PROPOSTA DE GUIA PARA ADEQUAÇÃO DE REPOSITÓRIOS DIGITAIS CONFIÁVEIS À LGPD

Marcio Aurélio de Souza Fernandes[1], Edna Dias Canedo[1], Carlos Eduardo Lacerda Veiga[2], Guilherme Fay Vergara[1], Daniel Alves da Silva[1] e Rafael Timóteo de Sousa Jr[1]

[1]Universidade de Brasília – UNB, Campus Universitário Darcy Ribeiro, Brasília – DF, CEP 70910-900, Brasil

[2]Advocacia-Geral da União – AGU, Sede II,Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 - Brasília, DF, 70610-460, Brasil

RESUMO

Diversos trabalhos têm investigado como realizar a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) em relação a privacidade dos dados dos usuários. Diante desse cenário de adequação à LGPD, esse trabalho tem como objetivo realizar uma análise dos princípios da LGPD e investigar o nível de conhecimento dos profissionais de ICT que trabalham direta e indiretamente com a lei. Além disso, investigou-se repositório digitais seguros, em conformidade com a ISO -16363, também em conformidade com as diretrizes da LGPD. A partir da revisão desse arcabouço legal e normativo, foi proposto um guia de auditoria que permite avaliar e direcionar os itens necessários para que um repositório digital seguro esteja adequado à LGPD.

PALAVRAS-CHAVE

Proteção de Dados, Segurança da Informação, Privacidade de Dados, Repositório Arquivístico Digital Confiável, LGPD, Conformidade e Adequação

1. INTRODUÇÃO

A disciplina de proteção de dados ganhou destaque quando foi lançada a *General Data Protection Regulation* – GDPR (REGULATION, 2018), que surgiu em substituição a 2 normas europeias, a saber: "Diretiva de Proteção de Dados da União Europeia" e o "Ato de Proteção de Dados do Reino Unido de 1998". 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.

A LGPD (BRASIL, 2018) foi elaborada em 2018 e entrou em vigor em 2020, com o objetivo de controlar e fortalecer os direitos dos cidadãos sobre suas informações pessoais e sua privacidade. 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.

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. O tratamento desses ativos deverá ser exercido a partir do cumprimento de normas mínimas de segurança, respeitando os pilares da informação: disponibilidade, integridade, confidencialidades, legalidade, auditabilidade e não repudio de autoria (SANTOS, 2019).

Todo esse cenário configura um grande desafio no que tange à 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: financeiros, na imagem, credibilidade, etc.

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 é confiável ou seguro, há um normativo da Organização Internacional de Normalização conhecido como TRAC, que detalha os requisitos mínimos para ser considerado seguro.

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) (CONARQ, 2019), 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. (DA SILVA, .2021).

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" (CONARQ, 2015).

Uma forma de atestar a confiabilidade de um repositório digital junto à comunidade-alvo se dá por meio da sua certificação por terceiros. Para esse fim, em parceria com o NARA, foi publicado, em 2007, o documento *Trustworthy Repository Audit and Certification: Criteria and Checklist* (TRAC) (TRAC, 2007), que serviu de base para a elaboração da norma ISO 16363(ISO, 2012). 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) (OAIS, 2022), referenciado na Resolução nº 43 do Conselho Nacional de Arquivos (CONARQ). A tramitação dos documentos digitais até sua admissão no RDC-Arq é um processo crítico, pois esses 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 do documento digital.

O presente trabalho teve como desafio analisar se os repositórios digitais aderente ao modelo OAIS e certificados pelo TRAC atendem aos requisitos da LGPD. Para tanto, serão analisadas as normas pertinentes, LGPD e normas brasileiras vigentes, como a resolução nº43 do CONARQ, para desenvolver um guia de auditoria que oriente as entidades que necessitem atender a todo o arcabouço legal e normativo vigente, garantindo assim o uso das melhores práticas previstas para a segurança de dados.

2. PROPOSTA DO GUIA

Esta pesquisa é quantitativa, teórica e investigativa, realizada através da análise de normas 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 foi feita com a utilização de ferramentas de verificação 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.

O Guia proposto para adequação à 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 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.

O Conselho Nacional de Arquivos (CONARQ) é o responsável pela definição da forma em que são avaliados os repositórios digitais 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 Arquivísticos Digitais Confiáveis. A resolução levou em consideração as diretrizes contidas no modelo utilizado para auditoria e certificação de repositórios confiáveis conhecido como TRAC e, como referência tecnológica, a do OAIS.

