo um risco apresentar mais de um controle. Em seu trabalho, os autores concluem que o processo de proteção de dados avaliado possui risco médio/alto e optam por mitigar os riscos mapeados (SANTOSA; YUSVININDYA, 2019).

Após análise é possível identificar mais uma ferramenta de gerenciamento de riscos que pode trazer benefícios quando aplicada ao processo de proteção de dados, a matriz de riscos e controles. Portanto é possível concluir, com base na literatura analisada, que ferramentas de gerenciamento de riscos trazem benefícios quando são aplicadas a proteção de dados. Destaca-se três que foram utilizadas nos casos analisados, primeiro majoritariamente as avaliações de impacto e riscos a proteção de dados, a análise de vulnerabilidades, e por fim, a análise de riscos e controles (matriz de riscos e controles).

A seguir o Quadro 4 sintetizando as ferramentas encontradas nos artigos analisados nesta revisão.

Quadro 4. Ferramentas Encontradas nos artigos. Porto Alegre, 2022.

Ferramenta	Artigo da RSL	Autor/Ano/Local	Periódico	Explicação
Registro de atividade de tratamento/Análise de Impacto a Proteção de Dados (DPIA)	A risk to a right? Beyond data protection risk assessments	DIJK*et al*. (2015). Europa	Freedom Collection Journals [SCFCJ]	Ferramenta utilizada para realizar o gerenciamento de riscos a proteção de dados com base no impacto que os processos têm para as organizações. Registradas na GDPR como obrigatória em alguns casos.
	A Data-Driven Security Risk Assessment Scheme for Personal Data Protection	CHA e YEH (2021). Taiwan	DOAJ Directory of Open Access Journals	
	Data protection impact assessments: a meta-regulatory approach	GELLERT (2017) Inglaterra	Oxford Journals Current Collection	
	Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations	GEORGIOU e LAMBRINOUDAKIS (2021). Grécia	DOAJ Directory of Open Access Journals	
	Risk Management In Data Protection	KUNER *et al*. (2015). Inglaterra	Oxford Journals Current Collection	
	Understanding the notion of risk in the General Data Protection Regulation	GELLERT (2018). Europa	Freedom Collection Journals [SCFCJ]	
Análise de Vulnerabilidades	Automated Cyber and Privacy Risk Management Toolkit	GRANADILLO *et al (*2021). Suíça	DOAJ Directory of Open Access Journals	Consiste no conhecimento das lacunas e fraquezas presentes no ambiente podendo expor a organização à ameaças
Análise de Riscos e Controles (Matriz de Riscos e Controles)	Risk Analysis and Control of Personal Data Protection in the Population Administration Information System	SANTOSA e YUSVININDYA (2019). Indonésia	DOAJ Directory of Open Access Journals	Mapeamento dos riscos e controles existentes nos processos. Tem como objetivo entender, avaliar, classificar e controlar os riscos existentes nos processos das organizações.
Aplicação do Gerenciamento de riscos a proteção de dados(Análise jurídica)	Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative	GELLERT (2015). Inglaterra	Oxford Journals Current Collection	Os autores defendem a utilização do gerenciamento de riscos aplicado a proteção de dados de uma forma geral. Trazem aspectos que evidenciam a eficiência do uso das ferramentas e recomendações do gerenciamento de riscos aplicado a proteção de dados.
	The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward	GONÇALVES (2017). Portugal	Computers & Applied Sciences Complete	

Fonte: Elaborado pela autora.

Com base nos conhecimentos obtidos na revisão sistemática e com o objetivo de entender sua aplicação no dia a dia da empresa analisada, foram realizadas perguntas para compor um questionário para conduzir as entrevistas na pesquisa qualitativa. O quadro abaixo relaciona o assunto encontrado na revisão sistemática com a pergunta que foi realizada nas entrevistas.

Quadro 5. Ferramentas Encontradas nos artigos e perguntas das entrevistas. Porto Alegre, 2022.

Ferramenta	Autor/Ano/Local	Explicação	Questionamentos nas entrevistas
Registro de atividade de tratamento (ROPA) /Análise de Impacto a Proteção de Dados (DPIA)	DIJK*et al*. (2015). Europa	Ferramenta utilizada para realizar o gerenciamento de riscos a proteção de dados com base no impacto que os processos têm para as organizações. Registradas na GDPR como obrigatória em alguns casos.	Quais as ferramentas gerenciamento de riscos utilizado pela área de proteção de dados?
	CHA e YEH (2021). Taiwan		Como a aplicação das ferramentas de gerenciamento de riscos aplicadas a proteção de dados influenciaram no seu processo de trabalho?
Análise de Vulnerabilidades	GRANADILLO *et al (*2021). Suíça	Consiste no conhecimento das lacunas e fraquezas presentes no ambiente podendo expor a organização à ameaças	Quais as principais facilidades e dificuldades que você encontrou na execução das ferramentas?
Análise de Riscos e Controles (Matriz de Riscos e Controles)	SANTOSA e YUSVININDYA (2019). Indonésia	Mapeamento dos riscos e controles existentes nos processos. Tem como objetivo entender, avaliar, classificar e controlar os riscos existentes nos processos das organizações.	Como você vê a mudança em seus processos depois da implantação das modificações sugeridas após a aplicação das ferramentas de gerenciamento de riscos aplicadas a proteção de dados?
Aplicação do Gerenciamento de riscos a proteção de dados (Análise jurídica)	GELLERT (2015). Inglaterra	Os autores defendem a utilização do gerenciamento de riscos aplicado a proteção de dados de uma forma geral. Trazem aspectos que evidenciam a eficiência do uso das ferramentas e recomendações do gerenciamento de riscos aplicado a proteção de dados.	Como o gerenciamento de riscos é utilizado na área de proteção de dados?
	GONÇALVES (2017). Portugal		Como as demais áreas receberam a implementação das ferramentas de gerenciamento de riscos da área de proteção de dados?

