UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE CIÊNCIAS CONTÁBEIS

Bruna Altevogt Libino

CONTROLE INTERNO COMO UMA FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UM ESTUDO DE CASO

Santa Maria, RS
2023

Bruna Altevogt Libino

CONTROLE INTERNO COMO UMA FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UM ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Ciências Contábeis**.

Orientadora: Profa. Dra. Ana Paula Fraga

Santa Maria, RS
2023

Bruna Altevogt Libino

CONTROLE INTERNO COMO UMA FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UM ESTUDO DE CASO

Trabalho de Conclusão de Curso apresentado ao Curso de Ciências Contábeis, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do título de **Bacharel em Ciências Contábeis**.

Aprovada em 07 de dezembro de 2023.

gov.br Documento assinado digitalmente
ANA PAULA FRAGA
Data: 14/12/2023 18:30:46-0300
Verifique em https://validar.iti.gov.br

Ana Paula Fraga, Msc. (UFSM)
(Presidente/Orientadora)

gov.br Documento assinado digitalmente
CLAUDIA DE FREITAS MICHELIN
Data: 14/12/2023 10:03:04-0300
Verifique em https://validar.iti.gov.br

Cláudia de Freitas Michelin, Dra. (UFSM)

gov.br Documento assinado digitalmente
MARIVANE VESTENA ROSSATO
Data: 14/12/2023 11:21:14-0300
Verifique em https://validar.iti.gov.br

Marivane Vestena Rossato, Dra. (UFSM)

Santa Maria, RS
2023

AGRADECIMENTOS

Agradeço primeiramente à minha família, por sempre estarem ao meu lado. Em especial a minha mãe, Léa, que apesar de todas as dificuldades nunca mediu esforços para me apoiar na realização dos meus sonhos. E ao meu avô, Ilmo (in memoriam) por ser a força e proteção que eu preciso, tenho certeza de que continuarás a me proteger espiritualmente.

Agradeço aos meus amigos e colegas que fiz durante os cinco anos de graduação, tenham a certeza de que sem vocês, tudo seria mais difícil. A instituição objeto deste estudo, fica o meu agradecimento pela confiança e pelos conhecimentos compartilhados.

A professora Ana Paula, pela sua orientação e dedicação. Bem como, a todos os professores e técnicos administrativos do departamento de Ciências Contábeis, que foram parte essencial da minha formação. Fica um agradecimento especial à Universidade Federal de Santa Maria, por ter me acolhido e me dado a oportunidade de receber um ensino gratuito e de qualidade. Por fim, agradeço a todos que fizeram parte direta ou indiretamente nessa jornada.

Ao Luis Suárez juntamente com o Grêmio, por toda emoção em 2023. Por último queria agradecer a mim mesma, sem mim isto não estaria acontecendo, não foi fácil, mas foi especial.

RESUMO

CONTROLE INTERNO COMO UMA FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UM ESTUDO DE CASO

AUTORA: Bruna Altevogt Libino
ORIENTADORA: Ana Paula Fraga

O presente estudo teve como objetivo analisar se as práticas de gestão e proteção de dados, atualmente utilizados por uma organização, são suficientes e adequadas para cumprir com os requisitos mínimos que são previstos na Lei Geral de Proteção de Dados Pessoais (LGPD). Para isso, foi realizado um estudo de caso em uma empresa de Saúde e Segurança do Trabalho na cidade de Santa Maria/RS. A justificativa pelo tema abordado, é a conscientização de toda a sociedade sobre a importância dos cuidados com os dados pessoais sensíveis e seus reflexos. A Lei 13.709/2018 foi um marco importante na garantia do direito à liberdade e à privacidade, com base nela, as instituições, tanto públicas, como privadas precisam estabelecer processos afim de cumprir e assegurar a proteção dos dados, aumentando a segurança e a credibilidade das organizações nos mercados onde estão inseridas. A metodologia usada neste estudo é o estudo de caso. A instituição estudada, adquiriu uma plataforma de adequação à norma vigente de proteção de dados, atrelado a criação de um comitê de LGPD. O grupo passou a se reunir para discutir ações e realizá-las dentro da organização. Com o modelo utilizado, o comitê passou a analisar as áreas do Jurídico, de Infraestrutura e Tecnologia, Governança e Cultura. Na tentativa de mapear todos os processos envolvendo o tratamento de dados, o grupo passou a estabelecer um conjunto de ações, métodos, com planos interligados, constituindo uma forma de controle interno. Após o estudo teórico da ferramenta, verificou-se a necessidade de adequações nos processos de tratamento de dados. O principal erro nos processos é a não definição clara da ação a ser realizada e o seu responsável, ocasionando o envolvimento de diversos colaboradores, desta maneira, deixando expostos os dados sensíveis. Além disso, as ações e os processos demonstraram a importância de se ter protocolos de ações pré-estabelecidos. O estudo contribui com as discussões acerca do tema de proteção dos dados, assunto recente que aos poucos vem tendo sua importância demonstrada. Ainda, ao final das ações realizadas, o comitê não foi extinto, precisará manter ativo o controle da segurança de proteção de dados dentro da instituição, realizando ações de conscientização e verificar se todas as ações realizadas seguem sendo cumpridas e se estão de acordo com as mudanças impostas pela legislação.

