SEMINÁRIO INTERNACIONAL
DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA
MOSTRA INTERNACIONAL DE TRABALHOS CIENTÍFICOS
REALIZAÇÃO UNISC UNIVERSIDADE DE SANTA CRUZ DO SUL
ISSN: 2358-3010

TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS E O ROADMAP DE ADEQUAÇÃO À LGPD DOS LABORATÓRIOS DE ANÁLISES CLÍNICAS

PROCESSING OF SENSITIVE PERSONAL DATA AND THE ROADMAP OF COMPLIANCE WITH THE LGPD OF CLINICAL ANALYSIS LABORATORIES

Fábio Mattos[1]
Ivone Junges[2]

Resumo: Os Laboratórios de Análises Clínicas tratam dados pessoais sensíveis das pessoas naturais, assim entendido como sendo os dados relativos à saúde ou à vida sexual, dado genético ou biométrico vinculado a uma pessoa natural, denominada de Titular dos Dados. Essas organizações estão sujeitas à LGPD, atuando como controladoras, quando tomam as decisões referentes ao tratamento de dados pessoais ou como operadoras, quando realizam o tratamento de dados pessoais em nome do controlador, e devem assegurar a proteção dos dados pessoais sensíveis dos titulares, que estejam em sua posse, pela adoção de 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. Nesse contexto, esse artigo busca identificar o roadmap inicial à adequação da organização sob a ótica do compliance. Os métodos utilizados são pesquisa documental, tendo sido realizada consulta a legislação, pesquisa bibliográfica livros e artigos científicos selecionados através de buscas nas seguintes bases de dados: EBSCO, SCOPUS e Base integrada da instituição Ânima Educação. As palavras-chaves utilizadas na busca foram: LGPD, Tratamento de dados pessoais sensíveis e LGPD na saúde e, por fim, estudo de caso em um empreendimento da área da saúde, no sul catarinense. Como resultado o artigo apresenta um *roadmap* para adequação das organizações à LGPD.

Palavras-chave: Compliance; Laboratórios de análises clinicas; Proteção de dados pessoais sensíveis; Roadmap de adequação.

Abstract: The Clinical Analysis Laboratories treat sensitive personal data of natural persons, thus understood as being the data related to health or sexual life, genetic or biometric data linked to a natural person, called data subject. These organizations are subject to the LGPD, acting as controllers, when they make decisions regarding the processing of personal data or as operators, when they process personal data on behalf of the controller, and must ensure the protection of sensitive personal data of the data subjects, which are in their possession, by adopting security, technical and administrative measures able to protect personal data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication or any form of improper or unlawful treatment. In this context, this article seeks to identify the initial roadmap to the adequacy of the organization from the perspective of compliance. The methods used are documentary research, and we have been consulted by legislation, bibliographic

[1] Mestrando. Unisul. E-mail: mattos.fabio@animaeducacao.com.br
[2] Doutora. Unisul. E-mail: ivone.junges@animaeducacao.com.br

research books and scientific articles selected through searches in the following databases: EBSCO, SCOPUS and Integrated Base of the Institution Anima Educação. The keywords used in the search were: LGPD, Treatment of sensitive personal data and LGPD in health and, finally, case study in a health enterprise in the south of Santa Catarina. As a result, the article presents an initial roadmap for the adequacy of organizations to the LGPD.

Keywords: Adequacy roadmap; Clinical analysis laboratories; Compliance; Protection of sensitive personal data.

1. Introdução

A Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados (LGPD), está em vigor desde 18 setembro de 2020. Fruto de intensos debates no congresso nacional e, também, na sociedade, a lei é reconhecida como importante avanço na proteção aos direitos fundamentais de liberdade e de privacidade e ao livre desenvolvimento da personalidade da pessoa natural.

A crescente virtualização das relações pessoais e sociais, verificada a partir dos anos 1990, acabaram por fragilizar o sigilo dos dados pessoais e, em consequência, por mitigar o direito à privacidade das pessoas. Segundo Lima "os dados são ativos valiosíssimos na sociedade da informação". De acordo com a autora, "a livre escolha faz parte da vida moderna, desde que as intenções, a finalidade, os riscos e os inconvenientes aos quais o indivíduo pode estar exposto ao ceder suas informações pessoais não sejam um mistério, ou um segredo, nem mesmo esteja de maneira incompreensível ao cidadão médio".

É fato que as organizações coletam informações pessoais daqueles que com elas se relacionam ou queiram se relacionar. Essas informações, na posse das empresas, tem significativo valor econômico e devem ser protegidas e resguardadas, vez que abarcadas pela categoria de direitos fundamentais da pessoa humana estabelecidas na Lei Geral de Proteção de Dados e na própria Carta da República que em seu art. 5º aponta como direitos fundamentais, dentre outros, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurado o direito à indenização; a inviolabilidade do domicílio; e a inviolabilidade do sigilo de dados.

A LGPD estabelece sua aplicação "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados" e define **tratamento de dados** como "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".

Para fins desse artigo, delineia-se o alcance da LGPD às pessoas jurídicas de direito privado, na forma de sociedades empresárias, a teor do art. 44, inciso II, da Lei nº 10.406/2002.

Sociedade empresária é a organização que exerce profissionalmente atividade econômica organizada para a produção ou a circulação de bens ou de serviços (art. 966, do Código Civil) sendo obrigatória a sua inscrição no Registro Público de Empresas Mercantis da respectiva sede, antes do início de sua atividade (art. 967, do Código Civil).