Fonte: Elaborado pela autora.

4.2 PESQUISA QUALITATIVA NA EMPRESA

De acordo com o gestor de proteção de dados da empresa analisada (G1), a área de proteção de dados levou cerda de dois anos para ser implementada de uma forma completa. Em 2019, iniciaram a possibilidade de solicitação de direito dos titulares e a gestão do consentimento do uso de dados dentro da organização, para clientes, parceiros, fornecedores, colaboradores e todo e qualquer titular que a empresa realize o tratamento de dados. Em 2020, os primeiros registros de processamento de dados foram realizados, e, em 2021, houve uma revisão dos processos estabelecidos dois anos antes, proporcionando uma maior aderência e eficiência neles, em consequência disso, a organização iniciou a implementação das primeiras ferramentas de gerenciamento de riscos aplicados a proteção de dados. Conforme dito por G1, “.... é difícil definir um momento exato da implementação... acredito que é quando se tem todo um arcabouço, todo um framework de trabalho que contemple todos os aspectos da lei, e isso leva mais tempo...”.

Hoje o gestor enxerga a área de proteção de dados como consolidada, pois é referencia do tema no mercado e no grupo que está inserida, e afirma que não existe alguma outra ferramenta de gerenciamento de riscos que seria interessante implementar na área pois, “... hoje as ferramentas que nós temos, nos atendem muito bem, e não tenho conhecimento de alguma outra que seria eficiente aplicar aqui...”. G1 acredita que os próximos passos para a área de proteção de dados envolvem gerar mais valor para a companhia e aumentar a mitigação de riscos existentes. Ele afirma que são muito eficientes em identificar riscos, mas ainda não tem tanta adesão da primeira linha de defesa para modificar os processos e mitigar os riscos existentes de maneira definitiva.

O gerenciamento de riscos é aplicado à proteção de dados na organização em todos os processos de tratamento. Todas as etapas da cadeira produtiva que resultam no produto final precisam ter os seus riscos analisados, com o objetivo de entendermos se o produto como um todo está gerando riscos de proteção de dados a organização. De acordo com G1, “... é necessário avaliar a cadeia como um todo, todas as etapas do tratamento de dados e identificar aonde eu estou tendo algum furo ou gap que está gerando risco para a companhia...”. G1 complementa, que as ferramentas são muito úteis para realizar essa gestão de forma eficiente. Os maiores benefícios do uso do gerenciamento de riscos aplicado a proteção de dados elencado

por G1 envolvem entender aonde a empresa está sendo exposta, conseguir monitorar essa exposição e, complementa, que ter uma gestão de riscos efetiva pode ser um ponto positivo em um caso de incidente de vazamento de dados, por exemplo, pois isso pode diminuir a multa ou a pena a ser aplicada. G1 finaliza afirmando, “... o gerenciamento de riscos é um trabalho preventivo e mitigativo, pois ajuda a prevenir e remediar...”.

A seguir será detalhado como as ferramentas são utilizadas na empresa.

4.2.1Utilização das ferramentas na empresa

Todas as ferramentas aplicadas na companhia são executadas pela chamada por G1 de “primeira linha de defesa”, ou seja, as demais áreas da companhia, todas são realizadas através do que foi chamado de “self assessment”, que consiste em uma auto-avaliação da área em relação aos riscos e impactos envolvidos nos seus processos. Segundo G1, essa metodologia é eficiente pois, “... eles são os maiores conhecedores dos seus processos, ninguém melhor que eles para realizar essa análise de forma eficiente, nós só precisamos perguntar as coisas certas...”.

A principal ferramenta de gerenciamento de riscos utilizada pela organização hoje é a Avaliação de Impacto para Proteção de Dados (DPIA), especialmente por sua obrigatoriedade prevista na legislação. Contudo, também são aplicadas a matriz de riscos e controles e a análise de vulnerabilidades. A primeira é antecedida pelo registro das atividades de tratamento (ROPA), o qual gera embasamento para eleger as áreas que irão participar do DPIA. Áreas que apresentaram processos de alta criticidade no ROPA participam do DPIA.

O ROPA é realizado através de uma planilha em que as demais áreas da organização precisam responder questionamentos acerca do tratamento de dados envolvidos no processo, não só dados pessoais. Já o DPIA é realizado através de uma ferramenta chamada Security.Ai, ferramenta específica para gestão de dados, conforme G1, “... em relação a privacidade ela é uma das líderes de mercado junto com a One Trust, por isso nós a escolhemos...”. Após a área responder o DPIA, o sistema automaticamente gera um resultado com os gaps encontrados no processo que oferecem risco a proteção de dados. Para os impactos altos e críticos identificados pelo sistema, a área precisa implementar um plano de ação, visando diminuir o impacto do processo para a empresa.