Palavras-chave: LGPD. Processos. Comitê. Controle interno.

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
ASO	Atestado de Saúde Ocupacional
AUDIBRA	Instituto dos Auditores Internos do Brasil
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*
GDPR	*General Data Protection Regulation*
LGPD	Lei Geral de Proteção de Dados Pessoais
PCMSO	Programa de Controle Médico de Saúde Ocupacional

SUMÁRIO

1 INTRODUÇÃO

1.1 CONTEXTUALIZAÇÃO E PROBLEMA DE PESQUISA

Atualmente, é perceptível que o avanço tecnológico possibilitou o acesso às informações de maneira mais ágil, simplificou processos, minimizou o uso do papel, tornando a apresentação e o armazenamento das informações, de uma forma geral, de forma digital. Com isso, milhares de dados circulam nas nuvens, como por exemplo, desde um simples cadastro em uma loja, até cadastros em instituições financeiras e governamentais.

Desde 2018, no Brasil passou a vigorar a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), com a finalidade de regulamentar o tratamento dos dados pessoais, incluindo os meios digitais, seja por pessoa física ou por pessoa jurídica. Esta lei tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O Art. 46 da Lei 13.709/2018 destaca 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 (BRASIL, 2018a).

Desta forma, as empresas precisam se adequar, buscando mapear seus processos, tendo o controle das ações e, principalmente, proteger as informações de seus colaboradores, clientes e fornecedores. Uma ferramenta de auxílio na implementação de ações para implantar as normas e procedimentos adequados sobre o tema de proteção de dados é o controle interno.

Controle interno é um conjunto de atividades, métodos, planos e procedimentos interligados. Destaca-se a definição de Franco e Marra (2001, p. 207) para controle interno:

> [...] todos os instrumentos da organização destinados à vigilância, fiscalização e verificação administrativa, que permitam prever, observar, dirigir ou governar os acontecimentos que se verificam dentro da empresa e que produzem reflexos em seu patrimônio.

Por outro lado, o Instituto dos Auditores Internos do Brasil (AUDIBRA) (1992) expressa com maior evidência o vínculo entre o processo de gestão e o controle interno. As perspectivas dela se alinham ao valor empresarial, eficácia da gestão e sua estruturação.

Para Floriano e Lozeckyi (2008), os controles internos podem ser encontrados em todas as áreas da empresa. Como, por exemplo, no operacional (fabricação, conserto, manutenção,

qualidade) e no administrativo (vendas, compras, tesouraria). A aplicabilidade do controle diariamente impacta significativamente nos resultados da instituição, afim de buscar os resultados definidos.

Diante deste cenário, considerando que a Lei nº 13.709/2018 já está em vigor e precisa ser cumprida, objetivou-se realizar o presente trabalho em uma empresa de Saúde e Segurança do Trabalho na cidade de Santa Maria/RS. A organização formou um Comitê de LGPD que deverá usar o controle interno como "uma ferramenta de gestão". O comitê contou com a formação do curso em *Data Protection Officer*, para que, desta forma, todo o processo de adequação e práticas à LGPD, seja realizado corretamente, transmitindo assim uma maior segurança aos clientes.

Para cumprir os aspectos preconizados pela LGPD é necessário que a organização estabeleça boas práticas de gestão, desta forma, questiona-se: as práticas de gestão e proteção de dados em uso pela organização, atualmente, são suficientes e adequadas para atenderem os requisitos mínimos exigidos por lei?

1.2 OBJETIVOS

A seguir são apresentados, os objetivos do presente trabalho. Os objetivos específicos se relacionam diretamente ao objetivo geral e serviram como um guia do conteúdo abordado ao longo do trabalho acadêmico.

1.2.1 Objetivo geral

Diante do problema proposto, o objetivo geral do estudo é analisar se as práticas de gestão e proteção de dados, atualmente utilizadas pela organização, são suficientes e adequadas para cumprir com os requisitos mínimos que são previstos na LGPD.

1.2.2 Objetivos específicos

Os objetivos específicos servirão como alicerce para o alcance do objetivo geral do estudo, sendo:

a) apresentar os principais aspectos da LGPD;
b) identificar e mapear as práticas de gestão voltadas à proteção de dados, implementadas pela organização;

c) analisar a adoção de práticas de gestão e proteção de dados, que garantam o cumprimento dos requisitos mínimos exigidos pela lei e se estão de acordo com o sistema implementado;
d) sugerir se necessário adequações ao modelo escolhido pela empresa e aconselhar estratégias preventivas através dos riscos avaliados, com a infraestrutura e os processos que formam a base do sistema de controle interno.