Assim, cumpre as organizações, ao fazer as operações de tratamento dos dados das pessoas naturais, observar os estritos limites da lei. Ressalta-se que as sanções administrativas previstas na LGPD tiveram sua vigência postergada para o dia 1º de agosto de 2021, nos termos do que dispõe o art. 65, I-A, do referido diploma, estando em vigor desde a mencionada data.

Segundo Bioni (2020, p. 59) "o conceito de dados pessoais é um elemento central" para o aperfeiçoamento da regra normativa. Os dados pessoais são ativos que a organização, na condição de **controladora**, a quem competem as decisões referentes ao tratamento de dados pessoais, ou **operadora**, que realiza o tratamento de dados pessoais em nome do controlador, deve mapear, entender e proteger (art. 5º, incisos VI e VII, da LGPD).

Dados pessoais, nos termos do art. 5º, da LGPD, é toda e qualquer informação relacionada a pessoa natural identificada ou identificável e **dados sensíveis** são aquelas informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político e dados referentes à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.

A LGPD cuida da proteção aos dados pessoais, ativos valiosos para as empresas e direito fundamental da pessoa humana, e estabelece a obrigatoriedade da adequação das organizações aos seus ditames, exigindo que sejam adotadas "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" (art. 46, LGPD).

No campo das medidas a serem adotadas pelas organizações, a lei estabelece que a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre padrões técnicos mínimos para tornar aplicável as medidas assecuratórias, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis e os princípios previstos na Lei.

Além disso, a lei prevê que os agentes de tratamento ou qualquer outra pessoa que atue em uma das fases do tratamento estão obrigados a garantir a segurança da informação em relação aos dados pessoais, mesmo após o seu término, devendo o controlador comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Nesse contexto, este artigo busca, pela análise da proteção dos dados pessoais sensíveis coletados pelos laboratórios de análises clínicas, de seus clientes, sob a ótica da das medidas assecuratórias de proteção exigidas pela lei nº 13.709/2018 e a conformidade das organizações à lei geral de proteção de dados – LGPD, responder a pergunta: a: **qual *roadmap* deve ser observado pelo laboratório de análises clínicas para que possa se adequar à lei geral de proteção de dados pessoais?**

O objetivo do artigo foi o de analisar a aplicação da Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/2018, nas organizações de saúde voltadas a coleta de materiais e realização de exames clínicos no que respeita a proteção dos dados pessoais sensíveis e direito à privacidade dos titulares dos dados e, como objetivos específicos, o entendimento dos conceitos gerais da Lei nº 13.709/2018 e a identificação do *roadmap* para a adequação da organização à Lei Geral de Proteção de Dados a serem adotadas pelos laboratórios de análises clínicas.

No campo normativo sobre o tema da privacidade de dados tivemos, no Brasil, em 2014, a edição do Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014 , que estabeleceu princípios, garantias, direitos e deveres para o uso da *Internet* e, na União Europeia, em 2016, a aprovação da Lei Geral Europeia sobre a proteção de dados – GDPR (General Date Protection Regulation), que serviu de fundamento para a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de dados Pessoais – LGPD, que dispôs sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O artigo está estruturado em cinco seções: na primeira a **introdução** com a discussão sobre a temática, incluindo reflexões, problema de pesquisa e objetivos. Na segunda seção, se apresenta as **discussões teóricas** trazendo uma visão geral da legislação sobre privacidade de dados e o posicionamento de alguns estudos sobre a utilização da informação nas organizações. Na terceira seção, **metodologia**, se apresenta o desenho metodológico, ou seja, como a pesquisa foi realizada, para, na quarta seção, **apresentação e discussão dos resultados**, se apresenta o

ISSN: 2358-3010

estudo realizado em um laboratório de análises clínicas da cidade de Tubarão, SC e o *roadmap* inicial a ser observado pela organização na proteção dos dados sensíveis em conformidade à LGPD e, por fim, na quinta seção, **considerações finais**, se apresenta as conclusões e as referências.

2. Discussões teóricas

Estamos vivendo na era da sociedade da informação, onde os dados pessoais dos cidadãos ganham especial importância econômica e são o novo produto gerador de riquezas para as organizações.

Nesse contexto, Nether (2018, p. 17) leciona que "o direito à privacidade tutela importante garantia individual dos cidadãos" e que "os dados pessoais dos indivíduos merecem um tratamento diferenciado com o objetivo de proteger também a privacidade deles nessa circunstância".

Bioni (2020, p. 4) aponta que a sociedade atual está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, entendendo que esta nova forma de organização da sociedade se funda nos avanços recentes da tecnologia, em contraponto ao tipo de organização existente nas sociedades agrícolas, industrial e pós-industrial.

O referido autor entende que a informação é o novo elemento estruturante que reorganiza a sociedade, citando as manifestações havidas em 2013 contra o aumento das passagens de ônibus como exemplo:

> Um exemplo sintomático foram as manifestações de junho de 2013. Nelas, o exercício da cidadania foi revitalizado por um fluxo informacional – em especial das redes sociais – que conectou seus manifestantes, facilitando a organização e a disseminação dos protestos. Verificou-se, sobretudo, um novo instrumento de engajamento social (BIONI, 2020, p.5)

Para Bioni (2020, p. 11), a informação deve ser convertida em conhecimento, tornando-se produtiva e estratégica para as organizações. Leciona o autor que:

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto a segmentação de bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação.