A matriz de risco e controle e análise de vulnerabilidades, assim como o ROPA, são realizadas através de planilhas que serão preenchidas com as informações solicitadas pela área técnica (forma que G1 denomina a área de proteção de dados). A matriz de risco e controle tem como objetivo fazer com que a própria área identifique seu risco e um controle para mitigá-lo, se algum risco não possui controle, ou do controle foi classificado como não efetivo, a área recebe uma recomendação de executar um plano de ação para elaborar um novo controle para a mitigação do risco identificado. Já a análise de vulnerabilidade, tem como propósito buscar os chamados por G1 de “furos na cadeia como um todo” que podem vir a gerar riscos para a companhia. Diferente da matriz de riscos e controles, essas vulnerabilidades precisam ser eliminadas antes que virem um risco para a companhia. Conforme G1: “... a ordem que deve ser seguida é ROPA, DPIA e análise de vulnerabilidades e matriz de riscos e controles, pois é identificado o processo crítico, é analisado seu impacto, é elencado suas vulnerabilidades e os riscos que no fim da aplicação de todas as ferramentas ainda não foi mitigado, vai para a matriz de riscos e controles...”.

Os maiores benefícios trazidos pelo gerenciamento de riscos aplicados a proteção de dados foi o maior conhecimento dos processos da companhia sob a ótica da gestão de dados. G1 afirma que hoje não existe um mapeamento completo de todos os processos da empresa, mas que, graças às ferramentas aplicadas, existe o mapeamento de todos os fluxos de dados existentes na empresa. Em contrapartida, G1 traz que a maior dificuldade encontrada na implementação das ferramentas foi a “... pulverização dos dados, existiam milhares de bases de dados, sem controle nenhum do que estava sendo feito com eles, realizar o mapeamento de onde estes dados passavam foi o nosso maior desafio...”. Já para as áreas, G1 afirma que inicialmente tiveram muito receio do que poderia acontecer, como seriam os processos a partir daquele momento. Devido ao recente conhecimento do tema, algumas áreas nem tinham a ciência de que estavam tratando dados pessoais e das consequências que isso poderia causar para a empresa caso não fosse gerido da maneira correta.

4.2.2 Benefícios, facilidades e dificuldades da aplicação das ferramentas

No Quadro 5 foram elencados os principais pontos obtidos na análise das entrevistas. É importante ressaltar que o Quadro abaixo é referente somente as três entrevistas realizadas com os colaboradores das demais áreas que já aplicaram as

ferramentas de gerenciamento de riscos para proteção de dados, por isso, a entrevista do gestor não está contemplada na análise abaixo.

Quadro 6. Categorias emergentes das opiniões dos participantes da pesquisa. Porto Alegre, RS, 2022.

Categoria	Subcategoria	Número de Entrevistados	Fala dos Entrevistados
Facilidades	Facilidade de execução	3	E1: “A principal facilidade foi a forma escolhido para preenchermos a ferramenta, foi um questionário que demorou cerca de 5 minutos para ser respondido e o sistema automaticamente já identificava os riscos e o seu nível de impacto”.
	Utilização de sistemas	3	E2: “O DPIA é ótimo porque é em sistema”.
	Apoio da área técnica	2	E1: “Contudo a equipe de proteção de dados prestou todo o apoio necessário para a execução”.
Dificuldades	Recente Legislação de Proteção de Dados	3	E1:”... Acredito que algumas dúvidas tenham surgido em razão da novidade do tema, e da recente legislação”.
	Utilização de Planilhas	3	E1 “:.. a Matriz de riscos e controles e a análise de vulnerabilidade são feitas por planilhas o que ocasiona em muita perda de tempo”.
	Tempo gasto na execução	3	E3: “... Ainda existem muitas manualidades envolvidas nos processos, e isso demora, e tempo é dinheiro né?...”.
Impactos causados pelas ferramentas	Impacto na Aplicação na área	3	E2: “... O período do ano que em as ferramentas estão sendo aplicadas, eu sempre preciso onerar 1 ou 2 analistas para focarem somente neste tema, o que gera atraso nos meus processos do dia a dia”.
	Mudanças resultantes	3	E2: “... Mapeamos 2 de nossos processos que possuíam fluxo de dados e em cada um deles foram identificados 2 gaps a serem melhorados”.
	Sem Impacto	0	-
Resultado da Aplicação	Execução de Plano de Ação	2	E1: “... Para cada um dos gaps precisávamos apresentar um plano de ação a ser implementado até dia 31/12/2021, alguns tinham prazo final encerrando antes, dependendo da complexidade do plano de ação. Isso foi realizado”.
	Sem Execução de Plano de ação	1	E3: “... Até a data final havíamos realizado a implementação de aviso de privacidade para coleta de dados de terceiros, contudo não estabelecemos procedimento de eliminação, pois não concordávamos com a necessidade de eliminação...”.
Entendimento da importância do Gerenciamento de Risco para Proteção de Dados	Sim	2	E2: “... Hoje é claro, pois a LGPD e suas sanções já estão sendo aplicadas, e em razão disso, a empresa organizou diversos treinamentos de conscientização sobre o tema...”.
	Não	1	E3: “...: Acredito que até seja importante, mas vejo hoje mais como mais uma burocracia, já existem tantas na empresa, acho que é só mais uma...”.

Fonte: Elaborado pela autora.

5 DISCUSSÃO DOS RESULTADOS

Na revisão sistemática da literatura observou-se uma predominância de casos relatados em empresas de saúde. Contudo, foi identificado que no viés de gerenciamento de riscos aplicado à proteção de dados, estas organizações se assemelham em diversos aspectos a organização analisada neste estudo.