1.3 JUSTIFICATIVA

Em suma, a LGPD trouxe uma cultura de privacidade e proteção de dados para o Brasil, exigindo a conscientização de toda a sociedade sobre a importância dos cuidados com os dados pessoais e sua reflexão sobre direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da natureza pessoal. Dessa forma, pela análise do dispositivo depreende-se a importância atribuída à adoção de práticas de gestão e proteção de dados, que garantam o cumprimento dos requisitos mínimos exigidos pela lei. Em agosto de 2018, criou-se no Brasil a LGPD, Lei nº 13.709/2018, sob influência da *General Data Protection Regulation* (GDPR). A GDPR nasceu na Europa, com a finalidade de regulamentar procedimentos e processos associados à integridade, segurança e privacidade de informações pessoais.

Em consequência disso, no Art. 5º da Lei nº 13.709/2018, destaca:

> 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 (BRASIL, 2018a).

A existência de controles internos eficazes que subsidiem a execução adequada de atividades e processos envolvendo informações com dados sensíveis, o controle e auditoria, são de suma importância na manutenção de boas práticas de gestão.

De acordo com Jesus e Barbosa (2016), a gestão de uma instituição consiste em identificar as ações susceptíveis de reforçar a estratégia, de pilotar a sua implementação operacional e, por fim, de controlar os resultados. Seguindo esta linha, Garcia, Kinzler e Rojo (2014) afirmam que o controle interno se refere a todo o sistema de verificação interna, que pode através de uma auditoria interna e outras formas de controle conduzir os negócios de maneira segura. Sendo essencial para que uma instituição consiga minimizar o risco de negócios, garantir a continuidade do funcionamento eficaz da empresa e garantir que a empresa cumpra as leis e regulamentos relevantes. Desta forma, o presente trabalho constitui uma

importante forma de aliar os conhecimentos teóricos adquiridos na academia com uma vivência prática dentro da organização em estudo.

Além disso, no meio acadêmico, evidencia-se a necessidade de estudos relacionados à LGPD e suas implicações no dia a dia das organizações, cujos resultados da pesquisa poderão contribuir para apontar os determinantes para o seu cumprimento efetivo, bem como, no aspecto prático, evitar problemas para as organizações no que tange ao cumprimento desta legislação.

1.4 ESTRUTURA DO TRABALHO

Este trabalho é composto por uma introdução, onde apresentam-se o tema problema e os objetivos gerais e específicos. Ainda na parte inicial, é contemplada a justificativa do trabalho apresentado. A segunda parte é composta pelo referencial teórico, trazendo a teoria de autores da área, com comentários a respeito do tema proposto para estudo. Na terceira parte é evidenciada a metodologia, a partir da abordagem utilizada neste estudo, com destaque para os procedimentos de coleta e análise de dados.

No quarto capítulo, é apresentada a análise dos dados obtidos e, por fim, no quinto capítulo, se apresenta a conclusão, seguida das referências utilizadas neste estudo.

2 REFERENCIAL TEÓRICO

Com base no problema apresentado, faz-se necessário fundamentar este trabalho com base nas teorias relacionadas ao tema. Nesse sentido, Marion, Dias e Traldi (2002, p.38), comentam que “o referencial teórico deve conter um apanhado do que existe de mais atual na abordagem do tema escolhido, mesmo que as teorias atuais não façam parte de suas escolhas.”

Os principais temas abordados neste capítulo são: a história e características da LGPD, os impactos na área da saúde, treinamento voltado a LGPD e por fim, o controle interno.

2.1 HISTÓRIA DA LEI GERAL DE PROTEÇÃO DE DADOS

Historicamente, iniciou-se uma nova cultura de proteção de dados na Alemanha, na década de 70, devido aos avanços na tecnologia de computação e ao foco urgente e contínuo do governo alemão em proteger seus cidadãos dos efeitos da experiência do país durante o regime nazista. Com base nisso, em 1978 foi promulgada a primeira norma regulamentadora.

Em 1995, a União Europeia promulgou a Diretiva 95/46/EC, que continha as primeiras regulamentações da União Europeia, aproximando o conceito de proteção de dados da legislação existente (CONSELHO DA UNIÃO EUROPEIA, 1995). Em 2018, surgiu a GDPR. Uma das primeiras consequências da regra foi o sucesso em forçar o Facebook e o Google, por exemplo, a mudar a forma como coletavam e processavam os dados. O GDPR inspirou outros países a buscar regulamentar a proteção de dados, inclusive o Brasil.

A motivação para a criação de um quadro que regulamenta a proteção de dados pessoais advém do fato de a economia digital ter se tornado mais dependente do fluxo de dados, principalmente os que envolvem os dados pessoais (PINHEIRO, 2020). Teves (2019) cita que os dados pessoais são vistos como o novo petróleo, pois são considerados um recurso essencial para o desenvolvimento de uma economia da informação, assim como o petróleo sustenta uma economia industrial.

2.2 LEI GERAL DE PROTEÇÃO DOS DADOS

A Lei Geral de Proteção de Dados (LGPD, Lei nº 13.709/2018) representa uma grande conquista no tratamento adequado dos dados das pessoas naturais no Brasil. A LGPD foi inspirada no GDPR, regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia.