ISSN: 2358-3010

A questão proposta nesse artigo busca analisar e apresentar o *roadmap* necessário a adequação do laboratório de análises clínicas à LGPD, uma vez que, dos setores que coletam e utilizam dados pessoais dos cidadãos para o atendimento de suas finalidades, a área da saúde é dos mais impactados pela Lei Geral de Proteção de Dados.

No campo da saúde, diversos dados pessoais são coletados pelas organizações para o atendimento de suas finalidades. Ainda, muitos dos dados coletados dos pacientes pelos laboratórios de análises clínicas são dados pessoais sensíveis, pois se referem a saúde do indivíduo, nos termos do que preceitua o art. 5º, II, da Lei nº 13.709/2018, que verbera:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> 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; (grifo nosso).

Na sociedade da informação em que vivemos, a coleta e o uso dos dados pessoais sensíveis são partes fundamentais para o desenvolvimento das atividades no setor de saúde e, dessa forma, os impactos da legislação de proteção de dados são maiores nessas organizações.

O art. 11, da LGPD, aponta a possibilidade de tratamento dos dados pessoais sensíveis, indicando que:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Assim, o tratamento de dados pessoais sensíveis pela organização só pode ocorrer se houver consentimento expresso do titular ou de seu responsável, e mediante especificação clara

ISSN: 2358-3010

da finalidade do tratamento, ou, ainda que sem o consentimento, quando para atendimento as hipóteses do art. 11, inciso II, alíneas de "a" a "g", da LGPD

De acordo com Telles; Maruco e Silva, "o uso dos dados sensíveis deve ser mais cauteloso e depende de autorização expressa concedida pelo paciente, cuja informação deve estar bem clara ao usuário, bem como a finalidade para a qual estão sendo solicitados, como por exemplo, para informações médicas".

Para os autores, "hospitais, clínicas médicas, e até médicos que atuam de forma autônoma em consultórios particulares, estão mais expostos a possíveis processos por parte de pacientes e outros titulares de dados, bem como a sanções de órgãos fiscalizadores na área de proteção de dados", uma vez que tratam dados pessoais sensíveis dos seus pacientes.

Para a Lei nº 13.709/2018, **tratamento de dados** é 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 (art. 5º, X).

Para cumprir as exigências da LGPD, a empresa deve estar em *compliance*. A expressão *compliance* tem origem na língua inglesa *to comply* que expressa a ideia de cumprir ou satisfazer determinações jurídicas impostas pelo ordenamento, assim como as normas internas daquela organização (PORTO, 2020, p. 33)

No âmbito da Lei Geral de Proteção de Dados são encontradas as figuras do Controlador e do Encarregado de dados, responsáveis pelo tratamento de dados pessoais dos indivíduos. De acordo com o art. 5º, VI e VII, da LGPD:

> VI - **controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - **operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

No capítulo VI, que trata "dos agentes de tratamento de dados pessoais", na seção I, a LGPD determina em seu art. 37, que "o controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse", estabelecendo, ainda, que "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" (art. 38).

ISSN: 2358-3010

Ainda, compete ao controlador indicar o encarregado pelo tratamento de dados pessoais (art. 41), que pode ser pessoa física de fora da organização, sendo que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador (§1º, art. 41, LGPD)

O DPO (Data Protection Officer), ou o **encarregado de dados**, na nomenclatura adotada pela LGPD, é o profissional da organização que cuida dos dados pessoais tratados pela companhia, sendo suas atribuições: **a)** aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; **b)** receber comunicações da autoridade nacional e adotar providências; **c)** orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e **d)** executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. (§2º, art. 41, LGPD).

No campo das medidas assecuratórias da privacidade dos dados tratados pela organização, a Lei nº 13.709/2018, estabelece em seu art. 46, que "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" sem especificar quais medidas devam ser implementadas.

Para a LGPD, 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, aos princípios gerais e às demais normas regulamentares (art. 49, LGPD).

Nessa senda, é necessário a empresa realizar um diagnostico organizacional, pois é através desse documento que "o empresário tomará conhecimento das dimensões essenciais mínimas de investimento, mercado, recursos humanos e materiais, e de um conjunto de restrições que podemos denominar massa crítica que assegurarão a sobrevivência da empresa" (CAVALCANTI, 1981, p. 14)

De fato, um programa de conformidade deve estar alicerçado em pilares como o comprometimento da alta administração; a avaliação de riscos; a criação de políticas e controles internos e o treinamento e a comunicação, dentre outros.

Na elaboração do programa de *compliance* à LGPD, necessário observar a adoção de medidas relativas à segurança e ao sigilo de dados, consoante dispõem os artigos de 46, 47 e 49, da Lei nº 13.709/2018:

ISSN: 2358-3010

> 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.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
> 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.
> 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.

A Norma ABNT NBR ISO/IEC 27001, é utilizada como fundamento nos programas de *compliance* à LGPD no que respeita a segurança da informação. Trata-se de norma de gestão de segurança da informação cujo objetivo é estabelecer boas práticas para que a empresa possa identificar, analisar e implementar controles de gerenciamento de riscos de segurança da informação e proteger a confidencialidade, integridade e disponibilidade de dados em poder da organização

Em linhas gerais, pode-se identificar 5 (cinco) etapas para a implantação da norma ABNT NBR/ISO 27001 na organização: **a) entender o contexto da empresa**, identificando as características e necessidades da organização para estabelecer as políticas e objetivos internos de segurança da informação; **b) avaliar os riscos à segurança da informação na organização**, identificando-os e classificando-os; **c) estabelecer controles operacionais** que permitam a organização gerir os riscos identificados; **d) analisar a eficácia e desempenho dos controles** adotados pela empresa para garantir a segurança da informação na organização e, por fim, **e) implantar processo de melhoria** realizando a avaliação contínua dos processos .