Ao confrontar os resultados obtidos nas entrevistas com as informações resultantes da revisão sistemática, é possível chegar a algumas considerações. As três ferramentas citadas pelos autores na revisão sistemática, ROPA/DPIA, matriz de riscos e controles e análise de vulnerabilidades, são aplicadas na empresa TX, que foi analisada neste estudo. A empresa já executa as ferramentas com o viés de proteção de dados desde 2019, e a cada ano evoluem em sua aplicabilidade.

A primeira ferramenta implementada foi o ROPA/DPIA. Em um primeiro momento foi realizado o mapeamento dos processos que envolviam o fluxo de dados pessoais em sua execução, utilizando o ROPA, realizado em uma planilha de Excel com alguns parâmetros, escolhidos pela empresa. Gonçalves (2017) e Cha e Yeh (2021) referem que não existe uma padronização de parâmetros para esta ferramenta. A legislação atual exige a sua realização, mas não estabelece nenhum framework específico. A TX, segundo G1, utiliza o framework de origem europeia ENISA. Os parâmetros quando respondidos pela área possibilitam classificar a criticidade do processo para a companhia. Após este mapeamento, os processos classificados como críticos, no ROPA, tornaram-se elegíveis ao DPIA. Vale lembrar que o DPIA é obrigatório na LGPD, assim como na GDPR. De acordo com o encontrado na revisão sistemática, defendido pelos autores Gonçalves (2017) e Cha e Yeh (2021), o DPIA não deve ser aplicado apenas em processos críticos, a fim de cumprir somente o que está previsto na legislação. Os autores defendem que todos os processos da empresa devem passar pelo DPIA, pois a ferramenta é eficiente para prevenir riscos e entender impactos que podem atingir a organização. Aqui encontramos o primeiro ponto de confronto entre que é aplicado pela empresa TX e o que é recomendado pela literatura.

A matriz de riscos e controles foi outra ferramenta identificada como eficiente na revisão sistemática e que também é aplicada na empresa TX. Os autores Santosa e Yusvinindya (2019) propõem um modelo de aplicação da matriz de riscos e controles de acordo a norma ISO 31.000:2018, norma também utilizada na aplicação da matriz

de riscos e controles na TX. Assim como o realizado pelos autores, a empresa segue as etapas definidas na norma, que envolvem os aspectos que serão detalhados a seguir. Definição de escopo, contextos e critérios: nesta etapa os processos que contém fluxo de dados, são avaliados sob a ótica de proteção de dados pessoais e são identificados em quais pontos dos processos existem riscos, e se existem controles para mitigá-los. Após é necessário definir critérios para a avaliação dos riscos, assim como no proposto por Santosa e Yusvinindya (2019), a TX realiza sua avaliação com base na taxa de ocorrência do risco e o impacto que tem na companhia. Em seguida os controles existentes também são avaliados, em preventivo, sucessivo e corretivo, dependendo da classificação do controle, a avaliação do risco pode ser influenciada. Todas essas informações são inseridas pela área na matriz de riscos e controles, na TX é feita de forma manual por meio de uma planilha. Ao final, o resultado obtido pela ferramenta é analisado pela área técnica, que definirá a necessidade de plano de ação ou não, conforme o proposto por Santosa e Yusvinindya (2019). De acordo com a análise das entrevistas realizadas, ao final, dois dos entrevistados, implementaram as melhorias solicitadas, e tiveram seus riscos mitigados, gerando benefícios para a organização como um todo.

É relevante considerar que diferente da ferramenta ROPA/DPIA, a Matriz de riscos e controles não é exigida pela legislação. Contudo após a análise da literatura e da sua aplicação na empresa, é possível concluir que a ferramenta tem sua eficiência comprovada e por isso é recomendada sua aplicação.

A ferramenta Análise de Vulnerabilidades é um princípio básico a ser seguido pelo gerenciamento de riscos nas organizações de acordo com a Instrução Normativa Conjunta MP/CGU nº 01/2016 (BRASIL, 2016). Assim como as demais ferramentas analisadas, também foi possível identificar a sua eficiência quando aplicada a proteção de dados. Porém diferentemente das outras ferramentas analisadas neste estudo, observou-se que é pouco relatada e descrita na literatura. Na empresa analisada, a ferramenta é realizada através de uma planilha e tem como objetivo mapear as vulnerabilidades a partir do olhar do “dono do processo” (colaborador especialista na realização de determinado processo), pois, conforme o que foi respondido por G1 na entrevista, esta é maneira mais eficiente de se analisar um processo. Vale ressaltar que a dependência do fator humano na avaliação das fraquezas das operações, pode diminuir a confiabilidade dos resultados obtidos na ferramenta.

Com o intuito de resolver esta questão, Granadillo et al. (2021) propõem um sistema denominando de AMBIENT, que apresenta em uma de suas funções, a identificação automatizada de vulnerabilidades e ameaças que ocasionarão riscos de privacidade para a empresa.

Conforme dados obtidos nas entrevistas, hoje a TX faz uso de um sistema de gestão de dados, a Securiti.Ai, que automatiza a realização do DPIA, além de auxiliar a empresa na automatização de demais aspectos exigidos pela legislação. O sistema proposto por Granadillo et al. (2021), se assemelha com a Securiti.Ai em alguns aspectos, mas apresenta outras funcionalidades que também se revelaram eficientes, dentre elas a já supracitada identificação automatizada de vulnerabilidades.