O Guia proposto neste trabalho conta como uma matriz comparativa entre o TRAC e as diretrizes da LGPD com foco em Governança, Tratamento e Responsabilidades e Segurança da Informação. Assim, foi realizada uma análise comparativa entre as principais diretrizes da LGPD e as normas estabelecidas pelo TRAC para melhor compreensão e praticidade, a fim de analisar os itens que serão apresentados nas Tabelas 1, 2 e 3.

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

Tabela 1. Análise Comparativa LGPD versus TRAC - Governança

LGPD	*TRAC*	*LGPD*	*TRAC*
Art. 6º	SeçãoA.A3.8	Art. 50, § 2º, I	SeçãoA.A1.1
Art. 6º II	Não Compatível.	Art. 50, § 2º, I	Não Compatível
Art. 6º III	Não Compatível.	Art. 50, § 2º, I	SeçãoA.A3.2º
Art. 6º IV	SeçãoB..B6.3	Art.50,§2º,I	SeçãoC.C3.2
Art. 6º V	Não Compatível.	Art. 50, § 2º, I	SeçãoA.A3.7
Art. 6º VI	SeçãoA.A3.7	Art. 50, § 2º, I	SeçãoA.A4.2
Art. 6º VII	SeçãoB3.B6.4-B6.5	Art. 50, § 2º, I	SeçãoB.B6.6
Art. 6º VIII	SeçãoB.B3.1-B3.1	Art. 50, § 2º, I	SeçãoA.A3.9
Art. 6º IX	Não Compatível	Art. 50, § 2º, II	Não Compatível.
Art. 6º X	Não Compatível.	Art. 50, § 3º	Não Compatível.
Art. 50, § 1º	SeçãoA-3.6	Art. 51.	Não Compatível

Conforme apresentado na Tabela 1, 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 (TRAC, 2007) 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. (LGPD,2018)

O TRAC (TRAC, 2007) 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. (LGPD, 2018)

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 2 apresentará a comparação entre a LGPD e TRAC.

Tabela 2. Análise comparativa LGPD x TRAC - Tratamento e Responsabilidades

LGPD	*TRAC*	*LGPD*	*TRAC*	*LGPD*	*TRAC*
Art. 5º	SeçãoA.A3.8	Art. 9º- III -	Não Compatível	Art. 18º	Não Compatível.
Art. 6º	Não Compatível	Art. 9º- IV	Não Compatível	Art. 18º V	Não Compatível.
Art. 6º -IV	SeçãoB.B6.3	Art. 9º- V	Não Compatível	Art. 18º VI	Não Compatível.
Art. 6º-V	SeçãoA.A3.8	Art. 9. § 2º	Não Compatível	Art. 18º VII	Não Compatível.
Art. 6º-VII	SeçãoC.C1.6	Art. 11º	Não Compatível	Art. 18º IX	Não Compatível.
Art. 6º-VIII	SeçãoC.C1.6	Art. 12.	Não Compatível	Art. 18. § 6º	Não Compatível.
Art. 6º-X	SeçãoB.6.3	Art. 14º	Não Compatível	Art. 23º	Não Compatível.
Art. 7º- I	Não Compatível.	Art. 14º § 6º	Não Compatível	Art. 26º	Não Compatível.
Art. 7º-II	Não Compatível.	Art. 15.	SeçãoB.B3.2	Art. 26º IV	Não Compatível.
Art. 7º-III	Não Compatível.	Art. 15. II	Não Compatível.	Art. 32.	Não Compatível.
Art. 8º	SeçãoA.A3.3	Art. 15. III	Não Compatível.	Art. 33	Não Compatível.
Art. 8º § 3º.	Não Compatível.	Art. 15. IV	Não Compatível.	Art. 34	Não Compatível.
Art. 8º §4º	Não Compatível.	Art. 16º	Não Compatível.	Art. 34-II	Não Compatível
Art. 8º § 5º	Não Compatível.	Art. 16º II	Não Compatível.	Art. 37	SeçãoC.C3.3
Art. 9º- I	Não Compatível.	Art. 16º III	Não Compatível.	Art.38	SeçãoA.A3.8
Art. 9º- II	Não Compatível	Art. 16º IV	Não Compatível.	Art.41	SeçãoA.A2.1
				Art. 41. § 1º	Não Compatível

