



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE CIÊNCIAS EXATAS E DA COMPUTAÇÃO
ENGENHARIA DA COMPUTAÇÃO

**O MAPEAMENTO DO MODELO *DATA MANAGEMENT MATURITY* (DMM) À LEI
GERAL DE PROTEÇÃO DE DADOS (LGPD)**

LEONARDO NARCISO MARQUES

GOIÂNIA
2020

LEONARDO NARCISO MARQUES

**O MAPEAMENTO DO MODELO *DATA MANAGEMENT MATURITY* (DMM) À LEI
GERAL DE PROTEÇÃO DE DADOS (LGPD)**

Trabalho de Conclusão de Curso apresentado ao departamento Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Engenharia da Computação.

Orientadora: Profa. Msc. Adriana Silveira Souza

GOIÂNIA

2020

LEONARDO NARCISO MARQUES

**O MAPEAMENTO DO MODELO *DATA MANAGEMENT MATURITY* (DMM) À LEI
GERAL DE PROTEÇÃO DE DADOS (LGPD)**

Este Trabalho de Conclusão de Curso julgado adequado para obtenção o título de Bacharel em Engenharia da Computação, e aprovado em sua forma final pela Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, em 14/12/2020.

Orientadora: Profa. Msc Adriana Silveira Souza

Prof.^a Ms. Ludmilla Reis Pinheiro dos Santos
Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

Orientadora: Prof.^a Adriana Silveira Souza

Prof. Esp. Leodercio Lima Filho

Prof. Dr. Juliano Lopes de Oliveira

AGRADECIMENTOS

Agradeço a Deus, minha família, aos meus professores e colegas por me ajudarem a desenvolver este trabalho.

RESUMO

A Lei Geral de Proteção de Dados (LGPD) número 13.709/18 cujo propósito é proteger a privacidade e a liberdade dos cidadãos, determina que organizações alterem a forma de usar, guardar e obter dados pessoais, com isso também haverá transparência, segurança e privacidade no uso destas informações coletadas. A implementação das proposições deste dispositivo legal é um trabalho árduo e complexo porque é necessária uma mudança de consciência no que tange a gestão de dados, investimentos na área de segurança e capacitação ou contratação de especialistas. O *Data Management Maturity* - DMM (Maturidade na Gestão de Dados) é um modelo de melhoramento de capacidades e maturidade em processos na gestão de dados de uma. Este modelo de gestão de dados traz uma contribuição substancial para o correto manuseio dos ativos de dados, porque o DMM naturalmente atende ao que a LGPD propõe. O DMM claramente ajudará nesta tarefa, pois a sua essência para práticas funcionais está intimamente ligada à LGPD.

Palavras-chave: *Data Management Maturity*. Maturidade de Dados. LGPD

ABSTRACT

The General Data Protection Law (LGPD) number 13.709 / 18 whose purpose is to protect the privacy and freedom of citizens, determines that organizations change the way of using, saving and obtaining personal data, with that there will also be transparency, security and privacy in the use of this collected information. The implementation of the propositions of this legal provision is hard and complex work because it is necessary to change the conscience regarding data management, investments in the area of security and training or hiring specialists. Data Management Maturity (DMM) is a model for improving capabilities and maturity in processes in data management of a public or private institution. This data management model makes a substantial contribution to the correct handling of data assets, because DMM naturally meets what the LGPD proposes. DMM will clearly assist in this task, as its essence for functional practices is closely linked to the LGPD.

Keywords: *Data Management Maturity. Data Maturity. LGPD.*

SUMÁRIO

1 INTRODUÇÃO.....	7
2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)	9
3 MATURIDADE EM GESTÃO DE DADOS (<i>DATA MANAGEMENT MATURITY -</i> <i>DMM</i>).....	15
3.1 ÁREAS DE PROCESSO DO DMM	17
4 COMO O DMM PODE APOIAR AS ORGANIZAÇÕES NA ADEQUAÇÃO À LGPD.....	54
5 CONCLUSÕES E EXTENSÕES.....	72
REFERÊNCIAS	75

1 INTRODUÇÃO

A gestão de segurança da informação é um tema inovador de interesse das empresas e dos profissionais que nela atuam. Isso ocorre devido ao ambiente de negócios mais competitivo e à necessidade de inovar para sobreviver. Os sistemas de informação são os motores que impulsionam inovações de ideias à comercialização. Os projetos também são os propulsores que fazem com que as organizações sejam melhores, mais fortes e mais eficientes.

O uso cada vez maior das redes sociais, aplicativos bancários e outros no mundo traz a possibilidade de pôr uma falha na segurança, informações organizacionais sigilosas sejam expostas publicamente, sendo assim furtadas, copiadas ou utilizadas sem a devida autorização. A acessibilidade das redes sociais, aplicativos bancários e outros, está cada vez mais simples, pois pode ser feita utilizando vários dispositivos, inclusive móveis, mantendo as pessoas permanentemente conectadas. As informações empresariais sigilosas e sensíveis podem vazar nas redes sociais às pessoas não autorizadas, de forma acidental ou intencional (JUE, MARR, KASSOTAKIS, 2011).

As organizações que adotarem uma filosofia e uma prática madura de gerência de projetos de segurança da informação estarão mais aptas ao sucesso em um mercado competitivo do que aquelas que mantêm as mesmas práticas (KERZNER, 2010).

O gerenciamento de informações vem ganhando destaque entre os modelos de administração e tem se transformado em um fator para prover velocidade, robustez, consistência e excelência operacional no desenvolvimento de sistemas mais seguros.

Percebe-se também que a gestão de partes interessadas em gerenciamento de dados vem obtendo notoriedade e, cada vez mais, são feitos esforços para desenvolver competências nesta área. Identificar e gerir as expectativas das partes interessadas desde o início de um sistema seguro é ainda um desafio para os gestores. Nesse contexto, a presente pesquisa tem como objetivo mostrar como o modelo DMM pode ser considerado para a conformidade com a Lei Geral de Proteção de Dados (LGPD).

A principal função do DMM que é centralizar a gestão dos dados gerando assim o dado único e verdadeiro do cliente, o DMM também tem o controle dos sistemas que se integram e recebem a atualização destes dados, esta é a vantagem fundamental do uso do DMM para a LGPD, pois a empresa tem a garantia de precisão dos dados.

As empresas têm mostrado dificuldade para fazer uma gestão de dados eficiente, de forma a assegurar sua utilização de forma eficiente e apenas 13,8% das empresas têm como prioridade de negócios expandir sua capacidade de tirar proveito de dados para criar ou potencializar novas fontes de receitas (Associação Brasileira das Empresas de Software, 2019).

O correto tratamento dos dados é possível após uma conscientização concernente à gestão de dados, investimentos na área segurança e capacitação ou contratação de especialistas. O nível de exigência para o correto tratamento dos dados é complexo, agora com a Lei Geral de Proteção de Dados (LGPD), tudo fica ainda mais desafiador.

A LGPD é uma regulamentação para o território Brasileiro que está em vigor e tem como objetivo de garantir maior segurança em relação aos dados pessoais que podem ser coletados, não sendo exclusivo para meios digitais.

Esta lei impacta todas as instituições públicas ou privadas que agora precisam adequar às regras como segurança, privacidade dos dados e também as pessoas físicas que usam dos serviços ou produtos oferecidos por estas instituições e que agora precisam dar consentimentos para uso de dados pessoais.

Alguns dos problemas na adequação à LGPD são a ausência de políticas, gestão de dados, segurança, auditorias, mapeamento de fluxos por parte das organizações, que agora se vêm obrigadas a cumprir este dispositivo legal.

Com o uso do modelo DMM (*Data Management Maturity*) do Instituto CMMI (Modelo de Capacidade e Maturidade Integrado) para adequação à LGPD, os resultados podem ser otimistas, pois as práticas funcionais do DMM são próximas dos requisitos solicitados em cada artigo da lei.

A LGPD exige que sejam realizadas tratativas com o objetivo de proteger os dados pessoais e dados pessoais sensíveis dos titulares de dados, é necessário haver uma melhor rastreabilidade desses dados por organizações que tratam dados pessoais.

2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709/2018) representa uma evolução em termos de direitos à privacidade de dados das pessoas naturais no Brasil. A LGPD foi inspirada no GDPR (*General Data Protection Regulation*). (GARCIA et al., 2020, com adaptações). O GDPR consiste no regulamento criado na Europa, que dispõe sobre a proteção de dados pessoais de cidadãos europeus. O GDPR passou a vigorar em todo o continente europeu a partir de maio de 2018.

A LGPD é um evento novo no cenário brasileiro, demandando que as organizações implementem controles necessários para manter e assegurar o respeito à privacidade de dados de pessoas físicas. Qualquer organização que seja pública ou privada que coleta dados de pessoas físicas precisa se adaptar até agosto de 2021 sob pena de sanções. Seu principal objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O foco é resguardar os cidadãos brasileiros do uso inadequado ou abusivo de seus dados pessoais por organizações públicas ou privadas sem sua autorização expressa.

Esta lei https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337 estabelece uma estrutura legal constituída por meio de 65 artigos. No artigo 1º, é apresentado à disposição geral da lei. Esse artigo define o escopo e norteia a filosofia em que a lei se respalda, abordando sobre o tratamento de dados pessoais, inclusive nos meios digitais, penalidades, requisitos, princípios, estrutura de governança, entre outros aspectos.

Com o advento da LGPD, as organizações podem ser fortemente penalizadas, caso ocorra um uso inadequado de dados pessoais. Trata-se de uma questão nova, em que ainda não estão claras as regras e possíveis interpretações para esta lei. Com isso, sanções podem ser aplicadas isolada ou cumulativamente, a depender do caso concreto.

Por isso torna-se fundamental para as organizações expressar, exprimir e transparecer para a sociedade e, em especial, aos titulares de dados pessoais e à ANPD (Autoridade Nacional de Privacidade de Dados) a seriedade com que trata os dados dos titulares.

A LGPD possui sete fundamentos, que estabelecem os aspectos que devem ser levados em consideração, quando se interpreta a lei (BRASIL, 2018). O primeiro fundamento é o respeito à privacidade. Isto significa que os dados pessoais não podem ser utilizados de forma indiscriminada, isto é, que o titular dos dados devem ter seus direitos à privacidade respeitados. A autodeterminação informativa, segundo fundamento, consiste em que o titular tem o direito de decidir como seus dados devem ser tratados, garantindo ao Titular escolher como será realizada a gestão de seus dados pessoais. Para isso, toda a organização deve fornecer informações a respeito dos dados pessoais para seus respectivos titulares. Entre essas informações estão que tipos de dados são mantidos na organização, como eles são utilizados. O titular dos dados tem o direito de ter seus dados excluídos e ou atualizados sempre que considerar necessário.

Os fundamentos terceiro, quarto e sétimo consistem na liberdade de expressão, de informação, de comunicação e de opinião, bem como, na inviolabilidade da intimidade, da honra e da imagem. Com isso os direitos humanos, o livre desenvolvimento da personalidade, a dignidade da pessoa humana e o exercício da cidadania, que também são previstos na constituição, são por esta lei reforçados.

A lei também estabelece, para além dos fundamentos individuais, um conjunto de fundamentos voltados para a sociedade e o desenvolvimento nacional. São os fundamentos quinto e sexto que tratam do desenvolvimento econômico, tecnológico e a inovação e a referência à livre iniciativa, à livre concorrência e à defesa do consumidor. Neste sentido, a lei não descarta a importância dos dados na sociedade da informação e conhecimento dentro de um contexto, com objetivos e finalidades claros. Com isso os dados passam a dar suporte para o processo de tomada de decisão social, política e econômica. A lei não visa criar obstáculos ao desenvolvimento da nação, impedindo o tratamento de dados, mas utilizá-los de forma consciente e ética como estimulador econômico, tecnológico e da geração de valor agregado para os setores produtivos. Desta forma estabelece-se uma dialética entre o individual e o coletivo em uma solução de compromisso relativo à privacidade de dados.

Para a Lei um dado pessoal é o tipo de dado que pode identificar o indivíduo. São exemplos de dados pessoais o RG, CPF, sexo, nome, endereço. Além de dados pessoais, há o conceito de dados sensíveis. Dados sensíveis são os dados que podem

ser utilizados para discriminar uma pessoa. Entre os dados sensíveis estão religião, dado biométrico ou genético, dados sobre a saúde, à vida sexual, filiações religiosas, sindicais, políticas ou filosóficas, origem racial.

Em ocasiões que os dados são considerados sensíveis e na hipótese em que órgãos de saúde necessitem fazer uso destes dados, estes serão tratados sem o consentimento do Titular e nunca devem ser compartilhados.

A lei também dispõe de um conjunto de papéis com devidas responsabilidades associadas. Os principais papéis definidos pela LGPD são:

- Titular: Pessoa proprietária do dado pessoal que é objeto de tratamento e que a qualquer momento pode solicitar que tipos de dados e como eles estão sendo tratados.

- Controlador: Pessoa jurídica ou física de direito privado ou público responsável por tratar os dados pessoais.

- Operador: Pessoa jurídica ou física, de direito privado ou público que trata os dados em nome do controlador.