As ferramentas geram muitos dados que precisam ser analisados e avaliados de acordo com a LGPD. O sistema como o AMBIENT (GRANADILLO et al., 2021) e o Securiti.Ai, utilizado pela TX, auxiliam os gestores a estarem em conformidade com a legislação, automatizando todo o arcabouço de gestão de dados, facilitando os processos. Além disso, os entrevistados afirmam que das três ferramentas, ROPA/DPIA, Matriz de Riscos e Controle e Análise de Vulnerabilidade, apenas o DPIA é realizado via sistema, os demais são realizados por planilha, o que foi uma dificuldade relatada pelos entrevistados. Neste aspecto o AMBIENT, se mostra superior ao Securiti.Ai, principalmente no aspecto de análise de vulnerabilidade. Percebe-se que a utilização de sistemas além de facilitar a execução e avaliação das ferramentas, também gera mais confiabilidade aos resultados obtidos.

6 CONCLUSÃO

Ao final da pesquisa, estudando as ferramentas de gerenciamento de riscos aplicáveis à proteção de dados propostas na literatura, percebe-se uma convergência ao analisar a aplicação das ferramentas em uma empresa de tecnologia especializada em meios de pagamento do Rio Grande do Sul. As ferramentas de gerenciamento de riscos demonstraram sua eficiência para melhoria dos processos de proteção de dados.

Como limitações deste estudo destacam-se o pouco tempo de aplicabilidade da LGPD, assim como todas as demais legislações de proteção de dados a nível mundial. Na revisão sistemática não foram encontrados artigos descrevendo a realidade brasileira, a maioria dos artigos encontrados refere-se à legislação europeia, a GDPR, que muito se assemelha à brasileira. Além disso, não foram localizados artigos referentes ao gerenciamento aplicado à proteção de dados em empresas de tecnologia especializadas em meios de pagamentos. Por fim, em razão da dificuldade de acessar este nível de informação nas empresas privadas, o estudo foi realizado em uma só empresa.

Após as análises realizadas, observou-se que os sistemas automatizados auxiliam as organizações no cumprimento da legislação, e facilitam a execução dos processos. A partir das entrevistas, foi possível perceber que a realização das ferramentas via planilhas foi apresentada como uma dificuldade pelos usuários. Já a realização de forma automatizada via sistemas é dita como uma facilidade. Assim, conclui-se que a utilização de sistemas demonstra maior efetividade e credibilidade, quando comparados a aplicação destas ferramentas de forma manual.

Em razão do exposto acima e a relevância do tema, recomenda-se a realização de mais estudos sobre o tema.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR-ISO31000**: gestão de riscos: princípio e diretrizes. Rio de Janeiro: ABNT, 2009.

AHRENS, Jan Martinez. Vendaval Cambridge Analytica abala os EUA por fraudes com dados do Facebook. **El País**, Washington, 21 de mar, 2018. Disponível em: https://brasil.elpais.com/brasil/2018/03/20/internacional/1521574139_109464.html. Acesso em: 04 fev. 2022.

ALVES, Ana do C.M.R. **A evolução da auditoria interna após a Lei SOX**: impactos indirectos no caso português. Tese de Doutorado. Universidade de Aveiro, 2009. Disponível em: https://oatd.org/oatd/record?record=handle%5C%3ª10773%5C%2F3261. Acesso em: 06 abr. 2022.

ASSI, Marcos. **Gestão de Riscos com Controles Internos**: Como vencer os desafios e manter a eficiência dos negócios. 1. ed. São Paulo: Saint Paul, 2012.

BACEN. Banco Central do Brasil. Diretoria Colegiada. **Circular nº 3.681**, de 4 de novembro de 2013. Dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 04 novembro 2013.

BACEN. Banco Central do Brasil. Conselho Monetário Nacional. **Resolução nº 4.557**, de 23 de fevereiro de 2017. Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital. Diário Oficial da União: seção 1, Brasília, DF, n. 41, p. 41, 01 março 2017.

BACEN. Banco Central do Brasil. Diretoria Colegiada. **Resolução BCB nº 25**, de 22 de outubro de 2020. Altera a Circular nº 3.681, de 4 de novembro de 2013. Diário Oficial da União: seção 1, Brasília, DF, nº 205, p. 50, 26 outubro 2020.

BARDIN, Laurence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BINNS, Reuben. Data Protection Impact Assessments: a Meta-Regulatory Approach. **International Data Privacy Law**, v. 7, n. 1, p. 22-35, 2017. Disponível em: https://academic-oup-com.ez45.periodicos.capes.gov.br/idpl/article/7/1/22/3782692 Acesso em: 20 de jun. 2022.

BRASIL. **Instrução Normativa Conjunta MP/CGU nº 01/2016**, de 10 de maio de 2016. Brasília, DF: Ministério da Justiça e Segurança Pública, 2016.

BRASIL. **Lei nº 13.709**, de 14 de Agosto de 2018. Dispõe a Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Casa Civil, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 de fev. 2022.

BRASIL. **Lei nº 13.853**, de 8 de Julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 05 de fev. 2022.

CADBURY, Adrian. **Report of the committee on the financial aspects of corporate governance**. Sidney: Gee, 1992.

