DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)

Márcio Aurélio de Souza Fernandes

Brasília, 19 de setembro de 2022

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

SECURE REPOSITORY AN THE IMPACT GENERATED BY GENERAL PERSONAL DATA PROTECTION LAW (GPDP)

REPOSITÓRIO SEGURO E O IMPACTO GERADO PELA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

MÁRCIO AURÉLIO DE SOUZA FERNANDES

ORIENTADORA: EDNA DIAS CANEDO

DISSERTAÇÃO DE MESTRADO PROFISSIONAL EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: PPEE.MP.019
BRASÍLIA/DF, SETEMBRO - 2022

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

DISSERTAÇÃO DE MESTRADO PROFISSIONAL

Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)

Márcio Aurélio de Souza Fernandes

Dissertação de Mestrado Profissional submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Mestre em Engenharia Elétrica

Banca Examinadora

Profa. Edna Dias Canedo, Ph.D, CIC/FT/UnB _____
Orientadora

Prof. Rafael Timóteo de Sousa Junior, Ph.D, FT/UnB _____
Examinador Interno

Prof. Altair Olivo Santin, Ph.D, PUCPR _____
Examinador Externo

FICHA CATALOGRÁFICA

FERNANDES, MÁRCIO AURÉLIO DE SOUZA
Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD) [Distrito Federal] 2022.
xvi, 101 p., 210 x 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2022).
Dissertação de Mestrado Profissional - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica
1. Proteção de Dados
2. Segurança da Informação
3. Repositório Seguro
4. Conformidade
I. ENE/FT/UnB
II. Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)

REFERÊNCIA BIBLIOGRÁFICA

FERNANDES, M. A. S. (2022). *Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD)* . Dissertação de Mestrado Profissional, Publicação: PPEE.MP.019 Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 101 p.

CESSÃO DE DIREITOS

AUTOR: Márcio Aurélio de Souza Fernandes
TÍTULO: Repositório Seguro e o Impacto Gerado pela Lei Geral de Proteção de Dados Pessoais (LGPD) .
GRAU: Mestre em Engenharia Elétrica ANO: 2022

Márcio Aurélio de Souza Fernandes
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP 70919-970 - Brasília - DF - Brasil

DEDICATÓRIA

Dedico este trabalho especialmente aos meus pais, que com muito esforço e dedicação conseguiram dar um estudo de qualidade aos filhos, possibilitando que o sonho de continuidade na vida acadêmica fosse possível. Estendo essa dedicatória a todos os professores que contribuíram direta ou indiretamente, especialmente a professora Edna Dias Canedo que esteve comigo desde o começo dessa jornada. Finalizo dedicando também aos demais familiares e amigos que me apoiaram e estiveram sempre presentes.

AGRADECIMENTOS

Dedicarei breves palavras de agradecimento após esse longo período de estudos e pesquisas para a finalização e sucesso desse trabalho de mestrado. Inicialmente, meu agradecimento especial à minha orientadora professora Edna Dias Canedo, que soube lidar e superar o desafio de orientar um aluno a distância ante a pandemia, que dedicou boa parte do seu tempo e dividiu comigo seu conhecimento, agradeço ainda por não desistir e por várias vezes me dar o que ela mesmo chama de “puxão de orelha". Tenho certeza que sem eles nada disso teria acontecido.

Agradecimento sinceros a meu coorientador Daniel Alves da Silva, Carlos Eduardo L. Veiga, Guilherme Fay Vergara, Rodrigo M. dos Santos, Matheus Fonseca, Daniel Tavares, Fernando Gonçalves de Oliveira, Viviane Cristina Soares Alves, Ludmila Bravim da Silva, Fabio Lucio Lopes Mendonca e a todos os membros do Laboratório LATITUDE/UnB e IEEE VTS Centro-Norte Brasil Chapter, pelo incentivo, pelas valiosas sugestões e discussões construtivas sobre este trabalho.

Não posso deixar de agradecer a amigos e familiares que, por diversas vezes, tiveram que compreender a minha ausência em eventos e até mesmo no dia a dia deles. Agradeço especialmente aos meus pais, Sr. Antonio Fernandes e Sra. Maria Vieira, que sempre acreditaram que a educação é a única forma de fazer uma sociedade melhor e, acreditando nisso, fizeram o seu melhor para criar e educar seus filhos.

Agradeço ainda o apoio técnico e computacional do Laboratório de Tecnologias para Tomada de Decisão - LATITUDE, da Universidade de Brasília, que conta com apoio do CNPq - Conselho Nacional de Pesquisa (Outorgas 312180/2019-5 PQ-2 e 465741/2014-2 INCT em Cibersegurança), do Ministério da Economia (Outorgas 005/2016 DIPLA e 083/2016 ENAP), do Conselho Administrativo de Defesa Econômica (Outorga CADE 08700.000047/2019-14), da Advocacia Geral da União (Outorga AGU 697.935/2019),do Departamento Nacional de Auditoria do SUS (Outorga DENASUS 23106.118410/2020-85), da Procuradoria Geral da Fazenda Nacional (Outorga PGFN 23106.148934/2019-67) e dos Decanatos de Pesquisa e Inovação e de Pós-Graduação da Universidade de Brasília (Outorga 7129 FUB/EMENDA/DPI/COPEI/AMORIS).

RESUMO

Diversos trabalhos têm investigado como realizar a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) em relação à privacidade dos dados dos usuários. Diante desse cenário de adequação à LGPD, o trabalho tem como objetivo realizar uma análise dos princípios da LGPD e investigar o nível de conhecimento dos profissionais de tecnologias da informação e da comunicação (TIC) que trabalham direta e indiretamente com a lei. Além disso, procura-se investigar se Repositórios Digitais Seguros, em conformidade com a ISO 16363:2012 [1], também estão em conformidade com as diretrizes da LGPD. Para alcançar o objetivo dessa dissertação, foram estabelecidas três etapas de execução, a saber: 1) uma análise das legislações sobre a privacidade de dados; 2) a condução de um *survey* com 43 profissionais de ICT que atuam em organizações públicas e privadas - o *survey* contém 21 questões que abrangem legislação e tecnologia; e 3) uma análise técnica do Archivematica através de testes práticos, estáticos e dinâmicos com o auxílio de soluções open-source para realizar uma varredura de vulnerabilidades em sistemas. Os resultados demonstram que, mesmo após a LGPD entrar em vigor, 10% dos profissionais de ICT não conhecem os princípios da lei. Em relação à forma de armazenamento seguro, 45% dos profissionais de ICT afirmaram não ter conhecimento de como suas organizações realizam o armazenamento dos dados dos usuários ou o compartilhamento desses dados, 25% dos profissionais de ICT afirmaram que estão cientes que seus dados podem ser compartilhados pelas organizações. A análise realizada pela ferramenta Archivematica apresentou alguns problemas que podem indicar vulnerabilidades. A maioria dos problemas identificados pela ferramenta foram classificados como de níveis baixos e médios e podem resultar em oportunidades para possíveis atacantes, embora eles precisem de uma série de variantes para obter sucesso no ataque. Os resultados também demonstraram que os profissionais de ICT responsáveis pela adequação/conformidade da organização à LGPD precisam de cursos de aperfeiçoamento para realizar as atividades relacionadas à privacidade de dados e segurança da informação, e que o repositório seguro Archivematica, apesar de cumprir os requisitos definidos pelo órgão legislador para ser considerado seguro, não está em conformidade com a LGPD em relação às diretrizes relacionadas à Segurança e Privacidade de Dados. Dessa forma, faz-se necessária a realização de ajustes nos processos organizacionais e soluções de software das organizações. Sendo importante destacar dois pontos: o primeiro é a restruturação organizacional, que visa melhorar a integração entre áreas e departamentos; e o segundo é a transparência, pois a LGPD destaca que regras precisam ficar explícitas para os usuários, inclusive acessos e permissões.

Palavras chave: Proteção de Dados, Segurança da Informação, Privacidade de Dados, Repositório Seguro, LGPD, Conformidade.

ABSTRACT

Several studies have researched how to adapt the General Data Protection Law (GDPL) according to the privacy of the user's data. Facing this compliance scenario, this study aims to conduct an analysis of the principles of the LGPD and investigate the knowledge level of information and communications technology (ICT) professionals working directly and indirectly with this law. In addition, investigate whether Archivematica secure storage service is in accordance with the GDPL guidelines. To achieve this essay's purposes, three execution stages were established as follows: 1) an analysis of data privacy laws; 2) conducting a survey with 43 ICT professionals working in public and private organizations; and 3) a technical analysis of Archivematica through practical, static, and dynamic tests with the help of open-source solutions to perform a vulnerability scan. The results show that even after the GDPL enters into force, 10% of those ICT professionals do not know the principles of the law. Regarding the storage service, 45% of the ICT professionals stated they have no knowledge on how their organizations store user data or share them and 25% of the ICT professionals claimed they are aware that their data can be shared by the organizations. The analysis performed by Archivematica evidenced issues that may indicate vulnerabilities. Majority of the issues identified by the tool were classified as low and medium risks and could result in opportunities for attackers, although they would need a series of variants to succeed. The results also showed that the ICT professionals responsible for the adequacy/compliance of the organizations need further training courses to conduct activities related to data privacy and information security, and that the Archivematica secure storage service, whilst meets with the defined requirements by the legislating body to be considered safe, does not comply with the GDPL guidelines related to data security and privacy. Therefore, it is necessary to highlight two points: the first is the organizational restructuring, which aims to improve the integration between areas and departments, and the second is the transparency, as GLPD emphasizes that rules need to be explicit to users, including access and permissions.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIAÇÕES E SIGLAS

Siglas

AIP	Pacote de Informação do Arquivo
ANPD	Agencia Nacional de Proteção de Dados
APF	Administração Publica Federal
API	Application Programming Interface
Conarq	Conselho Nacional de Arquivos
CORS	Cross-Origin Resource Sharing
CSP	Content Security Policy
CWE	Common Weakness Enumeration
DAST	Dynamic Application Security Testing
DIP	Pacote de Informação e Disseminação
GDPR	General Data Protection Regulation
HTML	HyperText Markup Language
IAM	Identify and Access Management
ICA	International Council on Archives
ICT	Tecnologia da Informação e Comunicação
ISAD(G)	General International Standard Archival Description
ISO	International Organization for Standardization
LGPD	Lei Geral de Proteção de Dados
MDM	Master Data Management
NOBRADE	Norma Brasileira de Descrição Arquivistica
OAIS	Open Archival Information System
OCR	Optical Character Recognition
OWASP	Open Web Application Security Project
PDI	Informações de Descrição de Preservação
RAM	Random Access Memory
RDC	Repositório Digital Confiavel
SAST	Static Application Security Testing
SGSI	Sistema de Gestão de Segurança da Informação
SIP	Pacote de Informação e Submissão
SSD	Solid State Drive
TDR	Trusted Digital Repositories
TI	Tecnologia da Informação
TRAC	Trustworthy Respositories Audit and Certification Checklist
URL	Uniform Resource Locator
VPN	Virtual Protection Network
WASC	Web Application Security Consortium
XML	eXtensible Markup Language

1 INTRODUÇÃO

Com o aumento na utilização da internet, novas formas de ataques vêm surgindo, desde ataques através de engenharia social até ataques feitos com ferramentas, softwares maliciosos, invasões de força bruta, entre outros [6]. Em meio ao crescente aumento de usuários na internet, com a utilização de comércios eletrônicos (*e-commerce*), transações bancárias online, criações de novas mídias sociais e a própria digitalização de serviços públicos, que cada vez mais expõem os dados pessoais dos seus utilizadores, criminosos voltaram seus ataques para esses usuários.

Outro fator que despertou a atenção em segurança de dados pessoais foi o rápido desenvolvimento da disciplina de Big Data, o qual possibilitou o processamento automatizado de dados estruturados, semiestruturados e não estruturados, permitindo a criação de grandes repositórios de dados e o cruzamento desses dados para gerar valor em diversos tipos de negócios que podem se beneficiar desde somente contatos de um individuo ou empresa para o disparo de um *mailing*, até da definição de um perfil de consumo refinado desses clientes em potenciais.

A disciplina de proteção de dados ganhou destaque quando foi lançada a *General Data Protection Regulation* (GDPR) [7], que surgiu em substituição a duas normas europeias, a saber: “Diretiva de Proteção de Dados da União Europeia” e o “Ato de Proteção de Dados do Reino Unido de 1998” [8]. Essa diretiva surgiu como resposta ao aumento de “incidentes de segurança"em que criminosos cibernéticos vislumbraram nesse contexto a grande chance de aplicar golpes, fraudes, sequestro de dados, etc. [9].

O governo brasileiro, a partir de uma leitura da GDPR e com o interesse de minimizar riscos à segurança pública e privada, editou a Lei Geral de Proteção de Dados Pessoais (LGPD) [4]. Essa lei trouxe em seu texto várias diretrizes a serem seguidas, desde a forma do controle de acesso à informação até a forma como ela é armazenada. Para tanto, conta com várias regras que serão exigidas obrigatoriamente a toda e qualquer instituição pública, privada ou a terceiros que tenham posse de dados pessoas e cadastrais de seus usuários [4].

A LGPD foi elaborada com o objetivo de controlar e fortalecer os direitos dos cidadãos sobre suas informações pessoais e sua privacidade [4]. Adentra-se a operação pró-privacidade, na qual a segurança da informação exerce função essencial para a proteção adequada dos ativos, ou seja, nada mais é do que garantir que a informação esteja segura através de várias ações, entre elas, a conscientização dos colaboradores da organização, definição de processos e condutas, ferramentas, etc. [10].

A normatização representa um passo importante para a proteção dos dados dos cidadãos brasileiros, haja vista que a LGPD traz regras rígidas para a coleta, tratamento e o uso de informações pessoais, bem como prevê sanções para casos de inobservância e descumprimento [4]. O tratamento desses ativos deverá ser exercido a partir do cumprimento de normas minímas de segurança, respeitando os seguintes pilares da informação: disponibilidade, integridade, confi-

dencialidades, legalidade, auditabilidade e não repudio de autoria [10]. De maneira geral, a Lei Geral de Proteção de Dados Pessoais amplia a autonomia dos titulares sobre os seus próprios dados pessoais e acrescenta o dever de proteção das empresas frente a esses dados, além de exigir a notificação de violações de segurança de informações pessoais e, por fim, impõem penalidades significativas pelos descumprimentos da lei [11].

A proteção de dados ganhou ênfase nos últimos anos com o aumento de ataques e vazamentos de dados, deixando de ser um problema apenas de corporações bancárias ou agências financeiras, tornando-se um problema para todos os ramos de atividades. Como exemplo, tem-se o grande vazamento de aproximadamente 12 milhões de usuários da empresa Quest Diagnósticos; outro exemplo, em outro ramo de atividade, foi o vazamento da franquia Ceckers and Rally's, empresa do ramo alimentício; ambos em 2019 [12]. A utilização dessas empresas para ter os cadastros de usuários e clientes em seu banco de dados faz com que criminosos cibernéticos vislumbrem nesse contexto a grande chance de aplicar golpes, fraudes, sequestro de dados, etc. [9].

Ademais, dificilmente a implantação dessas novas tecnologias seguem as recomendações das boas práticas em gestão da informação, tais como as normas da *International Organization for Standardization (ISO)* e o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil)[13], que visam descrever os requisitos mínimos e os desejáveis para garantir a cadeia de custódia documental.

Todo esse cenário configura um grande desafio no que tange a Segurança da Informação, pois a informação é o ativo de maior importância nas organizações modernas. Uma vez que de posse de informações restritas, agentes maliciosos podem causar danos incalculáveis paras as organizações, sejam eles nas finanças, na imagem, na credibilidade, etc.

Desde a década de 1990, a comunidade internacional tem desenvolvido iniciativas no sentido de orientar a modelagem e implementação de repositórios arquivísticos digitais, além de apontar os requisitos para atribuir confiabilidade a esses repositórios. A implantação de um repositório arquivístico digital confiável é fundamental para assegurar a preservação, o acesso e a autenticidade de longo prazo dos materiais digitais.

Dessa necessidade de proteger os dados, garantindo a integridade e inviolabilidade desses, surgiu a necessidade de uma forma de armazenamento segura dos dados que garantisse o mínimo de segurança ao usuário e ao responsável pela guarda dos dados. Para garantir que um repositório digital seja confiável ou seguro, há um normativo da Organização Internacional de Normalização que detalha os requisitos mínimos para ser assim considerado. A ISO 16363:2012 [1] foi feita com base no *Trustworthy Respositories Audit and Certification Checklist* (TRAC) de 2007 [5], onde estão descritas as diretrizes que avaliam, certificam e auditam se o repositório pode ser considerado seguro.

Considerando que os órgãos da Administração Publica Federal (APF) se submetem aos requisitos estabelecidos pelo e-ARQ Brasil, é necessário a preservação dos documentos arquivísticos digitais nas fases correntes, intermediária e permanente, e que esteja associada a um repositório arquivístico digital confiável (RDC-Arq) [13].

Diante desse cenário, a APF vem buscando, gradativamente, desenvolver soluções para sanar parte dos problemas existentes em relação a esse contexto. Uma delas foi a adoção do sistema Archivematica, que é um repositório arquivístico digital confiável para armazenar documentos digitais de longa temporalidade ou de guarda permanente, isto é, tem por objetivo implementar todos os procedimentos de preservação digital necessários aos documentos de guarda permanente ou históricos.

Ademais, dificilmente a implantação dessas novas tecnologias seguem as recomendações das boas práticas em gestão da informação, tais como as normas da *International Organization for Standardization (ISO)* e o Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (e-ARQ Brasil) [13], que visam descrever os requisitos mínimos e os desejáveis para garantir a cadeia de custódia documental.

O pressuposto da autenticidade dos documentos arquivísticos digitais deve estar apoiado na evidência de que eles foram mantidos com uso de tecnologias e procedimentos administrativos que garantiram a sua identidade e integridade (componentes da autenticidade); ou que pelo menos minimizaram os riscos de modificações dos documentos a partir do momento em que foram salvos pela primeira vez e em todos os acessos subsequentes. Além disso, essa presunção se baseia na confirmação da existência de uma cadeia de custódia ininterrupta, desde o momento da produção do documento até a sua transferência para a instituição arquivística responsável pela sua preservação no longo prazo. Caso essa cadeia de custódia seja interrompida, o tempo em que os documentos não estiveram sob a proteção do seu produtor ou sucessor pode causar dúvidas sobre a sua autenticidade [14].

A Resolução nº 43 do Conarq afirma que: "Os documentos digitais em fase permanente são dependentes de um bom sistema informatizado que apoie o tratamento técnico adequado, incluindo arranjo, descrição e acesso, de forma a assegurar a manutenção da autenticidade e da relação orgânica desses documentos" [15, p.4].

A vulnerabilidade dos documentos arquivísticos digitais, os ciclos de obsolescência tecnológica efêmeros e a dificuldade de se provar a autenticidade dos documentos digitais apontam para a necessidade de se utilizar repositórios arquivísticos digitais confiáveis. O Repositório Arquivístico Digital Confiável (RDC-Arq) é um repositório digital que armazena e gerencia os documentos arquivísticos transferidos ou recolhidos de sistemas informatizados de gestão, os quais devem cumprir requisitos definidos no e-ARQ Brasil, de acordo com normas internacionais.

Uma forma de atestar a confiabilidade de um repositório arquivístico digital confiável junto à comunidade-alvo se dá por meio da sua certificação por terceiros. Para esse fim, o TRAC - *Trusted Digital Repositories* [16], em parceria com o NARA, publicou em 2007 o documento *Trustworthy Repository Audit and Certification: Criteria and Checklist (TRAC)*, o qual serviu de base para a elaboração da norma ISO 16363 [1]. No entanto, mesmo se cercando de todos os cuidados previstos nos padrões e normas, existe uma série de vulnerabilidades na cadeia de custódia, inclusive no próprio modelo *Open Archival Information System (OAIS)*, referenciado na Resolução nº 43 do Conselho Nacional de Arquivos (Conarq) [14]. A tramitação desses docu-

mentos digitais até sua admissão no RDC-Arq é um processo crítico, pois tais documentos ficam suscetíveis a vários tipos de ataques, por exemplo, os de modificação e fabricação. Dessa forma, para mitigar quaisquer ações que comprometam a integridade documental, faz-se necessária a adoção de medidas de segurança desde a fonte até o destino final do documento digital.

Diante desse cenário, esta dissertação de mestrado tem como escopo apresentar o conjunto de definições teóricas, metodológicas e soluções tecnológicas, com ênfase na segurança dos sistemas de informação e das redes, a serem utilizadas para assegurar o processo de proteção de dados, em conformidade com a LGPD. Para tanto, serão realizados testes com repositórios arquivísticos digitais seguros e ferramentas de detecção de falhas em sistemas, os quais avaliam as possíveis falhas de desenvolvimento e identificam os riscos de ataques e comprometimentos com a segurança da solução.

1.1 PROBLEMA DE PESQUISA

Devido a dezenas de soluções que prometem segurança e proteção de dados aos usuários e a dificuldade dessa garantia, uma vez que não é incomum notícias de invasão, vazamento de informações e/ou furto de dados pessoais, deixando a certeza da vulnerabilidade das plataformas existentes atualmente, situações de negligência, omissão e, até mesmo, inexistência de implementação de mecanismos de segurança, bem como de normas efetivas para garantir a proteção de dados pessoais e sensíveis dos consumidores digitais tornam-se um problema para as organizações.

Um dos maiores desafios para qualquer organização, seja ela pública ou privada, é ter um mecanismo ou solução que proporcione maior tranquilidade ao negócio e aos seus usuários, o que coloca a problemática de se ter a necessidade de adequação por força de uma norma vigente que impõe sanções pesadas em caso de descumprimento da legislação relacionada à privacidade de dados.

Um item importante de cumprimento da LGPD é a exigibilidade de comprovação e documentação do uso dos dados pessoais dos usuários, tais como transparência com o usuário não somente no tratamento dado às informações pessoais, mas também ao armazenamento dos dados. Em caso de possível vazamento ou perda dos dados, a causa deverá ser divulgada, o que, para o prestador de serviço, pode ser uma perda muito grande de confiança por parte dos seus usuários. Outro problema que apresenta uma grande dificuldade no cumprimento da LGPD é a integração de diversas áreas de negócio para o sucesso da implementação da lei, que vai desde a tecnologia da informação e comunicação (TIC) até o departamento jurídico da organização, passando pela administração e pelos colaboradores, além de contar com ferramentas tecnológicas e a conscientização da importância do coletivo na implantação de processos, métodos e soluções.

1.2 JUSTIFICATIVA

Das falhas de segurança de sistemas de rede, o vazamento de dados pessoais e sensíveis é o incidente que possui maior repercussão moral, social, econômica e jurídica ao usuário-consumidor. É de conhecimento público a ocorrência de diversos casos de vazamento e roubo de dados pessoais de usuários de grandes lojas e serviços online. Apenas no ano de 2018, podemos elencar os seguintes vazamentos de dados:

- *Facebook*: mau uso de dados de usuários, exposição de mensagens privadas por organizações indevidas [17].
- *Twitter*: exposição da localização de usuários por meio de números de telefone [18].
- Rede Marriot: devido a ataques de hackers, cerca de 500 milhões de hóspedes dos hotéis da rede, inclusive do Brasil, tiveram informações sensíveis vazadas. Vale ressaltar que, em 2020, a empresa teve novo ataque e consequente vazamento de dados [19].
- *Netshoes*: vazamento de informações pessoais e sensíveis de clientes de um dos maiores *e-commerce* do Brasil ocorrido no início de dezembro de 2017. Merece destaque o posicionamento da Empresa que negou o incidente com veemência, só assumindo o ocorrido em fevereiro de 2019 [20].
- Porto Seguro: dados pessoais, imagens de documentos e até dados bancários dos clientes-consumidores, funcionários e executivos da Seguradora foram vendidos no mercado ilegal do crime [21].

Tais fatos refletem a vulnerabilidade das plataformas, situações de negligência, omissão e, até mesmo, inexistência de implementação de mecanismos de segurança, bem como de normas efetivas para garantir a proteção de dados pessoais e sensíveis dos consumidores digitais. Em 2020, entrou em vigor a Lei Geral de Proteção de Dados Pessoais, Lei n° 13.709/2018 [4], trazendo consigo grande impacto em organizações que detenham informações pessoais, sejam empresas de qualquer porte, área de atuação, setor público ou privado. O cenário está mudando e adentrando em uma era pro-privacidade, no qual será imprescindível a aplicação de boas práticas e políticas de segurança e prevenção de riscos.

A legislação garante ao consumidor/usuário uma série de direitos sobre suas informações, por outro lado, exige uma série de deveres para as organizações, no que tange a coleta, uso, correção, eliminação e, até mesmo, a portabilidade de dados. De forma resumida, a Lei Geral de Proteção de Dados amplia a autonomia dos titulares de dados sobre os seus próprios dados pessoais e acrescenta o dever de proteção das empresas frente a esses dados, além de exigir a notificação de violações de segurança de informações pessoais e impor penalidades significativas pelos descumprimentos da lei [4].

A governança, gestão e transparência de dados são os pilares da LGPD. Em todo o ciclo de vida, desde a concepção do produto ou serviço, será necessária a preocupação com a privacidade,

proteção, cuidado e segurança do usuário e seus dados pessoais e sensíveis [4]. Um aparato de soluções de TI e de segurança da informação serão necessárias para se adequar às exigências legais da LGPD, tais como a análise e gerenciamento de dados, gerenciamento de consentimento, restrição e controle de acessos, eliminação de dados duplicados em bases de dados, mascaramento de dados, entre outras providências [22].

1.3 OBJETIVOS

1.3.1 Objetivo Geral

O objetivo geral deste trabalho é identificar e realizar uma análise das ferramentas e metodologias existentes na literatura e na indústria que são utilizadas como repositórios arquivísticos digitais seguro, além de relacionar essas ferramentas com as diretrizes da Lei Geral de Proteção de Dados, com a finalidade de comprovar ou refutar se as ferramentas identificadas podem servir de apoio na aplicação da lei.

1.3.2 Objetivo Específico

Para alcançar o objetivo principal, será necessário o cumprimento dos seguintes objetivos específicos:

- Revisão de literatura sobre a privacidade de dados.
- Análise da legislação (LGPD) e leis complementares sobre privacidade de dados.
- Análise de soluções para repositórios arquivísticos digitais seguros (Archivematica).
- Análise de possíveis vulnerabilidades.
- Proposição de um modelo tecnológico em forma de guia via web ou metodológico no formato de livreto, contemplando as diretrizes da LGPD e a forma de adequação para os repositórios arquivísticos digitais seguros.
- Realização de validação do modelo/guia com especialistas da área.
- Realização de ajustes no guia caso necessário.

1.4 RESULTADOS ESPERADOS

Esperamos que, após a pesquisa e a coleta de informações, seja possível gerar um modelo de negócio e/ou modelo tecnológico capaz de adequar toda e qualquer ferramenta de repositó-

rio arquivístico digital confiável aos princípios da LGPD, servindo, assim, como um guia para repositórios confiáveis.

1.5 METODOLOGIA DE PESQUISA

Esta pesquisa é quantitativa, teórica e investigativa, realizada através da análise de discursos e do confronto com as ideias e publicações de especialistas na área de segurança da informação e na legislação que versa sobre a privacidade e o tratamento de dados pessoais. Essa análise será feita com a utilização de ferramentas de análise de soluções tecnológicas, pesquisas sobre publicações e enquetes com os profissionais envolvidos em todo processo de criação de soluções que devem seguir os preceitos da LGPD.

Para gerar o resultado esperado, será utilizada a metodologia mista [23], ou seja, elaboração de um questionário para avaliação do conhecimento das pessoas envolvidas no processo de desenvolvimento de ferramentas/soluções e/ou usuários sobre a temática da privacidade de dados (metodologia quantitativa) através da realização de testes práticos com foco na busca por vulnerabilidades (Investigativa) levantadas em cinco etapas.

1. A primeira etapa foi uma analise das legislacoes sobre a privacidade de dados;
2. A segunda etapa consistiu na conduçao de um survey com 43 profissionais de ICT que atuam em organizações públicas e privadas - o survey contem 21 questões que abrangem legislação e tecnologia;e
3. A terceira etapa foi uma analise técnica do Archivematica através de testes práticos, estáticos e dinâmicos com o auxilio de soluções open source para realizar uma varredura de vulnerabilidades em sistemas

Estas etapas serão utilizadas para responder as seguintes questões de pesquisa:

RQ.1. Qual o nível de segurança que o repositório arquivístico digital confiável de documentos digitais Archivematica proporciona aos usuários?

RQ.2 Quais são as diretrizes identificadas na LGPD que não estão contempladas e impactam o repositório arquivístico digital confiável?

RQ.3 Quais as diretrizes necessárias a um repositório arquivístico digital confiável para estar em conformidade com a LGPD?

Também será realizado um levantamento de informações do cotidiano dos usuários, através de uma pesquisa quantitativa, contendo perguntas objetivas que levarão em consideração o conhecimento de tecnologias no que tange segurança da informação e também questões quanto ao conhecimento dos profissionais das áreas de tecnologia em relação à legislação sobre a privacidade de dados, ou seja, a LGPD. Essa pesquisa é conhecida como *survey*, não se tratando

apenas de uma pesquisa, mas levando em consideração a forma como os dados serão tratados em conjunto com outras técnicas [24].

Figura 1.1: Etapas a Serem Executadas na Pesquisa

1.6 PUBLICAÇÕES RESULTANTES DESSA PESQUISA

1. Impactos da Lei de Proteção de Dados (LGPD) Brasileira no uso da Computação em Nuvem. Márcio Aurélio de Souza Fernandes, Fernando Gonçalves de Oliveira, Felipe Silva Ferraz, Daniel Alves da Silva, Edna Dias Canedo, Rafael Timóteo de Sousa Jr, Revista Ibérica de Sistemas e Tecnologias de Informação, Issue E42, pages: 374-385.