- Encarregado de dados: Pessoa jurídica ou física indicada pelo controlador e operador que é responsável pela comunicação entre ANPD, titulares dos dados e controlador. Esse papel requer conhecimentos nas áreas de gestão, tecnologia, comunicação e direito.

Figura 1 Atores da LGPD



Fonte: Gisele Kauer (2020)

- Autoridade Nacional de Proteção de Dados (ANPD): é a entidade responsável pela fiscalização e pela garantia da aplicação da lei de proteção de dados no Brasil.

Tanto o controlador, como o operador devem realizar uma gestão muito rigorosa sobre tudo que foi feito com os dados dos titulares. Eles respondem em conjunto quando da violação de dados pessoais.

A Lei Geral de Proteção de Dados possui um conjunto de requisitos que baliza o tratamento dos dados. São eles o consentimento expresso do titular dos dados; o cumprimento de uma obrigação legal ou regulatório pelo controlador; o tratamento e uso compartilhado de dados necessários à administração pública para gestão de políticas públicas; para estudo de órgãos de pesquisa, garantida a anonimização dos dados pessoais; para execução de contratos; para exercícios regular de direitos em processo judicial, administrativo ou arbitral; para proteção da vida do titular ou de terceiros; para a tutela da saúde, quando necessário para atender interesses legítimos do controlador; e para proteção do crédito.

Os princípios que orientam o uso dos dados pessoais na LGPD são dez ao todo. O primeiro é a finalidade, que consiste na realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular. Outro princípio é a adequação. A adequação refere-se à compatibilidade do tratamento com as finalidades informadas pelo titular. A necessidade é um princípio que visa limitar o tratamento ao mínimo necessário para a realização de suas finalidades. O quarto princípio é o livre acesso. Este princípio respalda-se no direito que os titulares têm de fazer consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. A qualidade dos dados, outro princípio, expressa por meio da exatidão e atualização dos dados dos titulares. O sexto princípio é representado pela transparência de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Outro princípio é a segurança da informação por meio da utilização de medidas técnicas e administrativas que protegem os dados de acessos não autorizados e/ou de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. A adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais é o princípio denominado de prevenção. O nono princípio de não discriminação baseia-se na impossibilidade de realização do

tratamento para fins discriminatórios ilícitos ou abusivos. Por fim, o último princípio é o da responsabilização e prestação de contas. Esse princípio tem por finalidade a adoção de medidas eficazes e capazes de comprovar o cumprimento das normas de proteção de dados pessoais.

As duas maneiras principais de tratamento de dados são por consentimento do Titular dos dados e por interesse legítimo do Controlador. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, quando se deseja oferecer um serviço/produto ou para melhorá-lo ou utilizar os dados para inovar, como por exemplo fazer uma carteira de estudante universitário.

No caso em que o Poder Público necessitar de algum dado para cumprimento de atribuições ou competências legais este poderá fazer uso sem o consentimento do Titular dos dados, como por exemplo sofrer um acidente de trânsito e ao chegar no hospital, este fazer acesso aos seus dados médicos.

Os direitos dos Titulares consistem na confirmação da existência de tratamento de dados consentidos, a revogação de seu consentimento, autorização para mudanças e/ou atualização dos dados, portabilidade e informações sobre possíveis compartilhamentos.

No que tange a transferência de dados entre países, essa situação só poderá ocorrer quando o país de destino possuir legislação equivalente à LGPD. A ANPD fica responsável por definir quais os países satisfazem esse critério. Outro requisito é que o Controlador demonstre que todos os direitos do Titular dos dados estejam resguardados. Principalmente no que diz respeito às cláusulas contratuais, seja elas padrões ou específicas, selos e normas corporativas, códigos de conduta e certificados. A transferência de dados internacionais também pode ocorrer nos casos em que haja situações de segurança nacional, como por exemplo, investigações, inteligência, persecução.

Em se tratando de incidentes como informações organizacionais sigilosas que sejam expostas publicamente, sendo assim furtadas, copiadas ou utilizadas sem a devida autorização a princípio a ANPD e o Titular devem ser comunicados imediatamente. Um caso de vazamento de dados foram as denúncias de espionagem da *National Security Agency* (NSA) por Edward Snowden (GREENWALD, 2014) que provocaram um grande tumulto na sociedade.

Nesta comunicação deve-se informar dados que foram comprometidos, as formas utilizadas para tratamento dos dados, os riscos, padrões técnicos e medidas de segurança adotadas.

A Autoridade Nacional de Proteção de Dados (ANPD) pode aplicar punições de acordo com a LGPD. As penalidades mencionadas na LGPD são: advertência, multa simples de 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, multa diária, publicação da infração, bloqueio dos dados pessoais, eliminação dos dados pessoais da infração, suspensão parcial do banco de dados por no máximo 6 (seis) meses, prorrogável por igual período, suspensão da atividade de tratamento de dados, proibição total ou parcial do exercício da atividade de tratamento de dados.

Para a avaliação da penalidade gerada pelo descumprimento da LGPD são considerados critérios objetivos e subjetivos, como gravidade e natureza da infração, boa-fé do infrator, vantagem auferida ou pretendida, condição econômica do infrator, reincidência, grau de dano, cooperação do infrator, reiteração na infração, a adoção de mecanismos de prevenção, a existência de políticas de boas práticas de governança e a pronta adoção de medidas de correção.

Para a organização se defender de eventuais penalidades, ela deverá utilizar os ritos e procedimentos do processo administrativo, demonstrando evidências objetivas da implantação e uso de padrões, medidas técnicas ou administrativas e governança dos dados, que foram implementadas com o intuito de proteger os dados pessoais.

Portanto, o modelo DMM pode ser uma forma para se realizar uma governança efetiva dos dados. O próximo capítulo apresenta uma visão geral da estrutura, processos e práticas do modelo DMM.

3 MATURIDADE EM GESTÃO DE DADOS (*DATA MANAGEMENT MATURITY - DMM*)

"O DMM define um conjunto de boas práticas para ajudar as organizações a construir, melhorar e medir sua capacidade de governança de dados corporativos. Trata-se de um modelo desenvolvido pelo CMMI *Institute*." (CMMI Institute, 2019) que visa conduzir as organizações a identificar o atual estado do gerenciamento de dados e apontar caminhos para conduzi-la para a maturidade de maneira gradativa.

A maturidade é caracterizada pela experiência que a organização tem na gestão eficiente de seus dados, isto é, o quanto ela consegue controlar e gerenciar de forma estratégica os ativos de dados. Este modelo está estruturado em categorias de processo e áreas de processo, conforme apresentado na Figura 2.

Figura 2 VISÃO GERAL DMM, CATEGORIAS E ÁREAS DE PROCESSO

ESTRATÉGIA DE GESTÃO DE DADOS	Estratégia de Gestão de Dados
	Comunicações
	Função de Gestão de Dados
	Caso de Negócio
	Financiamento do Programa
GOVERNANÇA DE DADOS	Gestão de Governança
	Glossário de Negócios
	Gestão de Metadados
QUALIDADE DE DADOS	Estratégia de Qualidade de Dados
	Perfil de Dados
	Avaliação da Qualidade dos Dados
	Limpeza de Dados
OPERAÇÕES DE DADOS	Definição dos Requisitos dos Dados
	Gestão de ciclo de vida dos dados
	Gestão de Provedor
PLATAFORMA E ARQUITETURA	Abordagem Arquitetural
	Padrões Arquiteturais
	Plataforma de Gestão de Dados
	Integração de Dados
	Dados Históricos, Arquivamento e Retenção
PROCESSOS DE SUPORTE	Medição e Análise
	Gerência de Processos
	Garantia da Qualidade de Processo
	Gestão de Risco
	Gestão de Configuração

Fonte: O autor (2020)

As categorias de processo do DMM são Estratégia de Gestão de Dados, Governança de Dados, Qualidade de Dados, Operações de Dados, Plataforma e Arquitetura e Processos de Suporte, totalizando seis categorias.

Na coluna da direita da Figura 1, mostra as áreas de processos. Os processos são a forma como o DMM faz a divisão em setores, para melhor trabalhar políticas específicas e fazer um controle mais efetivo na gestão de dados.

Outra estrutura que faz parte do DMM são as capacidades dos processos. As capacidades representam a maneira como os ativos de dados de uma organização estão sendo geridos. Os níveis de capacidades são classificados em cinco. Esses níveis iniciam do menos (nível 1) para o mais maduro (nível 5). Segue abaixo cada um dos níveis de capacidade.

- O nível 1 é denominado realizado. Esse nível abrange práticas com pouco controle, ou seja, sem documentação definida, com gerência de projeto ad hoc que pode ser feita por uma pessoa ou um setor, sem muito rigor.

- O nível 2 é chamado de gerido. Neste nível, já se encontra uma gestão de projeto. Verifica-se que há práticas de planejamento e de acompanhamento de projeto, bem como, utiliza-se um plano para guiar sua execução.

- O nível 3 recebe o nome de definido. Abrange um processo padronizado, estruturado não só em nível de projeto, mas em nível organizacional. Um processo definido como padrão faz com que todas as equipes conheçam e conduzam de forma semelhante os projetos. Essa característica faz com que os projetos produzam resultados que podem ser comparados e assim formas mais efetivas de melhorias de processos possam ser implementadas.

- O nível 4 é nomeado de medido. Neste nível acontecem diversas avaliações e medições que apontam as fragilidades ou as evoluções dos processos. A gestão de processos é mais efetiva com base em dados históricos e controle estatístico.

- O nível 5 é intitulado como otimizado. As práticas definidas já estão consolidadas e são seguidas pelas equipes. Neste nível, melhorias são mais facilmente incorporadas ao processo. Há um reconhecimento de pontos fortes e lacunas e intervenções mais precisas são realizadas. Desta forma, alavancando os ativos de dados para um melhor desempenho dos negócios na organização.

3.1 ÁREAS DE PROCESSO DO DMM

Esta seção apresenta as práticas de cada área de processo, juntamente com os respectivos níveis de capacidade.

Estratégia de Gestão de Dados

A área de processo Estratégia de Gestão de Dados define a visão, metas e objetivos para o programa de gestão de dados e garante que todas as partes interessadas estejam alinhadas com as prioridades e o programa de implementação e gestão.

Nível 1 realizado.

1.1 Objetivos, prioridades e escopo da gestão de dados refletem os objetivos de negócio das partes interessadas para pelo menos um projeto.

Nível 2 gerenciado.

2.1 Os objetivos, prioridades e escopo da gestão de dados são definidos e aprovados.

2.2 Os objetivos e prioridades de gestão de dados estão alinhados com os objetivos de negócio.

2.3 Um processo para priorizar projetos em uma empresa, em uma perspectiva de dados, bem como rastreabilidade para objetivos de negócios, é estabelecido e seguido.

2.4 Um plano tático para abordar os objetivos da gestão de dados e prioridades em toda a unidade de negócio é estabelecido e mantido.

2.5 Métricas são usadas para avaliar o cumprimento dos objetivos para gestão de dados.

Nível 3 definido

3.1 Uma estratégia de gestão de dados que representa um o escopo de toda a organização é estabelecido, aprovado, promulgado e mantido.

3.2 Os objetivos de gestão de dados para a organização são avaliados e priorizados em conexão aos motivos do negócio e objetivos são alinhados à estratégia de negócios.

3.3 Negócios e tecnologia são desenvolvidos colaborativamente na estratégia de gestão de dados da organização.

3.4 A sequência do plano para execução da estratégia de gestão de dados é monitorada e atualizada, com base no progresso das revisões.

3.5 A estratégia de organização da gestão de dados é documentada, mantida, revisada e comunicada de acordo com o processo padrão definido pela organização.

3.6 A estratégia de gestão de dados da organização é consistente com as políticas de gestão de dados.

3.7 Métricas são usadas para avaliar e monitorar o cumprimento dos objetivos de gestão de dados.

Nível 4 medido.

4.1 Estatísticas e outras técnicas quantitativas são usadas para avaliar a eficácia dos objetivos de gestão de dados estratégicos para atingir os objetivos de negócios e as modificações são feitas com base em métricas.

4.2 A organização pesquisa processos de negócios inovadores e encargos regulatórios emergentes para garantir que o programa de gestão de dados seja compatível com as necessidades futuras do negócio.

Nível 5 otimizado.

5.1 A organização pesquisa e adota as melhores práticas selecionadas da indústria para estratégia e desenvolvimento de objetivos.

5.2 As contribuições são feitas para as melhores práticas da indústria para o desenvolvimento da estratégia de gestão de dados e sua efetivação.

Comunicações

A área de processo de Comunicações garante que políticas, padrões, processos, anúncios, e outras comunicações de gerenciamento de dados sejam publicados, promulgados, compreendidos e ajustados com base em *feedback*.

Nível 1 realizado.

1.1 As comunicações relacionadas aos ativos de dados são gerenciadas em pelo menos um projeto.

Nível 2 gerenciado.

2.1 O plano de comunicação para gestão de dados é definido, documentado, aprovado pelas partes interessadas e programado.

2.2 Padrões, políticas e processos de gestão de dados são comunicados e ajustados com base em *feedbacks*.

Nível 3 definido.

3.1 A política de comunicação estabelece critérios para a disseminação ou promulgação de diferentes tipos de comunicações na gestão de dados.