Segundo a ANPD (2021), “um importante ponto é o gerenciamento de riscos, que consiste no processo de identificar, quantificar e gerenciar os riscos relacionados à segurança da informação dentro da organização. Ele visa a obter um equilíbrio eficiente entre a concretização de oportunidades de ganhos e a minimização de vulnerabilidades e perdas”.

Nesse sentido, existem diversos padrões recomendáveis, como por exemplo guias e frameworks, para operacionalizar a implementação de mecanismos relacionados à segurança da informação. Cabe destacar que muitos mecanismos estão disponíveis gratuitamente,

enquanto outros são utilizados como base para a certificação de conhecimentos profissionais. (ANPD, 2021)

Estabelece a LGPD, em seu art. 50, que os controladores e operadores, 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, levando em consideração, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

No caso da adequação da organização a LGPD, o programa de integridade observa algumas etapas para a sua implantação, que se inicia na fase de **preparação**, onde é feita a avaliação inicial das políticas de privacidade na organização, e avança para a fase de **organização**, onde são elaborados os programas de privacidade, políticas e governança, passa pela fase de **implementação e desenvolvimento da LGPD,** onde são efetivadas as medidas planejadas e realizado o DPIA (Data Protection Impact Assessment), ou relatório de impacto de dados, até chegar a fase de **avaliação e melhoria do programa**, com a adoção de regras de boas práticas e de governança no tratamento dos dados pessoais pela organização.

Nas empresas do setor de saúde, que tratam dados pessoais sensíveis, tem especial relevo o art. 42, da LGPD, que trata da responsabilidade e do ressarcimento de danos, e expressa:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

A lei expressa, ainda, que responderá pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as 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, der causa ao dano (parágrafo único, art. 45, LGPD), estabelecendo, ainda, que "é vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários" (§5º, art. 11, LGPD).

ISSN: 2358-3010

3. Aspectos metodológicos

Nesse tópico são demonstrados os procedimentos metodológicos utilizados pelos autores na realização do trabalho buscando proporcionar uma maior compreensão sobre o fenômeno estudado.

A abordagem utilizada neste trabalho foi a qualitativa, caracterizada por estudo descritivo. Segundo Godoy (1995) "a abordagem qualitativa oferece três diferentes possibilidades de se realizar pesquisa: a pesquisa documental, o estudo de caso e a etnografia". Assim, a pesquisa utilizada no presente trabalho é aplicada, do tipo exploratório, utilizando estudo de caso único, objetivando a pesquisa de aspectos específicos sobre a adequação da empresa à LGPD.

O objeto de estudo foi o laboratório de análises clínicas Dr. Roberto Silva, localizado no município de Tubarão, SC, que atua no setor de saúde e as informações foram obtidas da realização de entrevistas com a gestora da empresa e da análise dos documentos de controle existentes na organização tendo como limite da pesquisa a análise documental com base na LGPD, pautada na legislação, em livros e em artigos das bases de dados nacional e internacional. Foram realizadas três entrevistas com a gestora no mês de junho de 2022 com base em um roteiro de entrevistas contendo perguntas não estruturadas.

Além da pesquisa de estudo de caso, neste estudo também foi realizado neste um estudo de documentos, tendo sido realizada consultas a legislação, e estudo bibliográfico a livros e artigos científicos selecionados através de busca nas seguintes bases de dados: EBSCO, SCOPUS e Base integrada da instituição Ânima Educação. O período dos artigos pesquisados foram os trabalhos publicados nos últimos cinco anos, de 2018 a 2022. As palavras-chaves utilizadas na busca foram: LGPD, Tratamento de dados pessoais sensíveis e LGPD na saúde.

A análise dos dados se deu pela avaliação do estudo bibliográfico, análise documental (legislação pertinente à temática de estudo e documentos da empresa analisada) e análise das entrevistas realizadas.

4. Apresentação e discussão dos resultados

Para esse artigo foi realizado um estudo de caso com a elaboração do diagnóstico inicial da organização denominada laboratório de análises clínicas Dr. Roberto Silva, localizado na

ISSN: 2358-3010

cidade de Tubarão, SC, através de entrevistas pessoais realizadas com a Diretora Administrativa e Financeira da organização.

O diagnóstico é etapa necessária para se entender, no que respeita a coleta e tratamento de dados pessoais, o contexto da organização e, a partir dessa análise se estabelecer um *roadmap* inicial ao programa de *compliance* à LGPD.

De acordo com Cavalcanti (1981, p. 21), "a técnica de análise empresarial constitui-se na aplicação de uma metodologia sistemática, através de um detalhamento que possibilite uma reorientação da ação ou atividade empresarial para conseguir melhores resultados"

A coleta inicial das informações foi feita através de um total de 03 (três) entrevistas com a gestora da organização. As entrevistas foram realizadas de forma presencial na sede da organização e nelas se buscou levantar informações básicas para se entender o contexto inicial da empresa em relação ao fluxo de dados pessoais.

