Análise de Frameworks de Governança de TI em relação à LGPD

Rafael Hirata Santos[1], **Rodolfo Miranda de Barros** [1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

rhirata.s@gmail.com, rodolfo@uel.br

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 aims to study the ITIL and COBIT frameworks and analyse their security policy recommendations with the standards required by the LGPD.*

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 tem 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.*

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, entrou em vigor a *GDPR* (Regulamento Geral sobre a Proteção de Dados). Esse regulamento visa regimentar o tratamento de dados de cidadãos europeus, além dos direitos de privacidade dos usuários.

Seguindo o exemplo da União Europeia, em 2018 foi ratificada a Lei Geral de Proteção de Dados (LGPD)[3], esperada para entrar em vigor em setembro de 2021. 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 dizem estar preparadas às novas normas da LGPD.[1] 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[5] 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 descritos os objetivos do trabalho, seguido do capítulo 4, onde a metodologia é explicada. No capítulo 5 é encontrado o cronograma das atividades. Por fim, na seção 6, é descrita as contribuições esperadas do trabalho.

2. Fundamentação Teórico-Metodológica e Estado da Arte

Nesta seção serão descritos conceitos e ferramentas necessárias para o desenvolvimento deste trabalho.

2.1. Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei nº 13.709), foi uma lei aprovada em 14 de agosto de 2018, programada para entrar em vigor em 28 de setembro de 2021, 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.

Sob essa lei, todo cidadão brasileiro, estando em território nacional ou estrangeiro, tem a titularidade de seus dados pessoais, dando ao mesmo diversos direitos, como por exemplo[3]:

- **Confirmação da existência de tratamento**: O usuário tem o direito de saber como seus dados pessoais estão sendo tratados, categorizado e utilizado.
- **Acesso aos dados**: O usuário tem o direito de solicitar uma cópia de todos os seus dados pessoais armazenados pela empresa.
- **Correção de dados**: O usuário tem o direito de solicitar a correção de dados pessoais incompletos, equivocados ou desatualizados.
- **Eliminação dos dados pessoais**: O usuário tem o direito de solicitar a remoção ou anonimização de dados que forem ”desnecessários, excessivos ou tratados em desconformidade”pela empresa.

- **Portabilidade dos dados**: O usuário tem o direito de solicitar a transferência de seus dados pessoais para outra empresa.
- **Informações sobre o compartilhamento de dados**: O usuário tem direito de saber com quais entidades a empresa irá compartilhar seus dados.
- **Revogação do consentimento**: O usuário pode, a qualquer momento, revogar o consentimento apresentado à empresa.

2.2. Information Technology Infrastructure Library

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[2].

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[5].

O ITIL modela as tividades de TI á partir do ciclo de vida dos serviços. Essa metodologia possui cinco etapas: Estratégia de serviço, projeto de serviço, transição de serviço, operação de serviço e melhoria contínua de serviço.

Figura 1. Ciclo de vida de serviço[4]

Estratégia de serviço: Etapa onde são definidos os objetivos do serviço. Aqui são definidas as estratégias que serão utilizadas para atingir as metas da empresa.

Projeto de serviço: Etapa onde são descritas as ideias para o novo serviço. É nessa etapa onde os procedimentos planejados na etapa anterior são oficializados.

Transição de serviço: Nessa etapa, os serviços são implementados. Os colaboradores trabalharam no desenvolvimento, teste e liberação do serviço.

Operação de serviço: Após ser testado, o serviço está pronto para ser colocado em produção. Nessa etapa o serviço é disponibilizado para o cliente.

Melhoria contínua de serviço. Com o serviço implantado, é estabelecido uma rotina de testes, à fim de reconhecer problemas e possíveis melhorias.

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[7].

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. Para isso, são definidos objetivos de controle, que são específicos para cada organização[6].

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.

3. Objetivos

O objetivo desse trabalho será um estudo sobre a LGPD, verificando as regras e normas estabelecidas pela lei a fim de comparar com as práticas e regras recomendadas pelos *frameworks* de governança de TI ITIL e COBIT. Essa comparação será feita a fim de verificar até qual ponto os *frameworks* atendem a LGPD, e evidenciar os tópicos que não forem cobertos por eles.

4. Procedimentos metodológicos/Métodos e técnicas

Para que os objetivos sejam alcançados, o projeto se iniciará com um levantamento bibliográfico sobre a LGPD, ITIL e COBIT, a fim de se obter a fundamentação teórica necessária para a análise das diretrizes que serão comparadas. Em seguida, será feito a categorização das requisições da LGPD, além das regras de negócio apresentadas pelo ITIL e COBIT.

Com as informações categorizadas, será feito a comparação das mesmas a fim de verificar se os requisitos da LGPD são atendidos pelos *frameworks*.

5. Cronograma de Execução

As etapas descritas na seção 4 serão realizadas seguindo o seguintes passos:

Atividades:

1. Levantamento bibliográfico
2. Estudo teórico sobre a LGPD;
3. Estudo teórico sobre o ITIL;

4. Estudo teórico sobre o COBIT;
5. Levantamento dos dados;
6. Comparação dos dados;
7. Análise dos resultados;
8. Escrita do trabalho;

Tabela 1. Cronograma de Execução

	set	out	nov	dez	jan	fev	mar	abr	mai
Atividade 2	X	X	X						
Atividade 3			X	X					
Atividade 4				X	X				
Atividade 5			X	X	X	X			
Atividade 6						X	X		
Atividade 7							X	X	
Atividade 8	X	X	X	X	X	X	X	X	X

6. Contribuições e/ou Resultados esperados

Esse trabalho tem como objetivo apresentar os requisitos apresentados pela LGPD, e mostrar se os *frameworks* de governança de TI já atendem essas demandas, e quais pontos devem ser considerados na falta políticas que não satisfação a nova legislação..

7. Espaço para assinaturas

Londrina, *13 de Setembro de 2021*.

Aluno

Orientador

Referências

[1] 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-19152 Acessado: 06/09/2021.

[2] Itil 4 - the framework for the management of it-enabled services. https://www.axelos.com/best-practice-solutions/itil. Acessado: 06/09/2021.

[3] L13709. lei no 13.709. sobre a lei geral de proteç ao de dados pessoais (lgpd. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acessado: 06/09/2021.

[4] O que é itil e qual a vantagem da itil para sua empresa – aprenda a implementar. https://netsupport.com.br/blog/o-que-e-itil-qual-a-vantagem-itil/. Acessado: 06/09/2021.

[5] AXELOS. *foundation - ITIL 4 edition*. 2019.

[6] Erika Nachrowi, Yani Nurhadryani, and Heru Sukoco. Evaluation of governance and management of information technology services using cobit 2019 and itil 4. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 4(4):764 – 774, Aug. 2020.

[7] Dirk Steuperaert. Cobit 2019: A significant update. *EDPACS*, 59(1):14–18, 2019.