Universidade Estadual de Londrina

RAFAEL HIRATA SANTOS

ANÁLISE DE FRAMEWORKS DE GOVERNANÇA DE TI EM RELAÇÃO À LGPD

LONDRINA
2022

RAFAEL HIRATA SANTOS

ANÁLISE DE FRAMEWORKS DE GOVERNANÇA DE TI EM RELAÇÃO À LGPD

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

Orientador: Prof. Dr. Rodolfo Miranda de Barros

LONDRINA
2022

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

S237a Santos, Rafael Hirata.

Análise de Frameworks de Governança de TI em relação à LGPD / Rafael Hirata Santos. - Londrina, 2022.

52 f. : il.

Orientador: Rodolfo Miranda de Barros.

Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Graduação em Ciência da Computação, 2022.

Inclui bibliografia.

1. Governança de TI - TCC. 2. Lei Geral de Proteção de Dados - TCC. 3. ITIL - TCC. 4. COBIT - TCC. I. Miranda de Barros, Rodolfo. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Graduação em Ciência da Computação. III. Título.

CDU 519

RAFAEL HIRATA SANTOS

ANÁLISE DE FRAMEWORKS DE GOVERNANÇA DE TI EM RELAÇÃO À LGPD

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação da Universidade Estadual de Londrina para obtenção do título de Bacharel em Ciência da Computação.

BANCA EXAMINADORA

Orientador: Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina

Prof. Dra. Jandira Guenka Palma
Universidade Estadual de Londrina – UEL

Francyelcyo Pussi Farias
Universidade Estadual de Londrina – UEL

Londrina, 30 de maio de 2022.

Este trabalho é dedicado a todos os que me ajudaram ao longo desta caminhada.

AGRADECIMENTOS

Agradeço primeiramente os meus pais, que me apoiaram em toda a minha jornada e sempre estiveram ao meu lado e proporcionaram a oportunidade de conquistar a graduação.

Agradeço também a todos os professores que me ajudaram em toda a minha trajetória acadêmica. Agradeço principalmente meu professor e orientador Pr. Rodolfo, que me deu a oportunidade de realizar este trabalho e me direcionou em todo o caminho.

Agradeço também pelos amigos que fiz durante minha estadia na universidade, que me ajudaram nos momentos difíceis e cuja amizade dura fora dela.

Por fim, agradeço a toda a Universidade Estadual de Londrina e todos os seus membros por proporcionarem a oportunidade de muitos de conquistarem seus sonhos.

"Não vos amoldeis às estruturas deste mundo, mas transformai-vos pela renovação da mente, a fim de distinguir qual é a vontade de Deus: o que é bom, o que Lhe é agradável, o que é perfeito.
(Bíblia Sagrada, Romanos 12, 2))

SANTOS. R. H.. **Análise de Frameworks de Governança de TI em relação à LGPD**. 2022. 51f. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2022.

RESUMO

Com o aumento da importância da tecnologia na vida cotidiana, a preocupação com a privacidade dos dados pessoais armazenados pelas empresas responsáveis se torna cada vez maior. Influenciados por essa preocupação, diversos entidades governamentais de todo o mundo criaram leis para normalizar e assegurar o tratamento de dados pessoais de seus cidadãos. No Brasil, essa iniciativa toma a forma da Lei Geral de Proteção de Dados. Em conjunto com as novas legislações, diversos *frameworks* de gestão e governança de TI começaram a apresentar novas práticas e soluções com o objetivo de aumentar a segurança dos dados dos usuários. Esse trabalho teve como objetivo estudar os *frameworks* ITIL e COBIT e realizar uma análise comparativa entre suas recomendações de políticas de segurança com as normas requisitadas pela LGPD. Por fim, foi possível concluir que os *frameworks* analisados formam uma base sólida para a adequação à LGPD.

Palavras-chave: Governança de TI. Lei Geral de Proteção de Dados. ITIL. COBIT

SANTOS. R. H.. **Analysis of IT Governance Frameworks in relation to the LGPD**. 2022. 51p. Final Project (Bachelor of Science in Computer Science) – State University of Londrina, Londrina, 2022.

ABSTRACT

With the increasing importance of technology on everyday life, the worry with personal data privacy stored by companies is also increasing. Following this preoccupation, many government entities around the world started implementing new legislation to normalize and secure the handling of personal data of its citizens. In Brazil, this initiative takes the form of the General Personal Data Protection Law. Together with the new legislations, many IT management and governance frameworks started to work on new policies and solutions with the goal of increasing private personal data of it's users. This project aimed to study the ITIL and COBIT frameworks and analyse their security policy recommendations with the standards required by the LGPD. Finally, it was possible to conclude that the analyzed frameworks form a solid basis for compliance with the LGPD.

Keywords: IT Governance. General Personal Data Protection Law. ITIL. COBIT.

LISTA DE ILUSTRAÇÕES

Figura 1 – Modelo de Quatro Dimensões[1] 20
Figura 2 – Sistema de Valor de Serviço[1] 21
Figura 3 – Cadeia de Valor de Serviço[1] 22
Figura 4 – Modelo Essencial do COBIT[2] 28
Figura 5 – Princípios do Sistema de Governança[2] 28
Figura 6 – Princípios do *Framework* de Governança[2] 29
Figura 7 – Componentes de um sistema de governança[3] 30

LISTA DE TABELAS

Tabela 1 – Requerimentos da LGPD 42
Tabela 2 – Relação entre as práticas e princípios do ITIL 4 com os requerimentos da LGPD 49
Tabela 3 – Relação entre os objetivos do COBIT 2019 com os requerimentos da LGPD 51

LISTA DE ABREVIATURAS E SIGLAS

TI	Tecnologia da Informação
GDPR	*General Data Protection Regulation*
ITIL	*Information Technology Infrastructure Library*
COBIT	*Control Objectives for Information and Related Technologies*
LGPD	Lei Geral de Proteção de Dados
ANPD	Agência Nacional de Proteção de Dados
IP	Internet Protocol
SVS	Sistema de Valor de Serviço
EDM	*Evaluate, Direct and Monitor*
APO	*Align, Plan and Organize*
BAI	*Build, Acquire and Implement*
DSS	*Deliver, Service and Support*
MEA	*Monitor, Evaluate and Assess*

SUMÁRIO

1 INTRODUÇÃO 14

2 FUNDAMENTAÇÃO TEÓRICO-METODOLÓGICA E ESTADO DA ARTE 15

2.1 Lei Geral de Proteção de Dados 15

2.1.1 Definições 15

2.1.1.1 Definições sobre dados 16

2.1.1.2 Definiçoes sobre agentes responsaveis 16

2.1.1.3 Outras definições 17

2.1.2 Princípios 17

2.1.3 Direitos do titular 18

2.1.4 Requerimentos do Controlador 18

2.2 Information Technology Infrastructure Library (ITIL) 19

2.2.1 Modelo de Quatro Dimensões 20

2.2.2 Sistema de Valor de Serviço 21

2.2.2.1 Oportunidade e Demanda 21

2.2.2.2 Princípios Orientadores 21

2.2.2.3 Governança 22

2.2.2.4 Cadeia de Valor de Serviço 22

2.2.2.5 Melhoria Contínua 23

2.2.3 Práticas 23

2.2.3.1 Práticas gerais de gerenciamento 23

2.2.3.2 Práticas de gerenciamento de serviços 25

2.2.3.3 Práticas de gerenciamento técnico 26

2.3 Controle de Objetivos para a Informação e Tecnologia Relacionadas 27

2.3.1 Princípios 27

2.3.1.1 Princípios do Sistema de Governança 27

2.3.1.2 Princípios do *Framework* de Governança 29

2.3.2 Componentes 29

2.3.3 Objetivos de Gerenciamento e Governança 30

2.3.3.1 *Evaluate, Direct and Monitor* (EDM) 31

2.3.3.2 *Align, Plan and Organize* (APO) 31

2.3.3.3 *Build, Acquire and Implement* (BAI) 33

2.3.3.4 *Deliver, Service and Support* (DSS) 34

2.3.3.5 *Monitor, Evaluate and Assess* (MEA) 35

2.4 Trabalhos Relacionados 36

3 PROCEDIMENTOS METODOLÓGICOS 37
3.1 Requerimentos da LGPD 37

4 ESTUDO COMPARATIVO 39
4.1 Consentimento do uso de dados pessoais 39
4.2 Necessidade do uso de dados pessoais 39
4.3 Transparência do uso dados pessoais 39
4.4 Controle dados pessoais 40
4.5 Canal de comunicação com o titular 40
4.6 Gerenciamento de terceiros 40
4.7 Prevenção de incidentes 40
4.8 Respostas à incidentes 41
4.9 Relatórios organizacionais 41
4.10 Encarregado do uso de dados 41
4.11 Tabela 42

5 CONCLUSÃO 43

REFERÊNCIAS 45

APÊNDICES 47

APÊNDICE A – PRÁTICAS E PRINCÍPIOS DO ITIL 4 EM RELAÇÃO AOS REQUERIMENTOS DA LGPD 48

APÊNDICE B – OBJETIVOS DO COBIT 2019 EM RELAÇÃO AOS REQUERIMENTOS DA LGPD 50

1 INTRODUÇÃO

Nas últimas décadas, a presença da tecnologia na vida cotidiana do cidadão brasileiro se torna cada vez mais indispensável. Enquanto a presença da tecnologia traz diversos benefícios para o cidadão privado, a dependência de dispositivos e serviços tecnológicos permite que empresas tenham acessos a diversos dados pessoais de seus usuários. Desde dados cadastrais, como nome e endereço, até dados materiais, como localização e batimento cardíaco, empresas de tecnologia armazenam informações pessoais de seus usuários para utilização de suas funções, ou até para a venda desses dados para empresas terceiras.

Por esses fatores, a demanda por mais segurança desses dados por parte de usuários se torna cada vez maior. Seguindo a necessidade de regulamentação no tratamento de dados pessoais, em 2016, na União Europeia, foi sancionada a *GDPR* (Regulamento Geral sobre a Proteção de Dados)[4]. Esse regulamento visa regimentar o tratamento de dados de cidadãos europeus, além dos direitos de privacidade dos usuários.

Seguindo o exemplo da União Europeia[4], em 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD)[5], entrando em vigor propriamente em 2020. Essa lei segue o caminho da *GDPR* e visa proteger os dados pessoais dos cidadãos brasileiros, criando normas para a captação e armazenamento de dados de seus usuários.

Enquanto a nova lei propõe diversas mudanças para empresas, apenas 40% das empresas declaravam estar preparadas às novas normas da LGPD no momento em que entrou em vigor.[6] O não comprimento das diretrizes podem acarretar em multas para as empresas envolvidas.