Extraíram-se as seguintes informações das entrevistas realizadas na organização, conforme ilustrado no Quadro 1.

Quadro 1 – Análise das entrevistas realizadas

INFORMAÇÃO SOLICITADA	RESPOSTAS OBTIDAS DO LABORATÓRIO
CONTEXTUALIZAÇÃO DA EMPRESA	O Laboratório Roberto Silva existe desde maio de 1967 na cidade de Tubarão, SC e se dedica a realização de exames laboratoriais diversos (análises clínicas) para pessoas físicas atendendo particulares e convênios (UNIMED, CASSI, MEDPREV, PLADISA (AGEMED), SAÚDE CONCEIÇÃO) além de realizar atendimento pelo SUS e por planos de fidelidade (convênios diversos). A estrutura organizacional da empresa é composta por 6 (seis) pessoas, nas seguintes funções: a) Diretora administrativo financeira; b) Responsável técnica; c) Responsável técnica substituta; d) Atendente; e) Recursos humanos e f) Auxiliares de higienização Visão, missão e valores não estão definidos. Possui organograma definido
COMUNICAÇÃO COM CLIENTES E MIDIAS SOCIAIS DA EMPRESA	A empresa não possui sítio eletrônico próprio, na *Internet*. Para a comunicação com os clientes utiliza as seguintes mídias: Facebook, Instagran e Whatsapp. O Whatsapp é utilizado para entrega dos resultados dos exames aos clientes, sempre em arquivo PDF, também é utilizado para a realização de orçamentos e realização de campanhas promocionais e orientativas. A empresa utiliza software de terceiros no gerenciamento das atividades do laboratório. O sistema permite o acesso do cliente do laboratório ao sítio eletrônico do terceiro para obter o resultado de seus exames através de login e senha fornecido pelo próprio laboratório no ato do cadastramento do pedido, ou seja,

ISSN: 2358-3010

	o cliente obtém o resultado de seu exame a partir do acesso ao sistema do terceiro, onde estão armazenadas as informações. As comunicações com os clientes também são feitas por *e-mail* (recebem solicitações, pedidos de orçamentos e encaminham resultados) Outra forma de entrega de resultados é a presencial. Muitos resultados são pegos diretamente no laboratório (principalmente os resultados de exames de clientes do SUS)
ATIVIDADE REALIZADA PELA EMPRESA	São realizados todos os exames de laboratório: fezes, urina, sangue (que também podem ser terceirizados); toxicológico (coleta de pelo e cabelo e/ou unha) (este exame é coletado no laboratório e a análise é sempre terceirizada; seminal (espermograma); pele (alergia) e covid-19 (teste rápido (sangue) e cotonete nasal (antígeno) – coletados e analisados no laboratório). RTPCR é coletado no laboratório e a análise é terceirizada. O exame Papanicolau (preventivo de câncer) não é coletado no laboratório, mas recebida a amostra é cadastrada no laboratório e a análise é terceirizada. As biopsias, quando vem coletadas, seguem o mesmo padrão.
PROCEDIMENTO DE COLETA DOS EXAMES	O cliente vem a laboratório com a requisição (SUS e MEDPREV – indicação dos médicos ou cotas do SUS). O contato também pode se dar pelo WhatsApp, *e-mail* e presencial, quando o cliente é particular e pede orçamento. O cliente é atendido na recepção: é solicitado documento de identificação e a requisição do médico (se for o caso). Coletam os seguintes dados: nome, idade, CPF, endereço e telefone. É solicitado, também, informação sobre medicamentos de uso contínuo. Para alguns exames é solicitado também peso e altura. No exame de covid são requisitadas outras informações. É feita a coleta no local ou fornecido o material para a coleta das amostras em casa. Na coleta podem ser pedidas outras informações sobre o estado de saúde do cliente, quando necessário. Caso o exame seja terceirizado, o cliente é informado. (fase pré-analítica) Feita a coleta, a amostra é processada (preparação e separação de amostras). Análise (fase analítica). Soroteca (refrigerada): (controle interno de qualidade) toda coleta de sangue fica armazenada por 7 dias para eventual repetição do resultado. Depois do prazo é descartado como lixo hospitalar. Na fase de preparação e separação é definido qual o processamento das amostras (se interno ou terceirizado). Fase pós-analítica: elaboração dos laudos internos. Buscam informações nos terceiros acerca dos exames realizados fora (terceirizados) e anexam o resultado no laudo geral do cliente Disponibilização da informação ao cliente (pela *Internet* ou presencialmente)

ISSN: 2358-3010

	As informações disponibilizadas aos clientes ficam armazenadas no sistema "esmeralda" por 5 anos. (informação extraoficial da Vigilância Sanitária). Após esse prazo é descartado (deletado).

Fonte: Os Autores (2022).

O laboratório é uma organização longeva que existe há 55 (cinquenta e cinco) anos na cidade de Tubarão, SC, e se dedica a realização de exames clínicos para pessoas físicas, provenientes de convênios diversos ou particulares.

A empresa possui uma estrutura organizacional prática e enxuta, com divisão objetiva de atribuições, o que favorece o desenvolvimento das atividades de coleta e realização de exames laboratoriais diversos (análises clínicas) para os clientes, pessoas físicas.