3.2 A estratégia de comunicação é guiada por uma política de toda a organização e reflete a estratégia de gestão de dados.

3.3 Padrões, políticas e processos são promulgados em toda a organização e ajustados com base em *feedbacks*.

3.4 Métricas são desenvolvidas e usadas para medir eficácia das comunicações de gestão de dados.

3.5 As comunicações são revisadas pelas partes interessadas de acordo com um processo que é exigido por definição de padrões e processos.

3.6 Métricas são empregadas para melhorar a eficácia das comunicações na gestão de dados.

Nível 4 medido

4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação.

4.2 Estatísticas e outras técnicas quantitativas são empregados para melhorar o gerenciamento de dados e comunicações.

Nível 5 otimizado.

5.1 As comunicações de gerenciamento de dados externos são feitas com o objetivo de influenciar políticas públicas e práticas recomendadas do setor que afetam os dados.

Função de Gestão de Dados

A área de processo Função de Gestão de Dados fornece orientação para liderança e equipe de gestão de dados para garantir que os dados sejam gerenciados como um ativo corporativo. Preocupa-se em definir um escopo para estabelecer e

manter os princípios da gestão de dados, facilitando sua adoção e garantindo o alinhamento entre as equipes da organização

Nível 1 realizado.

1.1 As funções de gerenciamento de dados são estabelecidas para pelo menos um projeto.

Nível 2 gerido.

2.1 Uma interação aprovada e um modelo de engajamento, garantem que as partes interessadas se envolvam com a organização da gestão de dados.

2.2 Princípios são definidos e seguidos para orientar a consistência das práticas relacionadas à gestão de dados.

2.3 Funções e responsabilidades são especificadas para apoiar a governança de gestão de dados e a interação entre a governança e a função de gestão de dados.

2.4 Acordos que estão em vigor, fornecem expectativa explícita para o uso compartilhado de recursos pela equipe, com responsabilidade para gestão de dados.

2.5 Um mecanismo existe e é seguido para identificar e aplicar as mudanças necessárias para aprimorar ou redesenhar a função de gestão de dados.

Nível 3 definido.

3.1 Uma função de gerenciamento de dados é estabelecida com responsabilidade para gerenciar atividades que suportam dados objetivos de manejo.

3.2 O modelo de interação para a função de gestão de dados garante o envolvimento da governança de dados para projetos que usam dados compartilhados.

3.3 Uma organização de gestão de dados e estrutura especificada são definidas e revisadas periodicamente para garantir que elas atendam às necessidades da organização.

3.4 Processos de gestão de dados são estabelecidos e mantido pela função de gestão de dados com aprovação da governança.

3.5 O gerenciamento de dados é uma função de negócio explicitamente reconhecida e é alavancada em toda a organização.

Nível 4 medido.

4.1 A função de gestão de dados definiu tarefas que são medidas e avaliadas, usando estatísticas e outras técnicas quantitativas.

4.2 Modificações da função de gestão de dados e suas práticas são baseadas em uma análise de indicadores usando técnicas estatísticas e outras técnicas quantitativas.

Nível 5 otimizado.

5.1 O plano operacional para a melhoria contínua de atividades de gestão de dados deve ser priorizado.

5.2 Análise usando estatísticas e outras técnicas quantitativas, bem como o uso de desempenho de processo, os modelos aproveitam os dados para melhorar a eficiência operacional.

Caso de Negócio

A área de processo Caso de Negócio fornece uma justificativa para determinar quais iniciativas de gestão de dados devem ser financiadas, e garantir a sustentabilidade da gestão de dados por meio de decisões com base em considerações financeiras e benefícios para a organização.

Nível 1 realizado.

1.1 Um caso de negócio é desenvolvido para iniciativas de projeto.

1.2 Os benefícios e custos da gestão de dados são documentados e usados nas decisões de financiamento local.

Nível 2 gerido.

2.1 A metodologia dos casos de negócios é definida e seguida.

2.2 Os casos de negócios padrão apoiam as decisões de aprovação para gestão de dados de financiamento.

2.3 Os casos de negócios de gestão de dados para novas iniciativas alinham-se com os objetivos de negócios e objetivos de gestão de dados.

Nível 3 definido.

3.1 Os casos de negócios de gestão de dados são desenvolvidos de acordo com a metodologia padrão da organização.

3.2 Os casos de negócios refletem a análise do custo total de propriedade do programa de gerenciamento de dados e aloca elementos de custo para as organizações, programas e projetos de acordo com métodos de contabilidade financeira da organização.

3.3 Casos de negócios de gestão de dados exigem patrocínio.

3.4 Fatores de custo que compõem o documento Custo Total de Propriedade do gerenciamento de dados, são gerenciados e monitorados em todo o gerenciamento do ciclo de vida dos dados.

3.5 Métricas de custo e benefício orientam a gestão de dados prioritários.

Nível 4 medido.

4.1 O TCO de gestão de dados é empregado para medir, avaliar e financiar mudanças iniciais e de infraestrutura na gestão de dados.

4.2 Técnicas estatísticas e outras técnicas quantitativas são usadas para analisar métricas de custo de gestão de dados para avaliar a gestão de dados do TCO e métodos de cobrança.

4.3 Placar de desempenho do programa de gestão de dados incluem métricas de TCO.

4.4 O modelo de TCO de gestão de dados da organização é validado, verificado quanto à precisão e aprimorado por meio de revisões e análises regulares.

Nível 5 otimizado.

5.1 Resultados estatísticos e guia de *feedback* das partes interessadas melhoria contínua do TCO para gestão de dados.

5.2 A organização compartilha as melhores práticas de TCO para contribuir com a maturidade da indústria por meio de publicações ou conferências.

5.3 Técnicas de otimização e modelos preditivos são empregados para antecipar os resultados das alterações propostas antes da implementação.

Financiamento do Programa

A área de processo de Financiamento do Programa tem como propósito garantir a disponibilidade de financiamento adequado e sustentável para apoiar o programa de gestão de dados.

Nível 1 realizado.

1.1 Pelo menos um projeto de gerenciamento de dados foi financiado com base em análises de custo-benefício.

Nível 2 gerido.

2.1 Iniciativas de gerenciamento de dados são financiadas com base em critérios de financiamento abordados pelos casos de negócios.

2.2 As partes interessadas participam e apoiam o programa de financiamento da gestão de dados.

2.3 Os custos de gestão de dados são mapeados para as áreas de negócios, funções operacionais e tecnologia da informação (TI).

2.4 A governança do processo de financiamento é definida e implementada.

Nível 3 definido.

3.1 O financiamento do programa de gestão de dados está alinhado com padrões de tomada de decisão de investimento que são consistentemente empregados em toda a organização.

3.2 As prioridades de financiamento do programa se alinham com os objetivos e prioridades da gestão de dados.

3.3 Medidas definidas determinam a eficácia de financiamento do programa em relação aos seus objetivos e benefícios esperados.

Nível 4 medido.

4.1 As métricas são definidas e analisadas estatisticamente para avaliar a eficácia e precisão do financiamento do programa em atender aos objetivos organizacionais.

Nível 5 otimizado.

5.1 Lições aprendidas com o financiamento do programa em toda a organização para gerenciamento de dados são compartilhados com interessados da indústria.

5.2 Técnicas de otimização e modelos preditivos são empregados para a análise dos resultados esperados de modificações propostas nos métodos de financiamento do programa antes da implementação.

Gestão de Governança

A área de processo Gestão de Governança busca desenvolver a estrutura operacional necessária para garantir que os dados corporativos sejam gerenciados como um ativo e implementados de forma eficaz e sustentável.

Nível 1 realizado.

1.1 As funções de governança de dados são geradas em pelo menos um projeto.

1.2 Propriedade, administração e responsabilidade pelos conjuntos de dados são atribuições principalmente baseadas em projetos.

Nível 2 gerido.

2.1 Uma estrutura de governança de dados é definida e documentada.

2.2 Funções de governança de dados e responsabilidades de dados são estabelecidas para área em questão por prioridade, conforme declarado na estratégia de negócios ou de dados.

2.3 Representantes da área em questão participam da governança de dados e processos associados.

2.4 A governança de dados segue políticas definidas, processos e padrões.

2.5 Um processo de revisão é estabelecido e seguido para avaliar e melhorar a governança de dados.

Nível 3 definido.

3.1 Uma estrutura de governança de dados em toda a organização e o plano de implantação é estabelecido.

3.2 A governança de dados em toda a organização é operacional para assuntos de alta prioridade das áreas da organização.

3.3 A governança de dados inclui representantes de todas as unidades de negócios.

3.4 As políticas e processos de governança de dados são seguidos.

3.5 A governança de dados determina e aprova métricas para avaliar a eficácia das atividades de governança.

3.6 Um processo de avaliação é estabelecido para refinar a governança de dados, para se alinhar com a mudança de prioridades de negócios e para expandir conforme necessário, para abranger novas funções e domínios.

3.7 Aulas, mentorias, treinamento no trabalho em processos de governança de dados são necessários para novos membros da governança e outras partes interessadas.

3.8 São analisados as atividades e os resultados de governança de dados em contraste aos objetivos da organização e relatados à gestão.

Nível 4 medido.

4.1 Estatísticas e outras técnicas quantitativas são aplicadas para determinar se os esforços de governança estão mudando comportamentos organizacionais apropriadamente.

4.2 Ajustes nas atividades e estrutura de governança de dados são feitos com base nos resultados da análise.

Nível 5 otimizado

5.1 Estruturas de governança externas e estudos de caso da indústria são avaliados para as melhores práticas e lições aprendidas, fornecendo ideias para melhorias.

5.2 A estrutura de governança de dados é comunicada à indústria interessada em um modelo de boas práticas.

5.3 Os processos de governança de dados são continuamente refinados e melhorados.

Glossário de Negócios

A área de processo Glossário de Negócios tem como missão oferecer suporte a um entendimento comum de termos e definições sobre dados estruturados e não estruturados de suporte aos processos de negócios para todas as partes interessadas.

Nível 1 realizado.

1.1 Os termos de negócios são definidos para um propósito específico.

1.2 Modelos de dados lógicos são criados com referência a termos de negócios definidos e aprovados.

Nível 2 gerido.

2.1 Um processo é estabelecido, documentado e seguido para definir, gerenciar, usar e manter o glossário do negócio.

2.2 Os termos de negócios padrão estão prontamente disponíveis e promulgados para as partes interessadas relevantes.

2.3 Cada termo de negócio adicionado ao glossário do negócio tem um nome único e definição única.

2.4 Novo desenvolvimento, integração de dados e esforços na consolidação de dados aplicam termos de negócios padrão como parte do processo de definição de requisitos de dados.

Nível 3 definido.

3.1 A organização utiliza o glossário de negócios aprovado no desenvolvimento de repositórios compartilhados, transferência de dados padrões (por exemplo, XML), ontologias, modelos semânticos e iniciativas semelhantes envolvendo dados corporativos.

3.2 Governança de dados em toda a organização para conformidade com o processo de glossário de negócios é implementado e seguido.

3.3 A organização implementou um mecanismo para facilitar a transformação por meio de mapeamento entre negócios, termos, atributos e nomes de elementos de dados físicos ou sinônimos.

3.4 Avaliações de impacto são alcançadas e a aprovação de governança é obtida, antes de implementar mudanças nos termos de negócios.

3.5 Métricas são capturadas e usadas para avaliar o progresso da organização em direção a um abrangente glossário de negócios.

3.6 Processos de monitoramento de conformidade são usados para verificar uso correto de termos de negócios, exceções de destaque, e garantir que eles sejam abordados.

Nível 4 medido.

4.1 Estatísticas e outras técnicas quantitativas são usadas para gerenciar o processo e desenvolver relatórios e projeções sobre integração glossário de negócios para a administração.

4.2 O glossário do negócio é integrado ao repositório de metadados da organização com a apropriada permissão de acesso.

4.3 O glossário empresarial usa os termos padrões da indústria e definições de negócios como apropriado.

Nível 5 otimizado.

5.1 O glossário do negócio é aprimorado para conter regras de negócios associadas e estruturas de ontologia, e é consistente em toda a organização.

5.2 Técnicas de otimização são empregadas para melhorar o processo de desenvolvimento de taxonomias, ontologias, ou representações semânticas alavancando o glossário de negócios.

5.3 A organização publica *whitepapers* e estudos de caso abordando gestão eficaz de termos de negócios.

Gestão de Metadados

A área de processo Gestão de Metadados tem como propósito estabelecer os processos e a infraestrutura para especificar e expandir informações claras e organizadas sobre dados estruturados e ativos de dados desestruturados sob gestão, fomentando e dando suporte ao compartilhamento de dados, garantindo o uso compatível de dados, melhorar a capacidade de resposta às mudanças nos negócios e reduzir ameaças relacionados a dados.

Nível 1 realizado.

1.1 A documentação dos metadados é desenvolvida, armazenada e acessível.

Nível 2 gerido.

2.1 Um processo de gestão de metadados é estabelecido e seguido.

2.2 Documentação de metadados captura dados interdependentes.

2.3 Metadados são desenvolvidos e usados para realizar análise de impacto sobre possíveis mudanças de dados.

2.4 Categorias de metadados, propriedades e padrões são estabelecidos e seguidos.

Nível 3 definido.