2. Estudo de Caso Sobre a Adequação das Empresas Brasileiras às novas Diretrizes da Segurança de Dados da LGPD.(Submetido a 19ª Conferencia Ibero Americana WWW/Internet 2022 (CIAWI 2022))

3. Proposta de Guia para Adequação de Repositórios Digitais Confiáveis à LGPD.(Submetido a 19ª Conferencia Ibero Americana WWW/Internet 2022 (CIAWI 2022))

1.7 ESTRUTURA DA DISSERTAÇÃO

Este trabalho está organizado em seis Capítulos além deste.

Capítulo 2: Referencial Teórico: apresenta os principais temas relacionados a essa pesquisa:

- Segurança da informação: complementa o item anterior, aprofundando um pouco a análise, verificando não somente as metodologias, mas também as soluções e/ou ferramentas complementares na segurança dos sistemas, as contramedidas como formas de mitigar os riscos.
- General Data Protection Regulation (GDPR): neste subitem, é apresentada a lei que deu origem a atual LGPD, suas diretrizes e aplicações.
- Lei Geral de Proteção de Dados (LGPD): neste subitem, são apresentadas a motivação da criação da lei, a derivação desta, bem como as principais diretrizes para preservação e proteção de dados pessoais.
- Documentos Digitais e Cadeia de Custodia: neste subitem, é explicado o que é um documento digital e o conceito de cadeia de custódia, que garante a autenticidade de um documento.
- Trabalhos Correlatos: este subitem do projeto apresenta trabalhos elaborados com temas semelhantes ao objeto deste trabalho, o detalhamento e a conclusão de cada um deles no que tange LGPD, Repositórios Confiáveis e Documentos Digitais.

Capítulo 3: Análise e Validação do Archivematica - visão geral sobre o conceito de repositório confiável para documentos digitais, com foco em soluções *open-source*, especificamente na ferramenta Archivematica", por ser a mais utilizada em órgãos públicos e privados no Brasil. Assim, essa ferramenta será utilizada para realização dos testes práticos.

- Fluxo Operacional do Archivematica: aqui é apresentado o conceito do Archivematica, a motivação de sua concepção e seus principais atributos, além de detalharmos o Archivematica desde sua arquitetura até a forma de utilização, o fluxo de trabalho do momento da criação do pacote até a forma de armazenamento.
- Plataforma de Disseminação: apresentamos neste subitem a forma que o Archivematica trabalha para apresentar as informações para o usuário.
- Validação do Archivematica: este subitem apresenta a metodologia e forma que foi feita a validação na ferramenta Archivematica de acordo com os parâmetros preestabelecidos.

Capítulo 4: Proposta de Uma Guia com as Diretrizes para Conformidade com a LGPD - será apresentado um guia de implementação para repositórios confiáveis, analisando as premissas da LGPD. Esse guia irá demonstrar, através de tabelas comparativas, se o repositório está em conformidade com as diretrizes da LGPD e como se adequar.

- *Survey*: neste subitem, é apresentando uma lista de perguntas feitas para 43 respondentes, e os resultados forneceram insumos para elaboração do guia.

- Análise Comparativa do Arcabouço Legal e Normativo: este subitem apresenta as normas que foram a base para criação do Archivematica e outras normas que devem ser seguidas.
- Concepção do Guia: este subitem apresenta o foco do trabalho, a elaboração do guia contento as diretrizes que devem ser seguidas para garantir a privacidade e segurança dos dados.

Capítulo 5: Prova de Conceito - foi avaliada a ferramenta de forma manual para detectar se, através do checklist do guia, o sistema seria considerado ou não compatível com a LGPD.

- Descrição do Ambiente: este capítulo apresenta a configuração do ambiente que foi montado para instalação do Archivematica.
- Aplicação do Guia: neste capítulo será apresenta a aplicação do guia no Archivematica e os resultados encontrados.

Capitulo 6: Discussão dos Resultados: apresenta uma análise geral do que foi pesquisado neste trabalho em cada tema e apresentação do resultado detalhado.

Capítulo 7: Conclusão - finalizaremos os estudos, relatando os seguintes itens: resultado dos estudos sobre a LGPD e suas principais diretrizes; o impacto de seus regramentos em repositórios confiáveis; e como fazer para que as soluções fiquem em conformidade com a Lei.

2 REFERENCIAL TEÓRICO

Para entendimento da legislação, trataremos das leis que deram origem à LGPD e sua finalidade, além de verificar qual a motivação e o resultado esperado da sua aplicação. A preocupação com dados pessoais sempre foi objeto de grandes discussões, uma vez que fraudes ocorrem à todo momento. A informatização dos dados pessoais ampliou as atividades de golpistas que utilizam tais dados tanto para pequenas fraudes quanto para a venda de banco de dados pessoais para quadrilhas especializadas em fraudes.

Segundo relatório da Sonicwall, o Brasil vem em uma crescente no ranking dos países que mais sofrem ataques cibernéticos, sendo, somente em 2020, mais de 3.800.000 (três milhões e oitocentos mil) ataques, colocando o Brasil em 9° lugar [25]. Diante do crescente aumento de ataques e vazamentos em todo mundo, os países europeus e americanos deram o ponta pé inicial para combater e normalizar ações para o enfrentamento ante a vulnerabilidade e impunidade, divulgando suas leis de proteção de dados pessoais.

Vale ressaltar que é preciso garantir que os dados estejam seguros e protegidos, proteção essa que se inicia no recebimento da informação, passando pela manutenção e finalizando no armazenamento. O gerenciamento da informação deve ser protegido e monitorado, para tanto, pessoas e tecnologias devem trabalhar de forma conjunta, ressaltando que a segurança é de responsabilidade humana, iniciando na conscientização dos envolvidos no processo e finalizando com medidas tecnológicas de segurança [26].

2.1 SEGURANÇA DA INFORMAÇÃO

Podemos considerar que segurança da informação é uma forma de proteger o ativo mais importante da empresa. Através de metodologias e ferramentas tecnológicas, a informação pode ser relacionada ao próprio dono da informação (informação pessoal) ou a alguma empresa ou entidade pública (informações corporativas) [27].

A segurança da informação segue 4 pilares essenciais: confidencialidade, integridade, disponibilidade e autenticidade. Vale ressaltar que, para os padrões internacionais, são considerados básicos apenas 3, conhecidas como tríade de segurança: Confidencialidade, Integridade e Disponibilidade [28]. Ainda que não façam parte da tríade explicitamente, outras duas características são extremamente importantes: Irretratabilidade e Autenticidade [29].

A segurança não é somente para pessoas, mas também para sistemas. Para garantir a proteção, existem vários métodos e ferramentas de segurança e/ou contramedidas. Essas medidas vão desde a tentativa de bloquear qualquer entrada, restritivas de acesso (firewalls, gerenciamento de rede, etc.) até mecanismos de contramedida, ou seja, que trabalham após a invasão [30].

Essas tentativas de invasões normalmente tem uma finalidade bem clara: roubar dados de usuários para realizar possíveis fraudes, danificar os dados, tomar o controle de um sistema ou negócio ou simplesmente bloquear algum serviço [31].

2.1.1 Contramedidas

Da mesma forma que um possível atacante procura por vulnerabilidades e brechas em sistemas ou redes, há no mercado ferramentas e métodos para evitar ou minimizar os riscos de ter os equipamentos invadidos ou infectados. Uma ferramenta muito utilizada, conhecida como Firewall, que trabalha na porta de entrada, funciona com a utilização de um conjunto de regras parametrizáveis sobre o que pode ou não trafegar pela rede [32].

Os anti-vírus também devem ser utilizados, pois já possuem uma lista de softwares maliciosos que são bloqueados automaticamente, além de analisar o computador para detectar qualquer anomalia. Outras formas de proteção é a atenção no momento de acessar sites, clicar em links, clicar em fotos ou baixar imagens ou vídeos, uma vez que o monitoramento é constante. Verificações básicas também devem ser postas em prática, como analisar se o site contém um cadeado na barra da URL para identificar se o site possui o mínimo de segurança [33]

2.1.2 Sistema de Gestão de Segurança da Informação

Sistema de Gestão de Segurança da Informação (SGSI) é um conceito que engloba diversos métodos de segurança, metodologias, boas práticas, ferramentas, etc. Para executar esse gerenciamento de forma eficaz, é utilizada, entre outras, uma norma internacional chamada ISO 27001 [34], que estabelece todas as diretrizes necessárias para minimizar os riscos de sucesso do atacante. Vale ressaltar o desafio cultural, pois profissionais se mostram bastante resistentes em seguir regras e/ou padrões. Por ser uma questão geral de uma corporação, requer o apoio da alta gestão, bem como o comprometimento de todos envolvidos. Para uma gestão de segurança eficiente, é necessário que o conjunto de itens seja respeitado, análise de riscos seja feita de forma minuciosa, gestão de mudança, gestão de processos de negócios, entre outros [35].

2.2 *GENERAL DATA PROTECTION REGULATION* (GDPR)

A *General Data Protection Regulation* (GDPR) [7], assim como várias outras leis e regulamentos, surgiu com base em estudos de leis e normas anteriores que, por sua vez, não atendiam de forma clara regras sobre a privacidade de dados, bem como a Carta dos Direitos Fundamentais da Europa conhecida como "A Carta"e o Tratado de Lisboa. Ambas já tratavam de dados pessoais, porém, com pouco detalhamento.

Uma preocupação importante para GPDR é o compartilhamento de informações entre os países, com uma finalidade bem específica e clara em casos de investigações, prevenções e/ou pos-

síveis punições. O desafio, então, seria como fazer essa troca de dados sem ofender o direito à privacidade das pessoas, mesmo que fosse em prol de um bem maior, limitando-se à tramitação na esfera judiciária ou policial para efeitos de investigação de suspeitos. Porém, mesmo em casos de suspeitos, a lei é clara quanto aos dados genéticos dos indivíduos, descrevendo como dados com alto risco de utilização para outros fins que não os citados na lei [36](GDPR,2016).

> Art. 39. [...] Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas. (GDPR, 2016)

Outro ponto importante dessa lei é quanto ao consentimento por parte do titular sobre a utilização de seus dados, tratamento e guarda, deixando muito claro quem são os responsáveis pelo dados, bem como a finalidade da utilização. Há casos em que a anuência do titular poderá ser ignorada, por exemplo, em razão e interesse público no que tange a saúde geral. Uma vez que o titular dá ciência ou consente a salvaguarda dos seus dados, ele precisa saber como consultar esses dados ou a forma de disponibilização desses. Assim sendo, a GDPR trouxe como diretriz a Transparência, onde diz que titular e o público a quem possa ter direito devem ter a informação de forma clara e de fácil acesso (artigo 58).

Como nada é eterno, pode chegar o dia em que o titular não queira mais que seus dados fiquem em posse de terceiros, o que essa lei chama de "direito a serem esquecidos". Esse direito poderá ser exigido a qualquer tempo pelo titular dos dados, porém vale ressaltar que esse direito poderá ser desconsiderado nos casos previstos em lei, citados no artigo 65 [36].

> Art. 65. ... "Exercício do direito de liberdade de expressão e informação; cumprimento de uma obrigação jurídica; exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento; interesse público no domínio da saúde pública; para fins de arquivo de interesse público; para fins de investigação científica ou histórica ou para fins estatísticos; ou para efeitos de declaração; exercício ou defesa de um direito num processo judicial. (GDPR, 2016)

Mesmo nos casos citados acima, é direito do titular saber quem é o responsável pelo tratamento de seus dados, bem como finalidade, período e destinação final. Respeitando sempre o direito da criança, a lei faz uma distinção entre os menores, ou seja, somente poderá dar o consentimento se a criança tiver idade igual ou superior a 16 anos, ou seja, o consentimento ou não

para menores de 16 anos é obrigatoriamente dos responsáveis legais, porém essa mesma lei deixa a cargo dos Estados Membros a disposição legal sobre o devido tratamento, desde que a idade da criança não seja inferior a 13 anos. De forma mais genérica, a GDPR prevê tratamento diferenciado para alguns dados, são eles: dados referentes à raça ou etnia; opinião política; convicções religiosas ou filosóficas; filiação sindical; tratamentos genéticos; dados biométricos; sobre saúde; vida sexual ou orientação sexual [36].

> É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (GDPR, 2016)

Independente do tratamento ou destinação, o GDPR prevê que o titular dos dados é o principal prejudicado em caso de má utilização, utilização indevida ou divulgação de seus dados, assim sendo, a lei deixa claro sobre a comunicação ao titular, forma e prazo de até 72 horas para notificação. Para que não fique a cargo das empresas fazer a notificação ao Estado, a lei prevê que haja uma unidade de controle principal que deva receber as notificações, analisar e gerar relatórios, entre outras atribuições.

2.3 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Assim como a GDPR, a Lei Geral de Proteção de Dados Pessoais (LGPD) [4] surgiu da necessidade de uma legislação mais detalhada e rígida sobre o tratamento de dados pessoais [37]. Já havia no ornamento jurídico brasileiro legislação que trata do assunto, porém, não de forma detalhada e específica, como o Marco Civil da Internet de 2014.

Partindo do princípio que a LGPD teve como lei base a GDPR [7], as diretrizes, princípios, nomenclaturas, responsáveis e sanções são muito próximas da europeia. Para evitar redundância para falar sobre diretrizes já tratadas na GDPR e que a LGPD aderiu exatamente igual, nesta seção do trabalho falaremos sobre as principais diferenças ou diretrizes que não estão na legislação europeia.

A legislação estabelece ainda que as organizações devem adotar políticas e metodologias para prevenir a ocorrência de danos, de qualquer espécie, aos dados tratados, devendo comprovar que atendem tais requisitos [4]. Algumas tecnologias e metodologias serão necessárias para viabilizar, garantir e prover a segurança necessária, de acordo com o contexto moderno de proteção de dados, para a aplicação e aderência ao disposto na LGPD; entre elas, podemos citar:

- *Identity and Access Management* (IAM) - solução de Gestão de Identidades e Acesso, ou seja, garantir que apenas as pessoas credencias e autorizadas irão acessar a informação de acordo com o grau de restrição, autorização essa que pode variar desde uma simples consulta

até o backup e cópia de arquivos [38].

- *Master Data Management* (MDM): gestão dos dados utilizados como referência ou base para uma visão única, contendo todos os dados necessários para a gestão de negócios, infraestrutura, tecnologia, financeira, entre outras [39].
- *Privacy by Design e Privacy by Default*: consiste na incorporação de salvaguardas de privacidade e dados pessoais em todos os projetos desenvolvidos exatamente antes, ou seja, agindo como forma de prevenção, e não de tratamento da ação de alguma falha. A proteção da privacidade, de ponta a ponta, está no cerne do desenvolvimento de software [40].

Essas soluções ou metodologias podem evitar ou minimizar os riscos, o que se torna muito necessário devido ao fato da nova lei garantir ao consumidor/usuário, de um lado, uma série de direitos sobre suas informações e, do outro, uma série de deveres para as organizações, no que tange a coleta, uso, correção, eliminação, até mesmo a portabilidade de dados [4],[41], [42],[37].

Em relação ao tratamento dos dados pessoais, a LGPD repete o já mencionado na lei europeia, mas acrescenta algumas coisas importantes, por exemplo, no tratante a consentimento do titular, menciona o "tratamento mediante vício de consentimento", que se define com algo que o agente foi levado a fazer indiretamente contra sua vontade, seja por um erro de percepção da realidade ou mesmo por ignorância sobre o assunto [37].

> Art. 171. Além dos casos expressamente declarados na lei, é anulável o negócio jurídico:
>
> I - por incapacidade relativa do agente;
>
> II - por vício resultante de erro, dolo, coação, estado de perigo, lesão ou fraude contra credores (LGPD, 2018).

Diferentemente da GDPR, que define explicitamente a idade para consentimento por parte de crianças, a LGPD diz apenas que poderá ser consentido por apenas 1 dos pais ou responsável legal. Em relação às penalidades administrativas, a LGPD descreve a punibilidade monetária em percentual e valor máximo, sendo até 2% do faturamento no último exercício, não podendo ultrapassar R$ 50.000.000,00 (cinquenta milhões de reais), por infração. Porém, ainda que a devida lei regre de forma clara, deixa também algumas possíveis brechas para a não aplicação das sanções, entre elas: "a boa fé do infrator" e "a pronta adoção de medidas corretivas", 2 casos em que é possível a exclusão de punibilidade [4].

No que se refere à autoridade de fiscalização, normalização e sanções, no Brasil foi criada a Autoridade Nacional de Proteção de Dados (ANPD), vinculada diretamente à Presidência da República, cuja composição difere um pouco dos demais cargos da Administração Pública Federal, não havendo prazo mínimo ou máximo para o mandato dos membros do conselho. Vale ressaltar que essa regra não se aplica aos demais representantes do conselho, somente para os membros, ou seja, os demais terão mandato de 2 (dois) anos [4].

Dada a visão geral, para aprofundamento sobre o tema do trabalho, nos restringiremos a tratar do tópico "privacidade de dados", tratado em diversos pontos da LGPD. A privacidade de dados tem sido alvo de estudiosos, tanto no que tange o que é a privacidade em si, quanto o que é ou não privado. A Privacidade é um direito já protegido na própria Constituição Federal, no artigo 5° inciso X,[43] que, em resumo, determina que os dados são pessoais e invioláveis, ou seja, é facultado ao titular das informações dar ou não autorização para qualquer uso por parte de terceiros, inclusive sob risco de pena para quem fizer o uso de tais informações sem prévia autorização [4].

> Art. 5º - CF - Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (CF, 1988)

Seguindo o princípio da Constituição que a privacidade é algo inviolável, pela lógica, os dados fazem parte de sua privacidade. Para tanto, há a necessidade de se falar sobre quais são os dados, como devem ser tratados, armazenados e, se for o caso, até mesmo serem excluídos. Logo no início da LGPD, é definido quais são os dados pessoais, separando-os em dois tipos: "dados pessoais", que são dados que poderiam identificar ou deixar identificável o individuo; e "dados pessoais sensíveis", que pode gerar algum transtorno ao individuo em vários âmbitos, como racismo ou qualquer outra forma de segregação ou tratamento discriminatório.

> Art. 5º - LGPD - Para os fins desta Lei, considera-se:
>
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (LGPD, 2018)

Para efeito geral, trataremos dados pessoais e dados pessoais sensíveis apenas como "dados do titular". Sabendo que os dados pessoais são privados, a LGPD trouxe algumas diretrizes sobre o tratamento, armazenamento e descarte. O tratamento deverá ter uma finalidade específica, clara e não poderá ser feito sem o consentimento do titular dos dados, salvo em casos específicos da lei. Define-se como tratamento toda operação descrita do paragrafo 5°, inciso X da LGPD, bem como define, no inciso VII do mesmo artigo, o operador como responsável pelo tratamento dos dados pessoais em nome do controlador [4].

> Art. 5º - LGPD - Para os fins desta Lei, considera-se:

> [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (LGPD, 2018)

O armazenamento pode ser definido como todo e qualquer banco de dados, que pode ser físico ou lógico para guarda de dados pessoais do titular, independente do local onde fiquem guardados e a forma, por completo ou dividido, assim definido no inciso IV do art. 5° da LGPD [4]. A nomenclatura para o local pode ser variada de acordo com a área, podendo ser nomeada como: Banco de dados, Repositórios, Arquivos, etc. Para o trabalho em questão, utilizaremos o termo repositório.

2.4 DOCUMENTOS DIGITAIS E CADEIA DE CUSTÓDIA

Os documentos arquivísticos, sejam em meio analógico ou digital, são importantes fontes de informações e meios para que se cumpram as iniciativas de transparência governamental. Nesse sentido, precisam ser armazenados e preservados com critérios que visem à garantia de suas características de confiabilidade, autenticidade e acessibilidade.

A cadeia de custódia consiste em um conjunto de passos que promovem a garantia que uma evidência foi coletada da forma correta, ou seja, que não sofreu alteração no momento da coleta, no transporte/armazenamento e no momento da consulta e/ou entrega. Como toda e qualquer evidência que é utilizada, seja ela física ou digital, deve seguir quatro premissas para que seja confiável: rastreabilidade, verificabilidade, autenticidade e segurança [44]. O modelo *Open Archival Information System* (OAIS) [45] veio para promover a garantia da cadeia de custódia cumprindo todos os requisitos citados acima.[46].

2.4.1 Modelo *Open Archival Information System* (OAIS)

O Modelo *Open Archival Information System* (OAIS) nasceu de uma iniciativa conjunta do *Consultative Commitee for Space Data Systems* (CCSDS) da NASA com a *International Organization for Standardization* (ISO), com o objetivo inicial de estabelecer normas capazes de regular o armazenamento em longo prazo de informações digitais produzidas no âmbito de missões espaciais. Trata-se de um modelo complexo que tem como finalidade apresentar como deve ser a preservação da informação para arquivos permanentes [47]. Os resultados desse estudo motraram a versão inicial lançada em 1999, com mais uma evolução em 2002, antes de dar origem a norma ISO 14721:2003, que foi substituída em pela ISO 14721:2012 [48].

De acordo com esse modelo, as funcionalidades de um repositório devem estar organizadas

em seis grandes grupos: Admissão (*ingest*); Armazenamento; Gestão de dados; Planejamento da preservação; Administração; e Acesso. A Figura 2.1 ilustra o modelo conceitual do OAIS [2], com as funcionalidades, agentes e pacotes de informação.

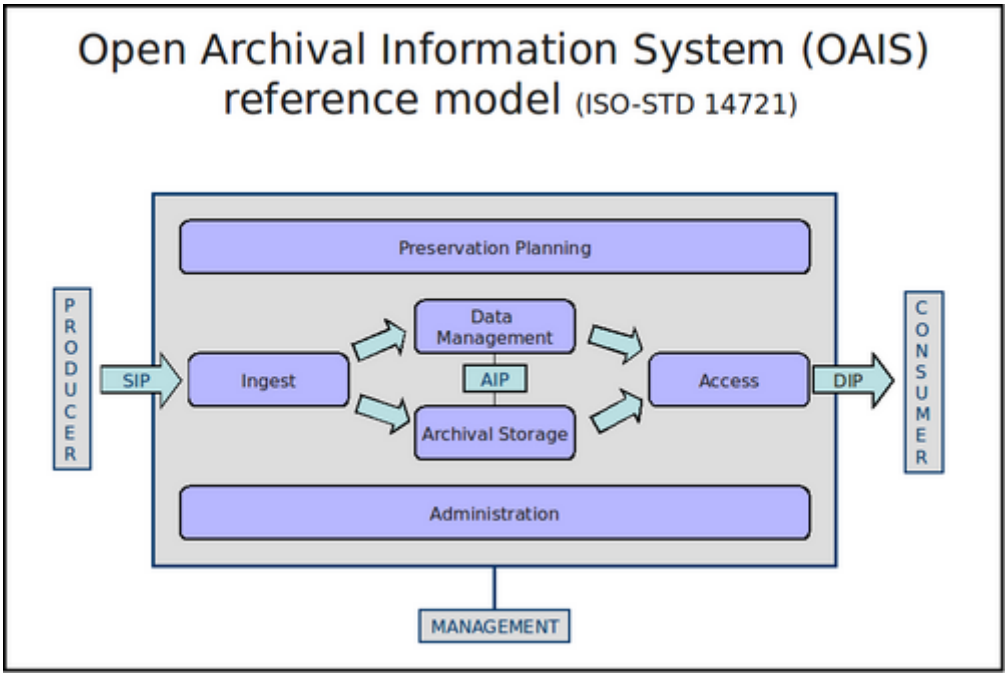


Figura 2.1: Modelo OAIS [2]

De acordo com Rocha [49], as funcionalidades de cada grupo são detalhadas no modelo e podem ser acessadas por três tipos de agentes: Produtores (pessoas ou sistemas que depositam os objetos digitais no repositório); Consumidores (pessoas ou sistemas que interagem com o OAIS para acessar os objetos digitais); e Administradores (responsáveis pelo estabelecimento das políticas e pela gestão dos objetos digitais preservados).

O modelo OAIS prevê a criação de recipientes conceituais chamados de pacotes, os quais armazenam a informação de conteúdo (o documento em si), informação de descrição de preservação (metadados necessários para apoiar a preservação e acesso do documento no longo prazo), bem como informações descritivas do pacote – metadados descritivos que possibilitam a localização do pacote no repositório [49]. Esses metadados estão previstos em normas de descrição arquivística, como a ISAD (G): *General International Standard Archival Description* [50] e a NOBRADE: Norma Brasileira de Descrição Arquivística [51].

2.4.2 Repositórios Seguros

Um Repositório Arquivístico Digital Confiável (RDC-Arq) é um local de armazenamento que deve seguir algumas regras específicas, bem como: preservar a autenticidade dos arquivos digitais, fornecer e disponibilizar a quem for por direito [52].

O e-ARQ Brasil é um modelo criado pelo Conarq o qual contém especificação de requisi-

tos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade. Essas especificações estão contidas no documento na ISO 16363:2012 [1] e no TRAC (*Trustworthy Repository Audit e Certification: Criteria and Checklist*) [5].

O TRAC é o conjunto de requisitos utilizado para auditar um repositório na validação se é ou não um Repositório Arquivístico Digital Confiável, tendo como referência o modelo OAIS e o padrão ISO 14721:2012 [53]. Entre as várias diretrizes de governança, segurança e análise de riscos, podemos citar: Necessidade de controle de acesso; Garantia de integridade da informação em cada etapa do seu registro (coleta, rastreabilidade e disponibilidade); Compartilhamento de informações com demais organizações; Backups; etc.

Na busca por soluções que viabilizassem a manutenção dos documentos arquivísticos digitais acessíveis e confiáveis por longo prazo, foram consideradas as soluções *Open Source* consolidadas, além de pesquisa a instituições nacionais que já utilizam ou que estão em fase de implantação de Repositórios Arquivísticos Digitais Confiáveis. Como resultado, obteve-se cinco soluções, a saber:

- Fedora: software *Open Source* que fornece um repositório de livre acesso por meio de ampla infraestrutura para o armazenamento, gestão e disseminação de objetos digitais, incluindo o relacionamento entre eles [54].
- EPrints: software *Open Source* compreendido como uma das mais usadas plataformas para repositórios institucionais. É classificado como o modo mais fácil e rápido de criar repositórios de acesso livre para base de dados científica [54].
- DSpace: software *Open Source* que fornece um repositório com funções de captura, distribuição e preservação da produção intelectual e científica, dando visibilidade e garantindo acessibilidade no decorrer do tempo [54].
- Archivematica: software *Open Source* que fornece um sistema de preservação digital para processamento e armazenamento de objetos digitais no longo prazo, fundamentado em estratégias de preservação digital e baseado no modelo OAIS [55].
- RODA: software *open source* que disponibiliza um sistema de repositório digital criado para recolher, armazenar, preservar e dar acesso continuado ao patrimônio arquivístico digital no longo prazo. Foi concebido com base no modelo de referência OAIS [55].

As ferramentas Fedora, EPrints e DSpace são utilizadas predominantemente para disseminação do conteúdo digital, produzido para pesquisa (produção intelectual e acadêmica). Lampert [55] destacou que a maioria dessas instalações poderia ser classificada como repositório institucional, pois geralmente é fornecida por um instituto de pesquisa, universidade ou departamento para uso de seus pesquisadores. No entanto, também podem ser considerados repositórios temáticos, por exemplo, na implementação de repositórios para banco de teses e dissertações. Essas

três soluções foram construídas dentro da filosofia da Iniciativa de Arquivos Abertos (OAI) e do Movimento de Acesso Aberto à Informação Científica (*Open Access*), os quais incentivam a publicação na web totalmente gerenciada pelo pesquisador (auto arquivamento), utilizam tecnologia aberta e podem ser acessados por diversos provedores de serviços, disponíveis em nível nacional e internacional [56]. Em outras palavras, conforme Leite [57]: “os repositórios permitem reunir, preservar, dar acesso e disseminar boa parte do conhecimento da instituição, aumentando a visibilidade da sua produção científica”.

De posse dessas informações, percebeu-se que as únicas ferramentas que implementam o modelo OAIS, pré-requisito para a implementação de repositórios arquivísticos digitais confiáveis, conforme a Resolução nº 39 no Conarq [15], são o Archivematica e o RODA. Além disso, esses repositórios destacaram-se por serem soluções voltadas essencialmente para preservação de documentos arquivísticos.

A vertente ou variação de repositório digital foco desse trabalho é o "Repositório Arquivístico Digital Confiável"ou "Repositório Digital Seguro", que leva em consideração a garantia de segurança, primando pela confidencialidade, autenticidade e preservação de documentos armazenados de forma digital [58]. Para efeito de estudo específico e mais detalhado, utilizaremos o Repositório Arquivístico Digital Confiável chamado de Archivematica [59], a escolha se deve ao fato do governo federal utilizar esse repositório em diversos órgão, como Senado Federal, Superior Tribunal de Justiça (STJ) entre outros.

2.4.3 *Trusted Digital Repositories: Attributes and Responsibilities* - TRAC

O Trac Surgiu de uma necessidade comum à todos os responsáveis por manter um repositório de arquivos, uma vez que, até então, não havia uma forma de mensurar o nível de segurança ou confiabilidade de ferramenta para considerar ou não como sendo segura. Para tanto, foi necessário analisar as principais normas que já tratavam do assunto, como: *Open Archival Information System (OAIS)* e a ISO 14721. O TRAC tem a função de avaliar repositórios para armazenamentos de arquivos digitais e com uma base de uma série de critérios, definir se ele pode ou não ser considerado confiável.

A primeira versão contendo uma estrutura mais sólida sobre os itens para análise, o *Trusted Digital Repositories: Attributes and Responsibilities (TDR)*, lançado em 2002, foi amplamente aceito e utilizado junto a outras metodologias. Através de uma força tarefa contando com várias entidades focadas para desenvolvimento de um documento capaz de identificar os melhores e mais seguros critérios, foi lançada a versão 1.0 do *Criteria for Measuring Trustworthiness of Digital Repositories & Archives: an Audit & Certification Checklist*, que define minimamente os itens básicos que devem ser seguidos em formato de um checklist.

O checklist é constituído de 3 seções divididas por áreas de atuação, a saber:

- A. *Organizational infrastructure*.

- B. *Digital object management*.
- C. *Technologies, technical infrastructure, and security*.