Em contrapartida, diversos *frameworks* de governança de TI trazem recomendações de boas práticas e metodologias na gestão de empresas, à fim de otimizar os sistemas organizacionais. Dois desses *frameworks* são o ITIL[1] e o COBIT[7]. Com as novas demandas globais por segurança e privacidade, esses *frameworks* possuem novas regras para aumentar a segurança dos dados da empresa.

Por fim, o objetivo desse trabalho será um estudo dos requisitos apresentados pela LGPD, e comparar com as práticas recomendadas pelo ITIL e COBIT. Será verificado as práticas que satisfazem os requisitos da LGPD, além dos requisitos que não são atendidos pelos *frameworks*.

O capítulo 2 traz a fundamentação teórica necessária para entender o trabalho, falando da LGPD, ITIL e COBIT. Na seção 3, são apresentados trabalhos correlatos, seguido do capítulo 4, onde a metodologia é explicada. No capítulo 5 é apresentado o estudo comparativo entre os requerimentos da LGPD e os processos apresentados pelos *frameworks* de gorvernança. Por fim, na seção 6, é apresentado a conclusão do trabalho.

2 FUNDAMENTAÇÃO TEÓRICO-METODOLÓGICA E ESTADO DA ARTE

Nesta seção serão descritos conceitos e ferramentas necessárias para o desenvolvimento deste trabalho. Primeiramente, será abordada a Lei Geral de Proteção de Dados a fim de melhor entender sua estrutura e seus requerimentos. Em seguida, os *frameworks* ITIL e COBIT são detalhados, apresentando sua estrutura e, principalmente, suas diretrizes e práticas recomendadas a fim de serem comparadas com o requerimentos da LGPD no final deste trabalho.

2.1 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709), é uma lei aprovada em 14 de agosto de 2018 que entrou propriamente em vigor em 2020, que tem como objetivo a definição de obrigações e normas sobre o tratamento de dados pessoais, tanto de pessoa natural quanto de pessoa jurídica, pública ou privada. Essa lei tem como objetivo seguir os padrões de privacidade internacionais estabelecidos em diversos países e regiões, como por exemplo a GDPR, instituída na União Europeia[8].

Sob essa lei, todo cidadão brasileiro, estando em território nacional ou estrangeiro, tem a titularidade de seus dados pessoais. Em contrapartida, quaisquer entidades que utilizem devem seguir diversas diretrizes para garantir os direitos dos titulares dos dados que utilizam[8].

A fiscalização da lei é realizada por uma Autoridade Nacional, que pode aplicar sanções e punições, como advertências, multas e até o bloqueio e remoção dos dados pessoais afetados[9].

A LGPD frequentemente se refere à uma Autoridade Nacional. A fim de efetuar essa função, foi criada a Agência Nacional de Proteção de Dados (ANPD)[9]. A ANPD é a instituição pública responsável por fiscalizar o cumprimento da LGPD por outras entidades, e caso necessário, advertir e penalizar os agentes que infringentes. A organização também é responsável por orientar o cumprimento da lei, divulgando informações e solucionando dúvidas sobre a lei.

2.1.1 Definições

Durante a criação da lei, 19 definições foram estabelecidas. Essas definições podem ser melhor organizadas em três categorias gerais[5]:

2.1.1.1 Definições sobre dados

Definições sobre dados manipulados por qualquer entidade:

- **Dado pessoal**: Dados pessoais podem ser definidos como qualquer tipo de informação pessoal que possa ser utilizado para identificar uma pessoa, tal como números de documentos, nome, endereço de e-mail e endereço IP;
- **Dado pessoal sensível**: Dados pessoais que, enquanto não identificadores por si, representam informações privadas de um indivíduo. Por exemplo, dados de origem étnica, religiosa e política. Além de dados relacionados a saúde, vida sexual ou genética de uma pessoa natural;
- **Dado anonimizado**: Dados anonimizados são referentes à dados de um indivíduo que não permitem a identificação de seu titular. Por exemplo, altura, cor dos olhos e idade;
- **Banco de dados**: Base estruturada de dados pessoais. Podendo ser física ou eletrônica, organizado de maneira centralizada ou distribuída;

2.1.1.2 Definiçoes sobre agentes responsaveis

As seguintes definições são relacionadas à agentes e entidades tratados na lei.

- **Titular**: Pessoa física sobre o qual os dados pessoais se referem.
- **Controlador**: Controlador se refere à entidade responsável pelas decisões sobre o tratamento dos dados pessoais. Pode tomar a forma de pessoa física ou jurídica, de direito público ou privado;
- **Operador**: Entidade responsável pela realização do tratamento de dados pessoais em nome do Controlador. Também pode tomar a forma de pessoa física ou jurídica, de direito público ou privado;
- **Encarregado**: Pessoa física, apontada pelo controlador, encarregada de manter um canal de comunicação entre o Controlador, os Titulares e a Autoridade nacional;
- **Autoridade Nacional**: Instituição pública responsável pela implantação e fiscalização da LGPD. Esse órgão nacional é Agência Nacional de Proteção Dados;
- **Órgão de pesquisa**: Instituição pública ou privada sem fins lucrativos com objetivo de realizar pesquisas básicas ou de caráter histórico, científico, tecnológico ou estatístico;
- **Agentes de tratamento**: Se referem ao Controlador e ao Operador;

2.1.1.3 Outras definições

Outras definições criadas para a lei.

- **Tratamento**: Tratamento se refere à qualquer operação realizada sobre dados pessoais. Por exemplo, coleta, produção, classificação, reprodução, distribuição, armazenamento, avaliação, entre outros;
- **Anonimização**: Utilização de técnicas a fim de dissociar dados pessoais do titular, tornando-o em Dados Anonimizados;
- **Consentimento**: Declaração explícita e informada pelo titular a fim de concordar com o tratamento de seus dados pessoais;
- **Bloqueio**: Cancelamento de qualquer procedimento de tratamento de dados pessoais;
- **Eliminação**: Remoção de dados pessoais armazenados em um Banco de Dados;
- **Transferência internacional de dados**: Transferência de dados pessoais armazenados no Brasil para um país estrangeiro;
- **Uso compartilhado de dados**: Tratamento de Dados Pessoais por múltiplas entidades públicas, ou com entidades privadas, com autorização específica das partes relacionadas;
- **Relatório de impacto à proteção de dados pessoais**: Documentação gerada pelo controlador descrevendo os processos de tratamento de dados pessoais;

2.1.2 Princípios

Além de partir do preceito da boa-fé, a lei também posiciona que o tratamento de dados deve-se observar os seguintes princípios[5]:

- **Finalidade**: Todo tratamento de dados pessoais dever ser legítimo, específico e informado ao titular;
- **Adequação**: A finalidade do tratamento deve permanecer a mesma que foi informada ao titular;
- **Necessidade**: O tratamento de dados pessoais deve abranger apenas o necessário para a sua finalidade;
- **Livre acesso**: Deve ser garantido ao titular, de maneira facilitada e gratuita, a habilidade de verificar informações a respeito do tratamento e integridade de seus dados pessoais;

- **Qualidade de dados**: O titular deve ser garantido de que seus dados pessoais são autênticos e atualizados;
- **Transparência**: O titular deve ter acesso às informações sobre o tratamento de seus dados pessoais de maneira clara e precisa;
- **segurança**: O controlador deve utilizar ferramentas e métodos adequados a fim de manter a segurança de dados pessoais;
- **prevenção**: O controlador deve adotar medidas a fim de prevenir eventuais perdas, destruição ou alterações acidentais de dados pessoais;
- **não discriminação**: O controlador não deve utilizar dados pessoais para fins discriminatórios ilícitos ou abusivos;
- **responsabilização e prestação de contas**: Os agentes devem comprovar a utilização de medidas eficazes para o cumprimento da lei;

2.1.3 Direitos do titular

A lei aborda primeiramente o direito à privacidade do titular, dispondo diversos direitos que devem ser obrigatoriamente oferecidos pelo controlador. A seguinte lista resume esses direitos[5]:

- **Consentimento**: Os dados do titular só podem ser capturados e tratados com seu consentimento explícito. O titular também possui o direito de revogar seu consentimento a qualquer momento;
- **Informação de Compartilhamento**: O titular deve ser informado sobre qualquer tipo de compartilhamento de seus dados pessoais com outras entidades;
- **Acesso**: O titular tem direito acessar seus dados de uma maneira simples e gratuita. Esse direito se estende para a modificação e exclusão de seus dados pessoais;
- **Segurança e Integridade**: O titular deve ter garantia de que seus dados pessoais são mantidos de forma segura e de que nenhuma modificação indevida pode acontecer;
- **Contato**: O titular tem direito de obter as informações de contato do titular;

2.1.4 Requerimentos do Controlador

A fim de assegurar os direitos do titular, o controlador é responsável em garantir que diversos requerimentos sejam cumpridos[5]:

- **Consentimento**: O controlador deve possuir o consentimento explícito do titular para a utilização de seus dados pessoais. O controlador deve declarar o proposito exato da captação dos dados pessoais.;
- **Necessidade**: Apenas os dados pessoais necessários para devem ser registrados;
- **Transparência**: O controlador deve garantir fácil acesso dos dados do titular e informações de seu tratamento e compartilhamento;
- **Segurança**: O controlador deve garantir a segurança e integridade dos dados do titular;
- **Prevenção**: O controlador deve seguir medidas de prevenção para a segurança dos dados pessoais do titular;
- **Encarregado**: O controlador deve apontar um encarregado para garantir a comunicação com outras entidades;

2.2 Information Technology Infrastructure Library (ITIL)

O ITIL (*Information Technology Infrastructure Library*, ou Biblioteca de Infraestrutura de Tecnologia da Informação), é uma metodologia que oferece um conjunto de boas práticas para a gestão de servições de tecnologia da informação[10].

A biblioteca de práticas ofertada pelo ITIL tem como objetivo melhorar a efetividade dos processos de uma organização, aumentando a produtividade, melhorando a experiência dos clientes e elevando o nível de confiança e segurança da empresa[11].

A estrutura do modelo de gerenciamento apresentado pelo ITIL possui 2 principais componentes[10]: O modelo de de quatro dimensões e o Sistema de valor de serviço. Esses dois modelos são essenciais para entender como os processos de gestão apresentado pelo ITIL funciona.