O laboratório possui alguns controles que buscam resguardar o sigilo das informações dos pacientes e atende as legislações e determinações dos órgãos regulatórios. Nessa linha, atende a RDC nº 302/2005, da ANVISA que dispõe sobre o regulamento técnico para funcionamento de laboratórios clínicos, e a RDC nº 63/2011, da ANVISA que estabelece requisitos de boas práticas de funcionamento para os serviços de saúde.

A RDC ANVISA nº 302/2005 que define "os requisitos para o funcionamento dos laboratórios clínicos e postos de coleta laboratorial públicos ou privados que realizam atividades na área de análises clínicas, patologia clínica e citologia", estabelece que "a direção e o responsável técnico do laboratório clínico e do posto de coleta laboratorial têm a responsabilidade de planejar, implementar e garantir a qualidade dos processos, incluindo: **a)** a equipe técnica e os recursos necessários para o desempenho de suas atribuições; **b)** a proteção das informações confidenciais dos pacientes; **c)** a supervisão do pessoal técnico por profissional de nível superior legalmente habilitado durante o seu período de funcionamento; **d)** os equipamentos, reagentes, insumos e produtos utilizados para diagnóstico de uso "in vitro", em conformidade com a legislação vigente; **e)** a utilização de técnicas conforme recomendações do fabricante (equipamentos e produtos) ou com base científica comprovada; **f)** a rastreabilidade de todos os seus processos.

Por seu turno, a RDC ANVISA nº 63/2011, estabelece em seu art. 9º, que "o serviço de saúde deve possuir regimento interno ou documento equivalente, atualizado, contemplando a definição e a descrição de todas as suas atividades técnicas, administrativas e assistenciais, responsabilidades e competências".

Observa-se que as exigências estabelecidas para o funcionamento dos laboratórios de análises clínicas expressas nas RDC nº 302/2005 e RDC nº 63/2011, ambas da ANVISA, no que respeita a privacidade das informações dos pacientes, estão em consonância com os ditames

ISSN: 2358-3010

da Lei nº 13.709/2018, quanto a possibilidade de tratamento dos dados pessoais sensíveis, conforme se verifica do art.11, inciso II, alínea "f", que estabelece:

> Art. 11. 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:
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (REDAÇÃO DADA PELA LEI Nº 13.853, DE 2019).

Se por um lado existe uma prévia orientação para a privacidade de dados e a garantia dos processos decorrentes do próprio regulamento de funcionamento dos laboratórios de análises clínicas, de outro lado, para a correta adequação da organização à LGPD é necessário implantar um programa de *compliance* alicerçado em valores sólidos e na completa observância a legislação.

A norma ABNT NBR ISO 37001 (2017), especifica requisitos e fornece orientações para o estabelecimento, implementação, manutenção, análise crítica e melhoria de um sistema de gestão antissuborno, definindo os requisitos e apontando as orientações para a implantação de um programa de *compliance* antissuborno na organização.

O Decreto nº 11.129, de 11 de julho de 2022, define que um "programa de integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes, com objetivo de: I - prevenir, detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira; e II - fomentar e manter uma cultura de integridade no ambiente organizacional" (art. 56), determinando que o "programa de integridade deve ser estruturado, aplicado e atualizado de acordo com as características e os riscos atuais das atividades de cada pessoa jurídica, a qual, por sua vez, deve garantir o constante aprimoramento e a adaptação do referido programa, visando garantir sua efetividade" (parágrafo único, art. 56).

Por seu turno, a norma ABNT NBR ISO/IEC 27001:2006, "foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um SGSI deve ser uma decisão estratégica para uma organização. A especificação e a implementação do

ISSN: 2358-3010

SGSI de uma organização são influenciadas pelas suas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização"

A norma adota o modelo PDCA (Plan-Do-Check-Act), que é aplicado para estruturar todos os processos do SGSI e que reflete os princípios definidos nas Diretrizes da OCDE (2002) para governar a segurança de sistemas de informação e redes, sintetizados no Quadro 2.

Quadro 2 - Princípios básicos de aplicação nacional

PRINCÍPIO DE LIMITAÇÃO DA COLETA	A coleta de dados pessoais deve ser limitada e os dados devem ser obtidos por meios legais e justos e, quando necessário, informando e pedindo o consentimento do titular dos dados.
PRINCÍPIO DE QUALIDADE DOS DADOS	Os dados pessoais devem ser relacionados com as finalidades de sua utilização e, na medida necessária, devem ser exatos, completos e permanecer atualizados.
PRINCÍPIO DE DEFINIÇÃO DA FINALIDADE	Os propósitos da coleta de dados pessoais devem ser indicados no momento da coleta de dados e o uso subsequente limitado à realização destes objetivos ou de outros que não sejam incompatíveis e que sejam especificados cada vez que mudar o propósito.
PRINCÍPIO DE LIMITAÇÃO DE UTILIZAÇÃO	Dados pessoais não devem ser divulgados, comunicados ou utilizados fora das finalidades que foram especificadas, exceto se houver o consentimento do titular dos dados; ou imposição legal.
PRINCÍPIO DO BACK-UP DE SEGURANÇA	Deve-se realizar Back-up de segurança regulares para proteger os dados pessoais contra riscos tais como perda, ou acesso, destruição, uso, modificação ou divulgação desautorizados de dados.
PRINCÍPIO DE ABERTURA	Deve haver uma política geral de abertura a respeito do desenvolvimento, da prática e da política referentes a dados pessoais. Devem estar prontamente disponíveis meios de estabelecer a existência e natureza de dados pessoais, as finalidades principais de seu uso, bem como a identidade e residência habitual do controlador de dados.
PRINCÍPIO DE PARTICIPAÇÃO DO INDIVÍDUO	Um indivíduo tem o direito de: 1. obter do controlador de dados, ou por outro meio, a confirmação de que este possui ou não dados referentes a ele; 2. de que lhe sejam comunicados dados relacionados a ele: a. dentro de um prazo razoável; b. por um preço, caso houver, que não seja excessivo; c. de maneira razoável; e d. de modo prontamente compreensível para ele; 3. obter explicações caso for rejeitado um pedido feito, e ter meios de contestar tal recusa; e 4. contestar dados relacionados a ele e, se a contestação for recebida, pedir que os dados sejam apagados, retificados, completados ou modificados.
PRINCÍPIO DE RESPONSABILIZAÇÃO	O controlador de dados terá de prestar contas pela observância das medidas que dão efeito aos princípios acima indicados.