3.1 Uma estratégia de gerenciamento de metadados para a organização é estabelecida, promulgada e mantida pela governança de dados com a contribuição de partes interessadas relevantes.

3.2 O repositório de metadados da organização é preenchido com categorias adicionais e classificações de metadados de acordo com um plano de implementação em fases, e está vinculado para camadas de arquitetura.

3.3 A função de gerenciamento de dados centraliza metadados esforços de gestão e é supervisionado pela governança de dados. Governança de dados aprova adições de metadados e alterações.

3.5 Medidas e métricas são usadas para avaliar a precisão e adoção de metadados.

3.6 Metadados, e quaisquer alterações nos metadados, são validados contra a arquitetura existente.

Nível 4 medido.

4.1 A organização desenvolveu um meta-modelo integrado e implantado através de plataformas.

4.2 Tipos de metadados e definições de dados oferecem suporte consistente em práticas de importação, assinatura e consumo.

4.3 As extensões do repositório de metadados incluem trocas padrões de representações de dados usados pela organização.

4.4 Novas atividades de gerenciamento de metadados são orientadas por métricas de metadados e informações históricas sobre metadados.

4.5 Objetivos quantitativos orientam a gestão de metadados e desempenho do processo de suporte.

4.6 Relatórios de análise estatística para processo, relatórios e o desempenho estão incluídos no repositório de metadados e empregados para apoiar a tomada de decisão baseada em fatos para novas iniciativas de gestão de metadados.

Nível 5 otimizado.

5.1 A análise da causa raiz é atingida para reduzir as variações entre as informações do repositório e as descrições de dados.

5.2 Modelos de previsão de desempenho guiam mudanças em processos de gestão de metadados.

5.3 Os objetivos de melhoria de metadados quantitativos são derivados da estratégia de metadados.

5.4 Alterações planejadas de dados são avaliadas para impacto no repositório de metadados; e captura de metadados, mudança e os processos de refinamento são continuamente melhorados.

Estratégia de Qualidade de Dados

A área de processo Estratégia de Qualidade de Dados tem como propósito definir uma estratégia integrada e organizacional para alcançar e manter o nível de

qualidade de dados necessários para suportar metas e objetivos de negócios. A cada nível atingido há uma evolução na capacidade da empresa.

Nível 1 realizado.

1.1 Objetivos, regras e critérios de qualidade de dados são documentados.

1.2 Os acionistas do negócio participam na definição da qualidade dos dados, critérios e objetivos.

1.3 Os planos de qualidade dos dados são seguidos; regras são implementadas e critérios são monitorados.

Nível 2 gerido.

2.1 Uma estratégia de qualidade de dados é definida, aprovada e gerenciada.

2.2 As partes interessadas da empresa participam na criação das estratégias de qualidade de dados.

2.3 A organização estabeleceu políticas, processos, e diretrizes para implementar a estratégia de qualidade de dados.

2.4 Os requisitos de qualidade de dados são articulados empregando dimensões de qualidade de dados selecionados pela organização.

2.5 A estratégia de qualidade de dados é criada com referência a objetivos e planos de negócios, e é aprovada pela gestão.

2.6 Planos para cumprir as metas e objetivos da estratégia de qualidade dos dados são monitoradas para avaliar o progresso.

Nível 3 definido.

3.1 A estratégia de qualidade de dados é seguida em toda a organização e é acompanhada correspondendo às políticas, processos e diretrizes.

3.2 Papéis e responsabilidades para a governança e gerenciamento de práticas de qualidade dos dados são definidas.

3.3 Um processo para definir benefícios e custos para iniciativas de qualidade de dados é empregado para orientar sobre a estratégia de qualidade de dados.

3.4 As políticas, processos e governança contidos na estratégia de qualidade de dados estão ancorados em todo o ciclo de vida dos dados, e correspondendo a processos que são obrigatórios no sistema de desenvolvimento da metodologia do ciclo de vida.

3.5 Projetos de qualidade de dados, como perfil de dados, avaliações de dados, limpeza de dados e avaliações de perigo estão alinhadas com as necessidades do

negócio identificadas na estratégia de qualidade dos dados e na análise do custo-benefício.

3.6 Um plano sequencial de esforços para melhoria da qualidade dos dados em toda a organização é desenvolvido, monitorado, e mantido.

Nível 4 medido.

4.1 Métricas de qualidade de dados são empregadas para analisar sugestões de mudanças na estratégia de qualidade de dados.

4.2 Priorizando problemas de qualidade de dados para remediação ou a prevenção é realizada uma avaliação quantitativa. Prioridades são regularmente revisadas e ajustadas para mudanças dos objetivos de negócios.

4.3 Os relatórios das partes interessadas sobre problemas de qualidade de dados são sistematicamente coletados. Suas expectativas para melhorar a qualidade dos dados estão incluídas na estratégia de qualidade dados que são medidos e monitorados.

4.4 O desempenho das políticas, processos e diretrizes, que são definidas para apoiar a estratégia de qualidade de dados, são ajustadas com base em resultados de análise das métricas de desempenho.

Nível 5 otimizado.

5.1 Os marcos e métricas do programa de qualidade de dados são regularmente revisados por executivos, e melhorias contínuas são implementadas.

5.2 A organização compartilha as melhores práticas e abordagens de sucesso para melhorar a qualidade dos dados com os parceiros do setor.

Perfil dos Dados

A área de processo Perfil dos Dados tem como alvo desenvolver uma compreensão do conteúdo, qualidade e regras de um conjunto especificado de dados sob gestão.

Nível 1 realizado.

1.1 O perfil básico é executado para um armazenamento de dados.

Nível 2 gerido.

2.1 Uma metodologia de perfil de dados é estabelecida e seguida.

2.2 Planos de perfil de dados são estabelecidos para projetos.

2.3 Os planos para traçar o perfil de um armazenamento de dados são compartilhados com as relevantes partes interessadas e governança de dados..

2.4 As atividades de perfil de dados são conseguidas de acordo com o plano, e esforços são exercidos quando desvios significativos do plano são detectados.

2.5 Resultados e recomendações de perfil de dados são relatados para as partes interessadas.

Nível 3 definido.

3.1 Metodologias de perfil de dados, processos, práticas, ferramentas e modelos de resultados foram definidos e padronizados.

3.2 Todas as técnicas identificadas para atender aos objetivos de criação de perfil são concluídas.

3.3 Rastreabilidade entre os requisitos de dados, metadados documentados, dados físicos e regras de qualidade de dados são capturados e mantidos.

3.4 A governança de dados está engajada para identificar os principais conjuntos de dados compartilhados e os armazenamentos de dados correspondentes que devem ser regularmente perfilados e monitorados.

3.5 Processos de criação de perfil são reutilizáveis e implantados através de vários armazenamentos de dados e repositórios de dados são compartilhados.

3.6 O *Software Development Life Cycle* (SDLC) inclui tarefas de criação de perfil de dados com adaptação de critérios, orientação e governança.

Nível 4 medido.

4.1 O desempenho dos processos de criação de perfil de dados é medido e usado para gerenciar atividades em toda a organização.

4.2 Os esforços de criação de perfil de dados incluem a avaliação da conformidade de conteúdo de dados com seus metadados aprovados e padronizados.

4.3 Durante uma atividade de criação de perfil de dados, os problemas reais são em comparação com as questões estatisticamente previstas com base em resultados históricos de perfil.

4.4 Os resultados são armazenados centralmente, sistematicamente monitorados, e analisados em relação às estatísticas e métricas para fornecer ideias sobre melhorias na qualidade dos dados ao longo do tempo.

Nível 5 otimizado.

5.1 A organização aborda as causas básicas dos defeitos e outras questões baseadas em uma compreensão do significado, características técnicas, e comportamento dos dados ao longo do tempo.

5.2 Processos de criação de perfil de dados e outras atividades são analisadas para identificar defeitos e fazer melhorias com base nos benefícios esperados quantificados, custos estimados e objetivos de negócios.

5.3 Relatórios de perfil automatizados em tempo real ou quase em tempo real são criados para todos os *feeds* de dados críticos e repositórios.

Avaliação da Qualidade dos Dados

A área de processo Avaliação da Qualidade dos Dados tem como propósito fornecer uma abordagem sistemática para medir e avaliar a qualidade dos dados de acordo com processos, técnicas e em contraste as regras de qualidade dos dados.

Nível 1 realizado.

1.1 Avaliações de qualidade de dados são realizadas e os resultados são documentados.

Nível 2 gerido.

2.1 Metas, limites, objetivos de avaliação de qualidade de dados são estabelecidos, usados e mantidos de acordo com técnicas e processos padrão.

2.2 A governança de dados determina o conjunto-chave de atributos por área sujeita para avaliações de qualidade de dados.

2.3 As avaliações de qualidade dos dados são finalizadas periodicamente de acordo com uma frequência aprovada pela avaliação da política de qualidade dos dados.

2.4 Os resultados de avaliação da qualidade dos dados incluem recomendações para remediação com apoio lógico.

2.5 Análise de impacto inclui estimativas dos custos de correções, o nível de esforço, caracterização do impacto do negócio, e benefícios tangíveis e intangíveis.

2.6 Relatórios de avaliações de qualidade de dados de informações de alto nível são rastreáveis para compor registros individuais para apoiar análise.

Nível 3 definido.

3.1 Avaliações periódicas de qualidade de dados são completadas de acordo com as políticas de qualidade de dados em um agendamento ou de acordo com acionadores de eventos especificados.

3.2 Os métodos para avaliar os impactos dos negócios, incluindo custos e riscos, são definidos, aprovados e consistentemente aplicados em toda a organização.

3.3 Planos de melhoria resultantes da qualidade dos dados as avaliações são integradas ao nível da organização.

3.4 A qualidade dos dados é avaliada utilizando-se de limiares estabelecidos e metas para cada dimensão de qualidade selecionada.

3.5 Os padrões de relatórios de medição de qualidade de dados são integrados ao ciclo de vida do desenvolvimento de sistemas e processos de conformidade.

Nível 4 medido.

4.1 Os relatórios de medição da qualidade dos dados são sistematicamente gerados com base na criticidade de atributos e volatilidade dos dados.

4.2 Os metadados operacionais de qualidade de dados são padronizados, capturados, e analisados usando estatísticas e outras técnicas quantitativas para orientar melhorias.

Nível 5 otimizado.

5.1 A organização pode avaliar quantitativamente os benefícios de propostas de mudanças de dados e refinar prioridades de gestão em consonância com as práticas de governança da qualidade dos dados.

5.2 Os processos de avaliação e emissão de relatórios de qualidade de dados são continuamente revisados e melhorados.

Limpeza dos Dados

A área de processo Limpeza dos Dados tem como objetivo definir os mecanismos, regras, processos e métodos utilizados para validar e corrigir dados de acordo com regras de negócios predefinidos.

Nível 1 realizado.

1.1 Os requisitos de limpeza de dados são definidos e executados.

Nível 2 gerido.

2.1 Atividades de limpeza de dados aderem à limpeza dos requisitos de dados, que estão vinculados a melhorias de processos para alcançar objetivos de negócios.

2.2 Atividades de limpeza de dados estão em conformidade com a qualidade dos requisitos de dados (por exemplo, dimensões de qualidade, tais como conformidade, precisão, singularidade) e critérios de qualidade.

2.3 O escopo da limpeza de dados é definido.

2.4 O processo de realização da limpeza de dados é definido por um plano.

2.5 Uma política de limpeza de dados é estabelecida e mantida.

2.6 Foram estabelecidos métodos para correção dos dados e são definidos dentro de um plano.

2.7 Problemas de limpeza de dados são comunicados e resolvidos, quando possível, na fonte interna ou externa.

Nível 3 definido.

3.1 O histórico de mudanças de dados é mantido através de atividades de limpeza.

3.2 Existem políticas, processos e procedimentos para garantir que as atividades de limpeza de dados sejam aplicadas no ponto de origem de acordo com as regras publicadas.

3.3 As regras de limpeza de dados são aplicadas de forma consistente em toda a organização.

3.4 Um grupo de governança estabelece, mantém e garante adesão às regras de limpeza de dados.

3.5 Modelos de relatórios de resultados de limpeza de dados padrão, no detalhe e em nível de resumo, são empregados.

Nível 4 medido.

4.1 Os contratos de nível de serviço incluem critérios de qualidade de dados para responsabilizar os provedores de dados por dados limpos.

Nível 5 otimizado.

5.1 A organização está envolvida no estabelecimento e manutenção de normas externas ou industriais para melhorar a qualidade do conteúdo de dados.

5.2 Os requisitos de limpeza de dados para provedores de dados são gerenciados de acordo com processos padronizados.

Definição de Requisitos de Dados

A área de processo Definição de Requisitos de Dados tem como finalidade garantir que os dados produzidos e consumidos satisfaçam os objetivos de negócios, é compreendido por todos os acionistas relevantes, e é consistente com os processos que criam e consomem os dados.

Nível 1 realizado.

1.1 As partes interessadas revisam e aprovam as cláusulas de dados.

1.2 O glossário empresarial é atualizado com formalidades de dados aprovados.

1.3 Os pressupostos de dados são avaliados e julgados contra entregas e confirmadas ou modificadas.

Nível 2 gerido.