No que tange ao tratamento e às responsabilidades, podemos ver, na Tabela 2, 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 com diz a lei. Vemos, por exemplo, que um dos itens de maior relevância, que é o "consentimento" ou “autodeterminação informativa” não é explicito no TRAC. O art. 8°, § 2º, é muito claro sobre o consentimento:

> 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 arquivísticos possam ser considerados seguros, ou seja, é o conjunto de regras que certifica um repositório arquivístico digital confiável - RDC. Para finalizar a análise, a Tabela 3 mostrará 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 3. Análise comparativa LGPD x TRAC – Sigilo e Privacidade

LGPD	*TRAC*	*LGPD*	*TRAC*
Art. 6º	SeçãoC.C1.5	Art. 47	Não Compatível.
Art. 6º VIII	SeçãoC.C2.1	Art. 48	Não Compatível.
Art. 9º	SeçãoB.B6.2	Art. 48§ 1º	Não Compatível.
Art. 34- I	Não Compatível	Art. 48-I -	Não Compatível.
Art. 34-II	Não Compatível.	Art. 48-III	SeçãoC.C3.1

Art. 34-III	Não Compatível.	Art. 48-IV	SeçãoC.C3.1
Art. 34-IV	SeçãoC.C3.1	Art. 48-V	Não Compatível
Art. 34-V	Não Compatível.	Art. 48-VI.	SeçãoC.C3.4
Art. 34-VI	Não Compatível.	Art. 49	SeçãoC.C3.2
Art. 46	SeçãoC.C1.6	Art. 50	SeçãoA.A3.1

Diretrizes importantes e obrigatórias da referida lei não estão claras no TRAC, por exemplo, o art. 47, 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. (TRAC, 2007)

Não menos importante, o art. 48 da LGPD (BRASIL, 2018) versa sobre a publicidade de incidentes que venham a ocorrer, ainda que o TRAC atenda a alguns requisitos desse artigo, 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 as 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. (LGPD, 2018)

Outro ponto importante ao analisar a lei é a questão do compartilhamento com organizações internacionais, em que a LGPD, em seu artigo 33, incisos de I a IX, é muito clara em relação a forma de compartilhamento.

O guia proposto neste trabalho leva em consideração a necessidade do usuário de acordo com o nível de segurança e negócio. Assim sendo, não é um guia padrão que deve ser usado por todos do começo ao fim, e sim de acordo com a necessidade da organização. Foi utilizado como base para esse guia as principais diretrizes da LGPD e do TRAC, pois este normatiza os parâmetros necessários para que um repositório seja considerado um RDC, enquanto a LGPD define as questões legais sobre privacidade, tratamento e armazenamento de dados.

O guia foi elaborado em forma de checklist, levando em consideração que foi elaborado de acordo com as diretrizes contidas na LGPD, conforme apresentados nas Figuras 1, 2 e 3.