Fonte: Adaptado pelos autores a partir de OCDE (2002).

Como resultado da coleta inicial de informações na organização e a partir da análise inicial de seu contexto, tendo por foco o fluxo de dados pessoais sensíveis, tratados pelo laboratório de análises clínicas, aponta-se o *roadmap* inicial necessário ao início da adequação da empresa a lei geral de proteção de dados pessoais.

O *roadmap* contempla 5 (cinco) fases macros ou principais, que por sua vez se subdividem em diversas ações que deverão ser adotadas pela organização no processo de adequação à LGPD, ver Quadro 3.

ISSN: 2358-3010

Quadro 3 - Ações que deverão ser adotadas pela organização no processo de adequação à LGPD

FASE	AÇÃO	ATIVIDADES
1	INVENTÁRIO DE ATIVOS:	Levantamento dos dados ativos da empresa e sua identificação de acordo com: o titular de dados, categoria do ativo (dados pessoais, dados pessoais sensíveis, dados de crianças e adolescentes e dados anonimizados), data de captação, finalidade da captação, último acesso, modificação e impactos.
2	MAPEAMENTO DE DADOS	Mapeamento do fluxo de dados dentro da organização de forma macro, e mapeamento do fluxo de dados por setor.
3	IDENTIFICAÇÃO DE VULNERABILIDADES	Identificar as vulnerabilidades existentes e os riscos à proteção de dados, em relatório à organização e estabelecer os planos de ação necessários para a mitigação dos riscos existentes quanto a privacidade e proteção de dados.
4	ADEQUAÇÃO DOCUMENTAL	Realizar a adequação necessária em todos os contratos ativos da organização; avaliar os documentos utilizados pela empresa inserindo cláusulas específicas de Privacidade e Proteção de Dados; realizar as Políticas específicas para o funcionamento da empresa em conformidade com as diretrizes da Lei Geral de Proteção de Dados.
5	ESTABELECIMENTO DA GOVERNANÇA DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS, SUA IMPLANTAÇÃO E MANUTENÇÃO.	O estabelecimento da estratégia de privacidade de dados e da estrutura organizacional de governança do programa; apresentação de indicadores de gestão e controle de privacidade; elaboração de políticas; estabelecimento de sistema de gestão de direitos do titular, dos contratos, de crises; adoção de ferramentas de segurança da informação; elaborar/executar plano de treinamento e conscientização dos colaboradores.

Fonte: Adaptado pelos Autores de 4Business Consultoria (2022).

O *kick off* do programa de adequação à LGPD é a reunião de conscientização e sensibilização com a alta direção da organização e com os responsáveis pelo tratamento de dados na empresa sobre a lei geral de proteção de dados. A seguir, se realiza o inventário dos ativos (dados pessoais, dados pessoais sensíveis, dados de crianças e adolescentes e dados anonimizados) através do mapeamento dos dados pessoais (data mapping), para então se estabelecer as políticas da empresa quanto a proteção de dados pessoais e segurança da informação, a reestruturação e adequação dos documentos existentes até o treinamento dos envolvidos no tratamento de dados (boas práticas).

5. Considerações finais

O objetivo do trabalho foi estudar a Lei nº 13.709/2018, nominada Lei Geral de Proteção de Dados, e analisar o tratamento de dados pessoais sensíveis pelas organizações do setor de saúde e, a partir de um estudo de caso, estabelecer um *roadmap* inicial necessário a adequação dessas organizações à LGPD.

O estudo de caso foi realizado em um laboratório de análises clínicas na cidade de Tubarão, SC. Pela análise dos dados obtidos, realizada através de estudo bibliográfico, análise

documental e análise das entrevistas com a gestora da organização, se pode estabelecer um *roadmap* inicial necessário a adequação do Laboratório de Análises Clínicas Dr. Roberto Silva à LGPD.