O TRAC inicia com a Seção A - Infraestrutura Organizacional, que trata de assuntos voltados para a parte de responsabilidades do checklist, bem como: planejamento, planos, políticas, documentação e procedimentos. Para melhor detalhamento, ele foi dividido em 5 itens, a saber:

- A1. Governança e viabilidade organizacional (Tabela 2.1.
- A2. Estrutura organizacional e pessoal (Tabela 2.1.).
- A3. Responsabilidade processual e estrutura política (Tabela 2.1.).
- A4. Sustentabilidade financeira (Tabela 2.1.).
- A5. Contratos, licenças e responsabilidades(Tabela 2.1.).

Continuando o checklist, o TRAC possui a Seção B - Gerenciamento de Objetos Digitais, conforme apresentado na Tabela 2.2, que trata da forma como os dados serão tratados, desde a forma de inserção na solução até a forma de armazenamento. Assim como na seção A, por se tratar de uma lista com vários critérios, foi dividida em subitens, a saber:

- B1: A fase inicial de ingestão que aborda a aquisição de conteúdo digital (Tabela 2.2).
- B2: A fase final de ingestão que coloca o conteúdo digital adquirido nos formulários, geralmente chamados de Pacotes de Informações de Arquivo (AIPs), usados pelo repositório para preservação de longo prazo (Tabela 2.2).
- B3: Estratégias de preservação atuais, sólidas e documentadas, juntamente com mecanismos para mantê-las atualizadas diante de ambientes técnicos em mudança.
- B4: Condições mínimas para a preservação de AIPs a longo prazo (Tabela 2.2).
- B5: Metadados de nível mínimo para permitir que objetos digitais sejam localizados e gerenciados dentro do sistema (Tabela 2.2).
- B6: A capacidade do repositório de produzir e divulgar versões precisas e autênticas dos objetos digitais (Tabela 2.2).

Por último, mas não menos importante, a lista de auditoria apresenta a Seção C - Tecnologias, Infraestrutura Técnica e Segurança, conforme apresentado na Tabela 2.3. De forma mais genérica, são apresentados os requisitos mínimos de segurança dos repositórios para cumprir o objetivo na gestão dos documentos digitais. A ISO 17999, que trata de boas práticas e segurança da informação, foi utilizada como referência para a criação desse checklist, logo, se o repositório foi validado a partir dessa ISO, provavelmente já contempla boa parte dos itens do TRAC. Igualmente as seções anteriores, esta seção foi subdividida para facilitar o entendimento e a análise, a saber:

- C1: Requisitos gerais de infraestrutura do sistema (Tabela 2.3).
- C2: Tecnologias apropriadas, com base nos requisitos de infraestrutura do sistema, com critérios adicionais especificando as tecnologias de uso e estratégias apropriadas para o repositório designado comunidade(s) (Tabela 2.3).
- C3: Segurança – desde sistemas de TI, como servidores, firewalls ou roteadores, até sistemas de proteção contra incêndio e detecção de inundações e sistemas que envolvem ações de pessoas (Tabela 2.3).

Tabela 2.1: TRAC - Seção A - Infraestrutura Organizacional

Trustworthy Repositories Audit & Certification: Criteria Checklist	
Organização:	
Seção:	A: Infraestrutura Organizacional
Aspecto:	A1. Governança e viabilidade organizacional
Critério	
A1.1 O repositório tem uma declaração de missão que reflete um compromisso com a retenção, gerenciamento e acesso a longo prazo às informações digitais.	
A1.2 O repositório tem um plano de sucessão formal adequado, planos de contingência e/ou acordos de custódia em vigor no caso de o repositório deixar de operar ou a instituição governante ou de financiamento alterar substancialmente seu escopo.	
Aspecto:	A2. Estrutura organizacional e pessoal
Critério	
A2.1 O repositório identificou e estabeleceu as funções que precisa desempenhar e nomeou funcionários com habilidades e experiência adequadas para cumprir essas funções.	
A2.2 O repositório tem o número apropriado de funcionários para dar suporte a todas as funções e serviços.	
A2.3 O repositório possui um programa ativo de desenvolvimento profissional que fornece à equipe oportunidades de desenvolvimento de habilidades e conhecimentos.	
Aspecto:	A3. Responsabilidade processual e estrutura política (documentação)
Critério	
A3.1 O repositório definiu sua (s) comunidade (s) designada (s) e base (s) de conhecimento (s) associada (s) e possui definições e políticas publicamente acessíveis para ditar como seus requisitos de serviço de preservação serão atendidos.	
A3.2 O repositório possui procedimentos e políticas em vigor e mecanismos para sua revisão, atualização e desenvolvimento à medida que o repositório cresce e a tecnologia e a prática da comunidade evoluem. Requisitos de serviço de preservação serão atendidos.	
A3.3 O repositório mantém políticas escritas que especificam a natureza de quaisquer permissões legais necessárias para preservar o conteúdo digital ao longo do tempo, e o repositório pode demonstrar que essas permissões foram adquiridas quando necessário.	

A3.4 O repositório está comprometido com a revisão e avaliação formal e periódica para garantir a capacidade de resposta aos desenvolvimentos tecnológicos e requisitos em evolução.
A3.5 O repositório tem políticas e procedimentos para garantir que o feedback dos produtores e usuários seja buscado e tratado ao longo do tempo.
A3.6 O repositório tem um histórico documentado das mudanças em suas operações, procedimentos, software e hardware que, quando apropriado, está vinculado a estratégias de preservação relevantes e descreve os efeitos potenciais na preservação de conteúdo digital.
A3.7 Repositório compromete-se com a transparência e responsabilidade em todas as ações de suporte à operação e gestão do repositório, especialmente aquelas que afetam a preservação do conteúdo digital ao longo do tempo.
A3.8 O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.
A3.9 O repositório se compromete com um cronograma regular de autoavaliação e certificação e, se certificado, compromete-se a notificar os organismos de certificação de mudanças operacionais que irão alterar ou anular seu status de certificação.
Aspecto: | A4. Sustentabilidade financeira
Critério
A4.1 O repositório tem processos de planejamento de negócios de curto e longo prazo em vigor para sustentar o repositório ao longo do tempo.
A4.2 O repositório possui processos para revisar e ajustar planos de negócios pelo menos uma vez por ano.
A4.3 As práticas e procedimentos financeiros do repositório são transparentes, em conformidade com os padrões e práticas contábeis relevantes e auditados por terceiros de acordo com os requisitos legais territoriais.
A4.4 O repositório tem o compromisso contínuo de analisar e relatar riscos, benefícios, investimentos e despesas (incluindo ativos, licenças e passivos).
A4.5 O repositório se compromete a monitorar e preencher as lacunas de financiamento.
Aspecto: | A5. Contratos, licenças e responsabilidades
Critério
A5.1 Se o repositório gerencia, preserva e/ou fornece acesso a materiais digitais em nome de outra organização, ele tem e mantém contratos ou acordos de depósito apropriados.
A5.2 Os contratos de repositório ou acordos de depósito devem especificar e transferir todos os direitos de preservação necessários, e esses direitos transferidos devem ser documentados.
A5.3 O repositório especificou todos os aspectos apropriados de aquisição, manutenção, acesso e retirada em acordos escritos com depositantes e outras partes relevantes.
A5.4 O repositório rastreia e gerencia os direitos de propriedade intelectual e as restrições sobre o uso do conteúdo do repositório conforme exigido pelo acordo de depósito, contrato

ou licença.
A5.5 Se o repositório ingere conteúdo digital com propriedades/direitos pouco claros, existem políticas em vigor para lidar com a responsabilidade e os desafios relacionados a esses direitos.

Tabela 2.2: Gerenciamento de Objetos Digitais.

Trustworthy Repositories Audit & Certification: Criteria Checklist	
Organização:	
Seção:	B. Gerenciamento de objetos digitais
Aspecto:	B1. Ingest: aquisição de conteúdo
Critério	
B1.1 Repositório identifica propriedades que irá preservar para objetos digitais.	
B1.2 Repositório especifica claramente as informações que precisam ser associadas ao material digital no momento de seu depósito (isto é, SIP).	
B1.3 Repositório tem mecanismos para autenticar a fonte de todos os materiais.	
B1.4 O processo de ingestão do repositório verifica cada objeto enviado (ou seja, SIP) quanto à integridade e exatidão, conforme especificado em B1.2.	
B1.5 Repositório obtém controle físico suficiente sobre os objetos digitais para preservá-los.	
B1.6 O repositório fornece ao produtor/depositante respostas apropriadas em pontos predefinidos durante os processos de ingestão.	
B1.7 O repositório pode demonstrar quando a responsabilidade pela preservação é formalmente aceita para o conteúdo dos objetos de dados enviados (ou seja, SIPs).	
B1.8 Repositório tem registros contemporâneos de ações e processos de administração que são relevantes para a preservação (Ingestão: aquisição de conteúdo).	
Aspecto:	B2. Ingest: criação do pacote de arquivo
Critério	
B2.1 Repositório tem uma definição escrita identificável para cada AIP ou classe de informação preservada pelo repositório.	
B2.2 Repositório tem uma definição de cada AIP (ou classe) que é adequada para atender às necessidades de preservação de longo prazo.	
B2.3 Repositório tem uma descrição de como AIPs são construídos a partir de SIPs.	
B2.4 O repositório pode demonstrar que todos os objetos enviados (ou seja, SIPs) são aceitos como um todo ou como parte de um eventual objeto de arquivo (ou seja, AIP), ou de outra forma descartados de forma registrada.	
B2.5 O repositório tem e usa uma convenção de nomenclatura que gera identificadores visíveis, persistentes e únicos para todos os objetos arquivados (ou seja, AIPs).	
B2.6 Se identificadores exclusivos forem associados a SIPs antes da ingestão, o repositório preserva os identificadores de uma maneira que mantém uma associação persistente com o objeto arquivado resultante (por exemplo, AIP).	

B2.7 O repositório demonstra que tem acesso às ferramentas e recursos necessários para estabelecer informações de representação autoritativas dos objetos digitais que contém.	
B2.8 Repositório registra informações de representação (incluindo formatos) ingeridos.	
B2.9 Repositório tem processos documentados para adquirir metadados de preservação (isto é, PDI) para suas Informações de Conteúdo associadas e adquire metadados de preservação de acordo com os processos documentados. O repositório deve manter a documentação visível sobre como o repositório adquire e gerencia Informações de Descrição de Preservação (PDI).	
B2.10 Repositório tem um processo documentado para testar a compreensibilidade do conteúdo da informação e trazer o conteúdo da informação até o nível acordado de compreensibilidade.	
B2.11 O repositório verifica cada AIP quanto à integridade e exatidão no ponto em que é gerado.	
B2.12 O repositório fornece um mecanismo independente para auditoria da integridade da coleção/conteúdo do repositório.	
B2.13 O repositório possui registros contemporâneos de ações e processos de administração relevantes para a preservação (criação de AIP).	
Aspecto:	B3. Planejamento de preservação
Critério	
B3.1 O repositório tem estratégias de preservação documentadas.	
B3.2 O repositório possui mecanismos para monitoramento e notificação quando as Informações de Representação (incluindo formatos) se aproximam da obsolescência ou não são mais viáveis.	
B3.3 O repositório possui mecanismos para alterar seus planos de preservação como resultado de suas atividades de monitoramento.	
B3.4 O repositório pode fornecer evidências da eficácia de seu planejamento de preservação.	
Aspecto:	B4. Planejamento de Preservação
Critério	
B4.1 Repositório emprega estratégias de preservação documentadas.	
B4.2 O repositório implementa/responde às estratégias de armazenamento e migração de objetos de arquivamento (isto é, AIP).	
B4.3 Repositório preserva as informações de conteúdo de objetos de arquivo (ou seja, AIPs).	
B4.4 O repositório monitora ativamente a integridade dos objetos de arquivo (ou seja, AIPs).	
B4.5 Repositório tem registros contemporâneos de ações e processos de administração que são relevantes para a preservação (Armazenamento em Arquivo).	
Aspecto:	B5. Gestão de informação
Critério	
B5.1 O repositório articula os requisitos mínimos de metadados para permitir que a (s) comunidade (s) designada (s) descubram e identifiquem o material de interesse.	
B5.2 O repositório captura ou cria metadados descritivos mínimos e garante que está associado ao objeto arquivado (ou seja, AIP).	
B5.3 O repositório pode demonstrar que a integridade referencial é criada entre todos os objetos	

arquivados (ou seja, AIPs) e as informações descritivas associadas.
B5.4 O repositório pode demonstrar que a integridade referencial é mantida entre todos os objetos arquivados (ou seja, AIPs) e as informações descritivas associadas.
Aspecto: | B6. Gerenciamento de acesso
Critério
B6.1 O repositório documenta e comunica à (s) sua (s) comunidade (s) designada (s) quais opções de acesso e entrega estão disponíveis.
B6.2 O repositório implementou uma política para registrar todas as ações de acesso (incluindo solicitações, pedidos, etc.) que atendam aos requisitos do repositório e dos produtores/ depositantes de informações.
B6.3 Repositório garante que os acordos aplicáveis às condições de acesso sejam cumpridos.
B6.4 O repositório documentou e implementou políticas de acesso (regras de autorização, requisitos de autenticação) consistentes com os acordos de depósito para objetos armazenados.
B6.5 O sistema de gerenciamento de acesso ao repositório implementa totalmente a política de acesso.
B6.6 O repositório registra todas as falhas de gerenciamento de acesso e a equipe analisa os incidentes de "negação de acesso" inadequados.
B6.7 O repositório pode demonstrar que o processo que gera o (s) objeto (s) digital (is) solicitado (s) (ou seja, DIP) é concluído em relação à solicitação.
B6.8 O repositório pode demonstrar que o processo que gera o (s) objeto (s) digital (is) solicitado (s) (ou seja, DIP) está correto em relação à solicitação.
B6.9 Repositório demonstra que todas as solicitações de acesso resultam em uma resposta de aceitação ou rejeição.
B6.10 Repositório permite a disseminação de cópias autênticas do original ou objetos rastreáveis aos originais.

Tabela 2.3: Tecnologias, Infraestrutura e Segurança.

Trustworthy Repositories Audit & Certification: Criteria Checklist	
Organização:	
Seção:	C. Tecnologias, infraestrutura técnica e segurança
Aspecto:	C1. Infraestrutura do sistema
Critério	
C1.1 Funções de repositório em sistemas operacionais bem suportados e outros softwares de infraestrutura central.	
C1.2 Repositório garante que tem suporte de hardware e software adequado para funcionalidade de backup suficiente para os serviços do repositório e para os dados mantidos, por exemplo, metadados associados aos controles de acesso, conteúdo principal do repositório.	
C1.3 Repositório gerencia o número e a localização de cópias de todos os objetos digitais.	
C1.4 O repositório possui mecanismos para garantir que quaisquer/várias cópias de objetos digitais	

sejam sincronizadas.
C1.5 O repositório tem mecanismos eficazes para detectar corrupção ou perda de bits.
C1.6 O repositório relata à sua administração todos os incidentes de corrupção ou perda de dados e as medidas tomadas para reparar/substituir dados corrompidos ou perdidos.
C1.7 O repositório tem processos definidos para mídia de armazenamento e/ou mudança de hardware (por exemplo, atualização, migração).
C1.8 O repositório tem um processo de gerenciamento de mudanças documentado que identifica mudanças em processos críticos que potencialmente afetam a capacidade do repositório de cumprir com suas responsabilidades obrigatórias.
C1.9 Repositório tem um processo para testar o efeito de mudanças críticas no sistema.
C1.10 O repositório tem um processo para reagir à disponibilidade de novas atualizações de segurança de software com base em uma avaliação de risco-benefício.
Aspecto: | C2. Tecnologias apropriadas
Critério
C2.1 O repositório tem tecnologias de hardware apropriadas para os serviços que fornece à (s) sua (s) comunidade (s) designada (s) e tem procedimentos em vigor para receber e monitorar notificações e avaliar quando mudanças na tecnologia de hardware são necessárias.
C2.2 O repositório tem tecnologias de software apropriadas para os serviços que fornece à (s) sua (s) comunidade (s) designada (s) e tem procedimentos em vigor para receber e monitorar notificações e avaliar quando mudanças na tecnologia de software são necessárias.
Aspecto: | C3. Segurança
Critério
C3.1 Repositório mantém uma análise sistemática de fatores como dados, sistemas, pessoal, planta física e necessidades de segurança.
C3.2 O repositório implementou controles para atender adequadamente a cada uma das necessidades de segurança definidas de software com base em uma avaliação de risco-benefício.
C3.3 A equipe do repositório definiu funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema.
C3.4 O repositório possui planos escritos de preparação e recuperação para desastres, incluindo pelo menos um backup externo de todas as informações preservadas junto com uma cópia externa do (s) plano (s) de recuperação.

2.5 TRABALHOS CORRELATOS

Apesar dos temas em questão (LGPD e Repositórios Digitais - RDs) serem assuntos relativamente novos, já existem alguns estudos na área, muito mais na temática dos repositórios do que na LGPD. Porém, há alguns estudos, por exemplo, Almeida *et al*. [60] que realizaram um estudo sobre os bancos de dados mais utilizados no mercado, seja por entidades públicas ou privadas. Os autores concluíram que os bancos de dados mais utilizadas são o ORACLE e a Microsoft.

Contudo, apesar das soluções serem robustas e estarem em constante atualização e melhora, não são aptas ou adequadas para conformidade da LGPD, citando algumas diretrizes da lei que não são contempladas como deveriam por essas soluções, tem-se por exemplo: "Sigilo, integridade, tempo de vida, anonimato, escopo de uso pela aplicação e a separação da função dos dados."

Biase e Aguilera [61] realizaram um estudo relacionado à privacidade e ao tratamento de dados, afirmando que, por parte de agentes privados e públicos, há uma discrepância na clareza no que se pode ou não fazer por ambos. Os autores chamaram atenção para a falta de clareza no tratamento das informações por parte do poder público, o que pode gerar dúvidas quanto à correta interpretação e aplicação dos dispositivos. Chamam ainda atenção quanto ao direito público que trata a LGPD, uma vez que a lei iguala o agente particular que esteja a serviço do setor público. É preciso, na visão dos autores, que fique claro a motivação e a forma do tratamento desses dados por tais atores. Outro fator importante por eles relatado é quanto ao compartilhamento de dados pelo setor público segundo à LGPD, pois sites governamentais não são padronizados, bem como a tecnologia utilizada por cada órgão, o que pode colocar em risco a privacidade dos dados. Por fim, os autores concluem que o tratamento, manipulação e compartilhamento dos dados ainda não possuem um regramento direto na lei.

Magacho e Trento [62] mencionaram 3 fatores que explicitam a necessidade de adequação à LGPD, um deles é como os dados sempre foram coletados e tratados, normalmente de forma frágil e desordenada, inclusive fazendo um compartilhamento desses dados sem nenhum tipo de critério. Os autores mencionam ainda o fator da motivação do tratamento, enfatizando que a LGPD veio para manter o controle da coleta. Porém, a lei precisa garantir a forma correta, e não a negação de qualquer coleta, uma vez que vários ramos de atividades necessitam da coleta de dados. E, por último, os autores explicitam que a adequação precisa ser feita de forma a deixar claros os regramentos, não dando chance para interpretações que possam ir contra a legislação e/ou preceitos da segurança e privacidade dos dados.

Aguiar [63] apresentou um conjunto de requisitos mínimos que compõem a arquitetura da informação, camada de metadados para organização, representação e recuperação da informação, sistemas de organização do conhecimento e aspectos fundamentais para subsidiar a gestão da preservação digital a longo prazo. O autor utilizou a plataforma de disseminação DSpace integrada com o Archivematica para prover o armazenamento, organização, representação, disseminação e preservação de documentos destinados à guarda permanente para constituir a memória institucional, aplicados ao domínio da Sociedade Brasileira para o Progresso da Ciência. Apesar de seguir o modelo OAIS, o autor não observou quesitos básicos de segurança, como a configuração das chaves assimétricas no armazenamento dos pacotes AIP.

Já da Silva *et al*. [64] relataram a importância da cadeia de custódia para documentos digitais, sempre mantendo os pilares de autenticidade, confiabilidade e disponibilidade. A cadeia de custódia garante que a informação é autentica e não foi alterada. A não observância desse item pode colocar o documento em risco. Além da importância com integridade e autenticidade dos dados, deixa-se clara a preocupação com a segurança da informação, uma vez que os usuários finais bus-

cam esses dados normalmente em locais que julgam confiáveis. Para aumentar a segurança, foram criados mecanismos que monitoram todo caminho do documento, com utilização de microsserviços que incluem criptografia, assinaturas digitais e gestão de certificados digitais. A proposta dos autores, além de aumentar a segurança e garantir a cadeia de custódia, vai de encontro com as diretrizes da LGPD, por exemplo, na anonimização de dados e controle de acesso.

Marques e Cardoso [65] mencionaram sobre a importância da segurança em banco de dados, uma vez que é o local onde estão guardados dados importantes de uma organização, o principal ativo. No dever de salvaguardar os dados, garantindo a integridade, disponibilidade e a confidencialidade, as informações devem estar protegidas contra roubo, em relação ao comprometimento de sua integridade, bem como a forma que será acessada. Para tanto, os autores propõem 4 medidas, que vão de encontro com a LGPD, são elas: Controle de Acesso, Controle de inferência, Controle de Fluxo e Criptografia. Em uma analogia com a LGPD, a medida de controle de fluxo desempenha um importante papel, pois refere-se ao fluxo percorrido pela informação, porém é feita de forma cruzada, impedindo que um usuário que tenha privilégios inferiores acesse uma informação através de outra que tem acesso. Outro fator importante e em consonância com a LGPD é a criptografia, prevista na lei, a respeito de anonimização e proteção de dados. Isso demonstra que não é apenas uma ferramenta, uma metodologia ou uma técnica, e sim um conjunto de fatores que fazem com que a segurança seja eficaz, conforme definição dos autores: é “utilização conjunta de ferramentas aplicadas a uma política de segurança adequada pode propiciar controle de acesso com qualidade satisfatória para atender as principais necessidades das empresas e das pessoas no que pertence, e os acontecimentos podem ser tomados como exemplo para obter um bom controle e prevenção dos dados".(MARQUES; CARDOSO, 2021).

2.6 SÍNTESE DO CAPÍTULO

O Capítulo 2 apresenta um estudo da legislação internacional e brasileira sobre a segurança e privacidade de dados, levando em consideração o histórico, motivação e a necessidade da criação de lei específica. A pesquisa demonstra que a legislação não acompanhou o crescente aumento da utilização da internet para transações comerciais, utilização de redes sociais e uso para rotinas diárias, deixando os usuários sem uma legislação específica que resguarde e dê diretrizes para utilização dos dados pessoais do indivíduo. Associado ao contexto legal sobre a privacidade de dados e como foco deste trabalho, foi apresentando o conceito de Repositórios Digitais (RDs) e os trabalhos correlatos que tratam tanto de privacidade de dados quanto da segurança da informação restrita a repositórios digitais. O Capítulo 3 apresentará a análise de segurança do Archivematica.

3 ANÁLISE E VALIDAÇÃO DE SEGURANÇA DO ARCHIVEMATICA

Neste capítulo, é apresentado um breve estudo sobre o Archivematica, explorando suas característica, tais quais: método de armazenamento; fluxo de geração e transmissão de pacotes, conforme detalhado na seção "Fluxo Operacional do Archivematica". Também serão realizados experimentos para validação de segurança estática e dinâmica, em ambiente controlado a partir de uma instalação padrão do Archivematica, na versão 1.13.2.

O Archivematica é um Repositório Arquivístico Digital Confiável (RDC), criado como princípio básico que busca garantir a integridade, confiabilidade e autenticidade, tendo como ideia principal garantir a cadeia de custódia [66]. Vale ressaltar que a solução é *open-source* com a liberação do uso através de licença pública. A ferramenta permite aos usuário o estudo e a possibilidade de melhorias e evoluções, tendo como uma grande vantagem a customização e flexibilidade do seu uso, desde o controle de acesso, inserção de conteúdo, tratamento da informação, armazenamento e descarte. Outra vantagem dessa solução é a diversidade de formatos de arquivos que suporta a flexibilidade que permite a praticidade no armazenamento. Vale o estudo, no momento da implementação, da avaliação do formato de arquivo, uma vez que pode ficar oneroso para o projeto já que essa decisão influenciará diretamente do espaço de armazenamento.

Há ainda a possibilidade de integração com outros sistemas, como é o caso do DSPACE [67], muito utilizado para criação de bibliotecas digitais ou *OpenStack*, [68], muito usado na questão infraestrutura, armazenamento em nuvem, virtualização de corporações de pequena e médio porte. Porém, o Archivematica é mais utilizado para integração com o AtoM, por serem dos mesmos criadores e terem seus princípios e licenças do mesmo tipo. Para tanto, qualquer organização pública ou privada que deseje implantar um repositório arquivístico digital confiável precisa seguir o modelo descrito e a arquitetura correta. Vale ressaltar que o modelo foi projetado para armazenamento de arquivos digitas e, assim, como outros grandes repositórios digitais, foram criados antes das publicação da LGPD, que trouxe novas diretrizes para o armazenamento de informações pessoais, então, é preciso verificar se as diretrizes da LGPD estão ou não contempladas.

O primeiro ponto da validação é o controle de acesso, levando em consideração que a LGPD é muito clara quanto aos acessos aos dados do usuário. A validação prova que a versão padrão do Archivematica não há itens de criação de opções de perfis de acesso, havendo apenas o perfil administrador e a possibilidade do perfil arquivista, porém não há opção para inserir ou retirar permissões. Isso possibilita que as informações do usuário fiquem disponíveis para quaisquer pessoas que possuam determinados perfis. Ainda no que tange o controle de acesso, foi verificado que não há no Archivematica regramentos pré-estabelecidos em relação a políticas de acesso e/ou políticas de segurança.

Quanto ao tratamento dos dados, vale ressaltar que a validação deixou claro que a ferramenta

não possui controle de tratamento, nem quanto aos dados nem quanto aos responsáveis pelo tratamento. Não há nada nativo na ferramenta que garanta que a forma de tratamento dada aos dados do usuário segue o previsto em lei. Vale ressaltar que a legislação em vários artigos enfatiza que o usuário deve ter, de forma fácil e clara, uma maneira de consultar sobre os dados tratados que serão tratados, a forma, responsável e finalidade para tal. Avalidação da ferramenta prova que não existe essa opção, ficando a cargo do usuário um pedido ao administrador da ferramenta.

Um item preocupante na validação é quanto ao armazenamento, pois, por ser um repositório não estruturado, assim como é um banco de dados, é possível armazenar arquivos que podem conter dados pessoais e até mesmo dados pessoais sensíveis. Foi verificado ainda que não há nenhuma rotina de análise e/ou backup, ou seja, caso haja algum incidente que comprometa a base de dados, o risco de perda total sem recuperação é alto.

3.1 FLUXO OPERACIONAL DO ARCHIVEMATICA

A arquitetura do Archivematica é baseada em microsserviços, ou seja, pequenas atividades executadas isoladas ou em paralelo para formação de um pacote final de informação (OAIS), são eles: pacote de informação de envio (SIP), pacote de informações de arquivamento (AIP) e pacote de informação de disseminação (DIP).

- SIP - É o pacote que contem as informações e os metadados que são necessários para criação do objeto.
- AIP - É gerado através das informações recebidas do pacote SIP, tendo a função de armazenar, preservar e sustentar.
- DIP - É o pacote criado para distribuir as informações coletadas.

O Archivematica é separado em cinco principais conjuntos de funcionalidades, seguindo o modelo OAIS 3.1. O *Transfer*, onde o pacote SIP é criado; o *Ingest*, onde os pacotes DIP e SIP são criados; o *Archival Storage*, onde os pacotes são armazenados; o *Preservation Planning*, onde é configurado no plano de preservação como normalização e ferramentas de *OCR* e verificação de formatos; e, por último, o *Access*, onde pode ser visualizado todos os DIPs criados.