O modelo de quatro dimensões[10] tem o papel de auxiliar a companhia a melhor entender os componentes que compõe a organização, abstraindo estes elementos para uma melhor análise de seu conteúdo e relacionamento. O sistema de valor de serviço oferece uma visão panorâmica do sistema de gerenciamento de serviços da organização, descrevendo os processos organizacionais a fim de melhor entender o fluxo de valor da empresa.

Como parte do sistema de valor de serviço[1], são apresentadas 34 práticas de governança para auxiliar a organização a atingir seus objetivos. Essas práticas não são regras estritas, mas instruções e diretrizes flexíveis garantir que as modificações sejam feitas sob medida para as necessidades da organização.

2.2.1 Modelo de Quatro Dimensões

O *framework* descreve quatro dimensões fundamentais no gerenciamento de uma organização quando buscando produzir um serviço de qualidade e gerar valor efetivo para todas as partes interessadas. Esse modelo é aplicado ao Sistema de Valor de Serviço e possuem os seguintes elementos[1]:

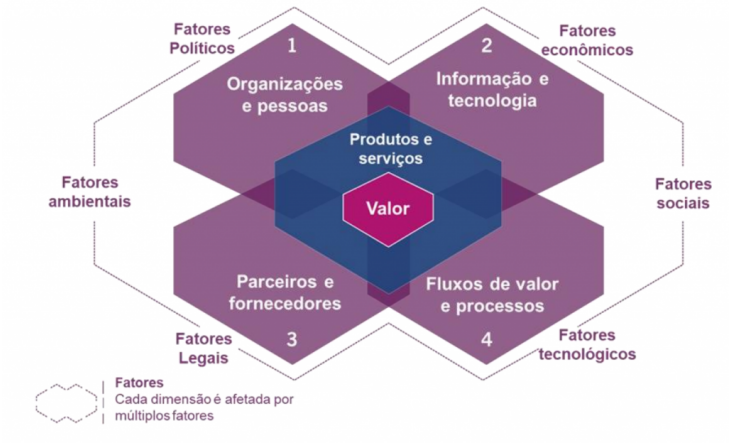

Figura 1 – Modelo de Quatro Dimensões[1]

Organizações e pessoas: Refere-se ao aspecto humano da instituição. Essa dimensão considera não apenas os membros do time, mas como ele é gerenciado, seu nível de competência técnica, qualidade da comunicação entre seus membros e até mesmo a cultura da organização;

Informação e tecnologia: Essa dimensão lida com as tecnologias e ferramentas utilizadas pela organização e como são empregadas no suporte do serviço. Devem ser analisadas as tecnologias que compõe o serviço e quais informações são necessárias para manter e melhorar o serviço, incluindo ferramentas analíticas, bases de conhecimento e sistemas de comunicação;

Parceiros e fornecedores: Dimensão que explora os relacionamentos com outras organizações e entidades. Devem ser analisados os serviços prestados por outras entidades, seu custo, eficiência e necessidade para o desempenhar do serviço;

Fluxo de valor e processos: Esta dimensão abrande os processos, procedimentos e atividades necessários para a efetuação do serviço em questão. Também é examinado como os elementos da organização interagem para a geração dos produtos;

Além das quatro dimensões descritas, a organização também deve estar ciente de de diversos fatores internos e externos que podem influenciar como as dimensões são operadas. Essa análise serve para para adequar o modelo para os contextos específicos de cada organização.

2.2.2 Sistema de Valor de Serviço

Sistema de Valor de Serviço (SVS) é uma análise geral dos diversos elementos necessários para a administração de uma organização eficiente e efetiva em seus valores e objetivos. O sistema pode ser visualizado na figura 2 e é explicado em detalhe nas próximas seções[1].

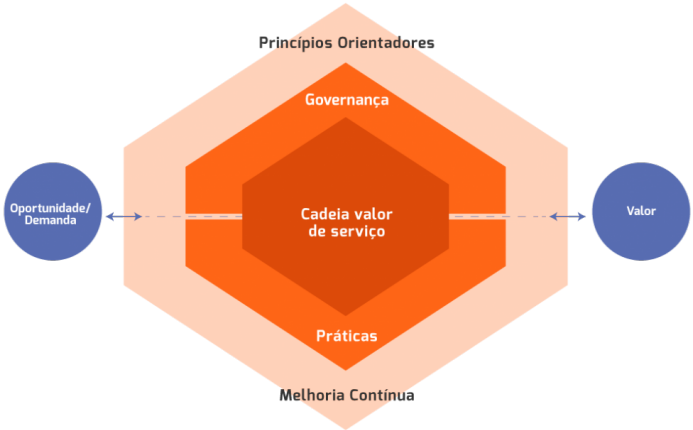

Figura 2 – Sistema de Valor de Serviço[1]

2.2.2.1 Oportunidade e Demanda

Representa o potencia da criação de valor ou a necessidade do serviço ou produto. A demanda pode ser gerada da necessidade por um produto, mas também pode tomar a forma de informações ou de resposta à uma falha interna ou externa.

2.2.2.2 Princípios Orientadores

Esses princípios orientadores são as sete principais recomendações do ITIL 4, eles sevem para orientar a organização em qualquer situação independente de seus objetivos[12].

- **Foco no valor**: As ações da organização devem estar focadas em gerar valor para si, seus clientes e todas as partes interessadas;
- **Comece onde você está**: A organização deve analisar métodos e soluções já existentes na própria organização ou no mercado antes de criar ou implementar algo novo. Utilizar ferramentas disponíveis ajuda a agilizar a produção do serviço e consequentemente otimiza a geração de valor;
- **Progrida iterativamente e com *feedback***:Tarefas complexas devem ser divididas em passos menores. Esta tratativa refina o gerenciamento dos requerimentos e melhora o entendimento do processo por todas as partes responsáveis;

- **Colabore e promova visibilidade**: A organização deve se dedicar à comunicação transparente com todas as partes envolvidas. A melhor colaboração torna o processo de criação do serviço mais confiável e informado quando todas as partes estão colaborando de forma aberta;
- **Pense e trabalhe holisticamente**: Todos os elementos da organização trabalhão em conjunto para um objetivo final. As ações de uma organização devem ser analisadas em relação à todos os outros elementos e como esses serão afetados;
- **Mantenha-se simples e prático**: Processos devem ser simplificados e otimizados de maneira a diminuir sua complexidade. Ações e atividades desnecessárias devem ser eliminadas a fim de atingir os objetivos da maneira mais eficiente possível;
- **Otimize e automatize**: Intervenção humana deve acontecer apenas quando pode gerar valor. A organização deve dispor-se a otimizar seus processos e a automatizar tarefas repetitivas de maneira que seus funcionários foquem em ações construtivas;

2.2.2.3 Governança

Técnicas de governança se referem aos indivíduos ou grupo de indivíduos que administram a organização[1]. Essas pessoas possuem a responsabilidade de monitorar, avaliar e gerir os setores da empresa e garantir que estes estão avançando os objetivos de negócio da organização de maneira eficiente. Para organizações muito grandes, não é viável alocar todas as decisões de governança para seus diretores, logo é comum que as responsabilidades sejam divididas entre os vários setores da organização.

2.2.2.4 Cadeia de Valor de Serviço

A cadeia de valor de serviço são uma combinação de seis práticas de gestão que, em conjunto, operam de maneira a gerar valor através da entrega do produto final[1].

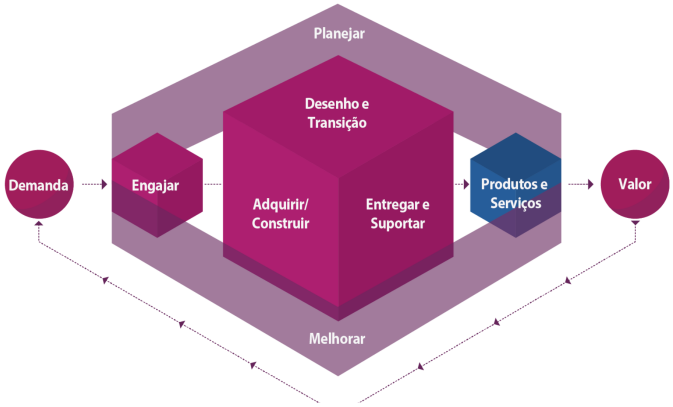

Figura 3 – Cadeia de Valor de Serviço[1]

- **Planejar**: Definição de planos, processos e ações necessárias para o desenvolvimento do produto ou serviço;
- **Melhorar**: Assegurar a melhoria contínua dos processos e técnicas em todos os níveis da organização;
- **Engajar**: Garantir a boa comunicação e transparência entre todas as partes interessadas;
- **Desenho e Transição**: Garantia que produtos e serviços produzidos continuem a atender as partes interessadas mesmo após a fase de planejamento;
- **Adquirir e Construir**: Garantia que os componentes necessários estejam disponíveis para o desenvolvimento do produto, e que estes estejam em condições estabelecidas;
- **Entregar e Suportar**: Garantia que o produto seja entregue da maneira esperada para as partes envolvidas, oferecendo ajuda e informações se necessário;

2.2.2.5 Melhoria Contínua

O conceito de melhoria deve ser aplicado de maneira que todos os elementos da organização sejam encorajados melhorar a qualidade do serviço ou produto, buscando oportunidades e colaborando a fim de gerar mais valor. Esta mentalidade deve incentivada em todos os setores da organização, desde os funcionários, gestores, diretores e clientes[1].