Ao responder a pergunta de pesquisa: qual *roadmap* inicial deve ser observado pelo laboratório de análises clínicas para que possa se adequar à lei geral de proteção de dados pessoais? foi possível identificar 5 (cinco) etapas principais a serem observadas: **a)** a primeira etapa é a realização do INVENTÁRIO DE ATIVOS, com a identificação dos dados pessoais; dados pessoais sensíveis, dados anonimizados e dados de crianças e adolescentes tratados pela organização; **b)** a segunda etapa passa pelo MAPEAMENTO DE DADOS de acordo com o inventário dos ativos realizados, identificando o fluxo desses dados dentro da organização; **c)** a partir do mapeamento de dados e com base na LGPD é possível realizar a terceira etapa que é a IDENTIFICAÇÃO DAS VULNERABILIDADES o que permitirá à organização estabelecer um plano de ação para a correção dos problemas; **d)** paralelo a estas medidas, a organização deverá realizar a ADEQUAÇÃO DOCUMENTAL dos controles internos, comunicados, contratos e demais documentos existentes na organização que respeitam ao tratamento de dados de seus clientes, fornecedores e colaboradores; **e)** por fim, a organização deve ESTABELECER A GOVERNANÇA DO PROGRAMA DE PRIVACIDADE E PROTEÇÃO DE DADOS, assegurando a correta implantação e promovendo a adequada manutenção do programa de conformidade à LGPD pela organização.

A adequação de uma organização do setor de saúde à LGPD exige especial atenção e comprometimento da organização e, em especial da alta direção. Nenhum programa de *compliance* obterá sucesso sem o envolvimento e firme comprometimento dos gestores da empresa. Nesse sentido, a pesquisa se limitou, a partir das entrevistas realizadas e análise de documentos da organização estudada, a analisar o *roadmap* inicial à adequação, não contemplando as etapas anteriores como o *kick off* de sensibilização e as posteriores, traduzidas na efetiva implantação do programa de *compliance* à LGPD, com a execução das etapas apresentadas, o que poderá ser objeto de estudo futuro para atestar a eficácia do r*oadmap* proposto.

REFERÊNCIAS

ALENCASTRO, Mario Sérgio Cunha. **Ética empresarial na prática**: liderança, gestão e responsabilidade corporativa. Curitiba: Intersaberes, 2012.

ANVISA. **Resolução da Diretoria Colegiada - RDC Nº 63, 25 de Novembro de 2011**. Dispõe sobre os Requisitos de Boas Práticas de Funcionamento para os Serviços de Saúde. Disponível em: http://www. http://antigo.anvisa.gov.br/documents/10181/5919009/RDC_302_2005_COMP.pdf/bf588e7a-b943-4334-aa70-c0ea690bc79f . Acesso em: 18 jul 2022

ANVISA. **Resolução da Diretoria Colegiada - RDC Nº 302, de 13 de Outubro de 2005**. Dispõe sobre Regulamento Técnico para funcionamento de Laboratórios Clínicos. Disponível em: http://antigo.anvisa.gov.br/documents/10181/5919009/RDC_302_2005_COMP.pdf/bf588e7a-b943-4334-aa70-c0ea690bc79f . Acesso em: 18 jul 2022

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. LEI Nº 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. Acesso em: 18 jul 2022

BRASIL. LEI Nº 10.406, de 12 de janeiro de 2002. **Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 18 jul 2022

BRASIL. DECRETO nº 11.129, de 11 de julho de 2022. **Regulamenta a Lei nº 12.846, de 1º de agosto de 2013**, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm#art70. Acesso em: 18 jul 2022

CAMPOS, Claudinei José Gomes. **MÉTODO DE ANÁLISE DE CONTEÚDO**: ferramenta para a análise de dados qualitativos no campo da saúde. Rev Bras Enferm, Brasília (DF) 2004 set/out;57(5):611-4. Disponível em: https://www.scielo.br/j/reben/a/wBbjs9fZBDrM3c3x4bDd3rc/?format=pdf. Acesso em: 07 ago 2022

CAVALCANTI, Marli. **Diagnóstico organizacional:** uma metodologia para pequenas e médias empresas / Marli Cavalcanti, Osvaldo Elias Farah, Álvaro A.A. Mello. São Paulo: Ed. Loyola, 1981.

GODOY, Arlinda Schmidt. **INTRODUÇÃO À PESQUISA QUALITATIVA E SUAS POSSIBILIDADES**. Revista de Administração de Empresas São Paulo, v. 35, n. 2, p. 57-63 Mar./Abr. 1995. Disponível em: https://www.scielo.br/j/rae/a/wf9CgwXVjpLFVgpwNkCgnnC/?format=pdf. Acesso em: 07 ago 2022.

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice; MAROSO, Eduardo Pereira. **LGPD – Lei Geral de Proteção de Dados**: sua empresa está pronta? São Paulo, SP: Literare Books Internacional, 2020.

MALDONADO, Viviane Nóbrega. LGPD: **Lei Geral de Proteção de Dados**: Manual de implementação. São Paulo: Thomson Reuters Brasil, 2019.

NETHER, Nicolas Augustus de Barcellos. **Proteção de dados dos usuários de aplicativos**. Curitiba: Juruá, 2018

OCDE. Organização para a Cooperação e Desenvolvimento Econômico. **Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais**. Disponível em: https://www.oecd.org/sti/ieconomy/15590254.pdf. Acesso em: 18 jul 2022

PORTO, Ederson Garin. **Compliance e governança corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

TELLES, Elizabeth Trombini Góes; MARUCO, Fábia de Oliveira Rodrigues; SILVA, Vinícius Donato Saviano Teodoro da. A implementação da Lei Geral de Proteção de Dados no exercício profissional na área da saúde. **REVJUR** | e-ISSN: 1984-5405 | v. 1 | n.1 | Ago./Nov. 2021.

YIN, Robert K. **Estudo de caso**: planejamento e métodos [recurso eletrônico] / Robert K. Yin; [tradução: Cristhian Matheus Herrera]. – 5.ed – Porto Alegre: Bookman, 2015.