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

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

Figura 1. Análise de adequação – Governança

	Questionário de Auditoria	Norma/Lei Referência	Status			
Tratamento e Responsabilidades	Seu sistema possui algum relatório de impacto descrevendo quais processos podem colocar em risco os dados pessoais tratados?	LGPD. Art32	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui documentação para mitigação de riscos?	LGPD48,VI/TRAC.Seção C, item C1.5	○ TC	○ PC	○ NC	○ N/A
	Seu sistema tem algum controle que limite o tratamento dos dados de acordo com a finalidade?	LGPD.Art6, I	○ TC	○ PC	○ NC	○ N/A
	O sistema possui modulo ou meio de consulta do titular sobre seus dados, forma e duração do tratamento e sobre sua integridade?	LGPD. Art18	○ TC	○ PC	○ NC	○ N/A
	O sistema possui forma de atualização dos dados do titular?	LGPD.Art46 e art.18,III/	○ TC	○ PC	○ NC	○ N/A
	Existe alguma forma de comprovação que existe medidas eficazes que foram adotadas que comprovem a detecção de perdas?	TRAC.SeçãoC, Item C1.5	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui solicita consentimento do usuário para o tratamento dos dados?	LGPD.Art7,I	○ TC	○ PC	○ NC	○ N/A
	O controlador possui alguma prova ou comprovante que afirme que o titular dos dados autorizou o tratamento?	LGPD.Art8°,$2	○ TC	○ PC	○ NC	○ N/A
	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°,$4	○ TC	○ PC	○ NC	○ N/A
	O sistema possui metodo facilitado para o usuário solicitar a revogação do consentimento no tratamento dos dados?	LGPD.Art8°,$5	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum meio de consulta sobre as informações do controlador.	LGPD.Art9°,III e IV/TRAC. SeçãoB, Item B6.2	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum controle sobre aperfeiçoamento dos profissionais que estabeleça o desenvolvimento continuo dos profissionais atuantes?	TRAC:SeçãoA, item A2.2	○ TC	○ PC	○ NC	○ N/A
	O sistema possui mecanismos para transparência e idenficação de responsáveis no que tange a preservação digital?	LGPD.Art46/TRAC.SeçãoA, item 3.7	○ TC	○ PC	○ NC	○ N/A
	O sistema possui documentação sobre a forma de coleta dos dados?	LGPD.Art38/TRAC.SeçãoA, Item 3.8	○ TC	○ PC	○ NC	○ N/A
	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	○ TC	○ PC	○ NC	○ N/A
	O repositório possui controle e permissões de acordo com a responsábilidade dos atores?	TRAC.Seção 3, Item 3.3	○ TC	○ PC	○ NC	○ N/A
	Há no sistema alguma atualização sobre o termo de consentimento em caso de alteração da finalidade?	LGPD.Art8°,$8	○ TC	○ PC	○ NC	○ N/A
	O documento/formulário de consentimento diferencia dados pessoais e dados sensíveis?	LGPD,SeçãoII	○ TC	○ PC	○ NC	○ N/A
	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	○ TC	○ PC	○ NC	○ N/A
	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	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum mecanismo de exportação para portabilidade dos dados do titular?	LGPD.Art18,V	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum meio pelo qual o titular solicite a eliminação dos dados pessoais?	LGPD.Art7°	○ TC	○ PC	○ NC	○ N/A
	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	○ TC	○ PC	○ NC	○ N/A
	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	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum informativo sobre o compartilhamento de dados?	LGPD.Art18,VII	○ TC	○ PC	○ NC	○ N/A
	Você possui compartilhamento de dados com organismos internacionais de acordo com a segurança prevista em lei?	LGPD.Art33,I	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui algum meio de comprovar os registros das operações realizadas pelos operadores e controladores?	LGPD.Art37/TRAC. SeçãoA, Item A3.7	○ TC	○ PC	○ NC	○ N/A