A GDPR instituída na União Europeia teve início em 2012 e somente em 2016 foi concretizada. Embora essa região já tivesse leis direcionadas à privacidade desde o ano de 1995, com a evolução da tecnologia e globalização, nasceu a necessidade de atualizar e modificar (CRUZ; PASSAROTO; THOMAZ JUNIOR, 2021). Ainda que a LGPD e a GDPR sejam leis distintas, a principal semelhança é o controle rígido sobre as atividades de obtenção, processamento, compartilhamento e segurança dos dados.

Conforme o Art. 2º, da Lei n. 13.709/2018, a proteção de dados pessoais tem como fundamentos:

> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - à inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018a).

Com base nisso, a lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado. Com a chegada da LGPD, as instituições que não seguirem as normas, podem ser fortemente penalizadas, caso ocorra um uso inadequado de dados pessoais. Por se tratar de uma conduta nova, onde ainda não estão totalmente claras as regras e possíveis interpretações para esta lei, as sanções podem ser aplicadas de maneira isolada ou cumulativamente, a depender do caso concreto (MARQUES, 2020).

As atividades envolvendo o tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios, de modo a cumprir com as exigências estabelecidas no Art. 6º, da Lei nº 13.709/2018:

> 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; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; 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; 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; 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; 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; 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; VIII - prevenção: adoção de medidas para prevenir a

> ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; 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 (BRASIL, 2018a).

Com base nos princípios estabelecidos, pode-se dizer que eles norteiam a população, de forma a facilitar o entendimento de boas práticas e condutas, e de identificar práticas inadequadas, que devem ser evitadas, principalmente nas instituições. Ligado a isso, a Lei é transparente a respeito de vazamentos, disseminação, violações, exposição e acessos não autorizados de dados pessoais dos usuários (BRASIL, 2018a; CELIDONIO; NEVES; DONÁ, 2020).

Em razão das infrações cometidas às normas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

> I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração (BRASIL, 2018a).

Tais sanções são de responsabilidade da Autoridade Nacional de Proteção de Dados (ANPD), autarquia de natureza especial, dotada de autonomia técnica e decisória. A partir da Lei nº 13.853, de 2019, a ANPD se tornou responsável por:

> I - zelar pela proteção dos dados pessoais, [...];
> [...]
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo [...] (BRASIL, 2019).

Desde a criação da ANPD, até julho de 2023 não havia de fato casos de punição pecuniária por desrespeitar a legislação vigente. No dia 06 de julho deste ano a coordenação geral de fiscalização da ANPD publicou no Diário Oficial da União uma sanção decorrente da conclusão de processo administrativo sancionador contra a empresa Telekall Infoservice. O órgão fiscalizador, concluiu que a empresa infringiu os Arts. 7º e o 41 da LGPD, bem como o Art. 5º do regulamento de fiscalização da ANPD. Pelo descumprimento do Art. 41 da Lei

resultou em sanção de advertência, já para a infração ao art. 7º da LGPD e ao art. 5º do Regulamento de Fiscalização foram aplicadas sanções de multa simples. Com base no porte da empresa, a multa ficou limitada a 2% do faturamento, gerando assim uma multa no valor de R$14.400,00 (BRASIL, 2023).

Para garantir a segurança e o sigilo dos dados, os agentes de tratamento deverão assumir medidas de segurança e técnicas 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 (BRASIL, 2022a). Com isso, cresce a preocupação no tratamento de dados sensíveis.

Embora todo e qualquer tipo de dado pessoal deva ter o tratamento adequado e dispor de proteção, há uma distinção do que é sensível e o que são dados que devem ser protegidos. Os dados sensíveis são uma espécie de dados com uma maior vulnerabilidade, capazes de identificar um indivíduo, podendo gerar constrangimento, onde há uma grande chance de ser discriminatório o seu uso (DONEDA, 2006).

O Art. 5º da Lei nº 13.709/2018 destaca:

> 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 (BRASIL, 2018a).

Com base nisso, os dados pessoais sensíveis atingem a intimidade. Nesse aspecto, à área da saúde, por exemplo, está diretamente ligada a dados sensíveis. Para Mulholland (2018), proteger os dados sensíveis, consagra a garantia de diferentes direitos, como a liberdade comunicativa, religiosa, de associação e a saúde.

2.3 IMPACTO DA LGPD NAS ÁREAS DA SAÚDE

No contexto da pesquisa, os dados pessoais relacionados à saúde são considerados sensíveis porque revelam informações altamente pessoais e podem afetar diretamente os direitos de privacidade dos usuários, como a exposição dos pacientes afetados. No caso de doenças socialmente estigmatizadas, como AIDS, a exposição de imagens ou resultados de análises desses pacientes causa danos irreversíveis e, em alguns casos, permanentes, por isso é enfatizada a importância de uma proteção especial para informações pessoais tão sensíveis (BARRETO JUNIOR; FAUSTINO, 2019).

O Conselho Federal de Medicina, em sua Resolução nº 1.638/2002, trata sobre a confidencialidade das informações contidas, com o objetivo de proteger a privacidade dos pacientes e garantir que as informações não sejam conhecidas ou compartilhadas com pessoas não autorizadas pelo paciente (CONSELHO FEDERAL DE MEDICINA, 2002).