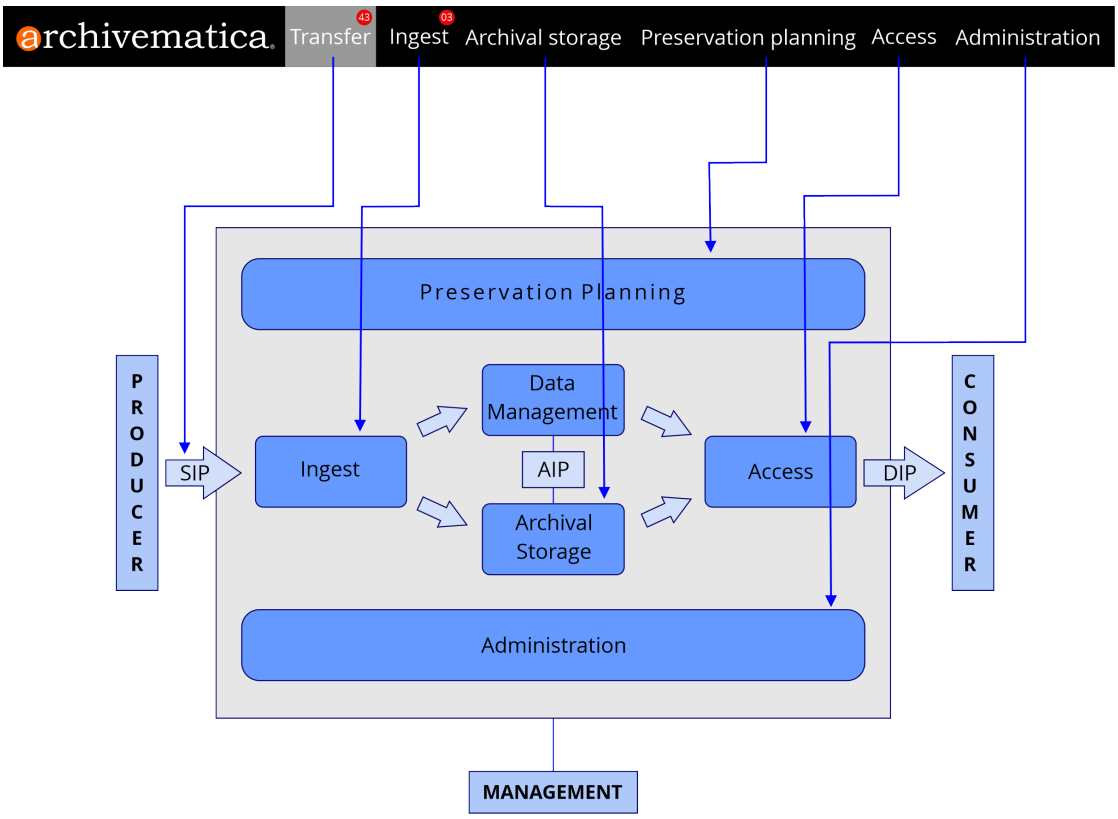


Figura 3.1: Modelo OAIS no Archivematica
[69]

O Diagrama da Figura 3.2 apresenta o fluxo de *Transfer*, processo que visa transformar qualquer conjunto de objetos, podendo ser pacotes zipados ou pacotes *BagIt's* para um pacote SIP. Essa transformação pode incluir metadados ou não. Os seguintes processos são executados:

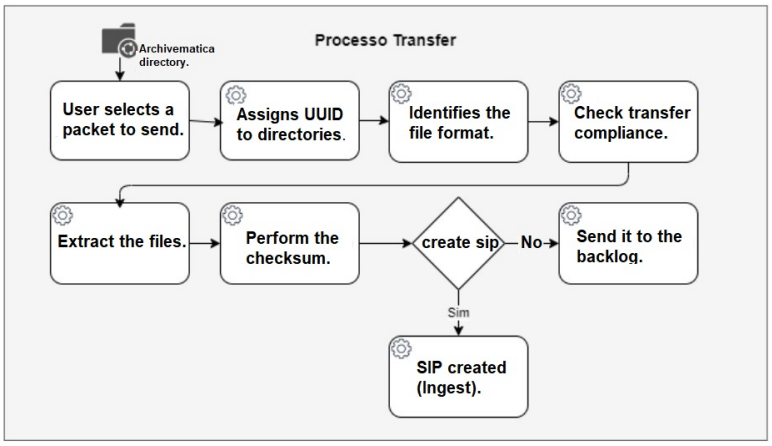


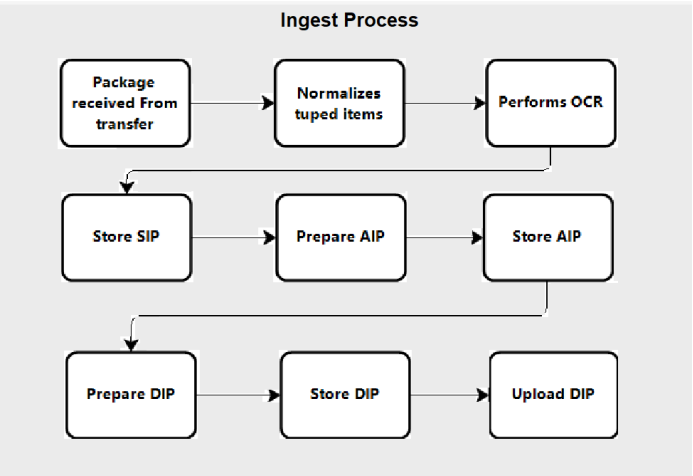
Figura 3.2: Diagrama de Processamento do *Transfer*

- O usuário seleciona, no diretório compartilhado, qual o pacote dele deseja enviar para o Archivematica, podendo ser pacotes ZIP ou *BagIt's*.

- O Archivematica atribui UUID's (identificador único) aos diretórios do pacote.
- O Archivematica identifica os formatos enviado para verificar se são formatos válidos e, posteriormente, realiza a normalização dos itens.
- O Archivematica verifica a conformidade da transferência.
- O Archivematica extrai os arquivos caso estejam zipados.
- O Archivematica cria um arquivo com os *checksums* dos arquivos enviados para, posteriormente, verificar se não houve alguma modificação nos arquivos.
- Por último, o usuário escolhe se deseja aceitar o SIP. Caso ele aceite, passa para o passo seguinte de Ingestão; caso não, esse envio vai para o *backlog* para poder ser recolhido posteriormente.

Em seguida, o pacote já transferido segue para o módulo Ingestão (em inglês, *Ingest*), que tem o objetivo de empacotar, em padrão SIP, os objetos digitais já validados. Nesse módulo também são criados os pacotes AIP e DIP.

Figura 3.3: Processo do módulo de Ingestão do Archivematica.



A Figura 3.3 apresenta o fluxo de ingestão de um pacote SIP para conversão em um pacote AIP para preservação. Os seguintes processos são executados:

- Primeiramente, o Archivematica pega o pacote SIP previamente verificado e prepara normalização.
- Normaliza os itens digitais, ou seja, aplica as regras de conversão de formatos de preservação e de acesso.
- Realiza o OCR, transcrevendo as imagens para texto sobreposto.
- Faz armazenamento final do SIP.

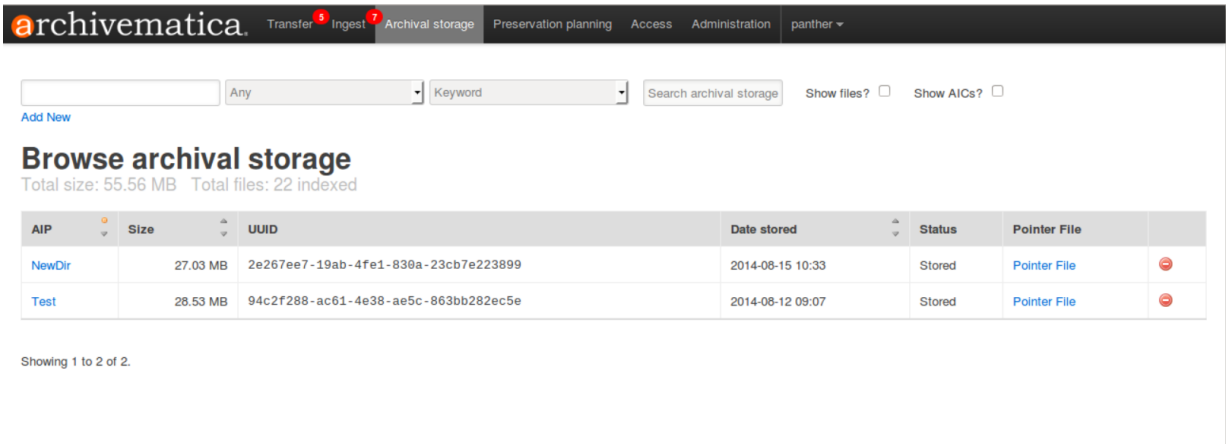
- Monta o pacote AIP através da cópia dos itens digitais de armazenamento e cria o pacote AIP.
- Armazena o pacote AIP no local escolhido.
- Monta o pacote DIP através da cópia dos itens digitais de disseminação e cria o pacote DIP.
- Armazena o pacote DIP no local escolhido.
- Se configurado, faz o upload do DIP para uma plataforma de disseminação como o AtoM [70].

Vale ressaltar que o DIP é o pacote responsável pela distribuição dos arquivos digitais e funciona basicamente em 3 etapas: acesso fácil para usuários; forma de troca de informações entre sistemas de armazenamento; e distribuição de arquivos [71]. Na segunda etapa, vemos que precisa ser verificado como é feita a troca de informações, uma vez que, nessa etapa, é possível compartilhar informações com outros sistemas ou corporações que também armazenem dados, o que é definido claramente no art. 26 da LGPD [4].

> Art. 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, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. (LGPD, 2018)

O último passo, no que tange o armazenamento seguro, ocorre no módulo Armazenamento Arquivístico (em inglês, *Archival Storage*), que recebe o pacote AIP gerado no Módulo de Ingestão e armazena esse pacote em um diretório local ou remoto, conforme definido pelo administrador. Tal processo pode ser evidenciado na interface dos sistema conforme a Figura 3.4.

Figura 3.4: Interface do módulo de armazenamento do Archivematica[3]



3.2 PLATAFORMA DE DISSEMINAÇÃO

A plataforma de disseminação é responsável por consumir os pacotes DIPs do Archivematica e prover acesso das informações aos usuários finais. Para isso, foi utilizado o software livre AtoM, abreviatura de *Access to Memory*. O AtoM [70] funciona em ambiente web, é multilíngue e pode ser usado em uma organização com múltiplos repositórios integrados. É uma aplicação de código aberto destinada à descrição normalizada em arquivos definitivos. Entre suas principais características, pode-se destacar:

- Web: todas as principais funções do AtoM podem ser controladas a partir de um navegador, e os requisitos do usuário são mínimos.
- *Open Source*: todo o código do AtoM é lançado sob uma licença GNU *Affero General Public License* (A-GPL 3.0), dando assim liberdade para que qualquer instituição possa o estudar, modificar, melhorar e distribuir.
- Baseado em padrões: o AtoM foi construído originalmente com apoio do *International Council on Archives* (ICA), para incentivar uma adoção mais ampla das normas internacionais.
- Multilíngue: os elementos de interface e o conteúdo da base de dados de todos os utilizadores podem ser traduzidos em vários idiomas, usando a interface de tradução embutida.
- Integração: o AtoM é facilmente integrável com o Archivematica, sistema utilizado para o armazenamento seguro.

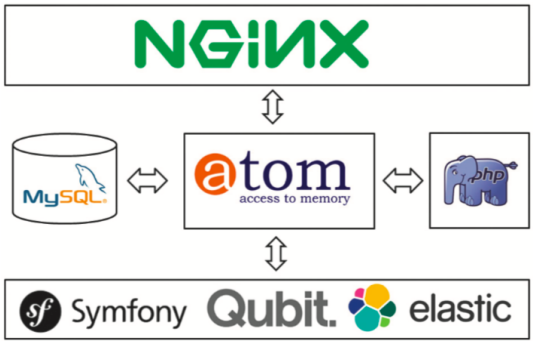


Figura 3.5: Interface de Acesso aos Objetos Digitais ATOM

Conforme apresentado na Figura 3.5, a arquitetura do AtoM é composta de: NGINX (servidor de aplicação recomendado), Synfony (framewok PHP), Qubit tools, Elasticsearch (indexador) e MySQL (banco de dados recomendado). O AtoM suporta vários formatos de objetos digitais, conforme a Tabela 3.1. A plataforma também consome formatos não suportados, a diferença nesse caso é que a ferramenta não irá gerar visualização do objeto, mas possibilitará seu download.

Tabela 3.1: Tabela de formatos de imagem, áudio e vídeo que podem ser visualizados no AtoM

Imagem	**Áudio**	**Video**
PDF	8SVX	AVS
BMP	AC-3	BFI
GIF	Apple Lossless	CamStudio CSCD
PNG	ATRAC3	Cinepak
JPEG	Cook Codec	Creative YUV (CYUV)
V.Flash PTX	EA ADPCM	DNxHD
SGI	FLAC	Flash Screen Video
Sun Rasterfile	Intel Music Coder	FFV1
FLIC	Monkey's Audio	H.261
TIFF and PNM	MP2 and MP3	H.263 and H.264/MPEG-4 AVC
	Nellymoser Asao Codec Flash	Huffyuv
	QDM2	id Software RoQ Video
	RealAudio 1.0 and 2.0	Intel Indeo 2 and 3
	Shorten	LOCO
	Truespeech	Mimic[3]
	TTA	MJPEG
	TXD	MPEG-4 Part 2
	Vorbis	Apple Comp. QuickDraw
	WavPack	Quicktime Graphisc SMC
	Windows Media Audio 1/2	RealVideo RV10/RL2
		Smacker video
		Snow
		Sorenson SVQ1 and SVQ3
		Theora
		Asus V1 and V2
		VMware VMnc
		On2 VP3, VP5 e VP6
		Westwood Studios VQA
		MS WMV v 7, 8 and 9
		Wing Comm/Xan Video

3.3 VALIDAÇÃO DE SEGURANÇA DO ARCHIVEMATICA

As formas de se analisar o desenvolvimento seguro de um software em seu ciclo de vida podem envolver diversas técnicas, entre as técnicas mais antigas e mais conhecidas, estão a SAST

(*Static Application Security Testing*)[72], que envolve uma análise estática do código-fonte do sistema; e o DAST (*Dynamic Application Security Testing*), que envolve um teste dinâmico da aplicação em execução. O SAST é um teste de caixa-branca, em que há a necessidade de ter acesso à fonte de aplicação, normalmente sendo empregado desde os estágios iniciais do desenvolvimento para identificação de falhas ou vulnerabilidades na aplicação. Já o DAST[73] é um teste de caixa-preta, podendo ser aplicado o quanto antes a aplicação puder ser testada funcionalmente, podendo até mesmo ser realizado por terceiros que somente tenham acesso ao endereço web da aplicação [74].

Como pode se observar, as análises SAST e DAST não são mutualmente exclusivas, idealmente devendo ser executadas em paralelo no ciclo de vida do software. Existem soluções proprietárias no mercado que executam ambas as funções, também existindo alguns softwares livres que executam partes do processo, podendo ser combinados. Um importante parâmetro a ser identificado para a escolha de ferramentas que realizam testes de segurança é se elas possuem aderência ao *Open Web Application Security Project* (OWASP) [75]. O OWASP é uma organização sem fins lucrativos que tem como objetivo promover a melhoria de segurança de aplicações web, propiciando uma comunidade para a geração de artigos, documentações e tecnologias para tal. Um dos seus mais conhecidos produtos é o OWASP 10, uma lista anualmente atualizada das 10 falhas de segurança mais comuns no momento, representando um consenso entre especialistas de todo o mundo na área de segurança cibernética.

O OWASP lista em seu site ferramentas aderentes ao OWASP e outro padrões internacionais de segurança, tanto para ferramentas SAST [1]quanto DAST [2].

Para a realização de testes de segurança no Archivematica, foram escolhidas duas ferramentas entre as recomendadas pelo OWASP. Para a análise estática, foi escolhida a ferramenta *bandit* [3], que é uma ferramenta livre e simples de linha de comando para a linguagem Python, que é a linguagem do Archivematica; além disso, essa ferramenta é utilizada como componente de outras ferramentas proprietárias mais complexas. Para a análise dinâmica, foi escolhida a ferramenta *OWASP ZAP* [4], que se trata justamente de um scanner de vulnerabilidades mantido pela própria OWASP, o que corrobora sua eficiência.

Para os cenários de teste, foi utilizada a versão estável mais recente do Archivematica (v1.13.2). Os mais importantes componentes da solução Archivematica são o *Dashboard* (painel de administração geral) e o *Storage Service* (serviço de administração dos pacotes SIP, AIP e DIP), ambos independentes e que estão separados em diferentes repositórios, surgindo, então, a necessidade de testes separados nos dois com as duas diferentes técnicas.

[1]Lista de ferramentas SAST: https://owasp.org/www-community/Source_Code_Analysis_Tools
[2]Lista de ferramentas DAST: https://owasp.org/www-community/Vulnerability_Scanning_Tools
[3]Ferramenta *Bandit*: https://pypi.org/project/bandit/
[4]Ferramenta OWASP ZAP: https://www.zaproxy.org

3.3.1 Descrição do ambiente de testes

Para realização dos testes, foi necessário montar um ambiente que propiciasse exatamente como é a utilização do Archivematica na prática, assim sendo, no que tange instalação e configuração de softwares, foi utilizado o sistema operacional Linux Min na versão 19.1 para a instalação do Archivematica em sua versão 1.13.2. As ferramentas de testes foram o Bandit v1.7.4 (pythonv 3.8.0) e OWASP ZAP v2.11.1. Quanto a configuração do hardware, foi utilizado um notebook com memória de 32GB RAM e 256GB SSD.

3.3.2 Teste Estático de Segurança de Aplicativo

A ferramenta Bandit foi utilizada para testes estáticos. O relatório da análise é composto por uma lista de potenciais problemas que foram identificados após analisar os códigos-fonte das aplicações. Os elementos de cada potencial problema são:

- Descrição do problema.
- **Test ID:** identificador do plugin que executou o referido teste, uma lista de todos os plugins disponíveis pode ser encontrada no site da ferramenta [5].
- **Severidade:** grau de gravidade do problema, podendo ser Indefinida, Baixa, Média e Alta.
- **Confiança:** grau de confiabilidade no resultado (pois existem falsos positivos), podendo ser Indefinida, Baixa, Média e Alta.
- **CWE**: é o identificador padrão de uma falha de segurança que é catalogada pelo CWE (*Common Weakness Enumeration*) [6], uma comunidade internacional.
- Arquivo, Número da linha e Mais informações.

Sumário sobre a execução da análise em cada um dos componentes da solução:

- ***Dashboard***
  - Total de linhas de código analisadas: 73610
  - Total de problemas por severidade:
    - Indefinida: 0
    - Baixa: 134
    - Média: 53
    - Alta: 0
  - Total de problemas por confiança:

[5] Lista de plugins do Bandit: https://bandit.readthedocs.io/en/latest/plugins/index.html
[6] CWE: https://cwe.mitre.org/

        * Indefinida: 0
        * Baixa: 2
        * Média: 13
        * Alta: 172

- ***Storage Service***
    - Total de linhas de código analisadas: 19105
    - Total de problemas por severidade:
        * Indefinida: 0
        * Baixa: 57
        * Média: 19
        * Alta: 1
    - Total de problemas por confiança:
        * Indefinida: 0
        * Baixa: 0
        * Média: 4
        * Alta: 73

Testes de segurança podem identificar problemas que, na realidade, são falsos positivos, por isso a análise dos relatórios pelos desenvolvedores ou analistas de segurança é essencial para avaliar a necessidade de correção. No caso do relatório SAST para os componentes do Archivematica, foram identificados, em grande maioria, problemas com severidade baixa, além de outra parte considerável de problemas com severidade média. Logicamente, a ordem de solucionamento de problemas deve seguir dos com severidade mais alta para os de mais baixa. Algumas vezes, problemas com severidade baixa podem até mesmo ser ignorados, seja pelo seu alto custo de manutenção ou por não representar um risco significativo. Não foi encontrado nenhum problema considerado alto no componente do *dashboard* e apenas 1 (um) no *storage service*, conforme apresentado na tabela 3.2.

Tabela 3.2: Resumo dos erros encontrados no Dashboard e Storage Service

Dashboard				
	Indefinida	Baixa	Média	alta
Severidade	0	134	53	0
Confiança	0	2	13	172
Storage Service				
	Indefinida	Baixa	Média	alta
Severidade	0	57	19	1
Confiança	0	0	4	73

Em sua grande maioria, os problemas de baixo risco indicados pelo relatório do *bandit* estão relacionados ao uso de uma biblioteca Python chamada *lxml*, por ser conhecida como vulnerá-

vel a ataques XML. No caso, os desenvolvedores ignoraram esses problemas porque os XMLs analisados pela biblioteca são, majoritariamente, de configuração da aplicação, com domínio de controle interno. Caso se tratassem de XMLs de entrada de alguma interface da aplicação, talvez esse tipo de problema mereceria tratamento.

Os testes demonstram alguns problemas. Foi possível identificar, por exemplo, uma vulnerabilidade de nível médio, sendo que o ID B320 indica chamadas feitas por métodos XML, e o código CWE-20 significa que esse erro já é conhecido e catalogado pela CWE. Outro problema identificado foi uma falha no módulo do subprocesso “clamscan.py"do Archivematica, o que pode implicar em possíveis falhas de segurança, sendo também um erro conhecido e catalogado pelo CWE. A Figura 3.6 apresenta uma pequena parte de um exemplo do relatório da ferramenta Bandit.

Figura 3.6: Parte do relatório SAST da ferramenta Bandit.

3.3.3 Teste Dinâmico de Segurança de Aplicativo

De forma similar ao relatório de teste estático, a ferramenta OWASP ZAP gera um relatório de testes dinâmicos com uma listagem dos problemas identificados. Os elementos de cada potencial problema são:

- **Risco:** grau de gravidade do problema, podendo ser Indefinida, Baixa, Média e Alta.
- **Confiança:** grau de confiabilidade no resultado (pois existem falsos positivos), podendo ser Indefinida, Baixa, Média e Alta.
  - Descrição do problema.
  - Nome do problema identificado.
  - URL onde o problema foi identificado.

- **Source**: identifica qual scanner da ferramenta identificou o problema
- **CWE ID**: é o identificador padrão de uma falha de segurança que é catalogada pelo CWE.
- **WASC ID**: similar ao CWE ID, só que se tratando de outra comunidade internacional que realiza o catálogo de problemas de segurança, a WASC (*Web Application Security Consortium*) [7]
- **Referência**: link para o site da ferramenta com mais informações sobre o problema.

Diferentemente do teste estático, que identifica no código-fonte a origem do problema, em testes dinâmicos isso não é possível, já que é um teste caixa-preta, onde só se possui acesso a um ambiente da aplicação. Em se tratando de uma aplicação web, o que a ferramenta tem acesso é uma URL dela, executando testes a partir desse ponto de entrada. O OWASP ZAP pode ser configurado com todas as URLs da aplicação, inclusive simulando autenticação ou qualquer outra entrada do usuário para executar os testes. Uma outra forma simplificada de se realizar os testes é utilizando a funcionalidade de testes automáticos da aplicação, que realiza uma análise exploratória da aplicação a partir de uma única URL (normalmente a página inicial da aplicação), onde a ferramenta, a partir dos links e botões da página HTML, vai descobrindo novas URLs e executando os testes nelas, de forma recursiva e automatizada. A tabela 3.3 apresenta o resumo dos problemas encontrados de acordo com o módulo que foi avaliado e a criticidade (severidade) do problema.

Tabela 3.3: Resumo dos problemas encontrados no teste DAST

Dashboard				
Severidade	Informacional	Baixa	Média	alta
	1	4	3	0
StorageService				
Severidade	Indefinida	Baixa	Média	alta
	1	5	2	0

O relatório possui a estrutura apresentada com os parâmetros dos resultados, apresentando a URL que foi analisada; o comando e/ou chamada para execução do teste, o exemplo apresenta o resultado do teste contendo o problema encontrado, conhecido como possibilidade de um ataque do tipo *"clickjacking"[76].* Esse método consiste em confundir o usuário no momento de clicar em botões ou links, de forma opaca ou transparente, o usuário acredita estar clicando na página que acessou, porém, os cliques estão sendo direcionados para outra página e sendo colhidos pelo atacantes, o resumo do teste é apresentado na Figura 3.7.

[7]WASC: http://projects.webappsec.org/.

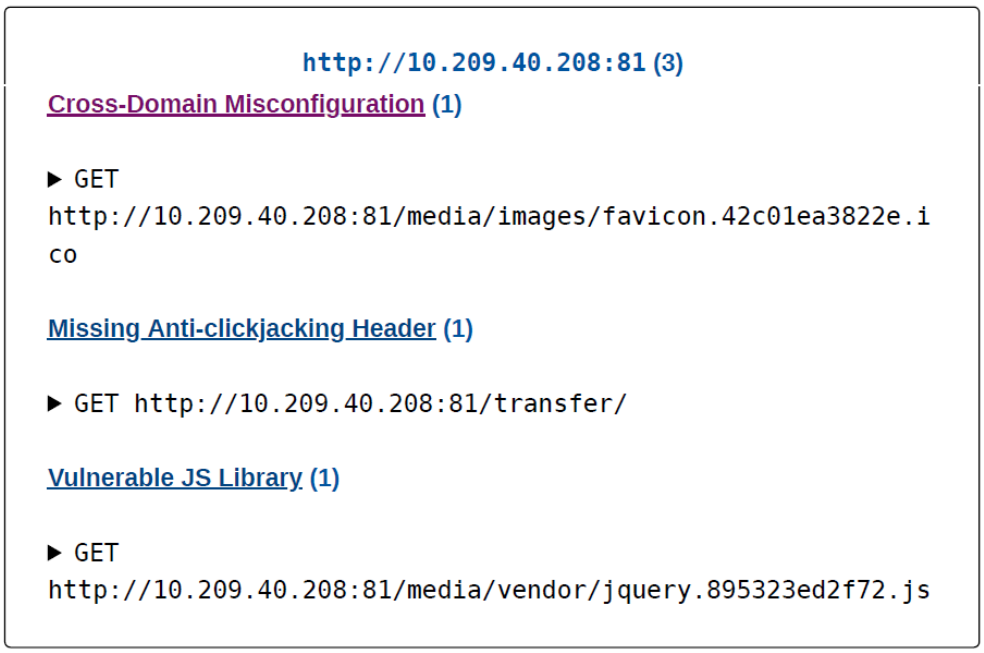


Figura 3.7: Parte do relatório DAST da ferramenta OWASP ZAP - Parte 1.

Um dos problemas mais identificados pela ferramenta com risco a ser considerado foi a falta de configuração na aplicação para evitar *Cross-Origin Resource Sharing* (CORS), que restringe o acesso às APIs Web da aplicação somente pelo domínio real da aplicação, não possibilitando que outros sites/aplicações não permitidos as acessem pelo navegador.

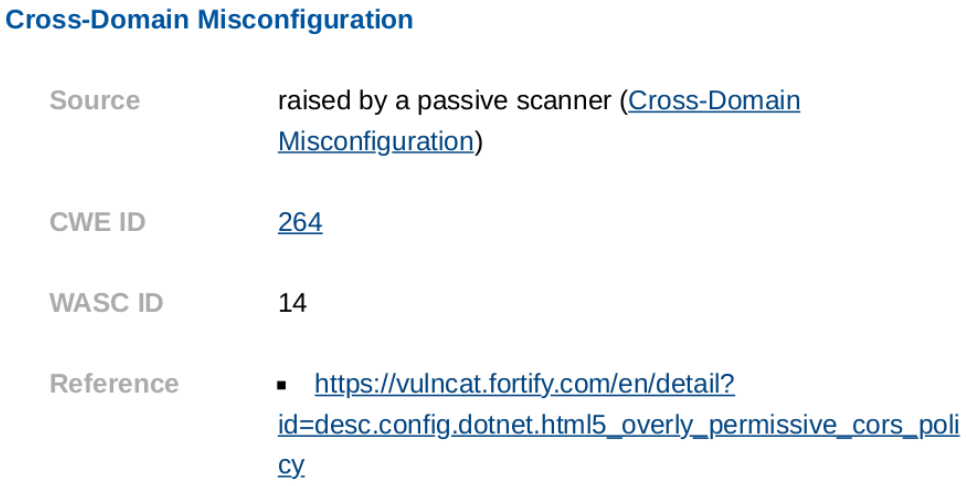


Figura 3.8: Parte do relatório DAST da ferramenta OWASP ZAP - Parte 2.

Vale ressaltar que alguns problemas encontrados foram considerados leves e não prejudicam ou causam nenhum risco a integridade da aplicação. Os erros considerados leves, são analisados de acordo com o fatores:

- Risco Potencial - qual é o potencial dano em caso de sucesso de um ataque bem sucedido.

- Reprodução do ataque - dificuldade em executar o ataque de acordo com o nível de conhecimento do atacante.
- Exploração da vulnerabilidade - facilidade de encontrar a vulnerabilidade ao atacar.
- Usuários afetados - quantidade de usuários que seriam afetados no caso de sucesso do ataque.

3.4 SÍNTESE DO CAPÍTULO

Neste capítulo 3, foi detalhado o que é um repositório digital seguro, os principais repositórios utilizados em órgãos públicos e privados, tecnologias envolvidas e a segurança aplicada para garantir a privacidade e segurança dos dados. Por ser o mais utilizados e de maior conhecimento para guarda e armazenamento de documentos digitais, foi escolhido o Archivematica para análise específica e testes práticos para verificação de segurança e conformidade segundo as diretrizes da LGPD. O padrão utilizado pelo Archivematica segue as diretrizes indicadas pelo Conarq, órgão responsável por determinar os regramentos mínimos que devem compor uma gestão segura de objetos e metadados.

Também foram realizados experimentos para validação de segurança do repositório Archivematica. Para essa validação, foram executados testes práticos na ferramenta web e testes práticos diretamente no código fonte através da utilização de ferramentas *open-source* de varredura de vulnerabilidades. Os testes demonstraram que a ferramenta Archivematica possui alguns erros que necessitam de correção, pois podem implicar em risco de segurança para a ferramenta e os dados de seus usuários. Vale ressaltar que a LGPD, por ter como principal diretriz o direito a privacidade e segurança dos dados, todo e qualquer indicativo de problema que possa resultar em risco deve ser eliminado.

O próximo capítulo 4 mostrará a forma como o guia foi elaborado, contendo a análise do TRAC - *Trustworthy Repositories Audit & Certification*, que é um documento que serve como métrica para certificar se um repositório é ou não seguro, além de contar com o resultado de um questionário aplicado com diversos profissionais para avaliar o nível de conhecimento e maturidade sobre a LGPD.

4 GUIA DE ADEQUAÇÃO À LGPD

O Guia proposto para adequação a LGPD é um documento baseado em regras e diretrizes no que diz respeito à governança, à segurança da informação e às boas práticas para garantir a segurança e privacidade dos dados, segundo análises feitas previamente para identificação das necessidades para adequação à legislação brasileira. A elaboração do guia seguiu as diretrizes definidas pela LGPD, no que tange a entrada, armazenamento e guarda de dados pessoais dos usuários. O Guia não se limita a informar a regra, e sim em como adequar um repositório digital seguro às diretrizes da LGPD de forma prática e segura. Para tanto, o guia é um passo a passo para garantir a segurança e a privacidade dos dados, identificando o momento da coleta desses dados (sejam eles dados sensíveis ou não), a forma como será recebido e as regras de segurança. No segundo passo, o guia definirá como deve ser feita a guarda desses dados, quem pode acessar e como será feito o acesso. Por fim, será definida a regra, sempre em conformidade com a legislação, a forma como esses dados serão descartados ou arquivados.

4.1 *SURVEY*

Para continuidade do trabalho e elaboração do guia, foi realizado um *survey*, ou seja, aplicação de um questionário para avaliar o nível e conhecimento dos profissionais de tecnologias e áreas afins. De acordo com Biemer e Lyberg [77], um *survey* efetivo precisa cumprir alguns requisitos, e o resultado depende de um conjunto de itens que incluem: uma população que será o alvo da pesquisa; a forma de avaliação para que seja possível mensurar o resultado; uma análise dos parâmetros para delimitação; uma forma de apresentação, como lista ou tabela associando a população com o objeto da pesquisa; e análise do resultado através de uma amostra.