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

Figura 2. Análise de adequação – Tratamento e Responsabilidades

	Questionário de Auditoria	Norma/Lei Referência	Status			
Sigilo e privacidade	As politicas de boas praticas e governanças são divulgadas?	LGPD.Art50,$3/TRAC.SeçãoB, Item B.6.3	○ TC	○ PC	○ NC	○ N/A
	Existe algum controle de alteração ou edição no sistema que identifique o responsavel e os riscos?	LGPD46,$1 /TRAC.SeçãoA, item 3.7	○ TC	○ PC	○ NC	○ N/A
	Há em seu sistema e/ou repositório alguma confirmação para alteração, adição ou exclusão de dados dos usuários?	LGPD.Art46/TRAC.SeçãoC, item 1.6	○ TC	○ PC	○ NC	○ N/A
	Seu sistema disponibiliza de facil acesso a forma de tratamentos dos dados do titular?	LGPD.Art18,II/TRAC	○ TC	○ PC	○ NC	○ N/A
	Seu sistema disponibiliza de facil acesso a forma de tratamentos dos dados do titular?	LGPDArt18,III/TRAC.SeçãoA, item 3.3	○ TC	○ PC	○ NC	○ N/A
	O sistema possui alguma medida ou plano para evolução tecnologica? (autoavaliação; revisão de resultados,etc)	TRAC.SeçãoA,item A3.9	○ TC	○ PC	○ NC	○ N/A
	O sistema possui mecanismos para garantir ou preservar a integridade dos dados?	TRAC.SeçãoA, item A3.8	○ TC	○ PC	○ NC	○ N/A
	O sistema possui controle de acesso com autenticaçao?	LGPD.Art6,VII/TRAC.SeçãoC, item 3.2	○ TC	○ PC	○ NC	○ N/A
	O sistema de gerenciamento de acesso contempla toda politica de de acesso?	TRAC.SeçãoB, item B6.5	○ TC	○ PC	○ NC	○ N/A
	O sistema possui alerta de acesso indevido ou negado?	TRAC.SeçãoB, item B6.6	○ TC	○ PC	○ NC	○ N/A
	O sistema tem documentação para integrações e contendo detalhes de infraestrutura?	TRAC.SeçãoC, item C1.1	○ TC	○ PC	○ NC	○ N/A
	Existe algum controle sobre a forma de armazenamento e controle de backups?	TRAC.SeçãoC, Item C1.2	○ TC	○ PC	○ NC	○ N/A
	O sistema possui formas de identificar perda ou incidentes de integridade?	LGPD/TRAC.SeçãoC, item C1.5	○ TC	○ PC	○ NC	○ N/A
	O sistema possui mecanismos para recuperação de dados?	TRAC.SeçãoC, item C3.4	○ TC	○ PC	○ NC	○ N/A
	O sistema possui monitoramento para análise de segurança de acordo com as normas legais?	TRAC.SeçãoC, C3.1	○ TC	○ PC	○ NC	○ N/A
	Há no sistema alguma forma do usuário consultar sobre o tratamento dos seus dados?	LGPD.Art18	○ TC	○ PC	○ NC	○ N/A
	Sua empresa segue alguma norma de segurança de instituições internacionais?	LGPD.Art34	○ TC	○ PC	○ NC	○ N/A
	O sistema possui algum meio de recuperação de dados?	LGPD.Art6,VII/TRAC.SeçãoC, item C3.4	○ TC	○ PC	○ NC	○ N/A
	O sistema tem algum mecanismo extra de autenticão: Ex: autenticação em duas etapas?	LGPD.Art6°,VII/TRAC.SeçãoB, item B6.4	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui algum controle sobre os responsáveis por acessar e/ou que possam ter acessado enquanto os dados estiveram sobre posse da instituição?	LGPD.Art6,X/TRAC.SeçãoB, item B6.5	○ TC	○ PC	○ NC	○ N/A
	Existe no sistema em alguna divulgação sobre incidentes que ocorreram?	LGPD.Art48S2,I	○ TC	○ PC	○ NC	○ N/A
	Em caso de incidente, o sistema tem mecanismos para avaliar quais os riscos?	TRAC.SeçãoA, Item A4.4	○ TC	○ PC	○ NC	○ N/A
	Em caso de incidente, o sistema tem algum mecanismo que alerte sobre o comunição aos orgãos competentes?	LGPD.Art48	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui contra-medidas a ataques ou perda de dados?	LGPD.Art6,VII/TRAC.SeçãoC, item C1.6	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui regras distintas para tratamento de dados sensiveis?	LGPD.Art11	○ TC	○ PC	○ NC	○ N/A
	Seu sistema possui algum informativo ou opção para reclamações e/ou solicitações dos usuários?	LGPD.Art41,$2/TRAC.SeçãoB, Item B6.2	○ TC	○ PC	○ NC	○ N/A
	O sistema possui normas ou manuais que orientem os controladores e operadores em suas funções?	LGPD.Art50,I/TRAC.SeçãoA3	○ TC	○ PC	○ NC	○ N/A

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

Figura 3. Análise de adequação – Sigilo e Privacidade

3. CONCLUSÃO

O Repositório Arquivístico Digital Confiável (RDC-Arq), a exemplo do Archivematica, ainda que esteja de acordo com o TRAC e o Conselho Nacional de Arquivos - CONARQ, não está adequado à Lei Geral de Proteção de Dados - LGPD. Para chegar à conclusão e objetivo, 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. Concluímos, então, que a criação da LGPD 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 especifico de auditar Repositório Arquivístico Digital Confiável (RDC-Arq) que adota o modelo OAIS, cuja sua 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 possibilitará apoiar com maior eficiência na auditoria, pois concentra todos os requisitos a serem cumpridos, dividido por área temática e questões objetivas. Por meio das Tabelas 1,2 e 3, foi possível identificar a quantidade de itens elencados na LGPD que não estão contemplados no TRAC. Em demonstração numérica, vemos que a comparação na área de Governança, de um total de 22 itens avaliados, apenas 13 (59%) estão compatíveis com a LGPD. Já quando a comparação é feita analisando Sigilo e Privacidade, dos 20 itens comparados, apenas 10 estão compatíveis, ou seja, apenas 50%. Por fim, ao comparar os itens de Tratamento e Responsabilidades, de 49 itens avaliados apenas 11 (22%) estão compatíveis, conforme apresentado na Tabela 4.