2.1 O processo de definição dos requisitos de dados é documentado e seguido.

2.2 Os requisitos de dados necessários para a realização de metadados de gestão são definidos e comprovadamente alinhados com os objetivos de negócios.

2.3 A rastreabilidade dos requisitos de dados para os requisitos de negócios e objetivos são mantidos.

2.4 Os requisitos de dados estão alinhados com os correspondentes modelos de dados e outros artefatos relacionados.

2.5 Funções e responsabilidades das partes interessadas para envolvimento com definição de requisitos de dados são especificados, planejados, monitorados e controlados.

Nível 3 definido.

3.1 Os requisitos de dados são definidos, validados e integrados usando a definição de requisitos padrão para todo o quadro da organização.

3.2 Os requisitos de dados são avaliados com base nas prioridades dos negócios.

3.3 Os processos de negócios que produzem dados são documentados e vinculados aos requisitos de dados.

3.4 Requisitos de dados em conformidade e incluem conformidade dos requisitos para dados físicos e lógicos, incluindo regras de segurança, bem como requisitos técnicos.

3.5 Os requisitos são avaliados para garantir que eles sejam implementados no ambiente de destino.

Nível 4 medido.

4.1 As dicas práticas da indústria relativas aos requisitos de dados foram avaliadas contra critérios selecionados para determinar se eles devem ser adotados no ciclo de vida de desenvolvimento.

4.2 Métricas definidas e gerenciadas garantem que os requisitos de dados definidos satisfaçam objetivos de negócios; ações corretivas são tomadas quando o desempenho não é atendido conforme às necessidades dos negócios.

Nível 5 otimizado.

5.1 A organização implementou um processo de melhoria contínua para garantir eficiência e consistente priorização, seleção e verificação de requisitos de dados.

5.2 A organização compartilha as melhores práticas com a indústria no vínculo aos requisitos de dados.

Gestão do Ciclo de Vida dos Dados

A área de processo Gestão do Ciclo de Vida dos Dados tem como desígnio garantir que a organização entenda, mapas, inventários e controle seus fluxos de dados através de processos de negócios ao longo do ciclo de vida dos dados desde a sua constituição ou sua retirada. O gerenciamento do ciclo de vida dos dados permite um melhor gerenciamento de riscos e suporta melhorias na qualidade dos dados, particularmente em situações envolvendo grandes volumes de dados ou altas velocidades do movimento de dados, que é complexo e interdependente de processos que compartilham dados.

Nível 1 realizado.

1.1 O ciclo de vida dos dados para uns processos de negócios são definidos e aplicados.

1.2 Dependências de dados - *upstream* e *downstream* desde a criação inicial ou ingestão foram identificadas e mapeadas.

1.3 As partes interessadas concordam com o escopo dos elementos de dados e fontes de dados confiáveis.

Nível 2 gerido.

2.1 Os requisitos dos consumidores e produtores de dados são mapeados e alinhados.

2.2 Processos de negócios para mapeamento de dados são definidos, mantidos e revisados periodicamente para conformidade.

2.3 Um processo definido para acordos de colaboração com respeito aos dados compartilhados e seu uso dentro dos processos da empresa são seguidos.

2.4 Os critérios de seleção são definidos e aplicados para designar fontes de dados confiáveis.

2.5 O processo de ciclo de vida de desenvolvimento de sistemas requer referência e adoção de representações de dados compartilhados aprovados e obtenção de fontes de dados de autoridades.

Nível 3 definido.

3.1 Os processos de gerenciamento do ciclo de vida dos dados são definidos e aprovados por partes interessadas, e processos gerenciados pela governança de dados.

3.2 Processos de gerenciamento de alterações que abordam o todo o ciclo de vida dos dados são estabelecidos e mantidos.

3.3 Responsabilidades do projeto para desenvolvimento do sistema de ciclo de vida incluem atividades de mapear atributos de dados para os processos de negócios, dados compartilhados, fontes e objetivos de dados são importantes para a organização.

3.4 Fluxos de dados completos para processar mapas do ciclo de vida para dados compartilhados são implementados para cada processo de negócio a nível organizacional.

3.5 Alterações nos conjuntos de dados compartilhados ou conjuntos de dados de destino para uma finalidade de negócio específica são gerenciadas por estruturas de governança de dados com acionistas relevantes.

3.6 As designações de fontes de dados autoritárias são revisadas e aprovadas pela governança de dados.

3.7 Medidas e métricas são definidas e associadas a informações que são coletadas para avaliar o progresso no processo para esforços de mapeamento de dados e a adoção de fontes de dados.

Nível 4 medido.

4.1 Um processo padrão é usado em toda a organização para análise de impacto do ciclo de vida dos dados e para identificar, estimar, e agendar alterações em interfaces e conjuntos de dados.

4.2 Métricas são usadas para expandir o reaproveitamento de dados compartilhados aprovado e eliminar a redundância do processo.

Nível 5 otimizado.

5.1 Métricas e *feedback* das partes interessadas são analisadas periodicamente com o propósito de introduzir melhorias no gerenciamento de dependências de dados.

5.2 As métricas do ciclo de vida dos dados são periodicamente refinadas e revisadas pela alta administração.

5.3 A organização compartilha experiências com a indústria e atraídos em relação aos processos de ciclo de vida de gerenciamento de dados.

Gestão de Provedor

A área de processo Gestão de Provedor tem a intenção de otimizar o fornecimento interno e externo de dados para satisfazer requisitos de negócios e para gerenciar o provisionamento de dados de acordos consistentes.

Nível 1 realizado.

1.1 Os requisitos de dados são traduzidos em fontes específicas de dados.

1.2 Análises e testes são praticados para verificar se os dados adquiridos atendem aos requisitos indicados.

Nível 2 gerido.

2.1 Um processo para analisar os requisitos de dados para o fornecimento de dados específicos e requisitos de mapeamento para fornecer elementos de dados, é definido e seguido.

2.2 Um processo de aquisição de dados para obtenção de provedores de dados externos são definidos e seguidos.

2.3 Os critérios de qualidade dos dados são definidos e incorporados em contratos de serviço de provedores, ambos externos e internos.

2.4 Discussões planejadas são terminadas com provedores de dados para desvios de endereço para limites de qualidade de dados estabelecidos e metas definidas no contrato de nível de serviço.

Nível 3 definido.

3.1 A governança de dados monitora todo o processo da organização usado para desenvolver o fornecimento de requisitos de dados.

3.2 Métricas para o processo de gerenciamento de fornecimento de dados são estabelecidos, mantidos e usados.

3.3 Os processos de avaliação e seleção de fontes de dados são definidos e empregados em toda a organização.

3.4 Os contratos de nível de serviço do provedor são desenvolvidos com base em modelos e processos padrão, são implementados em toda a organização, rastreados e forçados.

3.5 Os contratos de nível de serviço são periodicamente revisados para garantir a satisfação dos objetivos de negócios e requisitos.

3.6 Reuniões periódicas são concretizadas com provedores de dados para revisão de mudanças planejadas no conteúdo de dados, processos, formatos, qualidade etc.

Nível 4 medido.

4.1 Principais métricas de desempenho relacionadas ao nível de serviço são analisados usando estatísticas e outras técnicas quantitativas, são revisadas e usadas para identificar e resolver problemas.

4.2 Relacionamentos de parceria são desenvolvidos com provedores externos selecionados com base nos resultados de avaliação do provedor e necessidades de dados antecipadas.

Nível 5 otimizado.

5.1 Análises estatísticas e outras quantitativas do provedor processos são aplicados para melhorá-los e garantir que os objetivos de negócios são adequadamente apoiados.

5.2 Lições de buscas aprendidas e evoluídas das melhores práticas são compartilhadas com os pares da indústria.

Abordagem Arquitetônica

A área de processo de Abordagem Arquitetônica tem como intuito projetar e implementar uma camada de dados ideal que permite aquisição, produção, armazenamento e entrega de dados para atender objetivos empresariais e técnicos.

Nível 1 realizado.

1.1 Uma arquitetura de dados alinha os requisitos dos negócios com o armazenamento de dados implementado para pelo menos um projeto.

1.2 As partes interessadas em negócios e TI são identificadas e envolvidas em decisões arquitetônicas.

1.3 Recursos técnicos e requisitos são definidos para orientar a instalação.

Nível 2 gerido.

2.1 A arquitetura de dados de destino está alinhada e complementa a estratégia de gestão de dados.

2.2 Um processo de governança é estabelecido e seguido para garantir que a arquitetura de dados esteja racionalizada e aprovada pelas empresas e acionistas em TI.

2.3 Um plano de transição arquitetônica baseia-se em um mapeamento entre os componentes atuais da camada de dados e o estado futuro do ambiente.

2.4 Um processo é estabelecido e seguido para garantir que os dados especificados da interface são documentados para dados compartilhados, com rastreabilidade desde a criação até o consumo final por todas as fontes dentro do escopo.

2.5 Um processo de conformidade é estabelecido e seguido para garantir que os projetos se refiram e utilizem a arquitetura aprovada.

Nível 3 definido.

3.1 A abordagem arquitetônica para os dados é uma arquitetura seguida em toda a organização.

3.2 É efetivado um processo de racionalização de armazenamento de dados.

3.3 A arquitetura-alvo é desenvolvida de forma colaborativa e aprovada conjuntamente por unidades de negócios, TI e Governança de dados.

3.4 A organização cria e mantém métricas para avaliar o progresso na transição e rastreabilidade do mapeamento.

3.5 Tanto padrões de dados externos internos quanto selecionados são avaliados e aplicados ao desenvolvimento de projetos arquitetônicos e projetos de componentes.

3.6 A arquitetura, os requisitos técnicos e o suporte aos recursos de infraestrutura estão alinhados.

3.7 A arquitetura inclui a camada de integração de destino, também conhecido como design de interface comum.

3.8 O perfil de dados é cumprido antes de finalizar o projeto de um componente de armazenamento de dados que conterà os dados existentes.

Nível 4 medido.

4.1 Análise estatística do desempenho e das melhorias na qualidade dos dados são usadas como entrada para o processo de design arquitetônico.

Nível 5 otimizado.

5.1 Os modelos de predição são avaliados em nexos à arquitetura mudanças e ajustadas conforme necessário.

5.2 A organização compartilha arquitetura e lições de plataforma aprendidas através de publicações e conferências.

Padrões Arquitetônicos

A área de processo Padrões Arquitetônicos tem por meta fornecer um conjunto aprovado de expectativas para governar elementos arquitetônicos que suportam representações de dados aprovados, acesso a dados e distribuição de dados, fundamental para o controle de ativos de dados e o uso eficiente e troca de informações.

Nível 1 realizado.

1.1 Os padrões de arquitetura de dados são definidos e seguidos por pelo menos um projeto.

Nível 2 gerido.

2.1 Normas arquitetônicas que abordam representações de dados, segurança, acesso a dados e provisionamento de dados são definidos e seguidos.

2.2 Os padrões arquitetônicos são revisados com acionistas dos negócios e aprovados pela governança de dados.

2.3 Um processo que rege solicitações, aprovações e gestão de desvios de padrões arquitetônicos é definido e seguido.

2.4 A abordagem arquitetônica, projetos e projetos de componentes se alinham aos padrões selecionados.

2.5 As normas arquitetônicas são revisadas periodicamente contra mudanças nas necessidades de negócios, arquitetura e tecnologia.

Nível 3 definido.

3.1 Os padrões arquitetônicos são seguidos em toda a organização.

3.2 Os requisitos externos aplicáveis à organização são incluídos no desenvolvimento de padrões de arquitetura de dados.

3.3 Funções e responsabilidades de acionistas para as normas de arquitetura incluem prestação de contas de conformidade, propriedade e treinamento.

3.4 A governança de dados garante que os padrões arquitetônicos estão alinhados com as necessidades do negócio e alinhados com a governança de arquitetura da organização.

3.5 Métricas para monitoramento e controle da adoção e conformidade com padrões arquitetônicos são definidos e implementados.

3.6 Um processo de auditoria é desenvolvido, documentado e processado para avaliar a conformidade com o padrão de arquitetura.

Nível 4 medido.

4.1 Métricas de resultado de auditoria e padrões de desvio interno indicam alterações nos padrões de arquitetura de dados e com orientação aprimorada para aplicação de padrões necessários.

4.2 A organização realiza análise de impacto baseada em riscos para mudanças propostas na arquitetura de dados padrões organizacionais e orientações antes da aceitação.

Nível 5 otimizado.

5.1 O *feedback* é fornecido aos acionistas sobre novas ou propostas de mudanças nas normas de dados.

5.2 A organização contribui para padrões de arquitetura de dados dentro da indústria.

5.3 A organização pesquisa tecnologias inovadoras de dados e métodos para adoção potencial, e desenvolve novas normas apropriadas para aqueles que são implantados.

5.4 A organização compartilha as melhores práticas de padrões e lições aprendidas através de publicações, conferências e *whitepapers*.

Gestão da Plataforma de Dados

A área de processo Gestão da Plataforma de Dados garante que uma plataforma eficaz seja implementada e gerenciada para atender às necessidades dos negócios.

Nível 1 realizado.

1.1 Plataformas e componentes de gerenciamento de dados são documentados para pelo menos um projeto.

Nível 2 gerido.