2.2.3 Práticas

Práticas, no contexto do ITIL 4, refere-se a um conjunto de recursos organizacionais que promovem os valores da organização. Práticas não são processos definidos, mas apresentam procedimentos flexíveis a fim de atender a demanda de diversos tipos de organizações. 34 práticas são apresentadas pelo ITIL 4, sendo divididas em 3 categorias distintas: Práticas gerais de gerenciamento, Práticas de gerenciamento de serviços, Práticas de gerenciamento técnico. Essas práticas são descritas em seguida[1]:

2.2.3.1 Práticas gerais de gerenciamento

- **Gerenciamento de arquitetura**: Prática que tem como objetivo fornecer uma compreensão dos diferentes elementos que compõe a organização, e como esses elementos se relacionam;
- **Melhoria contínua**: Práticas é melhorar a capacidade da organização de continuar atendendo suas necessidades de negócio em constante mudança, garantindo que produtos, serviços e práticas continuem evoluindo com a organização;

- **Gerenciamento de segurança da informação**: Pŕaticas de segurança que visão proteger informações sigilosas da organização. Aborda o gerenciamento de confiabilidade e integridade das informações, além de questões de autenticação e não repúdio;
- **Gestão do conhecimento**: Práticas de gestão de conhecimento propõem-se em melhorar a eficácia e conveniência do acesso à informação e conhecimento em toda a organização;
- **Medições e relatórios**: Práticas de coleta e avaliação de vários dados relevantes da organização. O objetivo dessas práticas é auxiliar na tomada de decisões e na melhoria contínua da organização;
- **Gerenciamento de mudanças organizacionais**: Práticas que tem com propósito auxiliar em mudanças organizacionais e implementação de novos processos internos;
- **Gerenciamento de portfólio**: O objetivo da prática de gerenciamento de portfólios é auxiliar no garantir a proporção correta de produtos, serviços e programas a fim de alcançar seus objetivos organizacionais;
- **Gerenciamento de projetos**: A prática apresenta técnicas para o planejamento, monitoramento e controle de diversos aspectos de um projeto, garantindo que o projeto seja entregue de maneira satisfatória;
- **Gestão de relacionamento**: Estabelece estratégias para a identificação, análise e melhoria das relações entre a organização e quaisquer partes interessadas;
- **Gestão de riscos**: Prática central de todas as atividades de uma organização, a gestão de risco garante que a empresa entenda e lide com riscos de forma eficiente;
- **Gerenciamento financeiro de serviços**: Práticas para o gerenciamento eficaz dos recursos e investimentos financeiros da organização.;
- **Gestão da estratégia**: Práticas com o objetivo de auxiliar a organização na definição de objetivos e planos de ação. A prática ajuda a esclarecer prioridades e orienta a tomada de direção informada;
- **Gestão de fornecedores**: Prática que auxilia na organização e análise de desempenho de fornecedores. As práticas também menciona a criação e melhoria do relacionamento com fornecedores a fim de aprimorar a comunicação e reduzir o risco de falhas;
- **Força de trabalho e gestão de talentos**: Práticas focadas em melhorar a qualidade da força humana da organização. Contendo processos de planejamento, recrutamento, integração, aprendizado e desenvolvimento dos funcionários;

2.2.3.2 Práticas de gerenciamento de serviços

- **Gerenciamento de disponibilidade**: Práticas que tem com objetivo garantir a disponibilidade dos serviços à clientes e usuários;
- **Análise de negócios**: Prática que auxilia a análise do negócio em geral ou apenas parte dele, identificando problemas e necessidades e recomendando soluções a fim de facilita a geração de valor para as partes interessadas;
- **Gerenciamento de capacidade e desempenho**: Práticas que garante o desempenho esperado de serviços ofertados pela organização de maneira efetiva;
- **Controle de mudanças**: Prática que tem como objetivo reduzir os riscos inerentes à aplicação de mudanças no serviço ou produto, maximizando o número de mudanças bem sucedidas;
- **Gerenciamento de incidentes**: Práticas que auxiliam no tratamento de incidentes, reduzindo efeitos negativos e restaurando a normalidade das operação de maneira rápida e eficiente;
- **Gerenciamento de ativos de TI**: Práticas que auxiliam no gerenciamento do ciclo de vida de todos os ativos de TI, analisando a compra, custo, risco e remoção de ativos não eficientes;
- **Monitoramento e gerenciamento de eventos**: Prática que auxilia no gerenciamento de eventos, registrando estados dos serviços e detectando alterações. A coleta dessas informações é utilizada para providenciar respostas adequadas a esses eventos e detectando condições que podem levar a falhas e incidentes;
- **Gerenciamento de problemas**: Prática que tem como objetivo a redução do impacto de incidentes, criando sistemas de gerenciamentos a fim de identificar possíveis causas e adotar soluções;
- **Gerenciamento de versão**: Práticas que garantem a eficácia na disponibilização de novos servições ou recursos alterados;
- **Gerenciamento do catálogo de serviços**: Prática que garante o fornecimento de informações consistentes e atualizados dos serviços e produtos da organização para as partes interessadas;
- **Gerenciamento de configuração de serviço**: Prática que garante a disponibilidade de informações sobre a configuração do serviço e os itens de configuração que os suportam, incluindo informação do relacionamento entre eles ;

- **Gerenciamento de continuidade de serviço**: Práticas para garantir a disponibilidade e desempenho de um serviço mesmo em caso de falhas. A prática cita processos para aprimorar a habilidade de resposta efetiva, os interesses das partes interessadas;

- **Design de serviço**: Prática que tem como objetivo garantir que produtos e serviços gerados pela organização sejam adequados, tanto ao seu propósito quando a capacidade da organização de produzi-lo de maneira adequada;

- ***Service Desk***: Práticas que viabilizam o contato entre a organização e os utilizadores de seus serviços. Essas práticas auxiliam na captura de demanda e solicitações de serviços, além de auxiliar na resolução de incidentes;

- **Gerenciamento de nível de serviço**: Práticas que garantem um nível mínimo de qualidade dos serviços ofertados, gerenciando e monitorando seu desenvolvimento e funcionamento em relação a metas definidas;

- **Gerenciamento de solicitações de serviço**: Práticas que auxiliam a conservação da qualidade de um serviço, tratando solicitações de serviços advindas do usuário de maneira amigável e eficiente;

- **Validação e teste de serviço**: Técnicas que visam avaliar o nível de qualidade de serviços novos ou alterados, utilizando indicadores mensuráveis de qualidade e desenpenho ;

2.2.3.3 Práticas de gerenciamento técnico

- **Gerenciamento de implantação**: Práticas lidando com a implantação de componentes de *software* ou *hardware*, novos ou modificados, em um ambiente ativo;

- **Gerenciamento de infraestrutura e plataforma**: Práticas lidando com o gerenciamento da infraestrutura da organização. Estas práticas abrangem não somente o monitoramento eficiente dos processos da organização, mas também de prestadores de serviços externos;

- **Desenvolvimento e gerenciamento de software**: Práticas abordando o processo de desenvolvimento de *software*, atendendo as necessidades de todas as partes interessadas em termo de utilidade, funcionalidade, confiabilidade e auditabilidade;

2.3 Controle de Objetivos para a Informação e Tecnologia Relacionadas

COBIT (*Control Objectives for Information and Related Technologies*, ou Controle de Objetivos para a Informação e Tecnologia Relacionadas) é um *framework* de gerenciamento e governança corporativa de TI.

O *framework* visa aplicar diversas práticas de controle na estrutura da organização, indo desde o planejamento de novos serviços até o monitoramento de resultados, à fim de promover os objetivos da empresa[13]. As melhorias propostas pelo COBIT vão desde aumento da eficiência dos serviços de TI, melhoria na segurança e otimização dos investimentos na área de tecnologia da empresa. Em 2019, uma nova versão do COBIT foi lançada, o COBIT 2019, que trás foco em novas práticas de segurança de TI, seguindo a atual preocupação da indústria de tecnologia[7].

Portando diversos elementos, o COBIT apresenta 3 principais componentes de sua estrutura[3]: Princípios, Componentes e Objetivos. Os princípios orientadores são conceitos importantes para a criação e manutenção dos sistemas de gerenciamento, esses princípios são sempre relevantes, não importando a atividade ou setor empresarial. Por sua vez, os componentes correspondem à todos os elementos da organização e como estes interagem entre si, oferecendo uma visão holística de toda a organização.

Por fim, o COBIT oferece 40 objetivos divididos em 5 domínios distintos, também conhecido como o Modelo Essencial do COBIT[2], a fim de guiar organizações em seus objetivos. Os objetivos não são regras absolutas, mas metas organizacionais que a empresa deve buscar alcançar. A fim de alcançar cada objetivo, são apresentados diversos procedimentos, métricas e sub-objetivos para que a organização elabore um sistema de gerenciamento que melhor se encaixa com seus objetivos e metas.

2.3.1 Princípios

Os princípios apresentados pelo COBIT são divididos em duas categorias: Princípios do sistema de governança e Princípios do *framework* de governança.

2.3.1.1 Princípios do Sistema de Governança

O COBIT 2019 define 6 princípios do sistema de governança de uma organização. Esses princípios são necessários para melhor entender as necessidades e objetivos das partes interessadas, auxiliando no estabelecimento de uma direção clara e na tomada informada de decisões. Esses princípios são descritos a seguir[3]:

Proporcionar valor às partes interessadas: A organização deve equilibrar recursos, riscos e benefícios a fim de satisfazer as necessidades das partes interessadas e

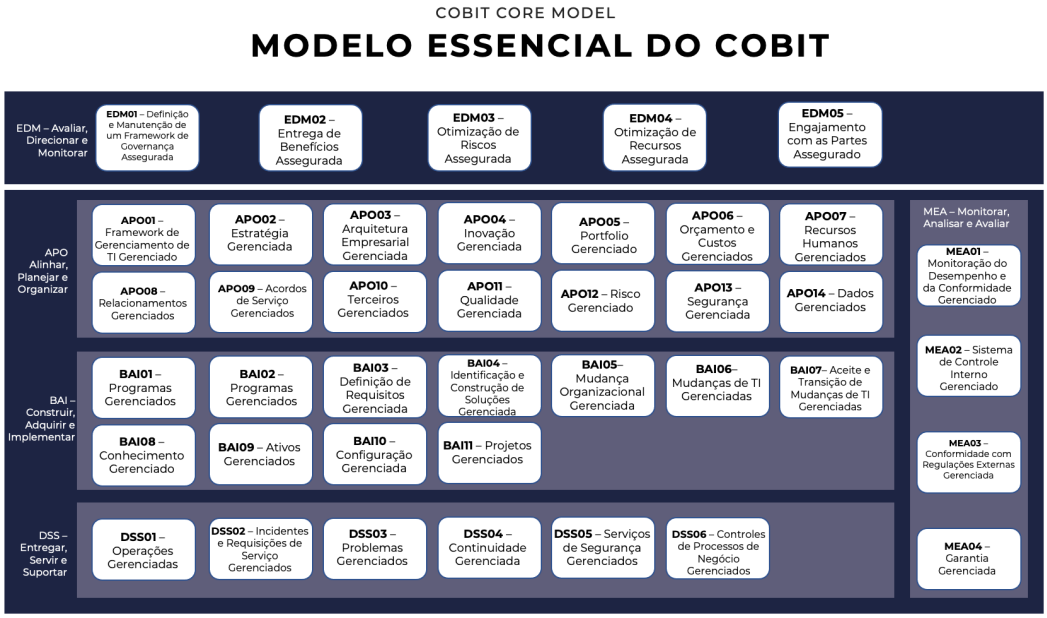

Figura 4 – Modelo Essencial do COBIT[2]