CHA, Shi-Cho; YEH, Kuo-Hui. A Data-Driven Security Risk Assessment Scheme for Personal Data Protection. **IEEE Access**, v. 6, p. 510-17, 2018. Disponível em: https://ieeexplore-ieee-org.ez45.periodicos.capes.gov.br/document/8454722. Acesso em: 05 de jul. 2022.

CORACCINI, Rafael. **Empresas não conseguem se adaptar à lei de proteção de dados aponta pesquisa CNN-Brasil**. São Paulo, ago. 2021. Disponível em: https://www.cnnbrasil.com.br/business/empresas-nao-conseguem-se-adaptar-a-lei-de-protecao-de-dados-diz-pesquisa/. Acesso em: 06 de fev. 2022.

COSO. Committee of Sponsoring Organizations. **Gerenciamento de Riscos Corporativos**: Estrutura Integrada, Técnicas de Aplicação. New York, USA: AICPA, 2007.

COSO. Committee of Sponsoring Organizations. **Internal Control**: Integrated Framework. New York, USA: AICPA, 1992.

COSO. Committee of Sponsoring Organizations. **The 2013 COSO Framework & SOX Compliance**. New York, USA: AICPA, 2013.

DIJK, Niels van; GELLET, Raphael; ROMMETVEIT, Kjetil. A Risk to a Right? Beyond Data Protection Risk Assessments. **The Computer Law and Security Report**, v. 32, n. 2, p. 286-306, 2016. Disponível em: https://doi.org/10.1016/j.clsr.2015.12.017. Acesso em: 18 de jul. 2022.

FAÇANHA, Magali C.; LIMA, Francisco de Assis P.; LUCA, Márcia Martins M.; VASCONCELOS, Alessandra C. Gerenciamento de riscos e gestão de controles internos em empresas brasileiras envolvidas em crimes de corrupção e lavagem de dinheiro. **Revista Contemporânea de Contabilidade**, v. 17, n. 43, p. 34-50, 2020. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8083798. Acesso em: 08 de mar. 2022.

FERREIRA, Ricardo B.; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor K. da. **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia**. Migalhas, 2018. Disponível em: https://www.migalhas.com.br/dePeso/16,MI281042,81042-. Acesso em: 08 de mar. 2022.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2020. Disponível em: https://indexlaw.org/index.php/rdb/article/view/5343. Acesso em: 08 de mar. 2022.

FRASER, J.; SIMKINS, B.J. **Enterprise Risk Management**: An Introduction and Overview, in Enterprise Risk Management. NJ: John Wiley & Sons, 2009.

GALVÃO, Maria Cristiane B.; RICARTE, Ivan Luiz M. Revisão sistemática da literatura: conceituação, produção e publicação. **Logeion Filosofia da informação**, v. 6, n. 1, p. 57-73, 2019. Disponível em: http://revista.ibict.br/fiinf/article/ download/4835/4187/. Acesso em: 08 de mar. 2022.

GAZOLA, Rodrigo. Tudo que você precisa saber sobre a análise de vulnerabilidades. **Addee**, n. 20, fev. 2020. Disponível em: https://addee.com.br/blog/analise-de-vulnerabilidade-2/. Acesso em: 25 de jul. 2022.

GELLERT, Raphael. Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. **International Data Privacy Law**, v. 5, n. 1, p. 3-19, 2015. Disponível em: https://academic-oup-com.ez45.periodicos.capes.gov.br/idpl/article/5/1/3/622981. Acesso em: 20 de jun. 2022.

GELLERT, Raphaël. Understanding the Notion of Risk in the General Data Protection Regulation. **The Computer Law and Security Report**, v. 34, n. 2, p. 279-88, 2018. Disponível em: https://www-sciencedirect.ez45.periodicos.capes.gov.br/science/article/pii/S0267364917302698?via%3Dihub. Acesso em: 05 de jul. 2022.

GELLERT, Raphaël. **Understanding the risk-based approach to data protection**: Ananalysis of the links between law, regulation, and risk. Tese (Doutorado). Faculteit Rechten Criminologie, Vrije Universiteit Brussel, 2017.

GEORGIOU, Dimitra; LAMBRINOUDAKIS, Costas. Data Protection Impact Assessment (DPIA) for Cloud-Based Health Organizations. **Future Internet**, v. 13, n. 3, p. 66, 2021. Disponível em: https://www.mdpi.com/1999-5903/13/3/66. Acesso em: 05 de jul. 2022.

GIL, Antonio C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GODOY, Arlida Schmidt. Introdução à pesquisa qualitativa e suas possibilidades. **Revista de Administração de Empresas**, v. 35, p. 57-63, 1995.

GOMES, I.S.; CAMINHA, I.O. Guia para estudos de revisão sistemática: uma opção metodológica para as Ciências do Movimento Humano. **Revista Ensaios**, Porto Alegre, v. 20, n. 01, p. 395-411, 2014.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. **Temas atuais de proteção de dados**, São Paulo, p. 245-71, 2020. Disponível em: https://thomsonreuters.jusbrasil.com.br/doutrina/secao/1207548519/capitulo-9-entre-o-metodo-e-a-complexidade-compreendendo-a-nocao-de-risco-na-lgpd-temas-atuais-de-protecao-de-dados. Acesso em: 06 de fev. 2022.

GOMES, Maria Cecília O. Relatório de impacto à proteção de dados. **Revista do Advogado**, São Paulo, n. 133, p. 6-15, 2019.