2.1 A implementação da plataforma suporta os objetivos estabelecidos na estratégia de gestão de dados.

2.2 Existe uma política e processo para garantir que construa ou compre decisões que consideram a arquitetura de dados alvo e apoie a estratégia de gerenciamento de dados.

2.3 Plataformas são consistentes com tecnologias e projetos arquitetônicos.

2.4 Plataformas suportam os requisitos de segurança e acesso da organização.

2.5 A governança de dados aconselha e fornece consentimentos sobre as principais decisões da plataforma.

Nível 3 definido.

3.1 Elementos de dados críticos para os quais a plataforma é uma fonte confiável ou sistema de registro estão documentados.

3.2 A duplicação do conjunto de dados entre os sistemas está documentada, planejada e justificada.

3.3 Planos de implementação da plataforma abordam a escalabilidade, resiliência, e segurança necessária para acomodar mudanças na complexidade prevista, bem como o volume de dados e número de usuários.

3.4 Design e recursos da plataforma garantem esse fluxo de trabalho e os requisitos de nível de serviço podem ser atendidos.

3.5 Dados de desempenho da plataforma são capturados, armazenados e usados para verificar se a plataforma atende aos desempenhos do negócio, necessidades e requisitos de capacidade.

3.6 A plataforma contribui com seus metadados para o repositório de metadados da organização.

Nível 4 medido.

4.1 Métricas de desempenho qualitativas e quantitativas para a plataforma de gerenciamento de dados são analisadas, utilizando estatísticas e outras técnicas quantitativas, para apoiar a plataforma nas mudanças de decisões.

Nível 5 otimizado.

5.1 Os objetivos de melhoria da plataforma são quantitativamente expressos e aprovados pela governança.

5.2 A organização melhora continuamente a plataforma com base em dados de desempenho estatístico e análise causal.

5.3 Os efeitos das mudanças na plataforma são comparados com modelos de previsão e analisados para melhorar a previsão de modelos.

5.4 A organização está compartilhando suas experiências relacionadas a design, desenvolvimento, implantação e operação de gerenciamento de dados da plataforma dentro de seu setor.

Integração dos Dados

A área de processo Integração dos Dados reduz a necessidade de a empresa obter dados de múltiplas fontes e para melhorar a disponibilidade de dados para processos de negócios que requerem consolidação e agregação de dados, como analíticos. A integração de dados permite a otimização de dados, a prática de redução de custos através da centralização, e melhor qualidade dos dados.

Nível 1 realizado.

1.1 A integração de dados entre sistemas foi realizada e documentada.

Nível 2 gerido.

2.1 Os planos de integração de dados estão documentados.

2.2 O conjunto de disciplinas e ferramentas de integração de dados usadas pela organização fornecem transporte e carregamento, mudança na captura de dados, controle de versão e configuração, captura e gerenciamento de metadados em linha de qualidade de dados com verificações e controles.

2.3 Um processo de controle de alteração é estabelecido e seguido para garantir que as mudanças no ambiente de integração, incluindo fontes *upstream* e alvos *downstream*, são controlados e coordenados.

2.4 Processos de remediação são estabelecidos e seguidos para abordar circunstâncias anormais selecionadas.

2.5 Verificação de integração é verificada para garantir que as especificações de arquitetura e interface estejam documentadas e será cumprido antes de ser lançado em produção.

Nível 3 definido.

3.1 A organização segue um conjunto padrão de práticas e regras para a realização de atividades de integração de dados.

3.2 Verificações de qualidade são definidas como parte do padrão de integração organizacional e desempenhadas como parte dos processos de dados de integração.

3.3 Um processo padrão é estabelecido e seguido para criar e verificar regras de precedência de dados com usuários de negócios com base em casos de uso, requisitos e gatilhos selecionados.

3.4 O desenvolvimento e implantação da integração de interfaces são especificados de acordo com arquitetura padrão que suporta reutilização.

3.5 Métricas de desempenho de interface e integração são coletadas e analisadas para identificar a não conformidade com padrões e critérios.

3.6 A organização de documentos e gerenciamento de mudanças para fontes de dados e através do processo de governança de dados.

Nível 4 medido.

4.1 Análise estatística das métricas de integração orienta decisões sobre alterações nas interfaces e integrações.

4.2 Dados selecionados e compartilhados estão totalmente integrados, centralmente gerenciados, e entregues conforme necessário para integração dos dados de armazenamento.

Nível 5 otimizado.

5.1 Os modelos de desempenho para integração de dados são periodicamente revisados, e são usados como entrada para melhorias.

5.2 A organização pública e compartilha as melhores práticas de integração dentro da indústria.

Histórico, Arquivamento e Retenção dos Dados

A área de processo Histórico, Arquivamento e Retenção dos Dados certifica que a manutenção de dados satisfaça a organização e requisitos regulatórios para disponibilidade de dados históricos, e que os requisitos legais e regulatórios para arquivamento de dados e a retenção de dados seja atendida.

Nível 1 realizado.

1.1 Dados históricos estão disponíveis e usados para apoiar negócios e decisões.

1.2 É produzido um backup e os dados são arquivados como prescrito em políticas.

Nível 2 gerido.

2.1 Políticas determinam a gestão do histórico de dados, incluindo requisitos de retenção, destruição e trilha de auditoria.

2.2 Um método definido garante que os dados históricos necessários para suportar as necessidades dos negócios sejam acessíveis.

2.3 O teste de restauração é elaborado em arquivos de dados selecionados.

2.4 Acesso, transmissão e modificações ao histórico e aos dados arquivados são controlados por políticas e processos.

Nível 3 definido.

3.1 A organização tem um *data warehouse* prescrito repositório que fornece acesso a dados históricos para atender às análises e precisa apoiar processos de negócios.

3.2 Contexto de dados em qualquer ponto específico do tempo podem ser recriados.

3.3 A política é definida e aprovada pela governança de dados e implementada no nível organizacional que exige registro de alterações de dados e retenção dos registros.

3.4 Um programa de auditoria garante o cumprimento da organização políticas de registro, arquivamento e retenção de dados.

3.5 Existe um mecanismo de *feedback* com os acionistas e reguladores para afirmar a retenção de dados e políticas de arquivamento existentes.

Nível 4 medido.

4.1 Técnicas estatísticas e outras quantitativas são utilizadas para analisar dados históricos para entrada no processo de negócios e melhorias na qualidade dos dados.

4.2 Modelos são empregados para prever o cumprimento do jurídico e requisitos regulatórios.

4.3 Os resultados das métricas e o *feedback* das partes interessadas estão acostumados a melhorar as políticas de retenção e arquivamento de dados.

Nível 5 otimizado.

5.1 A organização compartilha políticas e melhores práticas sobre dados históricos e arquivamento dentro de sua indústria.

Medição e Análise

A área de processo de Medição e Análise tem o intuito de desenvolver e sustentar uma capacidade de medição e analítica técnicas para apoiar o gerenciamento e a melhoria de dados das atividades de gestão. A cada Nível atingido há uma evolução na capacidade da empresa.

Nível 1 realizado.

1.1 O gerenciamento de configuração é documentado e implementado.

1.2 As informações de gerenciamento de configuração estão disponíveis para todos os acionistas relevantes.

Nível 2 gerido.

2.1 Estão previstas mudanças no ambiente operacional, gerenciado e testado para determinar o impacto nos armazenamentos de dados, interfaces e ativos de processos de gerenciamento de dados.

2.2 Alterações de dados, incluindo as originadas por dados externos aos provedores estão sujeitas à configuração da organização processos de gestão.

2.3 As alterações na interface de dados são gerenciadas e controladas.

Nível 3 definido.

3.1 Uma política de gerenciamento de configuração é definida, aprovada por governança e implementada para plataformas selecionadas e ativos de processos de gerenciamento de dados em toda a Organização.

3.2 Alterações em armazenamentos de dados, interfaces de dados e dados ativos de processo de gestão são planejados e aprovados por acionistas no Nível organizacional.

3.3 Um programa de auditoria garante a conformidade com a configuração política de gestão em toda a organização.

3.4 A governança de dados tem responsabilidade e supervisão autoridade para políticas de gerenciamento de configuração e processos.

Nível 4 medido.

4.1 Métricas são usadas para medir a conformidade e eficácia das políticas de gerenciamento de configuração e procedimentos.

Nível 5 otimizado.

5.1 Os modelos preditivos são avaliados e melhorados após conclusão da mudança.

5.2 Métricas e *feedback* das partes interessadas são analisados para melhorar o gerenciamento de configuração de novas versões de provedores de dados.

Gestão de Processo

A área de processo Gestão de Processo busca estabelecer e manter um conjunto utilizável de processo organizacional ativo, planejar, implementar e implantar o processo organizacional de melhorias informadas pelas metas e objetivos do negócio e as lacunas atuais nos processos da organização.

Nível 1 realizado.

1.1 Um grupo é criado para coordenar a melhoria de processos, normas e procedimentos.

1.2 As necessidades do processo são identificadas por meio de avaliações ou apresentação de propostas de mudança.

1.3 Problemas de processo ou oportunidades de melhoria são abordados.

1.4 Os produtos de dados, processos e trabalhos são armazenados, mantidos e disponibilizados.

Nível 2 gerido.

2.1 Estabelecer e manter a descrição das necessidades do processo e objetivos para a organização.

2.2 Avaliar processos conforme necessário para manter uma compreensão de seus pontos fortes e fracos.

2.3 Realizar avaliação de impacto sobre sugestão de melhorias.

2.4 Selecione e implemente melhorias para implantação com base em uma avaliação de custos, benefícios e outros fatores.

2.5 Estabelecer, manter e seguir planos de ação de processo para abordar melhorias nos processos.

Nível 3 definido.

3.1 Estabelecer e manter o Conjunto de Processos Padrão da Organização (OSSP).

3.2 Estabelecer e manter critérios e diretrizes de padrões de processos.

3.3 Estabelecer e manter o processo da organização como um ativo da biblioteca.

3.4 Estabelecer e manter a medição da organização como um repositório.

Nível 4 medido.

4.1 Estabeleça e mantenha o quantitativo da organização objetivos para a qualidade e desempenho do processo, que são rastreáveis aos objetivos de negócios.

4.2 Analisar o desempenho dos processos selecionados, e estabelecer e manter o desempenho do processo base.

4.3 Estabelecer e manter modelos de desempenho de processos para processos selecionados no padrão de processos da organização.

Nível 5 otimizado.

5.1 Manter os objetivos de negócios com base em um entendimento de estratégias de negócios e resultados reais de desempenho.

5.2 Analisar dados de desempenho do processo para determinar a capacidade da organização de atender a objetivos de negócios.

5.3 Identificar áreas potenciais para melhorias que possam contribuir para o cumprimento dos objetivos de negócios.

Garantia de Qualidade de Processo

A área de processo Garantia de Qualidade de Processo tem por missão fornecer staff e gestão com visão objetiva sobre a feitura de processos e os produtos de trabalho associados.

Nível 1 realizado.

1.1 Problemas de processo e produto são identificados e abordados.

Nível 2 gerido.

2.1 Avaliar objetivamente os processos selecionados preparados contra as descrições de processos aplicáveis, normas e procedimentos.

2.2 Avalie objetivamente os produtos de trabalho selecionados contra descrições de processos aplicáveis, padrões e procedimentos.

2.3 Comunique problemas de qualidade e garanta a resolução de questões de descumprimento com a equipe e os gerentes.

2.4 Estabelecer e manter registros de garantia de qualidade das atividades.

Nível 3 definido.

3.1 Estabelecer, manter e seguir as políticas de organização, processos e procedimentos para a garantia de qualidade do produto.

3.2 Estabelecer, manter e seguir as políticas da organização, processos e procedimentos para reportar qualidade dos resultados e problemas de não conformidade crescentes quando eles não podem ser resolvidos em níveis mais baixos.

3.3 Estabelecer, manter e aplicar um sistema de medição para problemas de qualidade.

Nível 4 medido.

4.1 A organização utiliza estatísticas e outras quantitativas técnicas para prever onde surgirão problemas de qualidade.

Nível 5 otimizado.

5.1 A organização utiliza estatísticas e outras quantitativas técnicas para gerenciar compensações entre o custo e qualidade para atender aos objetivos de negócios.

Gestão de Risco

A área de processo Gestão de Risco vai identificar e analisar possíveis problemas a fim de tomar a ação apropriada para garantir que os objetivos possam ser alcançados.

Nível 1 realizado.

1.1 Os riscos são identificados, documentados e monitorados.

Nível 2 gerido.

2.1 Analisar riscos identificados.

2.2 Monitor de identificação de riscos.

Nível 3 definido.

3.1 Determine fontes e categorias de risco.

3.2 Defina parâmetros utilizados para analisar e categorizar riscos e controlar o esforço de gerenciamento de riscos.

3.3 Estabeleça e mantenha a estratégia a ser usada para a Gestão de Risco.

3.4 Identificar, analisar e documentar riscos seguindo o processo padrão da organização.

3.5 Avaliar e categorizar cada risco identificado utilizando-se de categorias de riscos definidos e parâmetros, e determinar sua prioridade.

3.6 Desenvolver um plano de mitigação de riscos de acordo com o risco da estratégia de gestão.

3.7 Monitore o status de cada risco periodicamente e implemente o plano de mitigação de riscos conforme apropriado.

Nível 4 medido.