Com base nos itens da LGPD, foi executado um questionário contendo 21 questões, com foco na segurança da informação. Basicamente, os questionamentos do formulário buscaram coletar informações sobre o conhecimento dos regramentos da LGPD por profissionais de empresas públicas e privadas que trabalham com tecnologia. Os resultados foram avaliados segundo a escala de Likert, com as opções: 1) discordo totalmente; 2) discordo; 3) indiferente (ou neutro); 4) concordo e 5) concordo totalmente.

Tabela 4.1: Lista de Questões da Pesquisa

ID	**Título das questões**
Q.1	Você trabalha em instituição pública ou privada?
Q.2	Você tem conhecimentos sobre as regras básicas da Lei Geral de Proteção de Dados LGPD?
Q.3	Em relação ao tratamento de dados pessoais, sua empresa solicita autorização (consentimento) para os tratamentos dos seus dados?
Q.4	Sobre o documento de consentimento que informa sobre os dados que serão tratados (finalidade), sua empresa solicita a assinatura desse documento?
Q.5	Em relação a privacidade, sua empresa utiliza sistemas que permitem controlar acessos?
Q.6	Você tem conhecimento sobre a forma que seus dados são armazenados?
Q.7	Como é feita a guarda dos dados em sua empresa?
Q.8	Existe algum aviso na intranet ou você recebeu algum aviso/alerta por e-mail informando sobre privacidade de dados?
Q.9	Você tem conhecimento sobre dados anonimizados e para que servem?
Q.10	Você tem conhecimento sobre ferramentas de segurança em sua empresa (Firewall, software de monitoramento, criptografias, antivírus, etc.)?
Q.11	Sua empresa divulga técnicas de segurança ou possui alguma política de segurança?
Q.12	Você já foi informado ou teve conhecimento de alguma tentativa de ataque cibernético que sua empresa sofreu (Transparência)?
Q.13	Quais meios de segurança abaixo sua empresa utiliza: Políticas de Senhas; Controle de Permissões; VPNs; Firewall.
Q.14	Você tem conhecimento se os seus dados pessoais são compartilhados com outros órgãos ou empresas?
Q.15	Você já foi informado sobre o direito ao esquecimento sobre seus dados pessoais?
Q.16	Você sabe a diferença entre "dados pessoais"e "dados pessoais sensíveis"?
Q.17	Em suas atividades do dia a dia, você recebe orientações sobre a conformidade da LGPD de sua gerência?
Q.18	Em relação à documentação, em suas atividades tudo é documentado? Ex: Processos, arquitetura, gestão de segurança, controle de acesso, etc.
Q.19	Sua empresa tem algum mecanismo de proteção ou contingência para casos de vazamento ou perda de dados?
Q.20	Sua empresa possui algum procedimento de eliminação ou exclusão automática de dados?
Q.21	Você tem algum comentário em relação a ações que sua empresa tomou para garantir a conformidade com a LGPD? Poderia descrever quais foram essas ações e quais são as suas percepções em relação a elas?

A Figura 4.1 apresenta o percentual de respostas que cada questão obteve, sendo que os 4 últimos itens (Q3_public,Q3_private, Q4_public e Q4_private) são relativas a combinações das questões 3 e 4 com os respondentes de instituições públicas e privadas. A pergunta Q1 da Tabela 4.1 visa identificar o perfil de respondente pelo tipo de instituição ou corporação. O intuito é fazer o cruzamento das respostas e identificar o nível de conhecimentos sobre a LGPD e as instituições as quais estão vinculados.

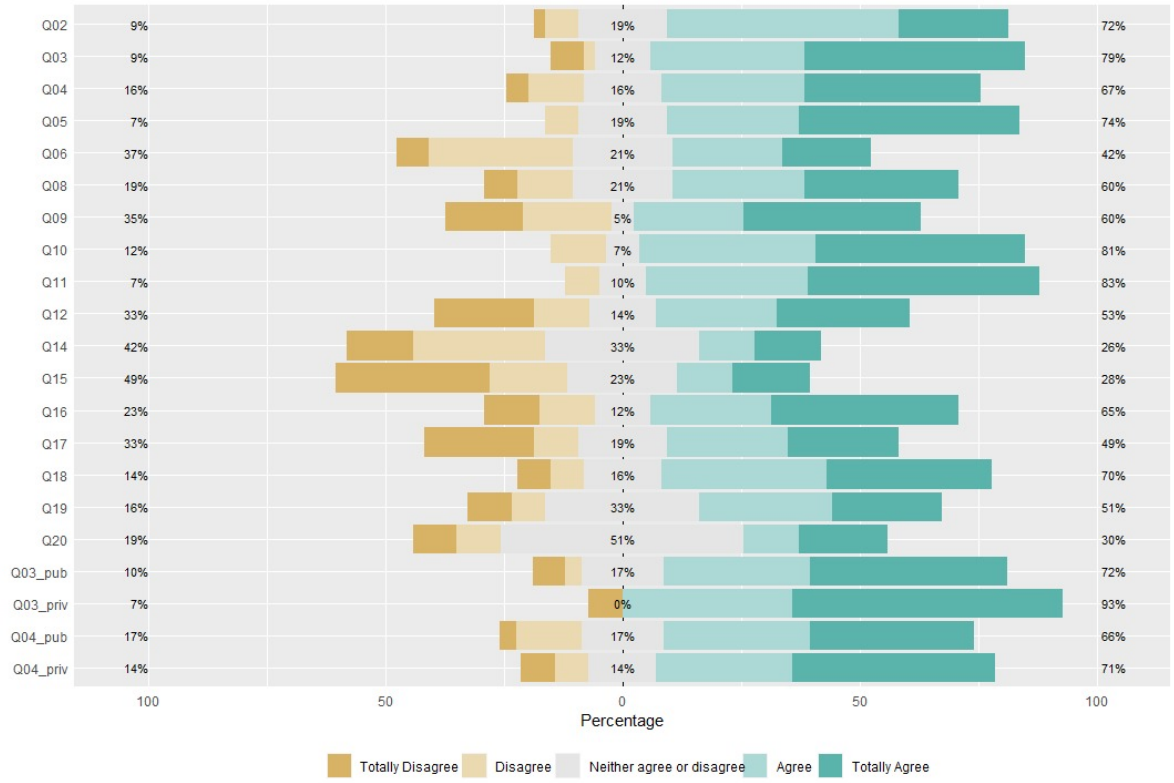


Figura 4.1: Respostas dos Participantes

A pergunta Q1 (Tabela 4.1) visa identificar o perfil de respondente pelo tipo de instituição ou corporação. O intuito é fazer o cruzamento das respostas e identificar o nível de conhecimentos sobre a LGPD e as instituições as quais estão vinculados. A partir dos resultados da Q2 (Tabela 4.1), foi possível verificar que menos de 28% das pessoas desconhecem completamente os requisitos básicos da LGPD, porém, com base em outras respostas do questionário, ficou claro que, se aprofundarmos a discussão, esse número tem um crescimento considerável. Como exemplo, temos outro dado preocupante, coletado na pesquisa da Q3 (tabela 4.1) em relação aos requisitos básicos: o fato que um dos principais itens do regramento, o "consentimento sobre o tratamento dos dados", não ser de conhecimento dos profissionais, ou seja, 21% dos entrevistados não foram informados por suas empresas sobre o tratamento; um número bastante expressivo pela gravidade, até mesmo pelo tempo em que a lei está em vigor, como pode ser observado na Figura 4.2.

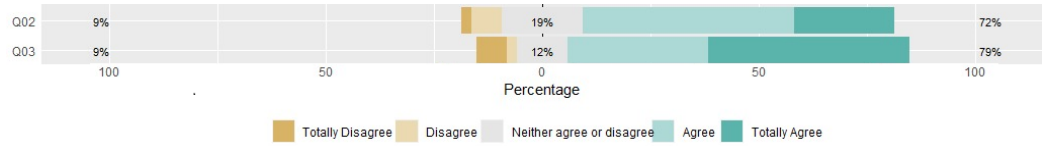


Figura 4.2: Relacionamento das questões 2 (conhecimentos básicos da LGPD e 3 (Consentimento para tratamento dos dados)

Fazendo um relacionamento entre a pergunta Q1 e Q3 (Tabela 4.1), entre os respondentes do questionário que fazem parte de instituições públicas, 72% informaram que suas instituições

fazem uso do documento de consentimento de tratamento dos dados pessoais. Já entre os respondentes de instituições privadas, esse número cresceu para 93%, conforme apresentado na Figura 4.3.

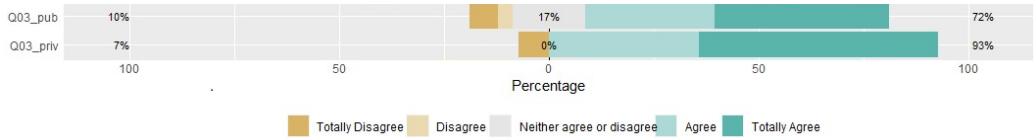


Figura 4.3: Comparativo entre respondentes de instituições públicas e privadas em relação ao documento de consentimento.

Se adicionarmos a Q4 da Tabela 4.1, há 66% dos respondentes de empresas públicas informando que, além de suas instituições solicitarem o documento sobre o consentimento, estava detalhado na solicitação quais os dados seriam recolhidos, bem como a finalidade do tratamento. Já em empresas públicas, o índice de respostas foi 71%, conforme apresentado na Figura 4.4.

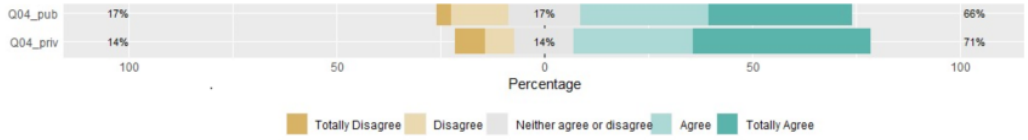


Figura 4.4: Análise de consentimento sobre quais dados são coletados.

O controle de acesso é a primeira barreira para impedir um possível acesso indevido. A utilização de senhas fortes, antivírus, firewalls, entre outras ferramentas de controle de acesso e monitoramento, diminuem consideravelmente o sucesso de um ataque virtual. O resultado obtido na Q5 (Tabela 4.1) demonstra que 74% dos participantes informaram que suas empresas utilizam meios de controle de acesso, um resultando bem satisfatório, conforme apresentando na Figura 4.5.

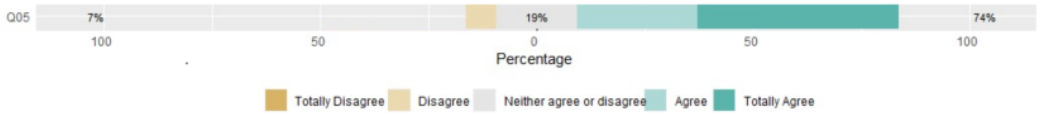


Figura 4.5: Resultado da questão 5 sobre controle de acesso.

Quanto ao armazenamento de dados, o problema é bem maior, pois mais de 58% dos entrevistados responderam na Q6 (Tabela 4.1) que não fazem ideia de como os dados são armazenado, conforme apresentado na Figura 4.6.

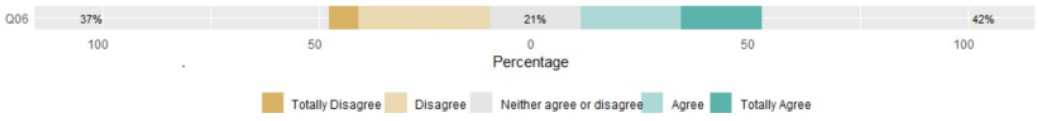


Figura 4.6: Pessoas que tem conhecimento sobre como os dados são armazenados.

Quanto a forma de armazenamento dos dados na Q7 (Tabela 4.1), 66% dos respondentes de entidade pública disseram que a mais utilizada é o armazenamento na forma hibrida, enquanto 31% disseram utilizar o armazenamento local, e somente 3% em nuvem. Quando falamos de empresa privada, o percentual é alterado para 36% na forma hibrida, 29% de forma local e 29% em nuvem, o que demonstra que as empresas privadas ainda são os maiores utilizadores do armazenamento em nuvem, conforme apresentado na tabela 4.2.

Tabela 4.2: Forma de armazenamento mais utilizado por tipo de instituição

Profissionais de Instituições Públicas				
ID	Local	Nuvem	Hibrido	NSR
Q7	31%	3%	66%	0%
Profissionais de Instituições Privadas				
ID	Local	Nuvem	Hibrido	NSR
Q7	29%	29%	36%	7%

No que tange a divulgação e conscientização sobre a LGPD, 40% dos entrevistados informaram na Q8 (Tabela 4.1) que nunca foram avisados ou orientados sobre a privacidade de dados, seja por meios virtuais, como intranet e e-mail, quanto de forma verbal em alguma reunião, palestra ou eventos de conscientização, conforme apresentado na Figura 4.7. Sabemos que, para implantar metodologias e normas, é necessário conscientização e engajamentos de todos da organização, bem como apresentar a todos os benefícios e deixar claro que não é apenas por questão de obrigatoriedade ou adequação às normas, e sim para segurança dos ativos da organização.

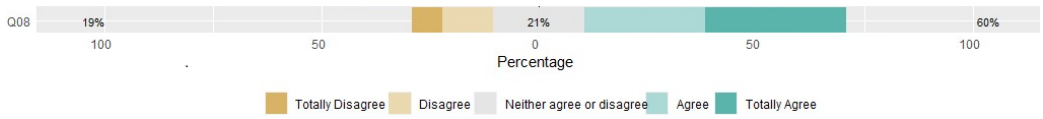


Figura 4.7: Percentual de profissionais que receberam algum tipo de orientação sobre privacidade de Dados.

Outra evidência de desconhecimento sobre as diretrizes da lei vemos ao questionar sobre a anonimização de dados. A Q9 (Tabela 4.1) mostra como resultado que não é de conhecimento de 40% dos entrevistados, sendo que 35% sequer conhecem ou sabem para que serve, levando-nos a crer que os próprios profissionais de TI não estão preparados para a implantação completa, conforme apresentado na Figura 4.8.

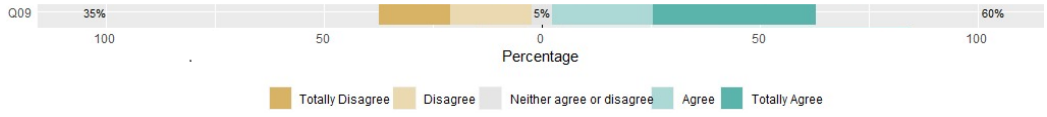


Figura 4.8: Resultado do questionamento conhecimento sobre anonimização de dados

No que diz respeito a soluções de mercado para área segurança de tecnologia, 81% dos participantes da pesquisa responderam, na Q10 (tabela 4.1), que tem conhecimento de ferramentas de apoio à segurança de informações, sendo estes os mais conhecidos: Firewall, softwares de monitoramento, antivírus, etc. As políticas de seguranças são responsáveis por direcionar os usuários

para metodologias que promovam maior segurança. 83% dos respondentes informaram na Q11 (Tabela 4.1) que suas corporações possuem uma política estabelecida. Esse dado é importante, pois algumas diretrizes contidas na LGPD devem estar inseridas na política de segurança, bem como política de controle de acesso, política de controle de backup e armazenamento, entre outras, conforme apresentado na Figura4.9.

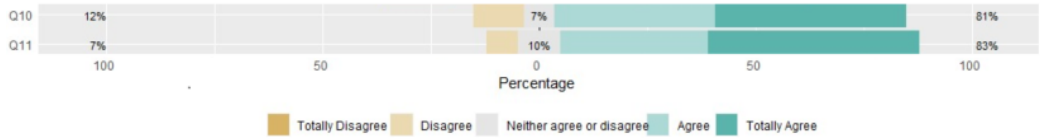


Figura 4.9: Resultado das questões sobre ferramentas de segurança da informação e conscientização sobre a importância de proteção dos dados

Com base nas respostas da Q13 (Tabela 4.1), é possível notar que as empresas fazem o básico, ou seja, controle de senhas, VPNs e Firewall, porém o questionário trouxe um dado importante para a segurança da informação, que é o controle de instalação de ferramentas por parte de usuários em suas estações de trabalho. Isso é uma falha antiga em políticas de segurança; não era comum ver usuários fazerem a instalação de ferramentas para facilitar o seu dia a dia, sendo que o problema desse fator é a forma de download e instalação, pois, normalmente, são softwares livres retirados de sites não confiáveis, colocando em risco a segurança da estação de trabalho e, consequentemente, toda rede da organização. O questionário demonstrou que 69,8% responderam que não tem permissão para instalação, demonstrando que suas organizações já estão atentas à essa prática. Automaticamente, esse percentual reflete na divulgação dessas técnicas e de políticas de segurança, não resolvendo tudo, mas amenizando os riscos.

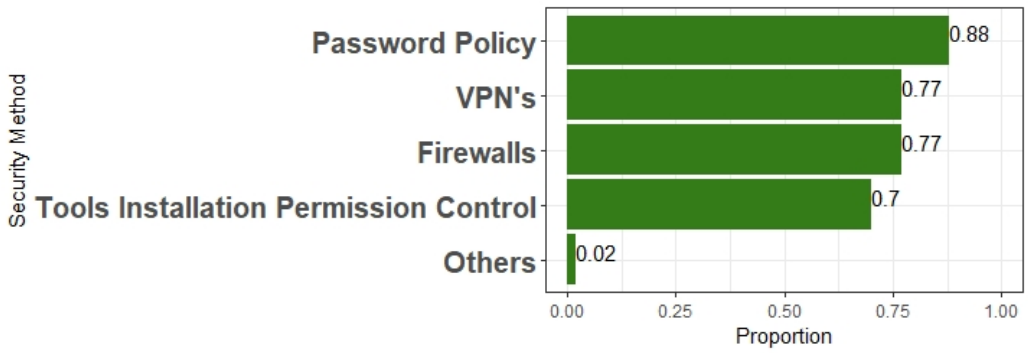


Figura 4.10: Questionamento sobre meios de segurança utilizando nas instituições

Como em vários ramos de atividades, a pesquisa demonstrou, através da Q12 (Tabela 4.1), que a transparência não é respeitada nas organizações, visto que aproximadamente 47% dos entrevistados responderam que não foram informados sobre tentativas de ataques ou forma de divulgação em caso de ataques que pudessem colocar seus dados em risco. Um fator importante e descrito claramente na LGPD é a obrigatoriedade das organizações de informar ao usuários se seus dados são ou não compartilhados com outras organizações, sendo que apenas 26% dos respondentes da Q14 (Tabela 4.1) estão cientes, ou seja, foram informados sobre essa possibilidade de compar-

tilhamento. Vale ressaltar que devem ser avisados não somente da possibilidade, mas também quem são os responsáveis e para qual finalidade o compartilhamento foi realizado, como pode ser observado na Figura 4.11

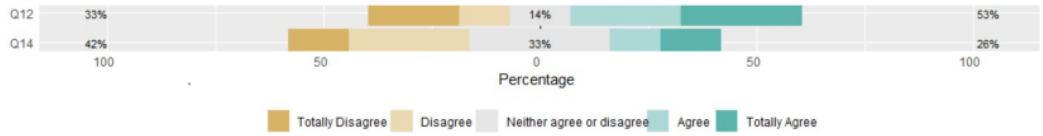


Figura 4.11: Relacionamento das Questões 12 e 14, sobre transparência na divulgação de ataques e na transparência quanto a compartilhamento de dados.

Os dados coletados por organizações devem ter uma finalidade específica e um prazo determinado, e o titular dos dados tem o direito ao "esquecimento", ou seja, a qualquer tempo, pode solicitar que seus dados sejam retirados em sua totalidade. A pesquisa demonstrou com a Q15 (Tabela 4.1) que 72% dos entrevistados desconhecem esse direito trazido pela LGPD. Associada com Q15 da (Tabela 4.1), a Q20 da (Tabela 4.1) buscou apresentar o conhecimento do respondente sobre a exclusão dos dados pessoais por parte dos responsáveis a pedido do usuário. Essa questão trouxe à pesquisa 2 (dois) dados importantes: o primeiro é que apenas 31% informaram que sua organização possui essa iniciativa em sua corporação, o que é um dado ruim para uma diretriz tão importante para a privacidade dos dados; e o segundo é que mais da metade, 51%, preferiu não opinar, provando total desconhecimento sobre esse direito ao esquecimento em sua corporação, conforme apresentado na Figura 4.12. Vale ressaltar que a legislação tem uma limitação para esse pedido, ou seja, se o estado necessitar desses dados para o interesse maior, esse pedido poderá ser negado.

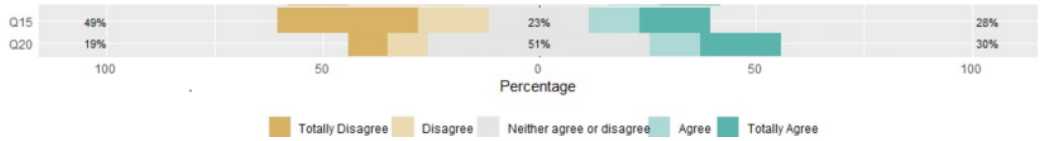


Figura 4.12: Relacionamento das Questões 15 (direito ao esquecimento) e 20 (Mecanismos de exclusão automática de dados.)

A LGPD aplica um tratamento especial para os chamados "dados sensíveis". Para tanto, a lei define dados sensíveis como quaisquer dados relativos à "origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou a organização de caráter religioso, filosófico ou político, ao dado referente à saúde ou à vida sexual e ao dado genético ou biométrico"[4]. Nesse sentido, o dado preocupando que foi possível coletar na Q16 (Tabela 4.1) é quanto ao conhecimento sobre essa diferenciação dos dados. Como resultado, temos que 65% dos entrevistados informaram não saber a diferença entre os dados pessoais e dados pessoais sensíveis, conforme apresentado na Figura 4.13

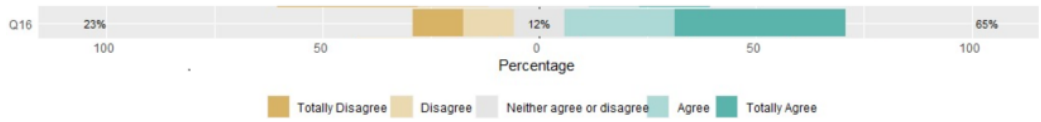


Figura 4.13: Resultado sobre conhecimento da diferença entre dados pessoais e dados pessoais sensíveis.

A pesquisa apresenta um dados preocupante quanto à conscientização por parte da alta gestão, ou seja, um desconhecimento ou descaso com a LGPD, uma vez que mais de 49% dos entrevistados declararam não receber nenhuma orientação quanto aos regramentos da lei em suas tarefas diárias, demonstrado pelo resultado da Q17 (Tabela 4.1). A questão anterior poderia ser resolvida com a governança e a auditoria, pois o cenário não parece tão ruim: 70% afirmaram, na Q18 (Tabela 4.1), que as organizações mantém a documentação organizada e atualizada, como mostra a Figura 4.14. Vale ressaltar que, em caso de auditorias, a documentação deve ficar disponível, contendo inclusive os dados dos responsáveis pela guarda e tratamento dos dados.

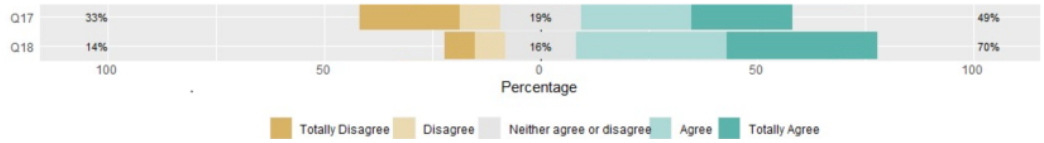


Figura 4.14: Relacionamento das questões sobre conscientização e documentação (governança)

O plano de contingência é previsto pela LGPD, também chamado de "Controle de incidentes", sendo um conjunto de ações que compõem um plano de ações diante de um incidente, ou seja, o que fazer caso haja algum vazamento de dados. A pesquisa demonstra, por meio da Q19 (Tabela 4.1), que as empresas continuam com a política do "não vai acontecer", prova disso é que pouco mais da metade, 51%, respondeu que sua corporação possui o plano de contingência.

A questão Q21 (Tabela 4.1) buscou ter um feedback sobre a visão dos respondentes no que tange uma visão geral sobre a lei, e foi possível constatar que muita gente sente falta, em suas instituições, de divulgação sobre normas e políticas de segurança. Transparência nos processos ainda é um grande desafio para as empresas e, quando há algum tipo de iniciativas, não há continuidade, segundo os respondentes. Outro fator importante analisado foi quanto a falta de ferramentas e/ou processos para apoio aos colaboradores, que muitas vezes ficam reféns da obrigatoriedade de seguir diretrizes internas criadas por profissionais que não possuem conhecimento adequado, o que normalmente não levam a um resultado positivo.

4.2 ANÁLISE COMPARATIVA DO ARCABOUÇO LEGAL E NORMATIVO

O Conselho Nacional de Arquivos (Conarq) é o responsável pela definição da forma em que são avaliados os repositórios seguros no Brasil, por meio da Resolução nº 43 de 2014, que foi editada em 2015. Foi definido um conjunto de regras para validação de Repositórios Digitais Confiáveis. A resolução levou em consideração as diretrizes contidas no modelo utilizado para

auditoria e certificação de repositórios confiáveis, conhecido como *Trustworthy Repository Audit e Certification: Criteria and Checklist - TRAC*[5]; e, como referência tecnológica, a do modelo *Open Archival Information System* - OAIS.

A análise comparativa é apresentada em 3 perspectivas: na de Governança (Tabela 4.3); seguida de Tratamento e Responsabilidades (Tabela 4.4); e finalizando com Segurança da Informação (Tabela 4.5). A Governança trata basicamente das diretrizes que a LGPD traz acerca do gerenciamento das informações, padrões, regras fundamentais, etc. A Tabela 4.3 apresenta, na primeira coluna, a diretriz apontada pela LGPD e, na segunda coluna, caso haja, o item correspondente no TRAC.

Tabela 4.3: Análise Comparativa LGPD [4] x TRAC [5] - Governança

Item de análise	LGPD	TRAC
Controle de Acesso	Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.	SeçãoA.A3.8- O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.
Plano de Contingência	II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.	Não contem no TRAC.
Monitoramento	III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.	Não contem no TRAC.
Controle de Acesso	IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.	SeçãoB..B6.3- O repositório garante que os acordos aplicáveis às condições de acesso sejam cumpridos.

Integridade	V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.	Não contém no TRAC.
Transparência	VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.	SeçãoA.A3.7- O repositório se compromete com a transparência e responsabilidade em todas as ações de suporte à operação e gestão do repositório, especialmente aquelas que afetam a preservação do conteúdo digital ao longo do tempo.
Controle de Acesso	VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	SeçãoB3.B6.4-B6.5 - O sistema de gerenciamento de acesso ao repositório implementa totalmente a política de acesso.
Prevenção	VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	SeçãoB.B3.1-B3.1 - O repositório tem estratégias de preservação documentadas.
	IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.	Não Contem no TRAC.
Plano de Contingência	X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	Não contém no TRAC.
Plano de Contingência	Art. 50, § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.	SeçãoA-3.6 - O repositório tem um histórico documentado das mudanças em suas operações, procedimentos, software e hardware que, quando apropriado, está vinculado a estratégias de preservação relevantes e descreve os efeitos potenciais na preservação de conteúdo digital.

Monitoramento	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais.	SeçãoA.A1.1 - O repositório tem uma declaração de missão que reflete um compromisso com a retenção, gerenciamento e acesso a longo prazo às informações digitais.
Transparência	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta.	Não contém no TRAC
Transparência	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.	SeçãoA.A3.2O - O repositório possui procedimentos e políticas em vigor e mecanismos para sua revisão, atualização e desenvolvimento à medida que o repositório cresce e a tecnologia e a prática da comunidade evoluem.
Prevenção	Art.50,§2º,I - implementar programa de governança em privacidade que, no mínimo: d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade.	SeçãoC.C3.2 - O repositório implementou controles para atender adequadamente a cada uma das necessidades de segurança definidas.
Transparência	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;	SeçãoA.A3.7 - O repositório se compromete com a transparência e responsabilidade em todas as ações de suporte à operação e gestão do repositório, especialmente naquelas que afetam a preservação do conteúdo digital ao longo do tempo.
Monitoramento	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos.	SeçãoA.A4.2 - O repositório possui processos para revisar e ajustar planos de negócios pelo menos uma vez por ano.

Plano de Contingência	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: g) conte com planos de resposta a incidentes e remediação.	SeçãoB.B6.6 - O repositório registra todas as falhas de gerenciamento de acesso e a equipe analisa os incidentes de "negação de acesso" inadequados.
Prevenção	Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.	SeçãoA.A3.9 - O repositório se compromete com um cronograma regular de autoavaliação e certificação e, se certificado, compromete-se a notificar os organismos de certificação de mudanças operacionais que irão alterar ou anular seu status de certificação.
Segurança da Informação	Art. 50, § 2º, II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.	Não contém no TRAC.
Transparência	Art. 50, § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.	Não contém no TRAC.
Controle de acesso	Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.	Não Contem no TRAC.

Conforme apresentado na Tabela 4.3, apesar de contemplar algumas diretrizes, várias outras importantes não foram contempladas. Vale ressaltar que, mesmo que alguns itens que a LGPD considera como diretriz de governança, o TRAC pode tratar de outras áreas temáticas. Podemos destacar como importante no tema de governança alguns itens, como:

- Art. 6°, III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos

em relação às finalidades do tratamento de dados.

Como vemos no trecho acima, a LGPD apresenta de forma clara sobre as limitações, já o TRAC detalha a forma como é armazenado, tipos, formatos, mas não indica qual ou quais dados podem ser armazenados.