Em relação aos documentos elaborados, o código de ética médica, também prevê obrigações de confidencialidade entre os médicos e pacientes, criando parâmetros legais para esse relacionamento. Isso inclui, a circulação de um conglomerado de informações sobre o paciente e seu tratamento. Para além das obrigações morais, nomeadamente existe a possibilidade de manipular nesse ambiente, informações a respeito de doenças que que impõem obrigações legais a quem as manipula e recebe, esta confidencialidade assegura u ma gestão destes dados pessoais (BARRETO JUNIOR; FAUSTINO, 2019).

Manter os dados dos pacientes em sigilo é tão forte, que nem mesmo o poder judiciário pode divulgar as informações do paciente. Conforme definido no Código de Ética Médica, os médicos proíbem:

> Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente. Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime o médico estar á impedido de revelar segredo que possa expor o paciente a processo penal (CONSELHO FEDERAL DE MEDICINA, 2019, p. 35).

Conforme exposto, o profissional da medicina, pela própria natureza da atividade em que atua, frequentemente está no meio do tratamento de dados pessoais sensíveis, por ser inerente a sua profissão, possui o acesso aos dados relativos à saúde dos pacientes. Portanto exige uma atenção especial por parte dos médicos quanto às obrigações decorrentes da LGPD.

A Lei Geral de Proteção de Dados Pessoais, estabelece a vedação aos compartilhamentos dos dados relacionados à saúde, conforme os incisos IV e V do Art. 11, que se dispõem nos seguintes termos:

> § 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I – a portabilidade de dados quando solicitada pelo titular; ou II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo.§ 5º 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 (BRASIL, 2018a).

Nesse sentido, os médicos e demais profissionais de saúde sempre devem ter cuidado e atenção com as informações dos pacientes. Afinal, elas são essenciais para acompanhar a evolução do tratamento e chegar a um diagnóstico correto. No âmbito da saúde o que muda com a LGPD é a forma como os dados pessoais são tratados e o aumento da transparência por parte das instituições. Com isso, foi criada a Lei nº 13.787, de 27 de dezembro de 2018, que dispõe sobre "a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente" (BRASIL, 2018b).

Conforme os Art. 1º e Art. 2º da Lei nº 13.787/2018, a digitalização será da seguinte forma:

> Art. 1º A digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente são regidas por esta Lei e pela Lei nº 13.709, de 14 de agosto de 2018 . Art. 2º O processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital. § 1º Os métodos de digitalização devem reproduzir todas as informações contidas nos documentos originais. § 2º No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito. § 3º O processo de digitalização deve obedecer a requisitos dispostos em regulamento (BRASIL, 2018b).

A partir da aplicação da LGPD, as clínicas se tornarão responsáveis pela segurança de todas as informações armazenadas em seu banco de dados. Decorrido o prazo mínimo de 20 (vinte) anos a partir do último registro, os prontuários em suporte de papel e os digitalizados poderão ser eliminados (BRASIL, 2018b). Por isso é preciso garantir que esses dados não sejam acessados por pessoas externas, sendo importante a verificação dos sistemas e plataformas utilizados, observando se há autorizações e políticas de privacidade disponíveis.

Portanto, à luz da LGPD, situações aparentemente triviais, como a de um indivíduo telefonar para o consultório médico, solicitando à secretária o endereço ou telefone de um paciente, devem ser absolutamente rejeitadas, pois "dados pessoais" tratam-se de bens que merecem a proteção de quem possui, sendo vedado o uso indevido e não autorizado. Nota-se que, em regra, o conhecimento e a compreensão dos princípios implicam automaticamente o cumprimento das disposições da própria lei, ressalvadas as condições excepcionais previstas na lei (CONSELHO FEDERAL DE MEDICINA, 2022).

2.4 TREINAMENTO DE LGPD

A ANPD busca orientar os diversos agentes sobre o tema de proteção de dados pessoais. No tocante às informações, ela criou um conglomerado de publicações, contendo guias e documentos técnicos. A LGPD já foi debatida e discutida em diversos fóruns antes mesmo de sua promulgação (BRASIL, 2022b). Suas implicações ainda devem ser discutidas e, sobretudo, experimentadas para que se tornem valores válidos para a sociedade.

Com base em seu planejamento estratégico, a ANPD busca "Promover o fortalecimento da cultura de Proteção de Dados Pessoais; estabelecer um ambiente normativo eficaz para a Proteção de Dados Pessoais; aprimorar as condições para o cumprimento das competências legais" (BRASIL, 2022b).

Atualmente, diversas instituições oferecem o curso de LGPD, muitas delas, são treinamentos *onlines*, como o caso do Sebrae, que aborda o funcionamento, as diretrizes e os impactos da sua implementação. No curso, as empresas aprendem a lidarem com os dados pessoais. De outra forma, as empresas privadas, formulam seus próprios cursos para seus colaboradores, como é o caso do Bradesco, que utiliza a Fundação Bradesco- escola virtual, como meio de formação, onde os funcionários e a comunidade podem aprender que o tratamento de dados pessoais é muito importante para proteger os indivíduos de exposições abusivas ou desnecessárias de seus dados (FUNDAÇÃO BRADESCO, 2020).