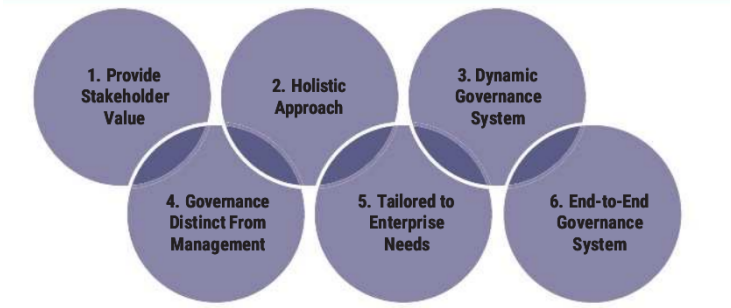

Figura 5 – Princípios do Sistema de Governança[2]

efetivamente gerar valor;

Abordagem holística: Um sistema de governança deve ser analisado de maneira holística, visto que a organização é composta de diversos tipos de componentes interagindo entre si;

Sistema de governança dinâmico: O sistema de analisar o impacto de possíveis mudanças a fim garantir o processo de evolução da organização ;

Governança separada da administração: O sistema de governança deve distinguir claramente as atividades de gestão e de governança da organização;

Moldado para as necessidades empresariais: Para a criação de um sistema de governança os padrões de projeto devem ser modificados e priorizados a fim de gerar um sistema moldado para as necessidades específicas da organização;

Sistema de governança de ponta a ponta: O sistema de governança deve

cobrir todas as áreas da organização, não apenas a área de TI;

2.3.1.2 Princípios do *Framework* de Governança

Os princípios do *framework* de governança estão relacionados à área estrutural da organização. Esses princípios pretendem guiar a organização à manter uma arquitetura clara, flexível a atualizada a fim de garantir os objetivos corporativos[3].

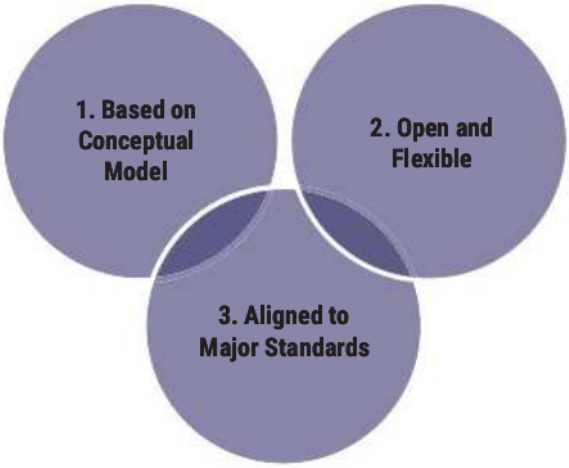

Figura 6 – Princípios do *Framework* de Governança[2]

Baseado em um modelo conceitual: A fim de otimizar a consistência e facilitar a automação, o *framework* de governança deve se basear em uma modelo conceitual, determinando os principais componenters e seu relacionamento;

Aberto e flexível: A estrutura de governança deve admitir a adição de novos componentes e ser capaz de lidar com novos problemas de maneira consistente e flexível;

Alinhado aos principais padrões: A estrutura de governança deve se alinhar aos principais padrões atuais, também levando em conta os regulamentos atuais;

2.3.2 Componentes

Para o COBIT, componentes são fatores que, individualmente ou coletivamente, influenciam o funcionamento da organização. Componentes podem tomar diversos aspectos, porém, independente da forma, todos os componentes interagem entre si, necessitando que sua compreensão seja feita a partir de uma visão holística do sistema de gerenciamento. O bom entendimento dos componentes é necessário para a criação de um sistema de gerenciamento eficiente, a fim de adaptar e sustentar uma arquitetura moldada especificamente para a realidade da organização. Os componentes descritos pelo COBIT são[3]:

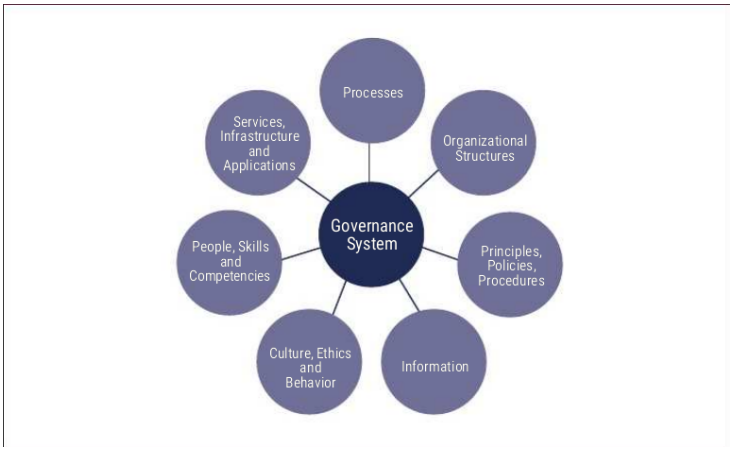

Figura 7 – Componentes de um sistema de governança[3]

Processos: Este componente representa um conjunto de atividades e práticas que, por sua vez, possuem um conjunto de objetivos e resultados esperados;

Estruturas organizacionais: Componente que representa as principais entidades responsáveis pelas tomadas de decisões em organização

Princípios, políticas e *frameworks*: Componente responsável por gerar comportamento e resultado desejado por meio de orientações e programas de gestão;

Informação: Inclui todos os tipos de informações utilizadas ou produzidas pela organização, focando apenas nas informações necessárias para o funcionamento eficiente do sistema de governança;

Cultura, ética e comportamento: Componente importante para boa tomada de decisões, implementações bem sucedidas e ações corretivas;

Pessoas, habilidades e competências: Componente necessário para a entação de atividades e processos de maneira bem sucedida;

Serviços, infraestruturas e aplicações: Componente que inclui a infraestrutura, tecnologias e aplicações de TI da organização;

2.3.3 Objetivos de Gerenciamento e Governança

Para que os objetivos da organização sejam atingidos, um conjunto de objetivos de governança e gerenciamento foram definidos. Todos esses objetivos são relacionados à pelo menos um processo e uma série decomponentes. Cada objetivo é explicado em detalhe, além de apresentar diversos processos que podem ser utilizados a atingir sua finalidade, oferecendo passos, métricas e resultados esperados[2].

Enquanto processos de governança são tipicamente praticados por executivos e diretores, os processos de gerenciamento são responsabilidade da gerência empresaria. Os objetivos de gerenciamento são divididos em 5 domínios, EDM representando os objetivos

da área de governança, e os outros representando os objetivos relacionados ao setor de gestão[2].

2.3.3.1 *Evaluate, Direct and Monitor* (EDM)

Domínio relacionado ao setor de governança contendo propostas de avaliação estratégica, direção do corpo de gestão e monitoramento da a organização a fim de garantir que os objetivos da organização sejam alcançados[2].

- **EDM01 - Garantia de definição e manutenção das estruturas de governança**: Processos para a análise e definição dos requisitos de governança da organização. Apresenta procedimentos para a implementação e manutenção dos elementos de governança, buscando manter a transparência das responsabilidades de todas as partes interessadas;
- **EDM02 - Garantia de entrega de benefícios**: Procedimentos que buscam otimizar a geração de valor em relação aos recursos disponíveis a partir de investimentos em processos, serviços e ativos;
- **EDM03 - Garantia de otimização de riscos**: Procedimentos para a identificação e gerenciamento de risco da organização, focando na compreensão, articulação e comunicação dos requisitos de segurança a fim de manter um nível de risco aceitável para os objetivos da organização;
- **EDM04 - Garantia de otimização de recursos**: Processos para a garantia de disponibilidade de recursos de TI em quantidade suficiente e adequada para suprir os requisitos dos processos e objetivos da organização de maneira efetiva;
- **EDM05 - Garantia de engajamento com as partes interessadas**: Processos que auxiliam a organização a identificar e engajar as partes interessadas, gerando relatórios e métricas mais transparentes a constante comunicação dos objetivos dos procedimentos organizacionais relevantes.;

2.3.3.2 *Align, Plan and Organize* (APO)

Domínio que trata da organização e estratégia das atividades da organização[2].

- **APO01 - Gerenciamento de estruturas de gerenciamento de TI**: Processo que auxilia na arquitetura do sistema de gerenciamento de TI da organização a fim de implementar componentes de gerenciamento direcionados aos objetivos da empresa;

- **APO02 - Gerenciamento de estratégia**: Processos que tem como objetivo orientar o melhor entendimento da organização, oferecendo uma visão holística de todos os seus componentes a fim de melhor definir os objetivos organizacionais e as iniciativas necessárias para atingir esses objetivos da maneira mais efetiva possível ;

- **APO03 - Gerenciamento da arquitetura empresarial**: Processos que auxiliam na modelagem unificada da arquitetura empresarial da organização, descrevendo os principais componentes que a constitui e como esses elementos se relacionam e evoluem. Também são modeladas práticas e processos que alinhem os componentes organizacionais com a estrategia empresarial;

- **APO04 - Gerenciamento de inovação**: Processos que incentivam monitoramento de novas tecnologias e tendências na área de TI com o intuito de identificar proativamente novas oportunidades de inovação;

- **APO05 - Gerenciamento de portfólio**: Processos que tem como objetivo otimizar portfólio de serviços e produtos oferecidos pela organização. Essa otimização é feita a partir de avaliações e métricas sobre o atual portfólio e de potencial demanda, considerando o custo e risco para a decisão de mudanças;

- **APO06 - Gerenciamento de orçamento e custos**: Processos que gerenciam as operações financeiras da organização, oferecendo práticas orçamentárias de priorização de gastos e gestão de custos e benefícios;

- **APO07 - Gerenciamento de recursos humanos**: Processos que auxiliam a avaliação e progresso de recursos humanos da organização ou de terceiros, além de facilitar o processo de recrutamento de novos indivíduos ;

- **APO08 - Gerenciamento de relacionamentos**: Processos que visam gerenciar o relacionamento da organização com todas as partes interessadas, formalizando as interações e garantido uma colaboração aberta e transparente, com todas as partes conscientes das responsabilidades e objetivos mutuo da parceria;

- **APO09 - Gerenciamento de acordos de serviço**: Procedimentos para melhor alinhar os produtos e serviços de tecnologia com as necessidades e expectativas da organização;

- **APO10 - Gerenciamento de terceiros**: Processos para o gerenciamento de serviços e produtos de TI fornecidos por outras organizações e entidades. Esses métodos incluem a busca, seleção, criação e revisão de contrato e monitoramento de desempenho;

- **APO11 - Gerenciamento de qualidade**: Procedimentos que visam a garantia de qualidade em todas as áreas da organização, aplicando técnicas de controle, monitoramento e definição de padrões de qualidade;
- **APO12 - Gerenciamento de risco**: Práticas de identificação, monitoramento e redução contínua de riscos a partir de níveis de tolerância definidos pela organização;
- **APO13 - Gerenciamento de segurança**: Processos que auxiliam da criação, operação e monitoramento de um sistema de gestão de segurança, criando planos de privacidade e tratamento de falhas;
- **APO14 - Gerenciamento de dados**: Procedimentos eficazes de gerenciamento de todos os dados da organização, monitorando todo seu ciclo de vida. Também são apresentados processos de otimização da criação, manutenção, entrega e arquivamento desses dados;

2.3.3.3 *Build, Acquire and Implement* (BAI)

Domínio que aborda o planejamento, implementação e integração de soluções de TI, tanto internas quanto externas[2].