4.1 Utilizando técnicas estatísticas e outras quantitativas, analisar e determinar o risco quantitativo para atender os objetivos.

Nível 5 otimizado.

5.1 Estabelecer e manter, utilizando estatísticas e outras técnicas quantitativas, a postura de risco quantitativo para objetivos quantitativos selecionados.

Gestão de Configuração

A área de processo Gestão de Configuração tem como intuito estabelecer e manter a integridade do ambiente operacional e ativos de processos de gerenciamento de dados, usando configuração, identificação, controle, contabilidade de status e auditorias.

Nível 1 realizado.

1.1 O gerenciamento de configuração é documentado e implementado.

1.2 As informações de gerenciamento de configuração estão disponíveis para todos os acionistas relevantes.

Nível 2 gerido.

2.1 Estão previstas mudanças no ambiente operacional, gerenciado e testado para determinar o impacto nos armazenamentos de dados, interfaces e ativos de processos de gerenciamento de dados.

2.2 Alterações de dados, incluindo as originadas por dados externos aos provedores estão sujeitas à configuração da organização processos de gestão.

2.3 As alterações na interface de dados são gerenciadas e controladas.

Nível 3 definido.

3.1 Uma política de gerenciamento de configuração é definida, aprovada por governança e implementada para plataformas selecionadas e ativos de processos de gerenciamento de dados em toda a Organização.

3.2 Alterações em armazenamentos de dados, interfaces de dados e dados ativos de processo de gestão são planejados e aprovados por acionistas no nível organizacional.

3.3 Um programa de auditoria garante a conformidade com a configuração política de gestão em toda a organização.

3.4 A governança de dados tem responsabilidade e supervisão autoridade para políticas de gerenciamento de configuração e processos.

Nível 4 medido.

4.1 Métricas são usadas para medir a conformidade e eficácia das políticas de gerenciamento de configuração e procedimentos.

Nível 5 otimizado.

5.1 Os modelos preditivos são avaliados e melhorados após conclusão da mudança.

5.2 Métricas e *feedbacks* das partes interessadas são analisados para melhorar o gerenciamento de configuração de novas versões de provedores de dados.

4 COMO O DMM PODE APOIAR AS ORGANIZAÇÕES NA ADEQUAÇÃO À LGPD

A LGPD exige uma governança de dados em decorrência aos direitos do Titular dos dados, ou seja, uma gestão dos dados, que seja clara e concisa para garantir como um dado é coletado, o porquê e por quanto tempo ele ficará armazenado / arquivado. Em contrapartida existem as punições legais caso isso seja descumprido. O modelo *Data Management Maturity* (DMM) fornece práticas para que as empresas executem, outras sejam modificadas para atender aos requisitos da lei. Este aborda em seu ciclo de vida a entrada dos dados, onde já se obtém o consentimento do Titular dos dados e de forma centralizada é sucedida a gestão dos consentimentos, tratamento, arquivamento quando necessário e o descarte que também é previsto na LGPD.

Ao realizar um mapeamento dos dados que é a finalidade de cada categoria e área do DMM a rastreabilidade do dado fica evidente para toda a empresa, usabilidade do dado, tempo em que este deve permanecer dentro da empresa e disponibilidade / comunicação somente para os respectivos setores que realmente tratam este dado. O aumento na segurança no tratamento do dado fica evidente com o uso do DMM e quais setores se enquadram no escopo da LGPD, quais processos existentes podem ser afetados, qual tem prioridade devido a criticidade na manipulação de dados, auxiliando em seus esforços de conformidade.

O DMM vai contribuir para que o inventário de dados possa ser auditado, com informações de quais e como cada dado é processado e com todas essas práticas funcionais recomendadas pelo DMM, uma análise / abordagem detalhada de brechas / vulnerabilidades na gestão dos dados podem ser identificadas, porque tem se a capacidade para realizar uma avaliação de fluxos de trabalho, processos e procedimentos atuais, podendo assim dar solução. O DMM irá trabalhar em cima das políticas da companhia e até contribuir no aprimoramento de cada uma e desenvolvimento de procedimentos e processos operacionais que viabilizem a melhor gestão do dado concernente à LGPD. Por meio destas atividades descritas acima há garantias de que a LGPD está sendo cumprida com excelência, pois medidas técnicas estão estabelecidas.

Como o DMM aborda em sua área de comunicação a promulgação das políticas internas da organização, logo, toda a equipe entende corretamente o que

deve fazer, mantendo assim a conformidade com a LGPD e em sua categoria de Plataforma e Arquitetura na área de Histórico e Arquivamento e Retenção dos Dados, auditorias internas periódicas são efetuadas, promovendo atualizações de processos e melhorias contínuas com base em *feedbacks*, incluindo a verificação de seus registros de atividades de processamento (*logs*), mecanismos de consentimento, testes de controles de segurança de informações e análises de impacto na privacidade.

Tabela 1 — Análise do DMM sob a luz da LGPD

Artigo	Artigo LGPD	DMM	Práticas do DMM
1	O tratamento de dados para proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural	Estratégia de Gestão de Dados	Permite definir o escopo da gestão de dados no nível organizacional. 3.5 A estratégia de organização da gestão de dados é documentada, mantida, revisada e comunicada de acordo com o processo padrão definido pela organização.
2	Fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.	Histórico, Arquivamento e Retenção dos Dados	4.2 Modelos são empregados para prever o cumprimento do jurídico e requisitos regulatórios.
3	Operação de tratamento de dados I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por		

	objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.		
4	Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos b) acadêmicos III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;		
5	Art. 5º Definições	Glossário de Negócios	2.2 Os termos de negócios padrão estão prontamente disponíveis e promulgados para as partes interessadas relevantes.
6		Comunicação	2.1 O plano de comunicação para gestão de dados é definido, documentado, aprovado pelas partes interessadas e programado.
6	Princípios: a) Finalidade b) Adequação c) Necessidade d) Livre acesso e) Qualidade dos dados f) Transparência g) Segurança h) Prevenção i) Não discriminação j) Responsabilização	Função de Gestão de Dados	2.2 Princípios são definidos e seguidos para orientar a consistência das práticas relacionadas à gestão de dados
6		Estratégia de Qualidade de Dados	3.5 Projetos de qualidade de dados, como perfil de dados, avaliações de dados, limpeza de dados e avaliações de perigo

			estão alinhadas com as necessidades do negócio identificadas na estratégia de qualidade dos dados e na análise do custo-benefício. 4.2 Priorizando problemas de qualidade de dados para remediações ou a prevenção é avaliada quantitativamente. Prioridades são regularmente revisadas e ajustadas para mudanças dos objetivos de negócios.
7	Hipóteses de tratamento: 1) Consentimento 2) Cumprimento de obrigação legal 3) Tratamento de dados necessários à execução de políticas públicas 4) Realização de estudos por órgão de pesquisa, com a anonimização dos dados pessoais; 5) Execução de contrato 6) Exercício regular de direitos em processo judicial, administrativo ou arbitral 7) Proteção da vida 8) Tutela da saúde 9) Atender aos interesses legítimos do controlador 10) Proteção do crédito	Comunicação	5.1 As comunicações de gerenciamento de dados externos são feitas com o objetivo de influenciar políticas públicas e práticas recomendadas do setor que afetam os dados
8	O consentimento deverá ser fornecido por escrito, demonstrando a manifestação de vontade do titular	Gestão de Provedor	2.2 Um processo de aquisição de dados para obtenção de provedores de dados externos são definidos e seguidos.
9	O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados 1) finalidade específica do tratamento; 2) forma e duração 3) identificação do controlador; 4) informações de contato do controlador; 5) informações do uso compartilhado	Comunicação	4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação.

	de dados pelo controlador e a finalidade; 6) responsabilidades dos agentes que realizarão o tratamento; e 7) direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei		
10	O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, I - Apoio e promoção II – Proteção, em relação ao titular, do exercício regular de seus direitos	Função de Gestão de Dados	2.2 Princípios são definidos e seguidos para orientar a consistência das práticas relacionadas à gestão de dados
11	Tratamento de dados pessoais sensíveis em situações especiais	Padrões Arquitetônicos	4.2 A organização realiza análise de impacto baseada em riscos para mudanças propostas na arquitetura de dados padrões organizacionais e orientações antes da aceitação.
12	Os dados anonimizados não serão considerados		
13	Estudos em saúde pública	Perfil dos Dados	3.3 Rastreabilidade entre os requisitos de dados, metadados documentados, dados físicos e regras de qualidade de dados são capturados e mantidos. 3.4 A governança de dados está engajada para identificar os principais conjuntos de dados compartilhados e os armazenamentos de dados correspondentes que devem ser regularmente perfilados e monitorados.
14	O Consentimento para tratamento de dados pessoais de crianças e de adolescentes deve ser realizado	Definição de Requisitos de Dados	1.1 As partes interessadas revisam e aprovam as cláusulas de dados.

	por um dos pais ou pelo responsável legal		
15	Término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: finalidade foi alcançada; fim do período de tratamento; comunicação do titular; determinação da ANPD.	Histórico, Arquivamento e Retenção dos Dados	2.1 Políticas determinam a gestão do histórico de dados, incluindo requisitos de retenção, destruição e trilha de auditoria.
16	Os dados pessoais serão eliminados após o término de seu tratamento	Histórico, Arquivamento e Retenção dos Dados	2.1 Políticas determinam a gestão do histórico de dados, incluindo requisitos de retenção, destruição e trilha de auditoria.
16		Abordagem Arquitetônica	2.4 Um processo é estabelecido e seguido para garantir que os dados especificados da interface são documentados para dados compartilhados, com rastreabilidade desde a criação até o consumo final por todas as fontes dentro do escopo.
17	Assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade	Histórico, Arquivamento e Retenção dos Dados	4.2 Modelos são empregados para prever o cumprimento do jurídico e requisitos regulatórios.
17		Perfil dos Dados	3.3 Rastreabilidade entre os requisitos de dados, metadados documentados, dados físicos e regras de qualidade de dados são capturados e mantidos.
18		Perfil de Dados	3.4 A governança de dados está engajada para identificar os principais conjuntos de dados compartilhados e os armazenamentos de dados correspondentes que devem ser regularmente perfilados e monitorados.

18	O titular dos dados pessoais tem direito a obter do controlador I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados IV - anonimização, bloqueio ou eliminação V - portabilidade dos dados VI - eliminação dos dados pessoais VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento,	Limpeza dos Dados	2.7 Problemas de limpeza de dados são comunicados e resolvidos, quando possível, na fonte interna ou externa, ou seja, os dados serão destruídos quando solicitados.
18		Gestão do Ciclo de Vida dos Dados	2.3 Um processo definido para acordos de colaboração com respeito aos dados compartilhados e seu uso dentro dos processos da empresa são seguidos. 2.5 O processo de ciclo de vida de desenvolvimento de sistemas requer referência e adoção de representações de dados compartilhados aprovados e obtenção de fontes de dados de autoridades. 3.4 Fluxos de dados e dados completos para processar mapas do ciclo de vida para dados compartilhados são implementados para cada processo de negócio a nível organizacional.
19	A confirmação de existência ou o acesso a dados pessoais serão	Gestão do Ciclo de Vida dos Dados	3.4 A governança de dados está engajada para identificar os principais conjuntos de dados

	providenciados, mediante requisição do titular	Perfil dos Dados Histórico, Arquivamento e Retenção	compartilhados e os armazenamentos de dados correspondentes que devem ser regularmente perfilados e monitorados.
20	O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade	Estratégia de Gestão de Dados	3.4 A sequência do plano para execução da estratégia de gestão de dados é monitorada e atualizada, com base no progresso das revisões.
21	Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.	Histórico, Arquivamento e Retenção dos Dados	4.2 Modelos são empregados para prever o cumprimento do jurídico e requisitos regulatórios.
22	A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente		
23	O tratamento de dados pessoais pelas pessoas jurídicas de direito público devido ao atendimento de sua finalidade pública		
24	As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares		
25	Os dados deverão ser mantidos em formato interoperável e estruturado	Abordagem Arquitetônica	2.4 Um processo é estabelecido e seguido para garantir que os

	para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral		dados especificados da interface são documentados para dados compartilhados, com rastreabilidade desde a criação até o consumo final por todas as fontes dentro do escopo.
26	O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas	Função de Gestão de Dados	3.2 O modelo de interação para a função de gestão de dados garante o envolvimento da governança de dados para projetos que usam dados compartilhados.
27	comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada à autoridade nacional e dependerá de consentimento do titular	Comunicação	4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação.
28	Vetado.		
29	A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais	Gestão do Ciclo de Vida dos Dados	3.3 Responsabilidades do projeto para desenvolvimento do sistema de ciclo de vida incluem atividades de mapear atributos de dados para os processos de negócios, dados compartilhados, fontes e objetivos de dados são importantes para a organização. 3.4 Fluxos de dados e dados completos para processar mapas do ciclo de vida para dados compartilhados são implementados para cada processo de negócio a nível organizacional. 3.5 Alterações nos conjuntos de dados compartilhados ou conjuntos de