No âmbito geral, todos os cursos ofertados buscam definir o que é a LGPD, quais os impactos positivos e negativos para as empresas, uma vez que os consumidores dão muita importância à proteção de seus dados pessoais, e como isto pode beneficiar ou prejudicar a imagem de uma empresa no mercado, dependendo da forma como ela trata as informações de seus clientes.

A LGPD aborda questões as quais as empresas devem se adequar em se tratando da forma como deve ocorrer o acompanhamento do ciclo de tratamento dos dados pessoais. Nesse sentido, o treinamento escolhido, será voltado aos riscos inerentes à instituição.

Scherer Filho (2020) explica que a gestão de riscos de segurança da informação envolve as atividades de todos os funcionários, usuários e permissões de uma empresa, além do monitoramento e recuperação de ataques. Os autores também observam que esse tipo de gestão é um dos maiores desafios das organizações.

A implementação da LGPD trará diversos benefícios para as empresas, entre eles uma melhor identificação dos riscos. Esses riscos serão avaliados em termos de consequências e chances de ocorrência, e as consequências dos riscos serão rapidamente compreendidas e

comunicadas de forma priorizada para desenvolver opções de tratamento e permitir uma redução e monitoramento mais eficazes desses riscos (OLIVEIRA; CAMPOS; MACEDO, 2022).

2.5 CONTROLE INTERNO

Controle interno se constitui em um conjunto de atividades, métodos, planos e procedimentos interligados. Tem como função dentro da empresa, manter a eficácia operacional, gerar relatórios confiáveis sobre desempenho e garantir a conformidade com leis, regulamentos e políticas (FIGUEIREDO, 2018). Diversos autores buscam definir o que de fato é um controle interno.

Para Almeida (2012), o controle interno representa um conjunto de procedimentos, métodos e rotinas de uma organização, com o objetivo de proteger os ativos e produzir dados contábeis confiáveis que auxiliem a entidade a atingir os seus propósitos. Em concordância com a NBC TA 315 (R1) entende que:

> Controle interno é o processo planejado, implementado e mantido pelos responsáveis pela governança, administração e outros empregados para fornecer segurança razoável quanto à realização dos objetivos da entidade no que se refere à confiabilidade dos relatórios financeiros, efetividade e eficiência das operações e conformidade com leis e regulamentos aplicáveis. O termo "controles" refere-se a quaisquer aspectos de um ou mais dos componentes do controle interno (CONSELHO FEDERAL DE CONTABILIDADE, 2016, p. 2).

De acordo com Monteiro (2015), o controle interno é o processo desenhado e executado pelos responsáveis pela gestão e demais encarregados da equipe interna para compelir a garantia razoável sobre a realização dos objetivos da organização no que diz respeito à confiabilidade dos relatórios financeiros, eficácia e eficiência das operações e conformidade com as leis. Ele é utilizado para abordar os riscos que possam ser ameaças às projeções da organização.

Silva, Abreu e Couto (2017), afirmam que a avaliação do controle interno pode minimizar a sensação de impunidade, ineficiência e o frágil controle e fiscalização dos recursos. Complementando estas assertivas, Almeida (2010, p. 5) traz que "com a grande expansão dos negócios, percebeu-se a necessidade de dar maior importância a normas ou aos procedimentos internos, devido ao fato do administrador não poder supervisionar pessoalmente todas as atividades".

De outra forma, Imoniana e Nohara (2005, p. 38) acreditam que o controle "é um importante recurso das funções administrativas de uma instituição, pois permite a constante

avaliação do alcance dos objetivos estratégicos e operacionais". Os autores afirmam que a implantação permite amenizar e reduzir situações que impedem os objetivos da organização serem atingidos.

Segundo Crepaldi (2013), os tipos de controle podem ser divididos em contábeis e administrativos. Os controles contábeis compreendem o plano da organização e todos os métodos e procedimentos utilizados para salvaguardar o patrimônio e a propriedade dos itens que o compõem e os controles administrativos compreendem o plano de entidade e todos os métodos e procedimentos utilizados para proporcionar eficiência às operações, dar ênfase à política de negócios da empresa, bem como seus registros financeiros.

Para que haja um controle interno adequado é necessário que ele seja bem elaborado pela administração, com medidas efetivas e seus custos razoáveis, reduzindo o nível de erros e possíveis irregularidades. De acordo com Franco e Marra (2001), o controle interno é de maneira geral todos os instrumentos da organização destinados à vigilância, fiscalização e verificação administrativa, capazes de prever, observar acontecimentos que se verificam dentro da empresa e que produzem reflexos.

Ressaltando a importante abrangência do controle interno, para Floriano e Lozeckyi (2008), os controles internos podem ser encontrados em todas as áreas da empresa. Como por exemplo, no operacional (fabricação, conserto, manutenção, qualidade) e no administrativo (vendas, compras, tesouraria). A aplicabilidade do controle diariamente impacta significativamente nos resultados da instituição, afim de buscar os resultados definidos.