- **BAI01 - Gerenciamento de programas**: Processos para o gerenciamento geral dos programas da organização, coordenando o planejamento, execução e monitoramento de forma eficiente a fim de gerar o valor esperado;
- **BAI02 - Gerenciamento de definições de requisitos**: Procedimentos para a identificação e analise dos requisitos para que a aquisição ou criação de serviços, produtos, processos e informações para que se alinhem aos objetivos estratégicos da empresa. Estes processos auxiliam na comunicação com as partes interessadas a fim de avaliar benefícios e riscos, além de garantir a aprovação de requisitos e soluções;
- **BAI03 - Gerenciamento de identificação e construção de soluções**: Procedimentos que visam o estabelecimento e manutenção de produtos e serviços de acordo com os requisitos da organização, levando em conta o desenvolvimento, aquisição de recursos e colaboração com fornecedores. Este processo abrande o gerenciamento, manutenção e teste de processos, produtos e serviços;
- **BAI04 - Gerenciamento de disponibilidade e capacidade**: Processos voltados à avaliação da disponibilidade de serviços e produtos ofertados pela organização. Estes processos incluem a análise de impact e avaliação de risco em relação à demanda atual e futura a fim de executar efetivamente os objetivos da organização

- **BAI05 - Gerenciamento de mudanças organizacionais**: Procedimentos que tem com objetivo auxiliar o processo de mudanças organizacionais, garantindo uma execução rápida, sustentável e com baixo risco de falhas.;
- **BAI06 - Gerenciamento de mudanças de TI**: Procedimentos relacionados ao processo de mudanças no ambiente de TI, abrangendo manutenções programadas e de emergência. Estes processos incluem a criação de padrões e procedimentos de mudança, avaliação de impacto, autorização e documentação das atividades de mudança;
- **BAI07 - Gerenciamento de aprovações e transições de mudanças de TI**: Processos que lidam com a liberação da implementação de novas soluções na organização. Estes processos incluem o planejamento, aprovação, testes, preparação e avaliação pós implementação das soluções de TI;
- **BAI08 - Gerenciamento de conhecimento**: Processos encarregados de garantir a disponibilidade de todo conhecimento e informação necessárias para a execução das atividades organizacionais de maneira atualizada, confiável e de fácil acesso para as partes interessadas. Estes processos incluem a identificação, coleta organização e manutenção das fontes de conhecimento organizacionais;
- **BAI09 - Gerenciamento de ativos**: Processos que tem com o objetivo gerenciar o ciclo de vida dos ativos de TI da organização, garantindo seu correto funcionamento, confiabilidade e disponibilidade. Estes procedimentos avaliam a necessidade dos ativos, e garantem que estes estarão disponíveis em quantidade e qualidade apropriada conforme os contratos de licença;
- **BAI10 - Gerenciamento de configuração**: Processos que garantem o correto fornecimento de informações sobre os recursos e serviços de TI necessários para o desenvolvimento das atividades da organização. Estes processos incluem a coleta de informação sobre as configurações dos diversos elementos da organização, além da verificação, inspeção e atualização do repositório de configurações;
- **BAI11 - Gerenciamento de projetos**: Processos relacionados ao planejamento, controle e execução de projetos iniciados pela organização, alinhando seu desenvolvimento com os objetivos estratégicos da organização;

2.3.3.4 *Deliver, Service and Support* (DSS)

Domínio que lida com a entrega e suporte dos serviços de TI, levando em consideração a qualidade e segurança[2].

- **DSS01 - Gerenciamento de operações**: Processos relacionados à coordenação e execução de procedimentos operacionais essenciais aos serviços de TI, incluindo operações operacionais predefinidas e atividades de monitoramento;
- **DSS02 - Gerenciamento de requisições e incidentes de serviço**: Processos direcionado à resolução de incidentes e à resposta de solicitações de usuários. Contém práticas para o melhor atendimento das solicitações, além do registro, investigação e diagnóstico dos incidentes;
- **DSS03 - Gerenciamento de problemas**: Processos cujo o objetivo é identificar e classificar problemas e suas causas, apresentar soluções para problemas recorrentes e fornecer recomendações para melhorias nos sistemas da organização;
- **DSS04 - Gerenciamento de continuidade**: Processos destinados à preservação contínua dos processos e recursos da organização. Oferece práticas para a criação de um plano de respostas à incidentes e otimiza a adaptação eficaz à interrupções não planejadas;
- **DSS05 - Gerenciamento de serviços de segurança**: Processos com o objetivo de reduzir o nível de risco de segurança da informação. Para isso, são apresentados métodos para o estabelecimento de funções de segurança da informação e privilégios de acesso, além do monitoramento da segurança da área de TI;
- **DSS06 - Gerenciamento de controles de processos de negócio**: Processos cujo o objetivo é a garantia de satisfação dos requisitos de segurança e controle de todas as informações relacionadas e processadas pelos procedimentos da organização ou terceiros.

2.3.3.5 *Monitor, Evaluate and Assess* (MEA)

Domínio que aborda o controle e monitoramento do nível de performance e conformidade dos objetivos internos e externos da organização[2].

- **MEA01 - Gerenciamento do monitoramento de performance e conformidade**: Processos de coleta, avaliação e validação de métricas organizacionais, apresentando práticas de monitoramento de desempenho de processos e práticas a fim de fornecer relatórios sistemáticos;
- **MEA02 - Gerenciamento do sistema de controle interno**: Processos que visam garantir a identificação de deficiências e ineficiências no controle interno da organização. Auxilia no planejamento, organização, monitoramento e avaliação do ambiente de controle interno, incluindo técnicas de autoavaliação e autoconsciência;

- **MEA03 - Gerenciamento de conformidade com requerimentos externos**: Práticas de avaliação da conformidade dos processos e serviços de TI em relação as leis, regulamentos e requisitos contratuais. Auxilia na identificação e cumprimento dos requisitos e na integração desses no ambiente da organização de maneira prática;
- **MEA04 - Gerenciamento de garantia**: Processes que auxiliam no planejamento, definição e execução de soluções para o cumprimento dos requisitos internos, leis, regulamentos e objetivos estratégicos;

2.4 Trabalhos Relacionados

No artigo [14], o autor realiza uma análise dos componentes da LGPD, citando *frameworks* de governanança, entre eles o COBIT 5 e ITIL 4.

Em [15], a autora aborda os requerimentos da lei Europeia GDPR em relação à diversos modelos de governança incluindo versões do COBT e ITIL.

Uma análise dos padrões apresentados pelo ISO 27001 é comparada com os requisitos da GDPR no artigo [16].

No artigo [17], o autor apresenta um modelo para a adequação à GDPR utulizando os padrões ISO.

Em [18], é apresentado um modelo de negócio que visa cumprir os requerimentos da LGPD.

Contudo, como os *frameworks* não oferecem ações específicas, ainda é necessário a criação de um plano de negócio a fim de garantir o total cumprimento da lei, como apresentado pelo artigo [18].

3 PROCEDIMENTOS METODOLÓGICOS

Para a realização deste trabalho, foi feito inicialmente um estudo sobre a LGPD, analisando suas regras e normas apresentadas pela lei. Em seguida, foi feita uma análise bibliográfica dos *frameworks* de governança ITIL 4 e COBIT 2019, analisando sua estrutura e descrevendo as diretrizes apresentadas por cada um.

Com a base de conhecimento estabelecida, resta a análise comparativa entre os requisitos da LGPD e as diretrizes dos *frameworks* de governança.

Primeiramente, foi definida uma lista de 10 requerimentos essenciais da LGPD (descritos na seção seguinte). Esses requerimentos foram elaborados em base dos requerimentos às organizações e aos direitos do titular descritos na legislação. Enquanto a lei lida com requisitos precisos, os *frameworks* de governança estudados não oferecem processos e atividades específicos, apresentando apenas diretrizes flexíveis que podem ser adotadas pela organização. Por este motivo, a definição dos requisitos leva uma aproximação mais ampla, não focando em ações específicas mas em conceitos gerais a fim de garantir uma comparação justa aos *frameworks* de governança.

Em seguida, cada um destes requerimentos são comparados com as diretrizes de cada *framework*, seguindo as descrições apresentadas nos livros do ITIL[1] e COBIT[2]. Para cada requerimento, cada *framework* é designado uma de 3 categorias:

- **Atende Satisfatoriamente**: O requisito é cumprido de maneira satisfatória, sendo o ponto principal de pelo menos uma diretriz;
- **Atende Parcialmente**: Existem diretrizes que cumprem parte do requisito ou que auxiliam de maneira periférica o possível cumprimento do requisito.;
- **Não Atende**: Não existem diretrizes que lidam direta ou indiretamente com o requisito em questão;

3.1 Requerimentos da LGPD

Nesta seção são listados e descritos os requerimentos da LGPD selecionados para a análise comparativa. Enquanto a LGPD lida com requisitos específicos, os requerimentos apresentados nesta seção representam uma interpretação ampla dos conceitos apresentados pela legislação a fim de garantir uma comparação justa com os *frameworks* de governança. Esses requerimentos foram elaborados seguindo os direitos dos titulares e requisitos das organizações apresentados pela lei e representam conceitos importantes que, se implementado pela organização, agregariam valor para o cumprimento da LGPD.