Tabela 4. Quadro Resumos de Compatibilidade por Área. LGPD versus TRAC

Área de Análise	*Qnt.Total*	*Resultado (Quantidade)*	
		Compatíveis	Não Compatíveis
Governança	22	13	9
Sigilo e Privacidade	20	10	10
Tratamento e Responsabilidade	49	11	38

Para os trabalhos futuros serão realizados testes de validação do modelo proposto aplicando a repositórios digitais seguros como o RODA e o Archivematica.

AGRADECIMENTOS

Laboratório de Tecnologias para Tomada de Decisão -LATITUDE, da Universidade de Brasília, CNPq – Conselho Nacional de Pesquisa (312180/2019-5 PQ-2 e 465741/2014-2), do Ministério da Economia (005/2016 e 083/2016), do Conselho Administrativo de Defesa Econômica (CADE 08700.000047/2019-14), da Advocacia-Geral da União (697.935/2019), do Departamento Nacional de Auditoria do SUS (23106.118410/2020-85), da Procuradoria Geral da Fazenda Nacional (23106.148934/2019-67).

REFERÊNCIAS

Albrecht, Jan Philipp. "How the GDPR will change the world." Eur. Data Prot. L. Rev. 2 (2016): 287.

Arquivos, C. C. N. de. Norma Brasileira de Descrição Arquivística - Nobrade. 2009.

Brasil. Lei nº13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Conarq, A. N. Diretrizes para a implementação de repositórios arquivísticos digitais confiáveis.2015.

COTS, Márcio, and Ricardo Oliveira. "Lei geral de proteção de dados pessoais: comentada." (2020).Abiteboul, S. et al, 2000.

Da Silva, D. A., de Sousa Jr, R. T., de Oliveira Albuquerque, R., Orozco, A. L. S., & Villalba, L. J. G. (2021). IoT-based security service for the documentary chain of custody. Sustainable Cities and Society, 71, 102940.

De Mouora Sousa, A. P., Rodrigues, A. S., Rodrigues, A. S., & de Oliveira, Â. A. (2006). Princípios da descrição arquivística: do suporte convencional ao eletrônico. Arquivística. net (www. arquivistica. net), 2(2), 38-51.

De Vaus, David, and David de Vaus. Surveys in social research. Routledge, 2013.

Dos Santos, Vanderlei Batista. Preservação de documentos arquivísticos digitais. Ciência da Informação, v. 41, n. 1, 2012.

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

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.

Goddard, Michelle. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, v. 59, n. 6, p. 703-705, 2017.

Gomes, W. D. S.; Autran, M. D. M. M. Análise dos aspectos de confiabilidade do repositório digital arquivístico archivematica à luz da resolução nº 43 do conselho nacional de arquivos. Ciência da Informação em Revista, v. 7, p. 105–120, maio 2020.

ISO-16363. Space Data and Information Transfer Systems-Audit and Certification of Trustworthy Digital Repositories: ISO 16363. [S.l.]: ISO, 2012.

ISO-16363. Space Data and Information Transfer Systems-Audit and Certification of Trustworthy Digital Repositories: ISO 16363. [S.l.]: ISO, 2012.

Lampert, Sérgio Renato. Os repositórios DSpace e Archivematica para documentos arquivísticos digitais. Acervo, v. 29, n. 2, p. 143-154, 2016.

Presidencia da República, “Marco Civil da Internet” (2020).

Ramos, Pedro. A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD. Publicado em, v. 16, n. 07, p. 17, 2019.

Regulation, G. D. P. EU data protection rules. 2018

RLG-OCLC. Trusted Digital Repositories: Attributes and Responsibilities–An RLG-OCLC Report.[S.l.]: Research Libraries Group available at: www. rlg. org/longterm/repositories. pdf, 2002.

Rocha, Cláudia Lacombe. Repositórios para a preservação de documentos arquivísticos digitais. Acervo, v. 28, n. 2, p. 180-191, 2015.

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.

Souza, Luciana Gonçalves Silva; Aganette, Elisângela Cristina. Repositórios digitais confiáveis: uma revisão da literatura nacional e internacional publicada em periódicos científicos. Informação & Sociedade, v. 30, n. 1, 2020.

Trustworthy Repositories Audite Certification Criteria and Checklist (TRAC). 2007.