			<p>dados de destino para uma finalidade de negócio específica são gerenciadas por estruturas de governança de dados com acionistas relevantes. 3.6 As designações de fontes de dados autoritárias são revisadas e aprovadas pela governança de dados. 3.7 Medidas e métricas são definidas e associadas a informações que são coletadas para avaliar o progresso no processo para esforços de mapeamento de dados e a adoção de fontes de dados. 4.1 Um processo padrão é usado em toda a organização para análise de impacto do ciclo de vida dos dados e para identificar, estimar, e agendar alterações em interfaces e conjuntos de dados.</p>
30	<p>A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais</p>	Comunicação	<p>4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação.</p>
31	<p>Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.</p>		
32	<p>A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados</p>		

peçoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados peçoais pelo Poder Público

33 A transferência internacional de dados I - para países ou organismos internacionais que proporcionem grau de proteção de dados peçoais adequado ao previsto nesta Lei; II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, III - quando a transferência for necessária para a cooperação jurídica internacional IV proteção da vida V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - política pública VIII - quando o titular tiver fornecido o seu consentimento IX - quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

34 O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional

35 Cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta

36	As alterações nas garantias apresentadas como suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no inciso II do art. 33 desta Lei deverão ser comunicadas à autoridade nacional	Comunicação	4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação.
37		Função de Gestão de Dados	2.2 Princípios são definidos e seguidos para orientar a consistência das práticas relacionadas à gestão de dados. 2.3 Funções e responsabilidades são especificadas para apoiar a governança de gestão de dados e a interação entre a governança e a função de gestão de dados. 2.4 Acordos que estão em vigor, fornecem expectativa explícita para o uso compartilhado de recursos pela equipe, com responsabilidade para gestão de dados.
37	O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse	Perfil dos Dados	3.4 A governança de dados está engajada para identificar os principais conjuntos de dados compartilhados e os armazenamentos de dados correspondentes que devem ser regularmente perfilados e monitorados.
37		Histórico, Arquivamento e Retenção dos Dados	1.2 É produzido um backup e os dados são arquivados como prescrito em políticas. 2.1 Políticas determinam a gestão do histórico de dados, incluindo requisitos de retenção, destruição e trilha de auditoria.

38	A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais	Avaliação da Qualidade dos Dados	5.2 Os processos de avaliação e emissão de relatórios de qualidade de dados são continuamente revisados e melhorados.
39	O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador		
40	A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência	Função de Gestão de Dados	3.2 O modelo de interação para a função de gestão de dados garante o envolvimento da governança de dados para projetos que usam dados compartilhados.
41	O controlador deverá indicar encarregado pelo tratamento de dados pessoais	Gestão de Governança	2.3 Representantes da área em questão participam da governança de dados e processos associados. 3.3 A governança de dados inclui representantes de todas as unidades de negócios, que são fornecedores ou consumidores de áreas do uso de dados.
42	O controlador ou o operador causar dano, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo		
43	Os agentes de tratamento só não serão responsabilizados quando provarem: I - que não realizaram o tratamento de dados pessoais que lhes é atribuído; II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à		

	legislação de proteção de dados; ou III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro		
44	O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar		
45	As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente		
46		Histórico, Arquivamento e Retenção dos Dados	1.2 É produzido um backup e os dados são arquivados como prescrito em políticas. 2.1 Políticas determinam a gestão do histórico de dados, incluindo requisitos de retenção, destruição e trilha de auditoria.
46	Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito	Definição de Requisitos de Dados	3.4 Requisitos de dados em conformidade e incluem conformidade dos requisitos para dados físicos e lógicos, incluindo regras de segurança, bem como requisitos técnicos.
46		Padrões Arquitetônicos	2.1 Normas arquitetônicas que abordam representações de dados, segurança, acesso a dados e provisionamento de dados são definidos e seguidos.

46		Gestão da Plataforma de Dados	2.4 Plataformas suportam os requisitos de segurança e acesso da organização. 3.3 Planos de implementação da plataforma abordam a escalabilidade, resiliência, e segurança necessária para acomodar mudanças na complexidade prevista, bem como o volume de dados e número de usuários.
47	Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.		
48	O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares	Comunicação	4.1 Comunicações de gerenciamento de dados externos as partes interessadas são planejadas e conduzidas de acordo com a estratégia de comunicação. 5.1 As comunicações de gerenciamento de dados externos são feitas com o objetivo de influenciar políticas públicas e práticas recomendadas do setor que afetam os dados.
49	Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares		

50	Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização		
51	A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais		
52	Os agentes de tratamento (Controlador e Operador) de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos sanções administrativas		
53	A autoridade nacional definirá, por meio de regulamento próprio sobre sanções administrativas a infrações a esta Lei		
54	O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a gravidade da falta e a extensão do dano ou prejuízo causado		
55 A - L	Fica criada ANPD com autonomia técnica e decisória. Também se define uma estrutura de governança (Conselho Diretor e Conselho Nacional de Proteção de Dados Pessoais e da Privacidade)	Gestão de Governança	5.2 A estrutura de governança de dados é comunicada à indústria interessada em um modelo de boas práticas.
56	Vetado.		
57	Vetado.		

-
- 58 O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto de 23 (vinte e três) representantes, titulares e suplentes
-
- 59 Vetado.
-
- 60 Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:
-
- 61 A empresa estrangeira será notificada e intimada de todos os atos processuais previstos nesta Lei, independentemente de procuração ou de disposição contratual ou estatutária, na pessoa do agente ou representante ou pessoa responsável por sua filial, agência, sucursal, estabelecimento ou escritório instalado no Brasil.
-
- 62 A autoridade nacional e o Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (Inep), no âmbito de suas competências, editarão regulamentos específicos para o acesso a dados tratados pela União para o cumprimento do disposto no § 2º do art. 9º da Lei nº 9.394, de 20 de dezembro de 1996 (Lei de Diretrizes e Bases da Educação Nacional) , e aos referentes ao Sistema Nacional de Avaliação da Educação Superior (Sinaes), de que trata a Lei nº 10.861, de 14 de abril de 2004 .
-

63 A autoridade nacional estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, consideradas a complexidade das operações de tratamento e a natureza dos dados.

64 Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

65 Data em que a Lei entra em vigor: I
- dia 28 de dezembro de 2018,
quanto aos arts. 55-A, 55-B, 55-C,
55-D, 55-E, 55-F, 55-G, 55-H, 55-I,
55-J, 55-K, 55-L, 58-A e 58-B
2 anos após para os demais artigos

Fonte: O autor (2020)

5 CONCLUSÕES E EXTENSÕES

As organizações sempre precisaram gerenciar seus dados, mas os avanços tecnológicos, considerando a onipresença dos dados, expandiram o escopo dessa necessidade de gerenciamento. Os dados são difundidos nas organizações. Quase todos os processos de negócios - desde a criação de clientes, transações de compras, contato com clientes para *feedback* e serviços - usam dados como entrada e produzem dados como saída. A maioria desses dados está em formato eletrônico, o que significa maleabilidade: podem ser armazenados em grandes quantidades, manipulados, integrados e agregados para diferentes usos, incluindo inteligência comercial e análise preditiva. Eles também fornecem evidências de conformidade de uma organização (ou falta de conformidade) com leis e regulamentos.

As mudanças técnicas permitiram que as organizações usassem os dados de novas maneiras para criar produtos, compartilhar informações, criar conhecimento e melhorar o sucesso organizacional. Mas, o rápido crescimento da tecnologia e, com ela, a capacidade humana de produzir, capturar e extrair dados para obter significado intensificaram a necessidade de gerenciar dados de maneira eficaz.

Com base nessa nova realidade foi criada a Lei Geral de Proteção de Dados, número 13.709 de 14 de agosto de 2018 que é considerada um avanço em relação aos direitos de proteção e privacidade de dados dos cidadãos brasileiros. A LGPD trouxe muitos benefícios para a sociedade. Entre esses benefícios está o cuidado que a lei tem com a manipulação de dados sensíveis com o objetivo de não discriminar ou excluir uma pessoa por sua crença religiosa ou sua opção sexual. Além disso, uma outra vantagem é que a lei restitui ao titular de dados o poder de administrar e controlar seus dados. Nos casos de vazamentos ou uso indevido dos dados, o cidadão pode buscar por reparações e / ou indenizações de seus direitos.

Este trabalho teve como objetivo estudar a LGPD e o modelo DMM com a finalidade de analisar como este último pode contribuir para a adequação de organizações a atenderem aos requisitos da lei.

A LGPD solicita a designação de dois integrantes nas empresas para o cumprimento da lei: o controlador e o operador. O operador realiza o tratamento segundo as instruções do controlador, também chamado de *Data Protection Officer*, que deve verificar e fiscalizar as normas sobre a regulamentação. Tanto o operador

quanto o controlador devem manter o registro de suas operações para o cumprimento dos princípios citados anteriormente.

A criação deste comitê de segurança auxiliará no desenvolvimento de políticas internas, metas, planos de gerenciamento e medidas de segurança para proteção de dados. Possibilitando o melhor mapeamento de processos e análise de riscos.

Para a adequação será necessário o mapeamento de todos os dados pessoais utilizados pela empresa e/ou instituição, além da realização de processos de anonimização de dados, de forma a reduzir o risco de vazamento de informações sensíveis, bem como o mapeamento do investimento pensado em segurança da informação. Através da centralização dos dados do titular no DMM, é possível gerenciar a exclusão dos dados necessários conforme a solicitação do titular.

Um programa de treinamento de funcionários aliado a um plano de redução de riscos em situação emergencial será fundamental na adequação ao novo cenário, serviço este oferecido através de um bom programa de *compliance* digital.

Entre as contribuições deste trabalho estão o estudo e a síntese da Lei Geral de Proteção de Dados e a identificação das boas práticas do modelo DMM, além da abertura de novos caminhos investigativos para futuras pesquisas a serem aplicadas na implementação da LGPD, utilizando o DMM ou modelos de governança de dados. Aprofundar o estudo para práticas do DMM em artigos específicos. Quais ferramentas podem colaborar na adequação à LGPD? Quais ajustes são necessários para que o DMM possa ser completamente aplicado a LGPD e atendê-la?

A ferramenta de DMM fornece uma visão geral de como suas práticas colaboram com os artigos da LGPD e poderá resolver muitas das dores de cabeça enfrentadas por uma empresa na tentativa de atender às regras da LGPD, principalmente porque a ferramenta fornece a visibilidade de seus dados e as fontes de onde é armazenado e usado, mantendo atualizado e relevante, salvo com algumas modificações.

É importante que as empresas façam um estudo e o devido planejamento para a implantação dos itens necessários para se fortalecer e manter-se competitivo no novo cenário que a LGPD está trazendo, que é essencial para a construção do respeito à identidade e privacidade dos indivíduos e já estão preparadas para transformar o digital de modo a aperfeiçoá-lo para que produza resultados reais e

pertinentes com um mundo cada vez mais conectado e cheio de complexidades nas relações digitais.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR 14724**: Informação e documentação. Trabalhos Acadêmicos – Apresentação. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE. **Mercado Brasileiro de Software: panorama e tendências. ABES associação brasileira das empresas de software**. São Paulo, 2019. 28 p. Disponível em: <https://abessoftware.com.br/wp-content/uploads/anterior/Arquivos/Dados%202011/ABES-EstudoMercadoBrasileirodeSoftware2019.pdf>. Acesso em: 22 nov. 2020.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. **Atos do Poder Legislativo. Lei n. 13709, de 14 de agosto de 2018**. Diário Oficial da União. Brasília, DF, 15 de agosto de 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337>. Acesso em: 1 out. 2020.

BRASIL. **Parecer nº 129, de 2018** - Plenário/Senado Federal. Disponível em: <<https://legis.senado.leg.br/sdleg-getter/documento?dm=7821097&ts=1538690046263&disposition=inline&ts=1538690046263>>. Acesso em: 1 out. 2020.

CMMI INSTITUTE. **Data Management Maturity (DMM) Model. CMMI Institute**. 2019. 60 p. Disponível em: <https://cmmiinstitute.com/getattachment/cb35800b-720f-4afe-93bf-86cceb1fb17/attachment.aspx>. Acesso em: 17 ago. 2020.

DA ROCHA, Camila et al. **Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD**. *Revista de Tecnologia da Informação e Comunicação da Faculdade Estácio do Pará*. 2019. 78 p. Disponível em: <<http://www.revistasfap.com/ojs3/index.php/tic/article/view/285>>. Acesso em: 8 dez. 2020.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD)**: Guia de implantação. Editora Blucher, v. 3, f. 64, 2020.

GREENWALD, Glenn. **Sem lugar para se esconder**. Rio de Janeiro: Sextante, 2014.

JUE, A. L.; MARR, J. A.; KASSOTAKIS, M. E. **Mídias sociais nas empresas: colaboração, inovação, competitividade e resultados**. São Paulo: Évora, 2011.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de**

Metodologia Científica. 7. ed. São Paulo: Atlas, 2010.

KERZNER, H. **Gestão de projetos:** as melhores práticas. Porto Alegre: Bookman, 2010.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei N. 13.709/2018 LGPD.** 1. ed. São Paulo: Saraiva Educação, 2018.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (*General Data Protection Regulation*). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 9 dez. 2020.