Para ser eficaz um sistema de controle interno, deve ter o foco em atividades adequadas, deve ser realizada no tempo certo e dentro de um custo aceitável. Além disso, deve ser preciso e realizado por todos os envolvidos na empresa. Segundo Maximiniano (2000), os custos de controle incluem custos *versus* benefícios, no sistema de controle.

Silva (2017, p. 4) chegou à conclusão de que quando há "um sistema de controle interno bem estruturado e operante garante a fiel observância à legislação e instrumentaliza procedimentos que se refletem em economicidade, eficiência, eficácia e efetividade da gestão pública". A partir disso, pode-se dizer que o controle interno tem como função legitimar as informações das instituições, sendo responsável pelo teste de sua veracidade.

De acordo com Costa (2019), à medida que as organizações vão crescendo, aumenta cada vez mais a necessidade de haver controles internos, à medida que aumenta o grau de especialização, é impossível estar totalmente ciente de tudo que está acontecendo em cada parte do negócio. Na sociedade limitada, o conselho de administração é responsável por garantir que os controles internos apropriados sejam exercidos.

Segundo Brito (2017) a implementação de controles resulta no desenvolvimento de um conjunto de regras e procedimentos que combinam os recursos da empresa. Com base nisso, Silva (2017) aborda a implementação de controle interno como ferramenta de prevenção, a ser realizada como um planejamento da cadeia empresarial, levando em consideração os setores da empresa, principalmente os que apresentam maior índice de falhas. Sendo assim, é preciso criar um sistema de verificação interna, como uma auditoria interna, por exemplo, ou outras formas de controle, financeiras e outras, estabelecidas pela direção para conduzir os negócios da empresa de uma maneira ordenada que proteja seus registros.

Em 1992, o *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) publicou o guia *Internal Control – integrated framework (COSO-IC ou COSO I)*, com o objetivo de orientar as instituições quanto a princípios e melhores práticas de controle interno, em especial para assegurar a produção de relatórios financeiros confiáveis e prevenir fraudes. Loureiro (2010) afirma que o COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa.

Nesse modelo, controle interno é definido como um "processo projetado e implementado pelos gestores para mitigar riscos e alcançar objetivos". No que lhe diz respeito, risco é definido como "a possibilidade de ocorrência de um evento que possa afetar o alcance dos objetivos" (COSO, 1992 apud UFSCAR, 2022, p. 8). Ou seja, para o COSO-IC, o controle interno é um processo que tem por objetivo atenuar riscos, com vistas ao alcance dos objetivos.

O modelo para controles desenvolvido pelo COSO (1994 apud LOUREIRO, 2010, p. 12) tem sido adotado por inúmeras empresas e incorporado às suas políticas, regras e regulamentos para melhor controle de suas atividades e orientação em relação à consecução de seus objetivos. O modelo propõe uma definição comum e uma estrutura de avaliação e melhoria dos sistemas de Controles Internos das organizações (COCURULLO, 2004).

De outra forma, Custódio *et al*. (2019) acreditam que o modelo COSO fornece um critério de avaliação dos componentes de controle com a finalidade de obter um elevado grau de transparência das demonstrações contábeis. Sua principal característica é fornecer *insights* sobre a integração dos controles contábeis internos. Os autores ainda colocam que a estrutura de controle interno proposto pela metodologia COSO, é formada por cinco componentes: Ambiente de Controle, Avaliação de Riscos, Atividade de Controle, Informação e Comunicação e Atividade de Monitoramento. Atrelado a este contexto, Sancovschi *et al*. (2019) complementa que a estrutura do modelo de controle interno do COSO é integrada por ainda

mais cinco componentes, que são ambientes de controle, avaliação de riscos, atividade de controle, informação e comunicação e monitoramento.

3 METODOLOGIA

Cervo, Bervian e Da Silva (2007) afirmam que um método é a sequência de diferentes processos que devem ser impostos para atingir um determinado objetivo ou resultado desejado. Segundo Crotty (1998), metodologia refere-se à estratégia, plano de ação, processo ou projeto por trás da seleção e uso de determinados métodos, vinculando a escolha e o uso de métodos aos resultados esperados.

O conhecimento científico mais pesquisado e divulgado são os achados apresentados por Fachin (2003), que segue uma abordagem baseada em problemas reais capazes de analisar, descobrir, resumir, criar e resolver fatos e fenômenos antigos e novos.

3.1 DELINEAMENTO METODOLÓGICO

Boente e Braga (2004) categorizam a pesquisa com finalidade científica e a pesquisa de ponta como pesquisa acadêmica, onde os autores a consideram científica, mas com foco no mercado e não no conhecimento. A primeira afabilidade a ser feita refere-se aos propósitos deste estudo, sendo o mesmo descritivo.

Segundo Selltiz, Wrightsman e Cook (1965), a pesquisa descritiva visa descrever de maneira detalhada um fenômeno ou situação, especialmente o que está acontecendo, capta com precisão as características de um indivíduo, situação ou grupo e revela a relação entre os eventos.