GONÇALVES, Maria Eduarda. The EU Data Protection Reform and the Challenges of Big Data: Remaining Uncertainties and Ways Forward. **Information & Communications Technology Law**, v. 26, n. 2, p. 90-115, 2017. Disponível em: https://web-p-ebscohost.ez45.periodicos.capes.gov.br/plink?key=100.65.167.246_8000_1610622560&site=ehost&scope=site&db=iih&AN=123150164&crl=f. Acesso em: 05 de jul. 2022.

GRANADILLO, Gustavo G.; MENESIDOU, Sofia Anna; PAPMARTZIVANOS, Dimitrios; ROMEU, Ramon et al. Automated Cyber and Privacy Risk Management Toolkit. **Sensores**, v. 21, n. 16, p. 5493, 2021. Disponível em: https://www.mdpi.com/1424-8220/21/16/5493. Acesso em: 18 de jul. 2022.

GUTIERREZ, Andriel. **Lei Geral de Proteção de Dados Pessoais** (bibliografias selecionadas). São Paulo: Revista dos Tribunais, 2021.

HERRERA, Fernando Bravo. **Caso Enron**. Universidad de Chile, 2002. Disponível em: https://repositorio.uchile.cl/handle/2250/127318. Acesso em: 06 de abr. 2022.

IBGC. Instituto Brasileiro de Governança Corporativa. **Gerenciamento de Riscos Corporativos**: Evolução em Governança e Estratégia. São Paulo: IBGC, 2017.

IBGC. Instituto Brasileiro de Governança Corporativa. **Guia de Orientação para o Gerenciamento de Riscos Corporativos**. São Paulo: IBGC, 2007.

KUNER, Christopher; MILLARD, Christopher; SVANTESSON, Dan Jerker; LYNSKEY, Orla; CATE, Fred H. Risk management in data protection. **International Data Privacy Law**, v. 5, n. 2, p. 95-8, 2015.

LOURENÇO, Ana Lucia; TAQUES, João Daniel V.B. O Papel das Ouvidorias Públicas na Implementação da Lei Geral de Proteção de Dados (LGPD). **Revista do Ministério Público de Contas do Estado do Paraná**, v. 7, n. 13, 2020. Disponível em: https://revista.mpc.pr.gov.br/index.php/RMPCPR/article/view/7. Acesso em: 09 de abr. 2022.

LUIZ, Thiago Tomaz; BEUREN, Ilse Maria; CORTES, Beatriz Costa. Capacidade de coordenação e gerenciamento de riscos interorganizacionais. **Revista Pensamento Contemporâneo em Administração**, v. 14, n. 4, p. 141-55, 2020. Disponível em: https://periodicos.uff.br/pca/article/view/43929. Acesso em: 08 de mar. 2022.

MARINHO, Fernando. Os 10 mandamentos da LGPD: como implementar a lei geral de proteção de dados em 14 passos. 1. ed. São Paulo: Atlas, 2020.

MARQUES, Leandro; MULLER, Suzana Habitzreuter; SILVA, Márcia Zanievicz da. Gestão de riscos corporativos: percepção dos chief risk officers.**Revista Facultad de Ciencias Económicas: Investigación y Reflexión**, v. XXVII, n. 2, p. 105-26, 2019. Doi: https://doi.org/10.18359/rfce.3932.

MENDES, Laura S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. 1. ed. São Paulo: Saraiva, 2014.

MOHER, David; LIBERATI, Alessandro; TETZLAFF, Jennifer; ALTMAN, Douglas G. PRISMA Group. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. **PLoS Medicine**, v. 6, n. 7, p. e1000097, 2009. Doi: 10.1371/journal.pmed.1000097.

OLIVEIRA, Jonathan. **Governança, Riscos e Compliance (GRC) aplicados à LGPD**. Linkedin: IBM TLC-BR. Brasil, maio, 2021. Disponível em: https://pt.linkedin.com/pulse/governan%C3%A7a-riscos-e-compliance-grc-aplicados-%C3%A0-lgpd-jonathan. Acesso em: 09 de abr. 2022.

PINHEIRO, Patricia P.; SLEIMAN, Cristina; ROCHA, Henrique; LOTUFO, Larissa et al. **Segurança digital**: proteção de dados nas empresas. São Paulo: Atlas, 2020.

PINHEIRO, Patricia P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva, 2020.

PINHEIRO, Patricia P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 3. ed. São Paulo: Saraiva, 2021.

PROVOST, Foster; FAWCETT, Tom. Data science and its relationship to big data and data-driven decision making. **Bigdata**, v. 1, n. 1, p. 51-9, 2013. Disponível em: https://www.liebertpub.com/doi/full/10.1089/big.2013.1508>. Acesso em: 19 de fev.2022.

ROGERS, David L. **Transformação Digital**: Repensando o seu negócio para a era digital. 1. ed. São Paulo: Autêntica Business, 2019.

SANTOSA, I.; YUSVININDYA, R. Análise de Risco e Controle de Proteção de Dados Pessoais no Sistema de Informação de Administração de População. **Journal RESTI (Rekayasa Sistem dan Teknologi Informasi)**, v. 3, n. 3, p. 496-504, 2019.

SILVA, Irménio Ferreira da. **O Acordo de Basileia II e o impacto na gestão de riscos da banca e no financiamento das empresas**. 2007. Tese de Doutorado. Disponível em: https://repositorium.sdum.uminho.pt/handle/1822/7940. Acesso em: 06 de abr. 2022.