- Art. 50, § 2º, I - implementar programa de governança em privacidade que, no mínimo: b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta.

No que tange à privacidade, o TRAC não define como deve ser feita a proteção de dados, mencionando apenas as questões relacionadas ao controle de logs de acesso, análise de perdas e recuperação de dados. O TRAC não deixa claro nas suas diretrizes o que deve ser feito para proteção à privacidade dos dados. Uma vez feita a comparação da definição básica sobre governança, o próximo passo é mencionar sobre o tratamento dos dados e seus respectivos responsáveis. A Tabela 4.4 apresenta a comparação entre a LGPD e TRAC.

Tabela 4.4: Análise comparativa LGPD [4] x TRAC [5] - Tratamento e Responsabilidades

Item de análise	LGPD	TRAC
Análise de Riscos	Art. 5º Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.	SeçãoA.A3.8 - O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.
	Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.	Não contem no TRAC.

Controle de Acesso e Permissões	IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.	SeçãoB.B6.3 - O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.
Integridade	V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.	SeçãoA.A3.8 - O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.
Controle de Acesso e Permissões	VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	SeçãoC.C1.6 - O repositório relata à sua administração todos os incidentes de corrupção ou perda de dados e as medidas tomadas para reparar/ substituir dados corrompidos ou perdidos.
Prevenção	VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	SeçãoC.C1.6 O repositório relata à sua administração todos os incidentes de corrupção ou perda de dados e as medidas tomadas para reparar/- substituir dados corrompidos ou perdidos.
Monitoramento	X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.	SeçãoB.6.3 - O repositório garante que os acordos aplicáveis às condições de acesso sejam cumpridos.
Sigilo e Privacidade	Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular.	
	II - para o cumprimento de obrigação legal ou regulatória pelo controlador;	Não contém no TRAC.

Compartilhamento e Armazenamento	III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei.	Não contém no TRAC.
Controle de Acesso e Permissões.	Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.	SeçãoA.A3.3 - O repositório mantém políticas escritas que especificam a natureza de quaisquer permissões legais necessárias para preservar o conteúdo digital ao longo do tempo, e o repositório pode demonstrar que essas permissões foram adquiridas quando necessário.
Controle de Acesso e Permissões.	§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.	Não contém no TRAC.
Controle de Acesso e Permissões.	§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.	Não contém no TRAC.
Controle de Acesso e Permissões.	§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.	Não contém no TRAC.
Controle de Acesso e Permissões.	Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento.	Não contém no TRAC.

	II - forma e duração do tratamento, observados os segredos comercial e industrial.	Não contém no TRAC
Transparência	III - identificação do controlador.	Não contém no TRAC
Transparência	IV - informações de contato do controlador.	Não contém no TRAC
Transparência	V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade.	Não contém no TRAC
Transparência	Art 9. § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.	Não contém no TRAC.
Sigilo e Privacidade	Art. 11º Art. 11º O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador.	Não contém no TRAC.
Sigilo e Privacidade	Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.	Não contém no TRAC.
Sigilo e Privacidade	Art. 14º O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.	Não contém no TRAC.

Transparência	Art. 14º § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.	Não contém no TRAC.
Monitoramento	Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.	SeçãoB.B3.2 - O repositório possui mecanismos para monitoramento e notificação quando as Informações de Representação (incluindo formatos) se aproximam da obsolescência ou não são mais viáveis.
Monitoramento	II - fim do período de tratamento.	Não contém no TRAC.
Transparência	III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público.	Não contém no TRAC.
Monitoramento	IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.	Não contém no TRAC.
Monitoramento	Art. 16º Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador.	Não contém no TRAC.
Sigilo e privacidade	II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.	Não contém no TRAC.
Compartilhamento e Armazenamento	III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei. ou	Não contém no TRAC.

Compartilhamento e Armazenamento	IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.	Não contém no TRAC.
Sigilo e Privacidade	Art. 18º O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei.	Não contém no TRAC.
Compartilhamento e Armazenamento	V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.	Não contém no TRAC.
Sigilo e Privacidade	VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei.	Não contém no TRAC.
Compartilhamento e Armazenamento	VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.	Não contém no TRAC.
Sigilo e Privacidade	IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.	Não contém no TRAC.
Sigilo e Privacidade	Art. 18. § 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.	Não contém no TRAC.

	Art. 23º O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que: I - Sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.	Não contém no TRAC.
Compartilhamento e Armazenamento	Art. 26º 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, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.	Não contém no TRAC.
Compartilhamento e Armazenamento	Art. 26º IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres.	Não contém no TRAC.
	Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.	Não contém no TRAC.

Compartilhamento e Armazenamento	Art. 33º A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei.	Não contém no TRAC.
Compartilhamento e Armazenamento	Art. 34º 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, que levará em consideração: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional.	Não contém no TRAC.
Sigilo e Privacidade	II - a natureza dos dados;	
Não contém no TRAC. Monitoramento	Art. 37º O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.	SeçãoC.C3.3 - A equipe do repositório definiu funções, responsabilidades e autorizações relacionadas à implementação de mudanças no sistema.
Monitoramento	Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial. Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.	SeçãoA.A3.8 A3.8 - O repositório se compromete a definir, coletar, rastrear e fornecer, sob demanda, suas medições de integridade de informações.

Transparência	Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.	SeçãoA.A2.1 - O repositório identificou e estabeleceu as funções que precisa desempenhar e nomeou funcionários com habilidades e experiência adequadas para cumprir essas funções.
Transparência	Art. 41. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.	Não contém no TRAC.

No que tange ao tratamento e às responsabilidades, podemos ver, na Tabela 4.4, que o TRAC não contempla boa parte das diretrizes da LGPD e, em alguns casos, apenas descreve superficialmente sobre outras regras semelhantes. Como o objetivo principal da LGPD é o cuidado com a privacidade, o tratamento dos dados deve ser feito exatamente como diz a lei. Vemos, por exemplo, que um dos itens de maior relevância, que é o "consentimento", não é explicito no TRAC. O art. 8°, § 2º, é muito claro sobre o consentimento: [4]

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. (LGPD, 2018).

A LGPD traz ainda uma diretriz muito importante, o "direito ao esquecimento", a qual versa sobre o direito que o titular dos dados tem de solicitar, a qualquer tempo, que seus dados sejam eliminados da base de dados do depositante. O TRAC, por se tratar de regras voltadas para repositórios arquivísticos que, por sua natureza, preservam por longo período, não deixa claro a forma e as regras de eliminação dos dados armazenados.

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
>
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
>
> [...]
>
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público. (LGPD, 2018)

Como já vimos as regras básicas sobre a forma de tratamento dos dados e seus respectivos responsáveis, vamos analisar agora a segurança e o sigilo das informações. Vale ressaltar que o TRAC dita as normas para que os repositórios digitais possam ser considerados seguros, ou seja, é o conjunto de regras que certifica um Repositório Digital Confiável - RDC. A Tabela 4.5 mostra que muitos itens de segurança e prevenção à incidentes, bem como ao sigilo dos dados, não estão de acordo com as diretrizes da LGPD.

Tabela 4.5: Análise comparativa LGPD [4] x TRAC [5] - Sigilo e Privacidade

Item de análise	LGPD	TRAC
Controle de Acesso	Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.	SeçãoC.C1.5 C1.5 - O repositório tem mecanismos eficazes para detectar corrupção ou perda de bits.
Plano de Contingência	VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.	SeçãoC.C2.1 - O repositório tem tecnologias de hardware apropriadas para os serviços que fornece à (s) sua (s) comunidade (s) designada (s) e tem procedimentos em vigor para receber e monitorar notificações e avaliar quando mudanças na tecnologia de hardware são necessárias.
	Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.	SeçãoB.B6.2 - O repositório implementou uma política para registrar todas as ações de acesso (incluindo solicitações, pedidos, etc.) que atendam aos requisitos do repositório e dos produtores/depositantes de informações.

Compartilhamento de Dados	Art. 34º 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, que levará em consideração: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional.	Não contém no TRAC.
Compartilhamento de dados	II - a natureza dos dados;	Não contém no TRAC.
Compartilhamento de Dados	III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei.	Não contém no TRAC.
Compartilhamento de Dados	IV - a adoção de medidas de segurança previstas em regulamento.	SeçãoC.C3.1 - O repositório mantém uma análise sistemática de fatores como dados, sistemas, pessoal, planta física e necessidades de segurança.
Compartilhamento de Dados	V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.	Não contém no TRAC.
Compartilhamento de dados	VI - outras circunstâncias específicas relativas à transferência.	Não contém no TRAC.
Plano de Contingência	Art. 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.	SeçãoC.C1.6 - O repositório relata à sua administração todos os incidentes de corrupção ou perda de dados e as medidas tomadas para reparar/-substituir dados corrompidos ou perdidos.
Plano de Contingência	Art. 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.	Não contém no TRAC.

Transparência	Art. 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.	Não contém no TRAC.
Transparência	§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:I - a descrição da natureza dos dados pessoais afetados.	Não contém no TRAC.
Transparência	I - a descrição da natureza dos dados pessoais afetados.	Não contém no TRAC.
Transparência	III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial.	SeçãoC.C3.1 - O repositório mantém uma análise sistemática de fatores como dados, sistemas, pessoal, planta física e necessidades de segurança.
Análise de Riscos	IV - os riscos relacionados ao incidente.	SeçãoC.C3.1 - O repositório mantém uma análise sistemática de fatores como dados, sistemas, pessoal, planta física e necessidades de segurança.
Monitoramento	V - os motivos da demora, no caso de a comunicação não ter sido imediata.	Não contém no TRAC.
Prevenção	VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.	SeçãoC.C3.4 - O repositório possui planos escritos de preparação e recuperação para desastres, incluindo pelo menos um backup externo de todas as informações preservadas junto com uma cópia externa do (s) plano (s) de recuperação.
Segurança da Informação	Art. 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.	SeçãoC.C3.2 - O repositório implementou controles para atender adequadamente a cada uma das necessidades de segurança definidas.

Monitoramento	Art. 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, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. g) conte com planos de resposta a incidentes e remediação.	SeçãoA.A3.1 - O repositório definiu sua (s) comunidade (s) designada (s) e base (s) de conhecimento associada (s) e possui definições e políticas publicamente acessíveis para ditar como seus requisitos de serviço de preservação serão atendidos.

Diretrizes importantes e obrigatórias da referida lei não estão claras no TRAC, por exemplo, o art. 47 [4], o qual diz respeito à responsabilidade da segurança da informação por parte dos agentes manipuladores das informações durante e, até mesmo, depois da utilização dos dados.

> Art. 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. (LGPD, 2018)

Não menos importante, o art. 48 da LGPD [4] versa sobre a publicidade de incidentes que venham a ocorrer, mesmo que o TRAC atenda a alguns requisitos desse artigo. Ainda no art.48, §2°, incisos I e II, "I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.", o qual diz sobre os possíveis medidas que devem ser adotadas após algum incidente, diretriz que também não fica clara no TRAC.

> Art. 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. IV - os riscos relacionados ao incidente. (LGPD, 2018)

4.3 CONCEPÇÃO DO GUIA

Após um estudo sobre a legislação internacional GDPR e outras legislações europeias, que servem de base para LGPD no que se refere a privacidade de dados, algumas diretrizes foram levantadas para servir como referência para o estudo do guia. Para chegar no modelo proposto, foi necessário uma análise da LGPD, do TRAC e de testes práticos de validação de segurança.

4.4 GUIA

O Guia proposto neste trabalho para realizar a adequação a LGPD é um modelo de referência que possibilitará à organização adequar seu negócio à legislação vigente. O guia leva em consideração às diretrizes da LGPD e as melhores práticas no que tange as técnicas e metodologias para segurança da informação e privacidade de dados.

Para adequação às normas, é preciso que haja um documento auxiliar com as regras ou diretrizes legais. Assim sendo, apresentamos uma série de técnicas e soluções que proporcionam a segurança dos dados e sua privacidade. Elas estão separados em 5 itens, a saber:

1. Gestão de acesso a informação.
    (a) Criação de tela que possibilite ao usuário consultar de forma simples os seguintes itens:
        i. Dados que estão sendo tratados.
        ii. Como esses dados estão sendo tratados.
        iii. Finalidade do tratamento.
        iv. Forma que os dados foram coletados.
        v. Indicação sobre a segurança quanto a integridade dos dados.
        vi. Log com a última análise e/ou tratamento dos dados (deve ser armazenado em redundância sempre em servidores diferentes de onde estiver a aplicação).
2. Tratamento e Consentimento.
    (a) Elaboração de tela que informe ao usuário qual a finalidade do tratamento dos dados coletados:
        i. Solicitação para tratamento dos dados (Consentimento).
            A. Em caso de documento físico, deverá ser assinado e armazenado em local seguro, para salvaguardo do controlar.
            B. Em caso de módulo sistêmico, deverá ficar contido em log os dados de dia e hora.
        ii. Revogação de consentimento.
            A. Em caso de documento físico, deverá ser assinado e armazenado em local seguro, para salvaguarda do controlador.

B. Em caso de módulo sistêmico, deverá ficar contido em log os dados de dia e hora.

iii. Contendo o responsável pelo tratamento e seu contato.

iv. Opção que indique e/ou diferencie dados pessoais de dados pessoais sensíveis.

A. Esse deverá será tratado de forma restrita, e o controle de acesso obrigatoriamente deverá ser mais rígido.

v. Informativo contendo a finalidade dos dados.

A. Descritivo exato da finalidade (Evitar o vício de consentimento). Em caso de alteração de finalidade, o titular deverá ser notificado.

(b) Elaborar de documento ou modulo sistêmico que informe ao usuário que, por força de lei, os dados serão tratados sem o consentimento.

i. Em caso de documento físico, deverá ser assinado e armazenado em local seguro, para salvaguarda do controlador.

ii. Em caso de módulo sistêmico, deverá ficar contido em log os dados de dia e hora, em local separado de onde o sistema estiver hospedado.

(c) Elaboração de documento físico ou eletrônico para usuário, informando que os dados do titular foram compartilhados com entidades governamentais por motivos de força de lei.

3. Segurança.

(a) Medidas técnicas para promover a segurança.

i. Controle e monitoramento de atividades de usuários.

ii. Controle de ações do tipo “delete”, contendo opção de confirmação informando que os dados serão perdidos. (Evitar perdas acidentais).

iii. Criação de papéis ou perfis de usuários que evitem acessos indevidos.

iv. Log contendo o controle de alterações:

A. Indicação dos campos alterados.

B. Indicação do responsável pela alteração.

v. Realizar a criptografia dos dados (anonimização), principalmente em casos de dados sensíveis.

4. Governança.

(a) Plano de Segurança

i. Política de Gestão de acesso - Senha.

A. Senha contendo pelo menos 8 caracteres.

B. Utilização obrigatória de letras maiúsculas e minusculas na senha.

C. Utilização obrigatória de números.

D. Utilização obrigatória de caracteres especiais.

E. Expiração da senha com obrigação de alteração por prazo mínimo de 6 meses.
F. Proibição de utilização da mesma senha no momento da alteração.
G. Bloquear a senha em caso de 5 tentativas incorretas.
H. Verificação de usuário que deverá ser removido, através de análise de acesso.

ii. Medidas técnicas e metodológicas que comprovem os cuidados com a segurança e privacidade dos dados.
iii. Monitoramento e avaliação de incidentes.
iv. Elaboração constante de relatórios contendo as boas práticas para garantir a segurança e privacidade dos dados.

(b) Plano de contingência.

i. Análise de incidentes.
A. Prova de incidente ocorrido (evidência).
B. Relatório de incidentes.
C. FAQ dos incidentes ocorridos.
D. Lições aprendidas.

ii. Resposta a incidentes.

(c) Análise de Riscos.

i. Análise dos riscos, contendo a criticidade.
ii. Indicação do risco em caso de incidente.
iii. Documento contendo medidas para minimizar os riscos.

5. Armazenamento.

(a) Criação de rotina de backup (evitar a perda de dados).

i. Análise de escalabilidade do volume de dados.

(b) Criação de atualização com redundância.
(c) Instalação de ferramenta para monitoramento de acesso.
(d) Log de atividades (inserir, alterar e apagar).
(e) Atualizar constantemente as soluções de armazenamento de códigos de sistemas.
(f) Atualização de plugins de sítios internos.

O guia foi elaborado em forma de checklist, conforme apresentados nas figuras 4.15, 4.16 e 4.17.

	Questionário de Auditoria	Norma/Lei Referência	Status TC	PC	NC	N/A
Governança	Sua empresa possui documentação contendo a motivação da coleta de dados?	LGPD. Art7°	◎	◎	◎	◎
	Há alguma opção no sistema para o usuário acompanhar, solicitar ou validar o tratamento dos seus dados?	LGPD. Art9°/TRAC. SeçãoB, Item B6.2	◎	◎	◎	◎
	O sistema possui alguma forma de tratamento diferenciado dados sensiveis?	LGPD. Art11	◎	◎	◎	◎
	O sistema possui alguma declaração de missão, contendo os requisitos legais e regulamentares?	TRAC. SeçãoA1, item A1.1	◎	◎	◎	◎
	O sistema possui algum plano de sucessão para garantir a continuidade, medidas e planos de contingencia?	TRAC: SeçãoA1, Item A1.2	◎	◎	◎	◎
	Você possui algum controle no que tange competencias, organograma, detalhamento do trabalho ou evolução dos requisitos do repositório?	TRAC. SeçãoA,item A2.2	◎	◎	◎	◎
	O sistema possui alguma politica de documentação para o sistema ou para o legado do conteúdo digital?	TRAC. SeçãoA. Item A3.6	◎	◎	◎	◎
	O sistema possui mecanismo para identificar a responsabilidade pela preservação e tratamento formalizados?	LGPD. Art9,VI/ TRAC.SeçãoC, item C3.3	◎	◎	◎	◎
	O sistema possui plano de preservação devidamente documentado?	TRAC. Seção B3, item B3.1	◎	◎	◎	◎
	O sistema possui uma politica de acesso documentada?	TRAC. SeçãoB, item B6.1	◎	◎	◎	◎
	O sistema possui documentação contendo plano de mudança e atualização?	TRAC. Seção C, item C1.8	◎	◎	◎	◎
	O sistema possui algum plano de contingencia ou mecanismo de recuperação em caso de incidentes?	LGPD.Art50/TRAC. Seção C, item C3.4	◎	◎	◎	◎
	O sistema possui documentação contendo as ações realizadas para garantir a proteção dos dados, bem como, a eficacia dessas ações?	LGPD. Art50,II	◎	◎	◎	◎
	O sistema possui algum documento contendo as boas-práticas adotadas pelos operadores para análise de riscos quanto aos dados que estão sendo ou serão tratados?	LGPD. Art.38	◎	◎	◎	◎
	Existe um documento ou meio de controle sobre todos os dados que estão sob seu controle?	LGPD. Art.50	◎	◎	◎	◎
	Existe algum controle sobre a escalabilidade dos dados que são tratados?	LGPD. Art50$2/ TRAC.A, item A3.4	◎	◎	◎	◎
	Há algum plano de governança contendo análise sobre os riscos?	LGPD.art48,VII/ TRAC. SeçãoC, item C3.2	◎	◎	◎	◎
	Existe plano de governança com foco em supervisão interna e externa?	LGPD. Art50	◎	◎	◎	◎
	Há um plano de governança que registre, monitore e informe como proceder em caso de incidente?	LGPD. Art48,VI/ TRAC. Seção C, item C3.4	◎	◎	◎	◎

Legenda: TC=Totalmente Compatível; PC=Parcialmente Compatível; NC=Não Compatível; N/A=Não se Aplica

Figura 4.15: Análise de Adequação - Governança.

	Questionário de Auditoria	Norma/Lei Referência	Status TC - PC - NC - N/A			
Tratamento e Responsábilidades	Seu sistema possui algum relatório de impacto descrevendo quais processos podem colocar em risco os dados pessoais tratados?	LGPD. Art32	◎	◎	◎	◎
	Seu sistema possui documentação para mitigação de riscos?	LGPD48,VI/TRAC. Seção C, item C1.5	◎	◎	◎	◎
	Seu sistema tem algum controle que limite o tratamento dos dados de acordo com a finalidade?	LGPD.Art6, I	◎	◎	◎	◎
	O sistema possui modulo ou meio de consulta do titular sobre seus dados, forma e duração do tratamento e sobre sua integridade?	LGPD. Art18	◎	◎	◎	◎
	O sistema possui forma de atualização dos dados do titular?	LGPD.Art46 e art.18,III/	◎	◎	◎	◎
	Existe alguma forma de comprovação que existe medidas eficazes que foram adotadas que comprovem a detecção de perdas?	TRAC.SeçãoC, Item C1.5	◎	◎	◎	◎
	Seu sistema possui solicita consentimento do usuário para o tratamento dos dados?	LGPD.Art7,I	◎	◎	◎	◎
	O controlador possui alguma prova ou comprovante que afirme que o titular dos dados autorizou o tratamento?	LGPD.Art8°,S2	◎	◎	◎	◎
	O formulário ou opção eletronica sobre o consentimento de tratamento de dados, é detalhado e direto o suficiente para evitar o vicio de linguagem?	LGPD.Art8°,S4	◎	◎	◎	◎
	O sistema possui metodo facilitado para o usuário solicitar a revogação do consentimento no tratamento dos dados?	LGPD.Art8°,S5	◎	◎	◎	◎
	O sistema possui algum meio de consulta sobre as informações do controlador.	LGPD.Art9°,III e IV/ TRAC. SeçãoB, Item B6.2	◎	◎	◎	◎
	O sistema possui algum controle sobre aperfeiçoamento dos profissionais que estabeleça o desenvolvimento contínuo dos profissionais atuantes?	TRAC:SeçãoA, item A2.2	◎	◎	◎	◎
	O sistema possui mecanismos para transparência e idenficação de responsáveis no que tange a preservação digital?	LGPD.Art46/TRAC. SeçãoA, item 3.7	◎	◎	◎	◎
	O sistema possui documentação sobre a forma de coleta dos dados?	LGPD.Art38/TRAC. SeçãoA, Item 3.8	◎	◎	◎	◎
	O sistema possui algum alerta quanto a obsolescencia ou das informações que não são mais uteis ou viaveis?	LGPD.Art18,VI/ TRAC. SeçãoB, item B3.2	◎	◎	◎	◎
	O repositório possui controle e permissões de acordo com a responsábilidade dos atores?	TRAC.Seção 3, Item 3.3	◎	◎	◎	◎
	Há no sistema alguma atualização sobre o termo de consentimento em caso de alteração da finalidade?	LGPD.Art8°,S8	◎	◎	◎	◎
	O documento/formulário de consentimento diferencia dados pessoais e dados sensíveis?	LGPD,SeçãoII	◎	◎	◎	◎
	O sistema possui informações claras e de facil entendimento em caso de solicitação por parte de menores, que possibilite o entendimento da criança?	LGPD.Art14$6	◎	◎	◎	◎
	O sistema possui mecanismo para o finalizar o tratamento dos dados de acordo com os itens: a) Finalidade alcançada e;e b) Os dados deixarem de ser necessários.	LGPD.Art.17/TRAC. SeçãoB, Item B3.2	◎	◎	◎	◎
	O sistema possui algum mecanismo de exportação para portabilidade dos dados do titular?	LGPD.Art18,V	◎	◎	◎	◎
	O sistema possui algum meio pelo qual o titular solicite a eliminação dos dados pessoais?	LGPD.Art7°	◎	◎	◎	◎
	O sistema possui algum meio de informar ao titular sobre as entidades publicas ou privadas com as quais seus dados foram compartilhados ou usados pelo controlador?	LGPD.Art9°,V	◎	◎	◎	◎
	O sistema possui uma forma de disseminação integrada ou não sobre as solicitações feitas pelo titular e que deverá ser replicada em outros locais que obtiveram acesso aos dados?	LGPD.Art25/TRAC. SeçãoC, Item C1.7	◎	◎	◎	◎
	O sistema possui algum informativo sobre o compartilhamento de dados?	LGPD.Art18,VII	◎	◎	◎	◎
	Você possui compartilhamento de dados com organismos internacionais de acordo com a segurança prevista em lei?	LGPD.Art33,I	◎	◎	◎	◎
	Seu sistema possui algum meio de comprovar os registros das operações realizadas pelos operadores e controladores?	LGPD.Art37/TRAC. SeçãoA, Item A3.7	◎	◎	◎	◎

Legenda:TC=Totalmente Compatível; PC=Parcialmente Compatível; NC=Não Compatível; N/A=Não se Aplica

Figura 4.16: Análise de Adequação - Tratamento e Responsabilidades.

	Questionário de Auditoria	Norma/Lei Referência	Status TC - PC - NC - N/A			
Sigilo e privacidade	As politicas de boas praticas e governanças são divulgadas?	LGPD.Art50,$3/ TRAC.SeçãoB, ItemB.6.3	◎	◎	◎	◎
	Existe algum controle de alteração ou edição no sistema que identifique o responsavel e os riscos?	LGPD46,$1 /TRAC. SeçãoA, item3.7	◎	◎	◎	◎
	Há em seu sistema e/ou repositório alguma confirmação para alteração, adição ou exclusão de dados dos usuários?	LGPD.Art46/TRAC. SeçãoC, item1.6	◎	◎	◎	◎
	Seu sistema disponibiliza de facil acesso a forma de tratamentos dos dados do titular?	LGPD.Art18,II/ TRAC	◎	◎	◎	◎
	Seu sistema disponibiliza de facil acesso a forma de tratamentos dos dados do titular?	LGPDArt18,III/ TRAC.SeçãoA, item3.3	◎	◎	◎	◎
	O sistema possui alguma medida ou plano para evolução tecnologica? (autoavaliação; revisão de resultados,etc)	TRAC.SeçãoA, itemA3.9	◎	◎	◎	◎
	O sistema possui mecanismos para garantir ou preservar a integridade dos dados?	TRAC.SeçãoA, itemA3.8	◎	◎	◎	◎
	O sistema possui controle de acesso comautenticaçao?	LGPD.Art6,VII/ TRAC.SeçãoC, item3.2	◎	◎	◎	◎
	O sistema de gerenciamento de acesso contempla toda politica de de acesso?	TRAC.SeçãoB, itemB6.5	◎	◎	◎	◎
	O sistema possui alerta de acesso indevido ou negado?	TRAC.SeçãoB, itemB6.6	◎	◎	◎	◎
	O sistema temdocumentação para integrações e contendo detalhes de infraestrutura?	TRAC.SeçãoC, itemC1.1	◎	◎	◎	◎
	Existe algum controle sobre a forma de armazenamento e controle de backups?	TRAC.SeçãoC, ItemC1.2	◎	◎	◎	◎
	O sistema possui formas de identificar perda ou incidentes de integridade?	LGPD/TRAC. SeçãoC, itemC1.5	◎	◎	◎	◎
	O sistema possui monitoramento para análise de segurança de acordo comas normas legais?	TRAC.SeçãoC, C3.1	◎	◎	◎	◎
	Há no sistema alguma forma do usuário consultar sobre o tratamento dos seus dados?	LGPD.Art18	◎	◎	◎	◎
	Sua empresa segue alguma norma de segurança de instituições internacionais?	LGPD.Art34	◎	◎	◎	◎
	O sistema possui algummeio de recuperação de dados?	LGPD.Art6,VII/ TRAC.SeçãoC, itemC3.4	◎	◎	◎	◎
	O sistema temalgummecanismo extra de autenticão: Ex: autenticação emduas etapas?	LGPD.Art6°,VII/ TRAC.SeçãoB, itemB6.4	◎	◎	◎	◎
	Seu sistema possui algumcontrole sobre os responsáveis por acessar e/ou que possamter acessado enquanto os dados estiveramsobre posse da instituição?	LGPD.Art6,X/TRAC. SeçãoB, itemB6.5	◎	◎	◎	◎
	Existe no sistema emalguna divulgação sobre incidentes que ocorreram?	LGPD.Art48$2,I	◎	◎	◎	◎
	Emcaso de incidente, o sistema temmecanismos para avaliar quais os riscos?	TRAC.SeçãoA, Item A4.4	◎	◎	◎	◎
	Emcaso de incidente, o sistema temalgummecanismo que alerte sobre o comunição aos orgãos competentes?	LGPD.Art48	◎	◎	◎	◎
	Seu sistema possui contra-medidas a ataques ou perda de dados?	LGPD.Art6,VII/ TRAC.SeçãoC, item C1.6	◎	◎	◎	◎
	Seu sistema possui regras distintas para tratamento de dados sensiveis?	LGPD.Art11	◎	◎	◎	◎
	Seu sistema possui alguminformativo ou opção para reclamações e/ou solicitações dos usuários?	LGPD.Art41,$2/ TRAC.SeçãoB, Item B6.2	◎	◎	◎	◎
	O sistema possui normas ou manuais que orientemos controladores e operadores emsuas funções?	LGPD.Art50,I/TRAC. SeçãoA3	◎	◎	◎	◎

Legenda: TC=Totalmente Compatível; PC=Parcialmente Compatível; NC=Não Compatível; N/A=Não se Aplica

Figura 4.17: Análise de Adequação - Sigilo e Privacidade.

4.5 SÍNTESE DO CAPÍTULO

No capítulo 4, foi descrito a forma de elaboração do guia, contendo a análise comparativa entre a LGPD e TRAC (*Trustworthy Repositories Audit & Certification*), que é um guia de re-

ferência para repositórios seguros; além de apresentar o resultado de um *survey* que contou com a participação de 43 respondentes. Esse questionário contou com 21 questões elaboradas para analisar o nível de conhecimento dos usuários de tecnologia no que tange à LGPD, à segurança da informação e à privacidade de dados. Uma vez realizada a comparação entre as métricas do TRAC e a LGPD, legislação vigente no Brasil sobre a privacidade de dados, o capítulo 5 traz um estudo que apresenta a aplicação do guia na ferramenta Archivematica.

5 PROVA DE CONCEITO

5.1 DESCRIÇÃO DO AMBIENTE DE TESTES

Para realização a validação dos itens do guia, foi necessário a criação de um ambiente que possibilitasse a navegação e análise dos resultados. Para tanto, foi feita a instalação do Archivematica em sua versão 1.13.2, executado no sistema operacional Ubuntu 18.04.05 através de virtualização no Windows. A validação foi feita em computador i5 com memória RAM de 16GB.