1. **Consentimento do uso de dados pessoais**: Consentimento de dados se aplica à processos de comunicação e consenso entre a organização e as partes interessadas;
2. **Necessidade do uso de dados pessoais**: Relacionado a procedimentos análise da necessidade de dados pessoais, evitando a utilização de dados desnecessários;
3. **Transparência do uso dados pessoais**: Disponibilização de informações a cerca de quais dados pessoais estão estão sob domínio da organização e quais tratamentos são aplicados sobre eles;
4. **Controle dados pessoais**: Processos que visam disponibilizar ao titular a capacidade de verificar, modificar e remover seus dados pessoais;
5. **Canal de comunicação com o titular**: Processos referentes à criação e melhora de canais de comunicação entre a organização e o titular ;
6. **Gerenciamento de terceiros**: Processos de gestão de quaisquer operador contratado pela organização a fim de garantir que estes também estejam seguindo as regras da LGPD ;
7. **Prevenção de incidentes**: Técnicas, procedimentos e planos de monitoramento e adequação a fim de prevenir, dentro da capacidade da organização, a ocorrência de acidentes e falhas que relacionadas aos dados pessoais sob poder da organização ;
8. **Respostas à incidentes**: Procedimentos e planos de resposta eficiente à incidentes, reduzindo o dano e comunicando o ocorrido à todas as partes interessadas ;
9. **Relatórios organizacionais**: Criação de documentação que comprove a utilização de procedimentos relevantes para o cumprimento da lei;
10. **Encarregado do uso de dados**: A organização deve definir um encarregado dos dados pessoais a fim de garantir a comunicação direta entre a organização, os titulares e a autoridade nacional ;

4 ESTUDO COMPARATIVO

Neste capítulo será apresentado o estudo comparativo proposto pelo trabalho. Os requerimentos da LGPD descritos no capítulo anterior foram comparados com cada *framework* e categorizado de acordo. Para cada requerimento é apresentado sua categoria com relação a cada um dos *frameworks* e, caso relevante, argumentação em relação ao motivo de sua categorização.

4.1 Consentimento do uso de dados pessoais

ITIL 4: O ITIL 4 atende **parcialmente** a obtenção e manutenção de consentimento do titular a partir da prática "**Gerenciamento de nível de serviço**", onde são definidas diretrizes para a criação de acordos de serviço entre a organização e o titular, porém não possui foco na utilização dos dados pessoais desses indivíduos.

COBIT 2019: O COBIT 2019 atende **parcialmente** a garantia de consentimento do titular a partir do objetivo "**APO09 - Gerenciamento de acordos de serviço**, onde é incentivada a formalização e manutenção dos acordos entre a organização e as partes interessadas, mas não foca necessariamente na utilização de dados pessoais.

4.2 Necessidade do uso de dados pessoais

ITIL 4: O ITIL 4 atende **parcialmente** a obtenção de dados necessários do titular. Enquanto não apresenta nenhuma prática que relacionada à seleção estrita de apenas dados necessários para o seu funcionamento, o princípio orientador "**Mantenha-se simples e prático**"incentiva a eliminação de práticas desnecessárias.

COBIT 2019: O COBIT 2019 **não atende** à necessidade da prática eliminação da coleta de dados pessoais desnecessários.

4.3 Transparência do uso dados pessoais

ITIL 4: O ITIL 4 atende **satisfatoriamente** os requisitos de transparência do uso de dados pessoais, desde o princípio orientador "**Colabore e promova visibilidade**"até à prática "**Gerenciamento do catálogo de serviços**", que auxilia na análise das especifidades dos serviços ofertados pela organização, promovendo a disponibilização de informações técnicas relevantes ao uso de seus dados pessoais.

COBIT 2019: O COBIT 2019 atende **parcialmente** os requisitos de transparência do uso de dados pessoais. Enquanto a definição dos requerimentos dos serviços

são organizados no objetivo "**BAI02 - Gerenciamento de definições de requisitos**", essas informações são utilizadas para a gestão dentro da organização e não para promover a transparência com o titular.

4.4 Controle dados pessoais

ITIL 4: O ITIL 4 **não atende** os requisitos de controle de dados pessoais. Enquanto o *framework* possui práticas de "Design de serviço"e "Desenvolvimento e gerenciamento de software", o ITIL 4 não lida diretamente com o fornecimento de controle dos dados por parte do titular.

COBIT 2019: O COBIT 2019 **não atende** os requisitos de controle de dados pessoais. Nenhum dos objetivos do COBIT 2019 lidam com a garantida de controle dos dados pessoais do titular.

4.5 Canal de comunicação com o titular

ITIL 4: O ITIL 4 atende **satisfatoriamente** os requisitos de comunicação com o titular, desde o princípio orientador "**Colabore e promova visibilidade**"até práticas de "**Gerenciamento de relacionamentos**"e "***Service desk***".

COBIT 2019: O COBIT 2019 atende **satisfatoriamente** com a garantia de comunicação com o titular, exemplificado pelos objetivos "**DSS02 - Gerenciamento de requisições e incidentes de serviço**"e "**EDM05 - Garantia de engajamento com as partes interessadas**".

4.6 Gerenciamento de terceiros

ITIL 4: O ITIL 4 atende **satisfatoriamente** os requisitos de gerenciamento de terceiros por parte da prática de "**Gestão de fornecedores**", apresentando procedimentos para analisar e monitorar a conformidade de fornecedores de serviço empregados pela organização.

COBIT 2019: O COBIT 2019 atende **satisfatoriamente** os requisitos de gestão de terceiros a partir do objetivo "**APO10 - Gerenciamento de terceiros**", oferecendo processos para a garantira de cumprimento de requerimentos legais por fornecedores da organização.

4.7 Prevenção de incidentes

ITIL 4: O ITIL 4 atende **satisfatoriamente** os requisitos de prevenção de incidentes de segurança a partir das práticas de "**Gerenciamento de segurança da infor-**

mação"e incidentes internos por parte da "**Validação e teste de serviço**".

COBIT 2019: O COBIT 2019 tende **satisfatoriamente** os requisitos de prevenção de incidentes de segurança a partir dos objetivos "**DSS05 - Gerenciamento de serviços de segurança**"e "**APO13 - Gerenciamento de segurança**".

4.8 Respostas à incidentes

ITIL 4: O ITIL 4 atende **satisfatoriamente** o requisito de resposta à incidentes a partir da prática de "**Gerenciamento de incidentes**". Esta prática prioriza reduzir o impacto de incidentes e a melhor comunicar o problema com todas as partes interessadas.

COBIT 2019: O COBIT 2019 atende **parcialmente** o requerimento de resposta adequada à incidentes a partir do objetivo "**DSS04 - Gerenciamento de continuidade**". Esse objetivo garante o eficaz retorno das atividades organizacionais porém não garante a comunicação do incidente com as partes interessadas.

4.9 Relatórios organizacionais

ITIL 4: O ITIL 4 atende **satisfatoriamente** os requisitos de relatórios organizacionais. Pelo simples fato de ser um *framework* de governança e da prática de "**Melhoria contínua**", a organização pode comprovar a utilização de procedimentos comprovados de segurança e organização. Além disso, as práticas de "**Gerenciamento de arquitetura**"e "**Gestão do conhecimento**"oferecem uma visão detalhada da organização a fim de gerar quaisquer relatórios organizacionais necessários.

COBIT 2019: O COBIT 2019 inerentemente atende **satisfatoriamente** os requisitos de relatórios organizacionais por ser um *framework* de governança, porém é auxiliado pelos objetivos "**EDM01 - Garantia de definição e manutenção das estruturas de governança**"e "**BAI08 - Gerenciamento do conhecimento**", que auxiliam na análise das polícias e processo organizacionais a fim de gerar relatórios completos.

4.10 Encarregado do uso de dados

ITIL 4: O ITIL 4 **não atende** os requisitos de definição do encarregado dos dados pessoais de uma organização.

COBIT 2019: O COBIT 2019 **não atende** os requisitos de definição do encarregado dos dados pessoais de uma organização.

4.11 Tabela

A seguir, os resultados são apresentados na forma de uma tabela. O requisitos também são mapeados em relação aos *frameworks* nos apêndices deste trabalho. O Apêndice A representando o relacionamento entre o ITIL 4 e os requisitos da LGPD, e o Apêndice B representando o COBIT 2019 e seu relacionamento com os mesmos requisitos.

Tabela 1 – Requisitos da LGPD

Requisito	**ITIL 4**	**COBIT 2019**
Consentimento do uso de dados pessoais	P	P
Necessidade do uso de dados pessoais	P	N
Transparência do uso dados pessoais	S	P
Controle dados pessoais	N	N
Canal de comunicação com o titular	S	S
Gerenciamento de terceiros	S	S
Prevenção de incidentes	S	S
Respostas à incidentes	S	P
Relatórios organizacionais	S	S
Encarregado do uso de dados	N	N

Com base na tabela 1 podemos ver que, entre os requisitos da LGPD selecionados, o *framework* ITIL 4 atende satisfatoriamente 6, parcialmente 2 e insatisfatoriamente 2, enquanto o *framework* COBIT 2019 atende satisfatoriamente 4, parcialmente 3 e insatisfatoriamente 3.

5 CONCLUSÃO

Com o objetivo de analisar a LGPD em relação aos principais *frameworks* de governança, este trabalho apresentou um estudo da estrutura e diretrizes do ITIL 4 e COBIT 2019.

O ITIL 4 é apresentado como um *framework* geral de governança, com maior foco nos processos internos de TI da organização. Seu foco são o pessoal interno da organização, auxiliando na definição e manutenção desses serviços.

O COBIT 2019 tem maior foco na área de TI, oferecendo diversas diretrizes para o aumento da eficiência de todos os elementos da organização. Mesmo sendo voltado para o quadro de diretores da organização, o *framework* oferece o aperfeiçoamento do relacionamento entre todas as partes interessadas.

Durante a análise dos *frameworks*, foi possível perceber que os mesmos não apresentam práticas diretas e específicas a serem implementadas pela organização. Por este motivo, a comparação foi feita de maneira mais ampla, a fim de verificar como os *frameworks* podem agregar valor para o comprimento da LGPD.

A partir da análise descrita no capítulo anterior é possível concluir que as ambos *frameworks* não oferecem diretrizes de gerenciamento de dados pessoais de maneira satisfatória em relação à LGPD. Isso pode ser visto pela falta de orientação no tratamento de consentimento, necessidade e controle dos dados pessoais utilizados, além da falta de indicação do encarregado de dados da organização.

Mesmo com essas lacunas, os *frameworks* se mostraram bastante eficazes na prevenção e resposta à incidentes de segurança, ponto fundamental da LGPD. Também são oferecidos diversos processos para a melhor comunicação direta entre a organização e o titular dos dados, e à comprovação de adequação ao uso de práticas eficazes de governança pela organização.

Seguindo essas duas observações, é possível concluir que a utilização dos *frameworks* ITIL 4 e COBIT 2019 resultam em uma base sólida para cumprir os requerimentos legais da LGPD, demonstrando que a simples utilização desses *frameworks* cobrem grande partes dos conceitos requeridos pela legislação.