SILVA, Rogério Gustavo P. **Gestão de Riscos e Controles Internos no ensino superior**: uma proposta de framework para uso e proteção de dados em uma instituição de ensino (Dissertação de Mestrado). Centro Universitário Álvares Penteado, Fundação Escola de Comércio Álvares Penteado, São Paulo, 2020.

SOUZA, Augusto Sérgio da S.; JERÔNIMO, Taciana de B. Revisão Sistemática das aplicações em Administração do uso dos Métodos de Decisão Multicritério nas organizações. **Revista dos Mestrados**, v. 9, n. 2, p. 115, 2020. Disponível em: https://periodicos.ufpe.br/revistas/RMP/article/viewFile/249439/37874. Acesso em: 08 de mar. 2022.

TCU. Tribunal de Contas da União. **Gestão de riscos**: Histórico. Brasília, DF: TCU, 2022. Disponível em: https://portal.tcu.gov.br/governanca/governancapublica/gestao-de-riscos/historico.htm. Acesso em: 05 de abr. 2022.

TENÓRIO, Juliene Gama. **Controle interno**: um estudo sobre a sua participação na tomada de decisão de investimento no mercado de capitais brasileiro. Recife: Universidade Federal de Pernambuco, 2007. Disponível em: <https://repositorio.unb.br/bitstream/10482/2703/1/2007_JulieneGamaTenorio.pdf> Acesso em: 09 de abr. 2022.

TEPEDINO, Gustavo. Desafios da Lei Geral de Proteção de Dados (LGPD). **Revista Brasileira Direito Civil**, v. 26, p. 11, 2020. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/rvbsdirec26&div=2&id=&page=. Acesso em: 06 de abr. 2022.

UNIÃO EUROPEIA. **Regulation (EU) 2016/679**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 06 de abr. 2022.

VEIGA, Thiago Martinelli. A LGPD nos escritórios de advocacia previdenciária: o registro das operações de tratamento de dados e o conceito de escritório digital como medidas de base para a conformidade. **Revista Jurídica da Escola Superior de Advocacia da OAB-SC**, Santa Catarina, 2021. Disponível em: https://oabsc.s3.sa-east-1.amazonaws.com/arquivo/update/331_58_617abcaa47d41.pdf#page=153. Acesso em: 09 de abr. 2022.

VESCO, Delci Grapegia; FERNANDES, Francisco Carlos; RONCON, Aleksander. Controles de gestão atrelados ao gerenciamento de risco: uma análise das produções científicas brasileiras sob a perspectiva de redes sociais. **Revista hispana para el análisis de redes sociales**, v. 25, n. 2, p. 163-85, 2014. Disponível em: https://www.redalyc.org/pdf/931/93131317009.pdf. Acesso em: 08 de mar. 2022.

WOLFORD, Ben. **Data Protection Impact Assessment (DPIA)**. GDPR.EU, 2020. Disponível em: https://gdpr.eu/data-protection-impact-assessment-template/?cn-reloaded=1&cn-reloaded=1. Acesso em: 25 de jul. 2022.

ZONATTO, Vinícius Costa. da S.; BEUREN, Ilse M. Evidenciação da gestão de riscos pela metodologia do COSO: um estudo nos relatórios da administração de empresas brasileiras com ADRs. **ConTexto - Contabilidade em Texto**, Porto Alegre, v. 12, n. 21, p. 69-86, 2012. Disponível em: https://www.redalyc.org/pdf/5707/570765367007.pdf. Acesso em: 08 de mar. 2022.

APÊNDICE A - ROTEIRO DE ENTREVISTA COORDENADOR DE PROTEÇÃO DE DADOS

1) Como foi a estruturação da área de proteção de dados na empresa? Quando ela foi oficialmente implementada?

2) Como o gerenciamento de riscos é utilizado na área de proteção de dados?

3) Quais as ferramentas de gerenciamento de riscos utilizado pela área de proteção de dados?

4) Como as demais áreas receberam a implementação das ferramentas de gerenciamento de riscos da área de proteção de dados?

5) Quais as facilidades e dificuldades percebidas pela empresa na aplicação destas ferramentas?

6) Ainda existe alguma outra ferramenta de gerenciamento de riscos que você considera interessante implementar na área de proteção de dados?

7) Em que estágio você considera que a área de proteção de dados da empresa se encontra no momento? Quais os próximos passos?

8) Quais os benefícios trazidos pela implementação do gerenciamento de riscos aplicados a proteção de dados?

APÊNDICE B - ROTEIRO DE ENTREVISTAS DOS COLABORADORES DAS DEMAIS ÁREAS (Administração de Pessoal (RH), Comercial e Controladoria)

1) Você entrou na empresa em que ano? Já participou de quantos exercícios de Proteção de Dados?

2) Como a aplicação das ferramentas de gerenciamento de riscos aplicadas a proteção de dados influenciaram em seus processos de trabalho?

3) Após a análise dos resultados obtidos com as ferramentas, foi necessário realizar modificações em algum dos seus processos de trabalho?

4) Como você vê a mudança em seus processos depois da implantação das modificações sugeridas após aplicação das ferramentas de gerenciamento de riscos aplicadas a proteção de dados?

5) Quais as principais facilidades e dificuldades que você encontrou na execução dos exercícios (ferramentas)?

6) É claro para você a importância que o gerenciamento de riscos aplicado a proteção de dados tem para a empresa? Por quê?