5.2 VALIDAÇÃO DO GUIA

O guia conta com um checklist composto por 71 itens separados em 3 categorias: 19 de Governança; 27 de Sigilo e Privacidade; e de 25 Tratamento e Responsabilidades. Para fazer a validação, foi analisado item por item diretamente na ferramenta, com o intuito de garantir a credibilidade e confiança no guia.

O método para validação se deu por meio de testes funcionais que avaliaram a resposta do RDC-Arq e, quando não foi possível avaliar um item do guia, foi feita uma consulta na documentação do sistema no repositório.

Os itens foram validados por área temática e, para cada item encontrado, foi registrado uma evidência de sucesso ou sinalização de insucesso, de acordo com a marcação definida na análise como: TC=Totalmente Compatível; PC=Parcialmente Compatível; NC=Não Compatível;e N/A=Não se Aplica.

5.2.1 Aplicação do guia na área temática governança

A Tabela 5.1 apresenta o resumo da validação do Archivematica dentro dos itens definidos para a área temática governança. A validação foi realizada com o suporte do checklist do guia proposto e de acordo com a metodologia prevista, ou seja, testes funcionais e consulta a documentação do sistema no repositório.

Tabela 5.1: Quadro resumo do resultado da aplicação do guia na temática - Governança

Temática: Governança	**Status**			
	TC	**PC**	**NC**	**N/A**
1. Sua empresa possui documentação contendo a motivação da coleta de dados?			✓	

2. Há alguma opção no sistema para o usuário acompanhar, solicitar ou validar o tratamento dos seus dados?			✓
3, O sistema possui alguma forma de tratamento diferenciado para dados sensíveis?			✓
4. O sistema possui alguma declaração de missão, contendo os requisitos legais e regulamentares?	✓		
5. O sistema possui algum plano de sucessão para garantir a continuidade, medidas e planos de contingência?		✓	
6. Você possui algum controle no que tange competências, organograma, detalhamento do trabalho ou evolução dos requisitos do repositório?		✓	
7. O sistema possui alguma política de documentação para o sistema ou para o legado do conteúdo digital?	✓		
8. O sistema possui mecanismo para identificar a responsabilidade pela preservação e tratamento formalizados?	✓		
9. O sistema possui plano de preservação devidamente documentado?	✓		
10. O sistema possui uma política de acesso documentada?			✓
11. O sistema possui documentação contendo plano de mudança e atualização?			✓
12. O sistema possui algum plano de contingência ou mecanismo de recuperação em caso de incidentes?			✓
13. O sistema possui documentação contendo as ações realizadas para garantir a proteção dos dados, bem como a eficácia dessas ações?			✓
14. O sistema possui algum documento contendo as boas práticas adotadas pelos operadores para análise de riscos quanto aos dados que estão sendo ou serão tratados?			✓
15. Existe um documento ou meio de controle sobre todos os dados que estão sob seu controle?			✓
16. Existe algum controle sobre a escalabilidade dos dados que são tratados?			✓
17. Há algum plano de governança contendo análise sobre os riscos?			✓
18. Existe plano de governança com foco em supervisão interna e externa?			✓
19. Há um plano de governança que registre, monitore e informe como proceder em caso de incidente?			✓

Legenda: TC-Totalmente Compatível; PC-Parcialmente Compatível; NC-Não Compatível; N/A - Não se Aplica

Detalhamento da aplicação do guia para área temática governança:

Item avaliados:

1. Sua empresa possui documentação contendo a motivação da coleta de dados?

   Resultado: O Archivematica não possui documentação que informe qual a finalidade de tratamento para os que estão sendo coletados.

2. Há alguma opção no sistema para o usuário acompanhar, solicitar ou validar o tratamento dos seus dados?

   Resultado: O usuário não tem a possibilidade de acompanhar como seus dados estão sendo tratados, somente o perfil arquivista e administrador acessam ou tem controle sobre os dados.

3. O sistema possui alguma forma de tratamento diferenciado para dados sensíveis?

   Resultado: A ferramenta não possui nenhuma diferenciação ou mecanismo que identifique o tipo de dado armazenado.

4. O sistema possui alguma declaração de missão, contendo os requisitos legais e regulamentares?

   Resultado. O sistema possui em sua comunidade uma missão, porém, não documentada. Há na página do Archivematica uma proposta de missão, conforme pode ser consultada na página https://www.archivematica.org/pt-br/.

5. O sistema possui algum plano de sucessão para garantir a continuidade, medidas e planos de contingência?

   Resultado: Parcialmente compatível, pois existe plano de continuidade e aperfeiçoamento constante, porém não tem medidas ou planos de contingência, como pode ser consultado na página do Archivematica: https://www.archivematica.org/pt-br/.

6. Você possui algum controle no que tange competências, organograma, detalhamento do trabalho ou evolução dos requisitos do repositório?

   Resultado: A solução possui um fluxo de trabalho definido e uma comunidade que contribui constantemente para evolução do repositório, mas não possui controle de competências e organograma definido. O fluxo de trabalho pode ser consultado em: <https://github.com/artefactual/archivematica/graphs/contributors>.

7. O sistema possui alguma política de documentação para o sistema ou para o legado do conteúdo digital?

   Resultado: Sim, o sistema possui documentação em forma de *release*, conforme evidenciado na figura 5.1

Figura 5.1: Menu contendo as Releases do sistema.

8. O sistema possui mecanismo para identificar a responsabilidade pela preservação e tratamento formalizados?

   Resultado: Não. O documento trata apenas da forma de preservação, não contendo nada sobre responsáveis e responsabilidades.

9. O sistema possui plano de preservação devidamente documentado?

   Resultado: Sistema possui um documento contendo o plano de preservação.

10. O sistema possui uma política de acesso documentada?

    Resultado: O sistema possui política de acesso básica e sem documentação.

11. O sistema possui documentação contendo plano de mudança e atualização?

    Resultado: Sistema não possui nenhuma documentação dos itens informados.

12. O sistema possui algum plano de contingência ou mecanismo de recuperação em caso de incidentes?

    Resultado: Não há documentação que descreva procedimentos a serem tomados em casos de incidentes.

13. O sistema possui documentação contendo as ações realizadas para garantir a proteção dos dados, bem como a eficácia dessas ações?

    Resultado: Sistema possui documentação sobre a forma técnica de preservação, porém, não há documentação sobre a eficácia.

14. O sistema possui algum documento contendo as boas práticas adotadas pelos operadores para análise de riscos quanto aos dados que estão sendo ou serão tratados?

    Resultado: O sistema não possui documento ou manual para o operador dos dados.

15. Existe um documento ou meio de controle sobre todos os dados que estão sob seu controle?

    Resultado: Não existe nada que registre os dados que estão armazenados em posse do operador ou instituição.

16. Existe algum controle sobre a escalabilidade dos dados que são tratados?

    Resultado: Não há nenhum mecanismo de mensurar a escalabilidade dos dados.

17. Há algum plano de governança contendo análise sobre os riscos?

    Resultado: Não há documentação ou processo de análise de riscos.

18. Existe plano de governança com foco em supervisão interna e externa?

    Resultado: Não há plano para nenhuma das opções (interna e/ou externa).

19. Há um plano de governança que registre, monitore e informe como proceder em caso de incidente?

    Resultado: Não possui documentação que informe ou monitore sobre incidentes.

A segunda verificação, tratou de sigilo e privacidade, para identificar os itens que estão de acordo com as diretrizes da LGPD, uma vez que o foco principal da lei é a privacidade dos dados.

5.2.2 Aplicação do guia na área temática sigilo e privacidade

A Tabela 5.2 apresenta o resumo da validação do Archivematica dentro dos itens definidos para a área temática de Sigilo e Privacidade. A validação foi realizada com o suporte do checklist do guia proposto e de acordo com a metodologia prevista, ou seja, testes funcionais e consulta em documentação do sistema no repositório.

Tabela 5.2: Quadro resumo do resultado da aplicação do guia na temática - Sigilo e Privacidade

Temática: Sigilo e Privacidade	**Status**			
	TC	**PC**	**NC**	**N/A**
1. As políticas de boas praticas e governanças são divulgadas?			✓	
2. Existe algum controle de alteração ou edição no sistema que identifique o responsável e os riscos?		✓		
3. Há em seu sistema e/ou repositório alguma confirmação para alteração, adição ou exclusão de dados dos usuários?	✓			
4. Seu sistema disponibiliza de fácil acesso a forma de tratamentos dos dados do titular?			✓	
5. O sistema possui alguma medida ou plano para evolução tecnológica? (autoavaliação; revisão de resultados, etc.)	✓			

6. O sistema possui mecanismos para garantir ou preservar a integridade dos dados?	✓		
7. O sistema possui controle de acesso com autenticação?	✓		
8. O sistema de gerenciamento de acesso contempla toda política de acesso?			✓
9. O sistema possui alerta de acesso indevido ou negado?			✓
10. O sistema tem documentação para integrações contendo detalhes de infraestrutura?	✓		
11. Existe algum controle sobre a forma de armazenamento e controle de backups?		✓	
12. O sistema possui formas de identificar perda ou incidentes de integridade?			✓
13. O sistema possui monitoramento para análise de segurança de acordo com as normas legais?		✓	
14. Há no sistema alguma forma do usuário consultar sobre o tratamento de seus dados?			✓
15. Sua empresa segue alguma norma de segurança de instituições internacionais?	✓		
16. O sistema possui algum meio de recuperação de dados?			✓
17. O sistema tem algum mecanismo extra de autenticação: Ex: autenticação em duas etapas?		✓	
18. Seu sistema possui algum controle sobre os responsáveis por acessar e/ou que possam ter acessado enquanto os dados estiveram sobre posse da instituição?	✓		
19. Existe no sistema alguma divulgação sobre incidentes que ocorreram?			✓
20. Em caso de incidente, o sistema tem mecanismos para avaliar quais os riscos?			✓
21. Em caso de incidente, o sistema tem algum mecanismo que alerte sobre o ocorrido comunicando órgãos competentes?			✓
22. Seu sistema possui contra-medidas a ataques ou perda de dados?	✓		
23. Seu sistema possui regras distintas para tratamento de dados sensíveis?			✓
24. Seu sistema possui algum informativo ou opção para reclamações e/ou solicitações dos usuários?			✓
25. O sistema possui normas ou manuais que orientem os controladores e operadores em suas funções?			✓

Legenda: TC-Totalmente Compatível; PC-Parcialmente Compatível; NC-Não Compatível; N/A - Não se Aplica

Itens avaliados:

1. As políticas de boas praticas e governanças são divulgadas?

   Resultado: Não há políticas de boas práticas no que tange sigilo e privacidade.

2. Existe algum controle de alteração ou edição no sistema que identifique o responsável e os riscos?

   Resultado: Sim, o sistema possui um log que identifica o autor e o tipo de alteração realizada, porém, não identifica os riscos.

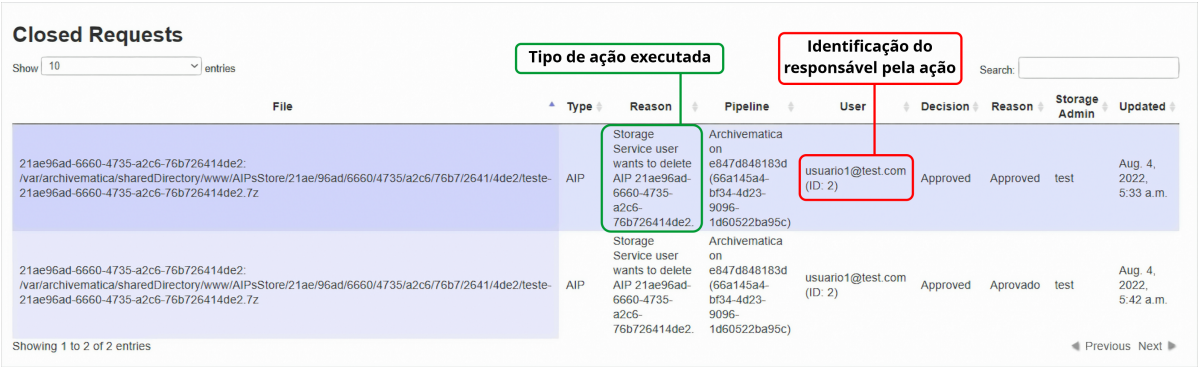


Figura 5.2: Log apresentando responsável e tipo de alteração

3. Há em seu sistema e/ou repositório alguma confirmação para alteração, adição ou exclusão de dados dos usuários?

   Resultado: Sim, o sistema apresenta mensagem solicitando confirmações sobre as alterações, conforme pode-se visualizar na evidência da figura 5.3

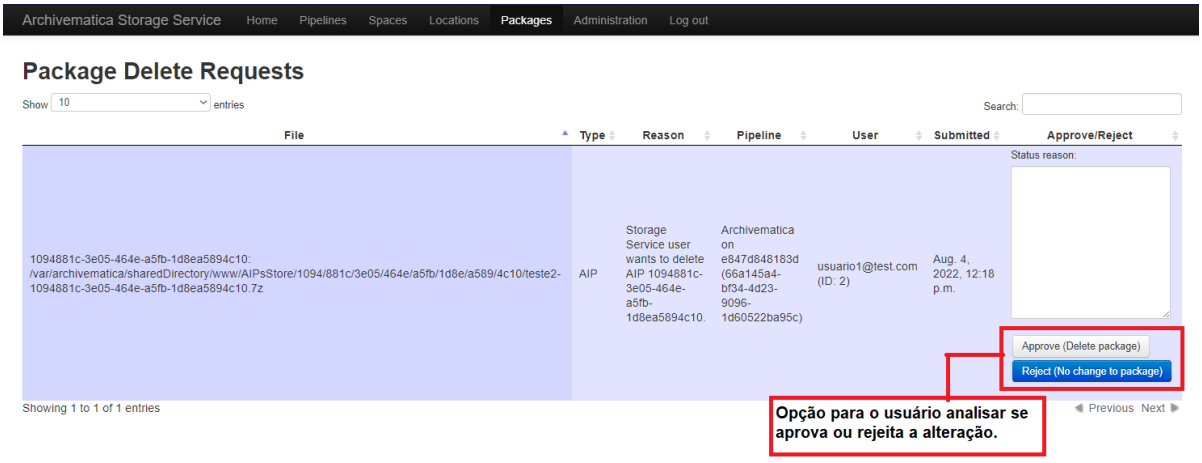


Figura 5.3: Tela de análise de alteração

4. Seu sistema disponibiliza de fácil acesso a forma de tratamentos dos dados do titular?

   Resultado: O titular do dados não tem acesso à forma que seus dados estão sendo tratados.

5. O sistema possui alguma medida ou plano para evolução tecnológica? (autoavaliação; revisão de resultados, etc.).

   Resultado: Sim, conforme figura 5.4.

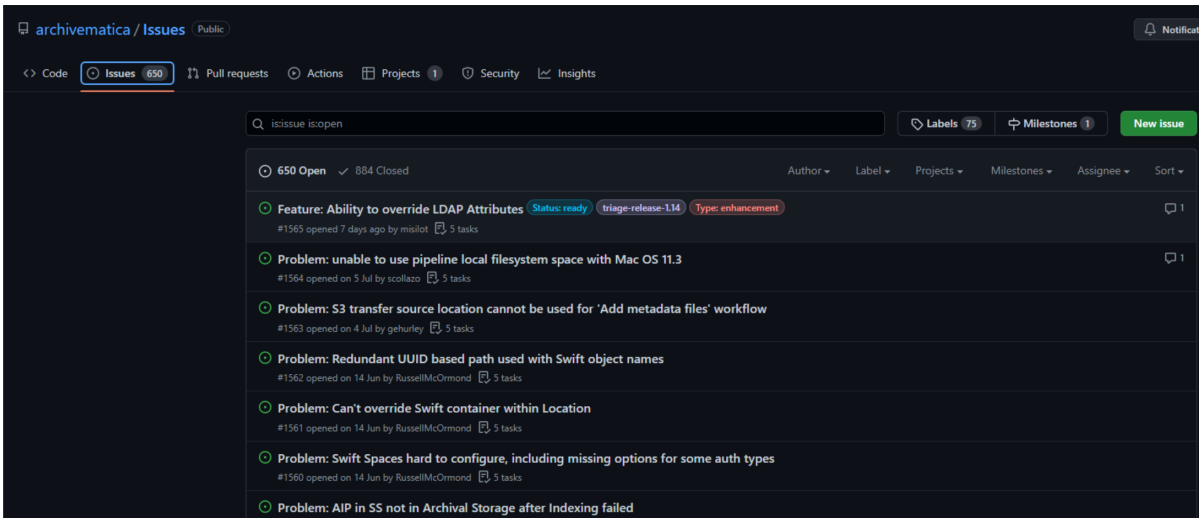


Figura 5.4: Metodologia e controle de evolução do sistema

6. O sistema possui mecanismos para garantir ou preservar a integridade dos dados?

   Resultado: Sim, o sistema utiliza o modelo OAIS para preservação e segurança dos dados.

7. O sistema possui controle de acesso com autenticação?

   Resultado: Sim, possui com usuário e senha, conforma figura 5.5.

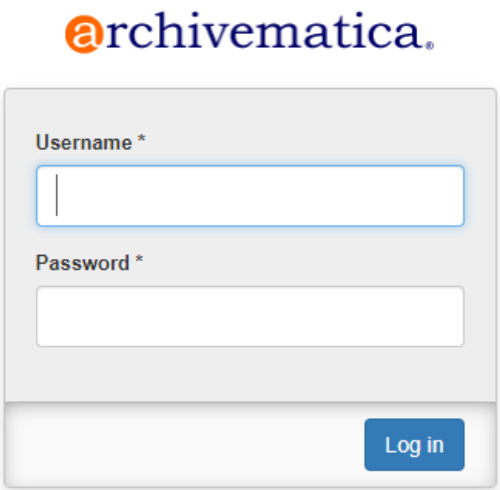


Figura 5.5: Tela de login para acesso ao Archivematica.

8. O sistema de gerenciamento de acesso contempla toda política de acesso?

   Resultado: Não, o sistema possui apenas política de acesso, mas não existe nenhuma política de permissões.

9. O sistema possui alerta de acesso indevido ou negado?

   Resultado: Não há nenhum alerta para nenhum dos casos.

10. O sistema tem documentação para integrações e contendo detalhes de infraestrutura?

    Resultado: Sim, o sistema possui documentação contendo detalhes de instalação e tecnologia utilizada.

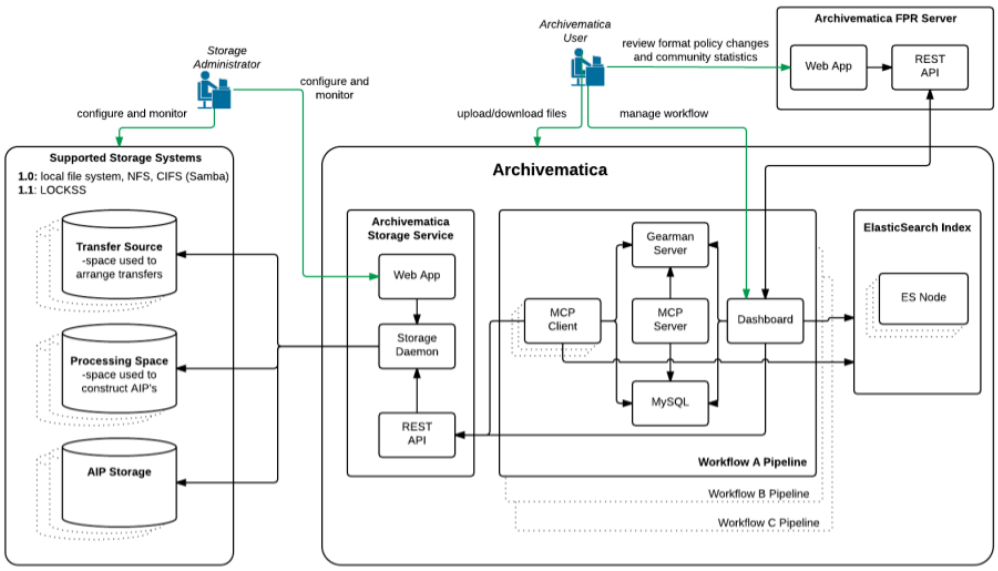


Figura 5.6: Demonstrativo da arquitetura padrão dos sistema.

11. Existe algum controle sobre a forma de armazenamento e controle de backups?

    Resultado: Há controle sobre a forma de armazenamento, porém, sobre o backup, requer uma configuração externa.

12. O sistema possui formas de identificar perda ou incidentes de integridade?

    Resultado:O sistema não possui análise ou detecção para identificar incidentes.

13. O sistema possui mecanismos para recuperação de dados?

    Resultado: Não existe mecanismos para recuperação de dados.

14. O sistema possui monitoramento para análise de segurança de acordo com as normas legais?

    Resultado: Não há no sistema mecanismo de análise de segurança.

15. Há no sistema alguma forma do usuário consultar sobre o tratamento dos seus dados?

    Resultado: O usuário não possui formas de consultar sobre o tratamento.

16. Sua empresa segue alguma norma de segurança de instituições internacionais?

    Resultado: Sim, o sistema é baseado nas normas ISOs e TRAC.

17. O sistema tem algum mecanismo extra de autenticação: Ex: autenticação em duas etapas?

    Resultado: O sistema possui apenas a autenticação padrão com login e senha.

18. Seu sistema possui algum controle sobre os responsáveis por acessar e/ou que possam ter acessado enquanto os dados estiveram sobre posse da instituição?

    Resultado: O sistema possui um log contendo os responsáveis pela alteração e o tipo de alteração, porém não tem nenhum impedimento para acessar.

19. Existe no sistema em alguma divulgação sobre incidentes que ocorreram?

    Resultado: Não, no sistema há alerta ou disparos de mensagens e/ou emails para informar sobre o incidente.

20. Em caso de incidente, o sistema tem mecanismos para avaliar quais os riscos?

    Resultado: Sistema não possui nenhum mecanismo que avalie os riscos.

21. Em caso de incidente, o sistema tem algum mecanismo que alerte sobre o ocorrido comunicando órgãos competentes em caso de incidentes?

    Resultado: Não há nenhuma automação informando sobre incidentes.

22. Seu sistema possui contra-medidas a ataques ou perda de dados?

    Resultado: Sim, com firewall; password validation; cookies and session security; Content Security Policy - CSP (experimental), conforme pode ser consultado na página <https://github.com/archivematica/Issues/issues.>.

23. Seu sistema possui regras distintas para tratamento de dados sensíveis?

    Resultado: O sistema não faz distinção do tipo de dado no tratamento e armazenamento.

24. Seu sistema possui algum informativo ou opção para reclamações e/ou solicitações dos usuários?

    Resultado: O sistema não possui formas de contato com os responsáveis pelo tratamento.

25. O sistema possui normas ou manuais que orientem os controladores e operadores em suas funções?

    Resultado: Não há documentos que informem a forma de procedimento no tratamento dos dados.

5.2.3 Aplicação do guia na área temática tratamento e responsabilidade

Para finalizar a análise, foram avaliados os itens relativos ao tratamento e a responsabilidade. A tabela 5.3 apresenta o resumo da validação do Archivematica dentro dos itens definidos para a área temática Tratamento e Responsabilidades.

A validação foi realizada com o suporte do checklist do guia proposto e de acordo com a metodologia prevista, ou seja, testes funcionais e consulta à documentação do sistema no repositório, além de apresentar o resumo do resultado da aplicação do guia.

Tabela 5.3: Quadro resumo do resultado da aplicação do guia na temática - Tratamento e Responsabilidade

Temática: Tratamento e Responsabilidade	**Status**			
	TC	**PC**	**NC**	**N/A**
1. Seu sistema possui algum relatório de impacto descrevendo quais processos podem colocar em risco os dados pessoais tratados?			✓	
2. Seu sistema possui documentação para mitigação de riscos?			✓	
3. Seu sistema tem algum controle que limite o tratamento dos dados de acordo com a finalidade?			✓	
4. O sistema possui módulo ou meio de consulta do titular sobre seus dados, forma e duração do tratamento e sobre sua integridade?		✓		
5. O sistema possui forma de atualização dos dados do titular?			✓	
6. Existe alguma forma de comprovação que existe medidas eficazes adotadas que comprovem a detecção de perdas?			✓	
7. Seu sistema possui solicitação de consentimento do usuário para o tratamento dos dados?			✓	
8. O controlador possui alguma prova ou comprovante que afirme que o titular dos dados autorizou o tratamento?			✓	
9. O formulário ou opção eletrônica sobre o consentimento de tratamento de dados é detalhado e direto o suficiente para evitar o vício de linguagem?			✓	
10. O sistema possui método facilitado para o usuário solicitar a revogação do consentimento no tratamento dos dados?			✓	
11. O sistema possui algum meio de consulta sobre as informações do controlador.			✓	
12. O sistema possui algum controle sobre aperfeiçoamento dos profissionais que estabeleça o desenvolvimento contínuo dos profissionais atuantes?			✓	
13. O sistema possui mecanismos para transparência e identificação de responsáveis no que tange a preservação digital?		✓		
14. O sistema possui documentação sobre a forma de coleta dos dados?			✓	
15. O sistema possui algum alerta quanto à obsolescência ou às informações que não são mais úteis ou viáveis?			✓	
16. O repositório possui controle e permissões de acordo com a responsabilidade dos atores?		✓		

17. Há no sistema alguma atualização sobre o termo de consentimento em caso de alteração da finalidade?	✓	
18. O documento/formulário de consentimento diferencia dados pessoais e dados sensíveis?	✓	
19. O sistema possui informações claras e de fácil entendimento em caso de solicitação por parte de menores, que possibilite o entendimento da criança?	✓	
20. O sistema possui mecanismo para finalizar o tratamento dos dados de acordo com os itens: a) Finalidade alcançada; e b) Os dados deixarem de ser necessários.	✓	
21. O sistema possui algum mecanismo de exportação para portabilidade dos dados do titular?	✓	
22. O sistema possui algum meio pelo qual o titular solicite a eliminação dos dados pessoais?	✓	
23. O sistema possui algum meio de informar ao titular sobre as entidades públicas ou privadas com as quais seus dados foram compartilhados ou usados pelo controlador?		✓
24. O sistema possui uma forma de disseminação integrada ou não sobre as solicitações feitas pelo titular e que deverá ser replicada em outros locais que obtiveram acesso aos dados?		✓
25. O sistema possui algum informativo sobre o compartilhamento de dados?		✓
26. Você possui compartilhamento de dados com organismos internacionais de acordo com a segurança prevista em lei?		✓
27. Seu sistema possui algum meio de comprovar os registros das operações realizadas pelos operadores e controladores?	✓	

Legenda: TC-Totalmente Compatível; PC-Parcialmente Compatível; NC-Não Compatível; N/A - Não se Aplica

Itens avaliados.

1. Seu sistema possui algum relatório de impacto descrevendo quais processos podem colocar em risco os dados pessoais tratados?

   Resultado: Não há nenhuma avaliação quanto aos riscos sobre os dados tratados.

2. Seu sistema possui documentação para mitigação de riscos?

   Resultado: Não há nenhum documento sobre a forma de minimizar os riscos.

3. Seu sistema tem algum controle que limite o tratamento dos dados de acordo com a finalidade?

Resultado: Não há nenhum documento que informe a motivação e/ou finalidade do tratamento dos dados.

4. O sistema possui módulo ou meio de consulta do titular sobre seus dados, forma e duração do tratamento e sobre sua integridade?

   Resultado: O sistema possui meios para garantir a integridade e possui o fluxo de trabalho definido, porém não há como o titular consultar e nem informações sobre o tempo de duração do tratamento.

5. O sistema possui forma de atualização dos dados do titular?

   Resultado: As atualizações são feitas pelo responsável pelo tratamento.

6. Existe alguma forma de comprovação que existe medidas eficazes adotadas que comprovem a detecção de perdas?

   Resultado: Sistema não possui nenhuma documentação que comprove a eficácia das medidas tomadas.

7. Seu sistema possui solicitação de consentimento do usuário para o tratamento dos dados?

   Resultado: O sistema não informa o usuário e nem solicita consentimento.

8. O controlador possui alguma prova ou comprovante que afirme que o titular dos dados autorizou o tratamento?

   Resultado: O responsável não possui nenhum comprovante ou forma de comprovar que o titular autorizou o tratamento dos seus dados.

9. O formulário ou opção eletrônica sobre o consentimento de tratamento de dados é detalhado e direto o suficiente para evitar o vício de linguagem?

   Resultado: Não existe formulário para consentimento.

10. O sistema possui método facilitado para o usuário solicitar a revogação do consentimento no tratamento dos dados?

    Resultado: Não, Toda alteração é feita pelo responsável pelo tratamento sem controle ou supervisão do titular.

11. O sistema possui algum meio de consulta sobre as informações do controlador.

    Resultado: Não, o titular não sabe quem é ou foi o responsável pelo tratamento dos seus dados.

12. O sistema possui algum controle sobre aperfeiçoamento dos profissionais que estabeleça o desenvolvimento contínuo dos profissionais atuantes?

    Resultado: Não há nenhuma opção para aperfeiçoamento dos profissionais

13. O sistema possui mecanismos para transparência e identificação de responsáveis no que tange a preservação digital?

    Resultado: O sistema possui log para identificar os responsáveis, porém não existe transparência sobre como estão sendo tratados e por quem está.

14. O sistema possui documentação sobre a forma de coleta dos dados?

    Resultado: Não, o sistema tem o fluxo de trabalho interno definido, porém não sobre a forma como foram coletados.

15. O sistema possui algum alerta quanto à obsolescência ou às informações que não são mais uteis ou viáveis?

    Resultado: Não existe nenhum mecanismo para essa função.

16. O repositório possui controle e permissões de acordo com a responsabilidade dos atores?

    Resultado: Sistema possui apenas 2 perfis, o administrador e o arquivista, mas não há controle de responsabilidades.

17. Há no sistema alguma atualização sobre o termo de consentimento em caso de alteração da finalidade?

    Resultado: O sistema não possui termo de consentimento.