Contudo, como os *frameworks* não oferecem ações específicas, ainda é necessário a criação de um plano de negócio a fim de garantir o total cumprimento da lei, como apresentado pelo artigo [18].

Esta conclusão é corroborada por [15], onde é concluído que o COBIT e ITIL não possúem foco explícito no fluxo de dados, além de [16] concluir que organizações que

implementaram outros *frameworks*, como o ISO/IEC 27001, também não estão totalmente em cumprimento da GDPR, porém possuem uma base excelente para tal.

Como trabalho futuro, seria interessante a realização de um estudo a fim de criar um modelo organizacional baseado em ITIL e COBIT que cumpra totalmente os requisitos da LGPD.

REFERÊNCIAS

[1] AXELOS. *foundation - ITIL 4 edition*. [S.l.: s.n.], 2019.

[2] ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. [S.l.: s.n.], 2019.

[3] ISACA. *COBIT 2019 Framework: Introduction & Methodology*. [S.l.: s.n.], 2019.

[4] ERICKSON, A. *Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges with the LGPD*. 2019. <https://brooklynworks.brooklaw.edu/bjil/vol44/iss2/9>. Acessado: 06/09/2021.

[5] L13709. Lei no 13.709. Sobre a Lei Geral de Proteçao de Dados Pessoais (LGPD). <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessado: 06/09/2021.

[6] APENAS 40% das empresas reconhecem estar preparadas para a LGPD. <https://canaltech.com.br/seguranca/apenas-40-das-empresas-reconhecem-estar-preparadas-para-a-lgpd-191526/>. Acessado: 06/09/2021.

[7] STEUPERAERT, D. Cobit 2019: A significant update. *EDPACS*, Taylor & Francis, v. 59, n. 1, p. 14–18, 2019. Disponível em: <https://doi.org/10.1080/07366981.2019.1578474>.

[8] TEFFé, C. S. d.; VIOLA, M. Tratamento de dados pessoais na lgpd: estudo sobre as bases legais. *civilistica.com*, v. 9, n. 1, p. 1–38, maio 2020. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/510>.

[9] QUEM vai regular a LGPD? <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd/>. Acessado: 20/04/2021.

[10] ITSFM. *Introductory Overview of ITIL 4*. [S.l.: s.n.], 2020.

[11] BERGER, D.; SHASHIDHAR, N.; VAROL, C. Using itil 4 in security management. In: *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. [S.l.: s.n.], 2020. p. 1–6.

[12] AGUTTER, C. *ITIL Foundation Essentials ITIL 4 Edition: The ultimate revision guide*. [S.l.: s.n.], 2020.

[13] NACHROWI, E.; NURHADRYANI, Y.; SUKOCO, H. Evaluation of governance and management of information technology services using cobit 2019 and itil 4. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, v. 4, n. 4, p. 764 – 774, Aug. 2020. Disponível em: <http://jurnal.iaii.or.id/index.php/RESTI/article/view/2265>.

[14] MUNCINELLI, G. et al. Components of the preliminary conceptual model for process capability in lgpd (brazilian data protection regulation) context. In: . [S.l.: s.n.], 2020.

[15] MAGNUSSON, L. et al. Searching for a governance model to manage and secure the data flow in organizations, as required by gdpr. In: *Information System Research Seminar in Scandinavia, Aarhus University in Odder, Denmark, August 5th - 8th 2018 :*. [S.l.: s.n.], 2018.

[16] LOPES, I. M.; GUARDA, T.; OLIVEIRA, P. How iso 27001 can help achieve gdpr compliance. In: *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*. [S.l.: s.n.], 2019. p. 1–6.

[17] TZOLOV, T. One model for implementation gdpr based on iso standards. In: *2018 International Conference on Information Technologies (InfoTech)*. [S.l.: s.n.], 2018. p. 1–3.

[18] FARIAS, R. B. F. P. Lgpd framework - from theory to practice. In: . [S.l.: s.n.], 2022.

Apêndices

APÊNDICE A – PRÁTICAS E PRINCÍPIOS DO ITIL 4 EM RELAÇÃO AOS REQUERIMENTOS DA LGPD

A seguinte tabela relaciona os requerimentos da LGPD com as práticas e princípios do ITIL 4. Esta tabela serve o objetivo de melhor visualizar quais práticas e princípios estão relacionados com os requerimentos da LGPD definidos neste trabalho. As intersecções representam essas relações, "P" representando uma relação parcial, "S", representando um relação satisfatória e vazio, significando nenhuma relação direta ou indireta.

			Requerimento da LGPD									
			Consentimento do uso de dados pessoais	Necessidade do uso de dados pessoais	Transparência do uso dados pessoais	Controle dados pessoais	Canal de comunicação com o titular	Gerenciamento de terceiros	Prevenção de incidentes	Respostas à incidentes	Relatórios organizacionais	Encarregado do uso de dados
Práticas e Princípios do ITIL 4			1	2	3	4	5	6	7	8	9	10
Práticas do ITIL 4	1	Gerenciamento de arquitetura									S	
	2	Melhoria contínua									S	
	3	Gerenciamento de segurança da informação							S			
	4	Gestão do conhecimento									S	
	5	Medições e relatórios:										
	6	Gerenciamento de mudanças organizacionais										
	7	Gerenciamento de portfólio										
	8	Gerenciamento de projetos										
	9	Gestão de relacionamento					S					
	10	Gestão de riscos										
	11	Gerenciamento financeiro de serviços										
	12	Gestão da estratégia										
	13	Gestão de fornecedores						S				
	14	Força de trabalho e gestão de talentos										
	15	Gerenciamento de disponibilidade										
	16	Análise de negócios										
	17	Gerenciamento de capacidade e desempenho										
	18	Controle de mudanças										
	19	Gerenciamento de incidentes								S		
	20	Gerenciamento de ativos de TI										
	21	Monitoramento e gerenciamento de eventos										
	22	Gerenciamento de problemas										
	23	Gerenciamento de versão										
	24	Gerenciamento do catálogo de serviços			S							
	25	Gerenciamento de configuração de serviço										
	26	Gerenciamento de continuidade de serviço										
	27	Design de serviço										
	28	Service Desk					S					
	29	Gerenciamento de nível de serviço	P									
	30	Gerenciamento de solicitações de serviço										
	31	Validação e teste de serviço							S			
	32	Gerenciamento de implantação										
	33	Gerenciamento de infraestrutura e plataforma										
	34	Desenvolvimento e gerenciamento de software										
Princípios Orientadores	35	Foco no valor										
	36	Comece onde você está										
	37	Progrida iterativamente e com feedback										
	38	Colabore e promova visibilidade										
	39	Pense e trabalhe holisticamente										
	40	Mantenha-se simples e prático		P								
	41	Otimize e automatize										

Tabela 2 – Relação entre as práticas e princípios do ITIL 4 com os requerimentos da LGPD

APÊNDICE B – OBJETIVOS DO COBIT 2019 EM RELAÇÃO AOS REQUERIMENTOS DA LGPD

A seguinte tabela relaciona os requerimentos da LGPD com os objetivos do COBIT 2019. Esta tabela serve o objetivo de melhor visualizar quais práticas e princípios estão relacionados com os requerimentos da LGPD definidos neste trabalho. As intersecções representam essas relações, "P" representando uma relação parcial, "S", representando um relação satisfatória e vazio, significando nenhuma relação direta ou indireta.

			Requerimento da LGPD									
			Consentimento do uso de dados pessoais	Necessidade do uso de dados pessoais	Transparência do uso dados pessoais	Controle dados pessoais	Canal de comunicação com o titular	Gerenciamento de terceiros	Prevenção de incidentes	Respostas à incidentes	Relatórios organizacionais	Encarregado do uso de dados
Objetivos do COBIT 2019			1	2	3	4	5	6	7	8	9	10
Evaluate, Direct and Monitor	1	EDM01 - Garantia de definição e manutenção das estruturas de governança									S	
	2	EDM02 - Garantia de entrega de benefícios										
	3	EDM03 - Garantia de otimização de riscos										
	4	EDM04 - Garantia de otimização de recursos										
	5	EDM05 - Garantia de engajamento com as partes interessadas					S					
Align, Plan and Organize	6	APO01 - Gerenciamento de estruturas de gerenciamento de TI										
	7	APO02 - Gerenciamento de estratégia										
	8	APO03 - Gerenciamento da arquitetura empresarial										
	9	APO04 - Gerenciamento de inovação										
	10	APO05 - Gerenciamento de portfólio										
	11	APO06 - Gerenciamento de orçamento e custos:										
	12	APO07 - Gerenciamento de recursos humanos										
	13	APO08 - Gerenciamento de relacionamentos										
	14	APO09 - Gerenciamento de acordos de serviço	P									
	15	APO10 - Gerenciamento de terceiros						S				
	16	APO11 - Gerenciamento de qualidade										
	17	APO12 - Gerenciamento de risco										
	18	APO13 - Gerenciamento de segurança							S			
	19	APO14 - Gerenciamento de dados										
Build, Acquire and Implement	20	BAI01 - Gerenciamento de programas										
	21	BAI02 - Gerenciamento de definições de requisitos			P							
	22	BAI03 - Gerenciamento de identificação e construção de soluções										
	23	BAI04 - Gerenciamento de disponibilidade e capacidade										
	24	BAI05 - Gerenciamento de mudanças organizacionais										
	25	BAI06 - Gerenciamento de mudanças de TI										
	26	BAI07 - Gerenciamento de aprovações e transições de mudanças de TI										
	27	BAI08 - Gerenciamento de conhecimento									S	
	28	BAI09 - Gerenciamento de ativos										
	29	BAI10 - Gerenciamento de configuração										
	30	BAI11 - Gerenciamento de projetos										
Deliver, Service and Support	31	DSS01 - Gerenciamento de operações										
	32	DSS02 - Gerenciamento de requisições e incidentes de serviço					S					
	33	DSS03 - Gerenciamento de problemas										
	34	DSS04 - Gerenciamento de continuidade								P		
	35	DSS05 - Gerenciamento de serviços de segurança							S			
	36	DSS06 - Gerenciamento de controles de processos de negócio										
Monitor, Evaluate and Assess	37	MEA01 - Gerenciamento do monitoramento de performance e conformidade										
	38	MEA02 - Gerenciamento do sistema de controle interno										
	39	MEA03 - Gerenciamento de conformidade com requerimentos externos										
	40	MEA04 - Gerenciamento de garantia										

Tabela 3 – Relação entre os objetivos do COBIT 2019 com os requerimentos da LGPD