18. O documento/formulário de consentimento diferencia dados pessoais e dados sensíveis?

    Resultado: O sistema não possui termo de consentimento.

19. O sistema possui informações claras e de fácil entendimento em caso de solicitação por parte de menores, que possibilite o entendimento da criança?

    Resultado: Não, sistema não faz distinção sobre dados e titulares.

20. O sistema possui mecanismo para o finalizar o tratamento dos dados de acordo com os itens: a) Finalidade alcançada; e b) Os dados deixarem de ser necessários.

    Resultado: Não possui meios automáticos para finalização do tratamento dos dados.

21. O sistema possui algum mecanismo de exportação para portabilidade dos dados do titular?

    Resultado: O sistema não possui exportação de dados.

22. O sistema possui algum meio pelo qual o titular solicite a eliminação dos dados pessoais?

    Resultado: Não, o sistema não possui nenhum meio de contato para solicitar a finalização.

23. O sistema possui algum meio de informar ao titular sobre as entidades públicas ou privadas com as quais seus dados foram compartilhados ou usados pelo controlador?

    Resultado: N/A

24. O sistema possui uma forma de disseminação integrada ou não sobre as solicitações feitas pelo titular e que deverá ser replicada em outros locais que obtiveram acesso aos dados?

    Resultado: O sistema não possui integração para replicação com outras soluções.

25. O sistema possui algum informativo sobre o compartilhamento de dados?

    Resultado: N/A

26. Você possui compartilhamento de dados com organismos internacionais de acordo com a segurança prevista em lei?

    Resultado: N/A

27. Seu sistema possui algum meio de comprovar os registros das operações realizadas pelos operadores e controladores?

    Resultado: Sim, o sistema possui um log contendo o responsável pela alteração, bem como a alteração feita.

5.3 SÍNTESE DO CAPÍTULO

Neste capitulo 5, foi apresentada a validação do guia referência proposto neste trabalho. Para que fosse possível identificar com mais clareza os resultados, foram inseridas evidências e/ou formas de certificar o que foi constatado. O capítulo 6 a seguir, tratará de uma análise mais ampla sobre os resultados encontrados.

6 DISCUSSÃO DOS RESULTADOS

Como toda pesquisa, essa também possui algumas limitações e ameaças à validação. Essa pesquisa está limitada ao repositório seguro Archivematica para efeitos de testes práticos, tratando como foco único a análise das diretrizes da LGPD e a conformidade da ferramenta. Cabe ressaltar que as tecnologias sofrem inovações a todo momento, o que poderá acarretar em algumas discrepâncias na análise com novas versões da solução, tanto para melhoria da ferramenta como para descontinuidade dela. Para essa validação, foi utilizado o Archivematica na versão 1.13.2.

Uma vez que não se faz necessário um estudo aprofundado para a validação da proposta dessa pesquisa, foram realizados alguns testes básicos de segurança, tais como: tentativas de ataques, análise de código, *pen testing*, etc. A análise aprofundada e mais técnica será objeto de trabalhos futuros. Outro fator importante quanto ao risco é a LGPD, sendo uma legislação recente e, assim como a tecnologia, as leis tendem a sofrer alterações constantes. Esse fato, por si só, já é uma ameaça a elaboração do guia, principalmente em relação ao seu tempo de validade.

Outro fator que pode ser uma ameaça é quanto ao resultado do *survey*, uma vez que vários fatores podem influenciar no futuro da pesquisa, tais como: interesse dos respondentes pelo assunto; disponibilidade (tempo para responder); por ser uma pesquisa online, há uma limitação de acesso à tecnologia; alcance de um número considerável de respondentes [78]. Como primeiro fator, podemos considerar que, apesar de não ser possível ter uma amostra perfeita para nenhuma pesquisa, neste trabalho a amostra foi gerada com o máximo de pessoas possíveis e com diferentes perfis. Quanto às questões, a elaboração foi feita pra que houvesse o mínimo de dúvidas possíveis no momento da análise do resultado; cada pergunta foi feita com o intuito de direcionar cada resposta e obter um resultado que diminuísse a margem de ambiguidade das respostas.

O levantamento inicial sobre a legislação relacionada à privacidade de dados, à segurança e ao tratamento de dados trouxe uma visão de como os países europeus estão bem à frente no que tange a proteção de dados. Com leis mais severas e melhor detalhamento sobre a forma de tratamento dos dados, a GDPR[7] se tornou uma legislação base para o restante do mundo. Nesse sentido, o Brasil elaborou a LGPD[4].

Comparada a GDPR, a LGPD ainda deixa algumas lacunas quanto ao tratamento e suas punições, como exemplo, o uso por parte de organizações públicas ou em casos de interesse do estado, que retiram do cidadão a opção de negar que seus dados sejam utilizados. Outro fator que pode ser observado neste trabalho é quanto a formas e técnicas de resoluções quanto à proteção de dados, sobre a qual a lei não detalha e/ou restringe, apenas aponta que deve ser feito algo de acordo com o meio disponível pelo agente responsável pelo tratamento dos dados. Isso por si só já incide em possíveis falhas, uma vez que não direciona ou coloca os mínimos regramentos necessários para a segurança e proteção dos dados.

Os fatores mencionados são importantes quando os dados a serem tratados estão em posse e/ou são dados utilizados por órgãos públicos, uma vez que são alvos constantes de ataques de criminosos, não somente por ser uma base de dados vasta com dados de várias pessoas, mas também por conter informações estratégicas. Como é notável, tudo que é relativo a cuidados é muito cultural, e não é uma prática normal a adesão às normas e novos métodos, fazendo com que legislações e metodologias não sejam seguidas de forma imediata e correta.

Com o foco na proteção de dados pessoais e proteção à privacidade, entramos, então, em quesitos não somente sobre forma como os dados são acessados, mas também como são armazenados. Para isso, há soluções de mercado e soluções abertas que "garantem"a proteção e confiabilidade dos dados armazenados. Conhecidos como Repositórios Digitais Confiáveis - RDCs, estes propõem uma segurança para os dados que armazenam. No sentido de garantir a segurança dos dados, o Conarq, órgão responsável por armazenamento de arquivos, usa como referência para análise de repositórios seguros o TRAC (*Trustworthy Repository Audit & Certification*), uma unidade certificadora que exige uma série de requisitos para considerar um repositório seguro ou não. Os repositórios atuais, tal qual o Archivematica, alvo deste trabalho, seguem as diretrizes do TRAC, que leva em consideração a cadeia de custódia para garantir a integridade dos dados.

Vale ressaltar que os requisitos elencados no TRAC não são os mesmos contidos nas diretrizes da LGPD. Para fazer tal verificação, foi feita uma análise comparativa entre os requisitos de ambos, com o objetivo de definir se, ao seguir as requisitos do TRAC, um repositório estaria cumprindo indiretamente as diretrizes da LGPD. As análises comparativas mostraram que o TRAC indica alguns itens de segurança que devem ser cumpridos e que também constam na LGPD, porém de formas distintas e não detalhadas. Ao analisar o inverso, vemos que vários itens elencados e inseridos na LGPD como diretriz para assegurar a privacidade dos dados não são contemplados pelo TRAC, nem mesmo de forma genérica.

Após essa análise, o próximo passo foi estudar o Archivematica, ferramenta que iria ser avaliada de acordo com as melhores práticas de testes em ferramentas tecnológicas; a principio, testes manuais com base nos resultados da comparação entre o TRAC e a LGPD. Essa avaliação foi importante para apresentar para o estudo que os primeiros itens que a LGPD insere em nosso ornamento jurídico como requisitos mínimos de segurança não estão contemplados no Archivematica de forma clara em sua versão padrão, e ainda que outros existissem na solução, não são exatamente como diz a lei. Apesar de ser uma ferramenta Open source, é muito utilizada por entidades públicas no Brasil para armazenamento de arquivos, por manter a cadeia de custódia do documento, ou seja, garantir que o documento é legítimo e autêntico desde a sua criação até o seu possível descarte.

Em posse das informações da legislação e da análise da ferramenta, foi necessário realizar um estudo sobre o nível de conhecimento da LGPD, metodologias e soluções tecnológicas que garantam a proteção e privacidade de dados pessoais, para ter direcionamento mais eficaz no momento de elaborar o guia modelo. Contendo 21 questões, o questionário contou com os principais assuntos que versa a LGPD, mais voltados para os profissionais de tecnologia. A fim de que

não houvesse um meio de atividades que tornasse a pesquisa enviesada, o público participante contou com profissionais de empresas privadas e públicas. As questões do *survey* trataram da segurança da informação, proteção e privacidade de dados, sempre limitando-se aos regramentos da legislação.

Essa análise possibilitou o levantamento de uma série de questões não tratadas nesses repositórios e que são importantes para que a implementação de um RDC - Repositório Digital Confiável - esteja de acordo com as diretrizes da LGPD. O resultado foi estudado, criando-se um Guia modelo, que tem como principal objetivo apresentar uma forma concreta de implantar uma gestão documental digital de forma segura e dentro da legislação vigente.

7 CONCLUSÃO

Este trabalho teve como objetivo demonstrar que os repositórios arquivísticos seguros, tal como o Archivematica, ainda que estejam de acordo com o *Trustworthy Repositories Audit & Certification* (TRAC) e o Conselho Nacional de Arquivos - Conarq -, não estão completamente adequados à Lei Geral de Proteção de Dados - LGPD. Para chegar a essa conclusão, foram levados em consideração vários fatores que são decisivos para comprovação do objetivo deste trabalho.

A revisão da literatura em relação à legislação vigente sobre a privacidade de dados dos usuários permitiu evidenciar que a LGPD detalhou de forma mais ampla a questão da privacidade de dados, deixando claro o que tem que ser feito para garantir a segurança dos dados dos usuários, bem como responsáveis e possíveis punições em casos de vazamento ou tratamento indevido das informações que estão em posse de instituições públicas e privadas, concluindo-se, assim, que foi um avanço para a legislação brasileira.

Quando comparado à LGDP, o TRAC não conseguiu atender a plenitude da extensão da lei normativa e ainda se mostrou pouco claro em outros itens. Três fatores claramente contribuem para isso: primeiramente, a ISO 16363, a qual institui que o TRAC é um norma internacional de tal maneira que não tem o objetivo de cobrir especificidades da realidade brasileira; outro fator é a questão temporal, pois o TRAC data de 2007, e a LGPD foi editada em 2018; e por fim, o TRAC foi construído com objetivo específico de auditar repositórios arquivísticos seguros que adotam o modelo OAIS, cuja principal função é proteger a informação durante todo o ciclo da cadeia de custódia documental, garantindo a autenticidade dos objetos documentais no tempo e espaço, principalmente os de guarda de longa duração.

O Guia proposto se mostrou uma eficiente ferramente para auxiliar auditoria, pois concentra todos os requisitos a serem cumpridos, dividido por área temática e questões objetivas.

Para validação do guia proposto, foi analisado o repositório digital Archivematica para verificação da seguração e adequação à LGPD. Foram realizados testes práticos em ferramentas e testes automatizados (Estáticos e Dinâmicos). Os resultados em relação à aderência a LGPD foram:

Tabela 7.1: Quadro resumo do resultado da aplicação do Guia

Total de Questões	**TC**	**PC**	**NC**	**N/A**
Governança				
19	4	2	13	0
Sigilo e Privacidade				
25	8	4	14	0
Tratamento e Responsabilidade				
27	1	3	19	4

Legenda: TC-Totalmente Compatível; PC-Parcialmente Compatível; NC-Não Compatível; N/A - Não se Aplica

Os testes práticos demonstraram que não há clareza quanto à forma de acesso aos dados do usuário. Isso se deve ao fato de não haver opção de gerenciamento de perfis. No que tange o tratamento de dados, os testes demonstraram que não há na solução um controle sobre o tipo de dados que está sendo tratado e nem quem é o responsável pelo tratamento. E em relação ao armazenamento, foi constatado que é possível salvar em banco da dados os arquivos, podendo fazer com que dados pessoais sensíveis ou não fiquem disponíveis em documentos sem a devida segurança e privacidade.

De forma complementar, foram realizados testes estáticos (*Static Application Security Testing* - SAST), analisadas 73610 linhas e códigos do *dashboard* e encontrados 134 problemas considerados de severidade baixa e 53 médias. Já no *Storage Service*, foram analisadas 19105 linhas e encontrados 57 problemas de severidade baixa e 19 média. Já os testes dinâmicos (*Dynamic Application Security Testing* - DAST), com a análise nas mesmas condições, detectou 1 problema informacional, 4 baixos e 3 médios no *Dashboard*; e no *Storage Service*, foi encontrado 1 problema indicado como indefinido, 5 como baixos e 2 como médios. Esses fatores comprovam que a ferramenta não está segura em seu modelo padrão e que não está adequada às diretrizes da LGPD.

Dando continuidade aos trabalhos, surgiu a necessidade de investigar o nível de conhecimento dos profissionais sobre a LGPD, segurança da informação e privacidade de dados. Foi realizado um *survey* que contou com 43 respondentes, sendo 14 de instituições privadas e 29 de instituições públicas. Entre os principais resultados, alguns são mais relevantes e, até mesmo, preocupantes, por exemplo, 12 participantes não terem o conhecimento básico sobre a LGPD. No que tange algumas obrigatoriedades básicas, ainda no sentido de tratamento de dados, a lei prevê o prévio consentimento do titular sobre os seus dados, sendo que a pesquisa mostrou que 72% dos respondentes de entidades públicas e 86% de entes privados foram informados sobre o documento. No quesito armazenamento, a pesquisa detectou um problema que pode ser tanto de desconhecimento por parte dos profissionais quanto por falta de transparência de suas instituições, pois 57% dos entrevistados informaram desconhecer a forma como seus dados são armazenados. Como os dados são considerados do titular, a pesquisa questionou sobre um direito importante que está contido na LGPD, o “direito ao esquecimento", e o resultado foi que 72% dos entrevistados desconhecem esse direito.

A partir dos testes executados na ferramenta Archivematica e no estudo realizado sobre a legislação com apoio do *survey*, é possível concluir que o repositório analisado não está em conformidade com a LGPD, uma vez que o *survey* revelou uma falta de conhecimento dos profissionais envolvidos nos projetos de tecnologia, bem como a falta de comprometimento por parte de gestores e instituições. Conclui-se, ainda, que se faz necessária uma ferramenta de apoio para que seja realizada a adequação à LGPD. Assim, o trabalho desenvolvido é relevante, uma vez que apresenta um guia que servirá de apoio aos profissionais de TI para que esse e outros repositórios entrem em conformidade com a legislação vigente.

REFERÊNCIAS

1 ISO-1636. Space data and information transfer systems-audit and certification of trustworthy digital repositories:ISO 16363. ISO, 2012.

2 OAIS. Open Archival Information System. 2021. Disponível em: <https://www.archivematica.org/en/docs/archivematica-1.7/getting-started/overview/intro/>.

3 ARCHIVEMATICA. Archive storage. 2022. Disponível em: <https://www.archivematica.org/en/docs/archivematica-1.5/user-manual/archival-storage/archival-storage/>.

4 BRASIL. Lei n°13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

5 TRAC. Trustworthy repositories audite certification criteria and checklist (TRAC). 2007. Disponível em: <https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac>.

6 COSTA, P. V.; GONÇALVES, W. I.; GONÇALVES, E. D.; LAZARIN, N. M. Nível de conhecimento de desenvolvedores sobre segurança em aplicações web: Pesquisa e análise. p. 92–99, 2018.

7 UNION, P. of the E. Eu data protection rules. 2018. Disponível em: <https://gdpr.eu/>.

8 PINHEIRO, P. P. Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd. Saraiva Educação SA, 2020.

9 SANTOS, E. E. dos; SOARES, T. M. M. K. Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações. *Revista Tecnológica da Fatec Americana*, v. 7, n. 02, p. 43–51, 2019.

10 FONTES, E. L. G. Segurança da informação. Saraiva Educação SA, 2017.

11 COTS, M.; OLIVEIRA, R. Lei geral de proteção de dados pessoais: Comentada. Revista dos Tribunais, 2019.

12 MACHADO, R.; KREUTZ, D.; PAZ, G.; RODRIGUES, G. Vazamentos de dados: Histórico, impacto socioeconômico e as novas leis de proteção de dados. p. 154–159, 2019. Disponível em: <https://sol.sbc.org.br/index.php/errc/article/view/9230>.

13 CONARQ. Diretrizes para a implementação de repositórios arquivisticos digitais confiaveis). 2015. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-43-de-04-de-setembro-de-2015>.

14 CONARQ, A. N. *Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais*. 2012. Disponível em: <http://conarq.gov.br/images/publicacoes_textos/conarq_presuncao_autenticidade_completa.pdf>.

15 CONARQ, A. N. *Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis*. 2015. Disponível em: <http://www.conarq.gov.br/images/publicacoes_textos/diretrizes_rdc_arq.pdf>.

16 RLG-OCLC. Trusted digital repositories: Attributes and responsibilities–an rlg-oclc report. 2002.

17 DIGITAL olhar. *Vazamento expõe dados de 267 milhões de usuários do Facebook*. 2019. Disponível em: <https://olhardigital.com.br/2019/12/20/noticias/vazamento-expoe-dados-de-267-milhoes-de-usuarios-do-facebook/#:~:text=Esta\%20n\%C3\%A3o\%20foi\%20a\%20primeira,milh\%C3\%B5es\%20de\%20pessoas\%20fossem\%20expostos.>

18 TECMUNDO. *Twitter revela vazamento de dados: ataque de hackers patrocinados*. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/137279-twitter-revela-vazamento-dados-ataque-hackers-patrocinados.htm>.

19 WELIVESECYRITY. *Vazamento de dados pode ter afetado milhões de hóspedes da rede de hotéis Marriott*. 2018. Disponível em: <https://www.welivesecurity.com/br/2018/12/04/vazamento-de-dados-pode-ter-afetado-milhoes-de-hospedes-da-rede-de-hoteis-marriott/>.

20 VENTURA, F. *MP pressiona Netshoes após vazamento que afetou 2 milhões de clientes*. 2018. Disponível em: <https://tecnoblog.net/233169/ministerio-publico-netshoes-vazamento/>.

21 PAYAO, F. *Dados bancários de centenas de clientes Porto Seguro vazam na internet*. 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/128896-dados-bancarios-centenas-clientes-porto-seguro-vazam-internet.htm>.

22 RAMOS, P. A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a lgpd. *Publicado em*, v. 16, n. 07, 2019.

23 COSTA, A. P.; REIS, L. P.; SOUZA, F. N. d. Investigação qualitativa para sistemas e tecnologias de informação. Associação Ibérica de Sistemas e Tecnologias de Informação (AISTI), 2014.

24 VAUS, D. D.; VAUS, D. de. *Surveys in social research*. [S.l.]: Routledge, 2013.

25 TECMUNDO. *Relatório mostra que Brasil é o nono país que mais sofreu ransomware em 2020*. 2021. Disponível em: <https://tiinside.com.br/19/03/2021/relatorio-mostra-que-brasil-e-o-nono-pais-que-mais-sofreu-ransomware-em-2020>.

26 HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. [S.l.]: Brasport, 2018.

27 NETO, P. T. M.; ARAÚJO, W. J. Segurança da informação: Uma visão sistemica para implantação em organizações. 2019.

28 MACHADO, F. N. R. Segurança da informação: princípios e controle de ameaças. Saraiva Educação SA, 2014.

29 SANTOS, I. Q. dos; GULO, C. A. Segurança da informação. Disponível em: <http://www.projectsevolution.com.br/Ebooks/Como_Estar_Seguro_Utilizando_Internet.pdf>.

30 MCCLURE, S.; SCAMBRAY, J.; KURTZ, G. *Hackers Expostos-: Segredos e Soluções para a Segurança de Redes*. [S.l.]: Bookman Editora, 2014.

31 CIBERATAQUES: riscos de ataques cibernéticos nas empresas. 2021. Disponível em: <https://br.claranet.com/blog/ciberataques-riscos-de-ataques-ciberneticos-nas-empresas>.

32 DUBOWSKI, S. Asics give a big boost to antivirus. *Network World Canada*, Laurentian Technomedia Inc., v. 13, n. 10, 2003.

33 SILVA, P. M. et al. Políticas de segurança da informação nas organizações. 2003. Disponível em: <http://repositorio.ufsc.br/xmlui/handle/123456789/84739>.

34 SISTEMA de Gestão de Segurança da Informação. 2022. Disponível em: <https://www.27001.pt/>.

35 OLIVEIRA, É. *Sistema de Informação para Gestão de Serviços Informáticos (SGSI)*. Dissertação (B.S. thesis) — Universidade do Mindelo, 2020.

36 EUROPEU, P. *Diretiva do parlamento europeu*. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32016L0680>.

37 FERRÃO, S. É. R.; CARVALHO, A. P.; CANEDO, E. D.; MOTA, A. P. B.; COSTA, P. H. T.; CERQUEIRA, A. J. Diagnostic of data processing by brazilian organizations - A low compliance issue. *Inf.*, v. 12, n. 4, p. 168, 2021.

38 ENGAN, M.; FARSAI, S.; IONESCU, A. C.; SMITH, B.; SEWARD, S.; JOUL, C. H.; YIU, A. *Identity and access management*. [S.l.]: Google Patents, 2017. US Patent 9,705,871.

39 LOSHIN, D. *Master data management*. [S.l.]: Morgan Kaufmann, 2010.

40 CAVOUKIAN, A. et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, v. 5, p. 12, 2009.

41 RIBEIRO, R. C.; CANEDO, E. D. Using MCDA for selecting criteria of LGPD compliant personal data security. In: *DG.O*. [S.l.]: ACM, 2020. p. 175–184.

42 CARVALHO, A. P.; CARVALHO, F. P.; CANEDO, E. D.; CARVALHO, P. H. P. Big data, anonymisation and governance to personal data protection. In: *DG.O*. [S.l.]: ACM, 2020. p. 185–195.

43 REPUBLICA, P. da. *Constituiçao Federal*. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>.

44 BONOMI, S.; CASINI, M.; CICCOTELLI, C. B-coc: A blockchain-based chain of custody for evidences management in digital forensics. In: DANOS, V.; HERLIHY, M.; POTOP-BUTUCARU, M.; PRAT, J.; PIERGIOVANNI, S. T. (Ed.). *International Conference on Blockchain Economics, Security and Protocols, Tokenomics 2019, May 6-7, 2019, Paris, France*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. (OASIcs, v. 71), p. 12:1–12:15. Disponível em: <https://doi.org/10.4230/OASIcs.Tokenomics.2019.12>.

45 LUZ, C.; FLORES, D. Cadeia de custódia e de preservação: autenticidade nas plataformas de gestão e preservação de documentos arquivísticos. *Seminário Serviços de Informação em Museus*, p. 171–181, 2018.

46 SANTOS, H. M. dos; FLORES, D. Modelo lógico da informação no open archival information system: uma reflexão arquivística sobre o pacote de informação para arquivamento. *Perspectivas em Gestão & Conhecimento*, p. 23–38, 2020.

47 FERREIRA, M. *Introdução à preservação digital: conceitos, estratégias e actuais consensos*. [S.l.]: Universidade do Minho, Escola de Engenharia, 2006.

48 OLIVEIRA, H. A. d.; PINTO, M. M. G. d. A. Da preservação da informação ao repositório confiável. *Seminário de Saberes Arquivísticos: SESA Intercâmbio Cooperação Acadêmica e Mediações Interdisciplinares*, 2017.

49 ROCHA, C. *Repositorios para preservação de documentos arquivisticos digitais.Acervo - Revista do Arquivo Nacional*. 2015.

50 NACIONAL, A. *Norma Geral Internacional de Descrição Arquivista*. 1999. Disponível em: <https://www.yumpu.com/en/document/view/52563862/norma-geral-internacional-de-descricao-arquivistica>.

51 ARQUIVOS, C. C. N. de. *Norma Brasileira de Descrição Arquivística - Nobrade*. 2009. Disponível em: <https://www.diariodasleis.com.br/legislacao/federal/210212-norma-brasileira-de-descricao-arquivistica-nobrade>.

52 ARQUIVOS, C. C. N. de. Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis. 2015.

53 SPACE data and information transfer systems — Open archival information system (OAIS) — Reference model. 2012. Disponível em: <https://www.iso.org/standard/57284.html>.

54 MARCONDES, C. H.; SAYÃO, L. F. Softwares livres para repositórios institucionais: alguns subsídios para a seleção. *Implantação e gestão de repositórios institucionais: políticas, memória, livre acesso e preservação. Salvador: EDUFBA*, p. 23–54, 2009.

55 LAMPERT, S. R. Os repositórios dspace e archivematica para documentos arquivísticos digitais. *Acervo*, v. 29, n. 2, p. 143–154, 2016.

56 CAFÉ, L.; MELO, B.; BARBOSA, E.; NUNES, E.; ARELLANO, M. M. Repositórios institucionais: nova estratégia para publicação científica na rede. In: *Congresso Brasileiro de Ciências da Comunicação*. [S.l.: s.n.], 2003. v. 26, p. 12.

57 LEITE, F. C. L.; COSTA, S. Repositórios institucionais como ferramentas de gestão do conhecimento científico no ambiente acadêmico. *Perspectivas em ciência da informação*, SciELO Brasil, v. 11, p. 206–219, 2006.

58 SOUZA, L. G. S.; AGANETTE, E. C. Repositórios digitais confiáveis: uma revisão da literatura nacional e internacional publicada em periódicos científicos. *Informação & Sociedade*, Universidade Federal da Paraíba-Programa de Pós-Graduação em Ciência da . . . , v. 30, n. 1, 2020.

59 SUMMERS, L.; TRAVERS, M. Ica-atom, archivematica and digital preservation. In: *iPRES*. [S.l.: s.n.], 2014.

60 ALMEIDA, A. C. B. de; VERONA, L. D.; CAMPOS, M. L. M.; BAIÃO, F. A. Lgpd em ambientes de bancos de dados nas organizações. *Sociedade Brasileira de Computação*, 2019.

61 BIASE, N. F. D.; AGUILERA, D. F. Dificuldades interpretativas no regime de tratamento de dados pelo poder público:: lacunas, contradições e atecnias da lgpd. *REVISTA ELETRÔNICA DA PGE-RJ*, v. 4, n. 2, 2021.

62 MAGACHO, B. T. P.; TRENTO, M. Lgpd e compliance na administração pública. *Revista Brasileira de Pesquisas Jurídicas (Brazilian Journal of Law Research)*, v. 2, n. 2, p. 7–26, 2021.

63 AGUIAR, F. L. d. *Dspace e archivematica: concepção e criação de um protótipo de repositório digital aplicado no domínio da SBPC: sob uma perspectiva interdisciplinar entre Arquivística e Organização e Represetação do Conheciimento*. Tese (Doutorado) — Universidade de São Paulo, 2018.

64 da Silva, D. A.; de Sousa, R. T.; de Oliveira Albuquerque, R.; Sandoval Orozco, A. L.; García Villalba, L. J. Iot-based security service for the documentary chain of custody. *Sustainable Cities and Society*, v. 71, p. 102940, 2021. ISSN 2210-6707. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2210670721002250>.

65 MARQUES, G. F.; CARDOSO, R. A importância da segurança em banco de dados. *Revista Eletrônica da Faculdade Invest de Ciências e Tecnologia*, v. 5, n. 1, p. 13–13, 2021.

66 GAVA, T. B. S.; FLORES, D. O papel do archivematica no rdc-arq e possíveis cenários de uso. *ÁGORA: Arquivologia em debate*, v. 31, n. 63, p. 1–21, 2021.

67 SILVEIRA, L. Â.; SHINTAKU, M.; GOMES, R. F.; SCHIESSL, I. T. Implementação de aspectos de acessibilidade em biblioteca digital desenvolvida com o dspace. *BIBLOS: Revista do Instituto de Ciências Humanas e da Informação*, Universidade Federal do Rio Grande, 2020.

68 MOU, C.; CHENG, Y. Research on information resource sharing and big data of sports industry in the background of openstack cloud platform. *Secur. Commun. Networks*, v. 2021, p. 2824146:1–2824146:12, 2021. Disponível em: <https://doi.org/10.1155/2021/2824146>.

69 WHAT is Archivematica? 2022. Disponível em: <https://www.archivematica.org/en/docs/archivematica-1.7/getting-started/overview/intro/>.

70 WHAT is AtoM? 2022. Disponível em: <https://www.accesstomemory.org/pt-br/docs/2.6/user-manual/overview/intro/>.

71 BRADLEY kevin. *Diretrizes sobre a produção e preservação de objetos de audio digital*. 2009. Disponível em: <https://www-iasa--web-org.translate.goog/tc04/open-archival-information-system-oais?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=ajax,sc,elem>.

72 GENTSCH, C. Evaluation of open source static analysis security testing (sast) tools for c. DLR DW, 2020. Disponível em: <https://elib.dlr.de/133945/>.

73 OCHOA, D. M. Dynamic Application Security Testing (DAST). 2021. Disponível em: <https://www.dianaochoa.com/s/CSOL560DianaOchoaM6Assignmentv2.pdf>.

74 LI, J. Vulnerabilities mapping based on owasp-sans: a survey for static application security testing (sast). *Annals of Emerging Technologies in Computing*, v. 4, 04 2020.

75 PANDYA, D.; PATEL, N. Owasp top 10 vulnerability analyses in government websites. *International Journal of Enterprise Computing and Business Systems*, v. 6, n. 1, 2016.

76 HUANG, L.-S.; MOSHCHUK, A.; WANG, H. J.; SCHECTER, S.; JACKSON, C. Clickjacking: Attacks and defenses. In: *21st USENIX Security Symposium (USENIX Security 12)*. [S.l.: s.n.], 2012. p. 413–428.

77 BIEMER, P. P.; LYBERG, L. E. *Introduction to survey quality*. [S.l.]: John Wiley & Sons, 2003.

78 VASCONCELLOS-GUEDES, L.; GUEDES, L. *E-surveys: vantagens e limitações dos questionários eletrônicos via internet no contexto da pesquisa científica*. [S.l.]: X SemeAd-Seminário em Administração FEA/USP (São Paulo, Brasil), 2007. 84 p.