Em referência à abordagem do problema, a pesquisa configura-se como qualitativa, baseada nas informações coletadas e observadas na empresa, objeto do estudo de caso. De acordo com Minayo (2014), a pesquisa qualitativa trabalha com o universo de significados, de motivações, aspirações, atitudes, e não pode ser quantificado. Dessa forma, o trabalho consiste em uma metodologia de pesquisa aplicada, descritiva, qualitativa e documental com fontes bibliográficas, em conjunto ao estudo de caso.

Quanto aos procedimentos técnicos, trata-se de um estudo de caso. Para Yin (2003), os estudos de caso são os mais adequados, quando o fenômeno sob investigação é contemporâneo e envolve uma gama de variáveis diretas ou indiretamente relacionadas ao objeto de estudo, mas que podem não ser necessariamente relevantes para o fenômeno de interesse, quando se utiliza a diferença entre o fenômeno e seu contexto por pesquisadores.

3.2 UNIVERSO DE ANÁLISE DO ESTUDO DE CASO

Os procedimentos deste estudo, incluem a pesquisa bibliográfica, que é desenvolvida a partir de material publicado em livros, artigos, teses e dissertações. Pode ser conduzida de forma independente ou como parte de pesquisa descritiva ou experimental. Segundo Cervo, Bervian e da Silva (2007, p. 61), a pesquisa bibliográfica "representa o procedimento fundamental para estudos monográficos por meio do qual se procura dominar o estado da arte sobre determinado tema".

Sampieri e Lucio (2013) trazem que a pesquisa qualitativa é mencionada em relação ao que as pessoas querem dizer, voltada às suas experiências no mundo social e como eles fazem sentido disso. Silva *et al.* (2012) ensinam que a pesquisa descritiva visa descrever uma situação ou fator de forma objetiva, mapeando um campo de conhecimento. Pesquisa qualitativa descritiva, baseada em Oliveira *et al.* (2020) é um estudo desenhado para responder às seguintes questões: Questões específicas detalhadas que requerem uma análise e descrição da situação que se está observando.

O estudo de caso pode ser caracterizado como uma forma de pesquisa, onde o objeto é uma unidade que se analisa profundamente. Silva e Menezes (2005) abordam o estudo de caso sendo o responsável por explicar por meio de informações, opiniões, avaliações para classificá-las e posteriormente analisá-las, de maneira com que se obtenha uma visão restrita do fato.

De outra forma, para Lüdke e André (1986) abordam o estudo de caso, como estratégia de pesquisa, onde ele é simples e concreto, podendo ser complexo e abstrato, devendo ser sempre bem definido. Pode ser semelhante a outros, mas também é diferente porque tem um interesse único e especial e representa o potencial da educação.

O universo de análise do estudo de caso compreende uma empresa de Saúde e Segurança do Trabalho, que busca se adequar a norma vigente de acordo com a Lei nº 13.709/2018. A técnica da observação é frequentemente combinada com a entrevista, o que ocorreu com o estudo em questão. Para a obtenção dos dados, a pesquisa contou com entrevistas (vide Apêndice A) desenvolvidas a partir da revisão da literatura, principalmente embasadas na Lei nº 13.709, de 2018.

3.3 PROCEDIMENTOS DE COLETA DOS DADOS/EVIDÊNCIAS

A fim de conseguir os dados necessários para o desenvolvimento do estudo, houve o acompanhamento das reuniões do Comitê de LGPD, instituído na empresa, e foi realizada uma

entrevista com o responsável pela TI. Além disso, foram realizadas observações das ações realizadas pela empresa. Ocorreu a investigação sobre a LGPD, Lei nº 13.709/2018, e as políticas por ela assumidas no que diz respeito ao tratamento de dados pessoais sensíveis.

As ações promovidas pelo Comitê abordaram o tratamento restrito dos dados pessoais sensíveis, como forma de proteção contra o seu uso discriminatório. A primeira estratégia, foi baseada na revisão da literatura, consistindo em seguir as proposições que deram origem ao estudo de caso. Como um guia, elas auxiliaram a selecionar os dados, a organizar o estudo e a definir explicações alternativas. Na sequência os dados levantados foram analisados.

Como instrumento de coleta de dados, nos anexos a apêndice A, que contém as perguntas realizadas ao profissional responsável pela TI da empresa.

3.4 PROCEDIMENTOS DE TRATAMENTO E ANÁLISE DOS DADOS

A etapa seguinte no desenvolvimento da metodologia de estudo de caso é a análise dos dados. A análise dos dados é uma fase muito importante em qualquer pesquisa. Estudos qualitativos, requerem a utilização de técnicas que simplifiquem a sua compreensão dos dados (MILES; HUBERMAN, 1994).

Segundo Lüdke e André (1986), analisar os dados qualitativos significa “trabalhar” todo o conteúdo obtido durante a pesquisa, dessa forma, todos os relatos das observações, as transcrições de entrevistas, as análises de documentos e as demais informações disponíveis.

3.5 LIMITAÇÕES DO MÉTODO

Este estudo descreve a adequação da LGPD em uma empresa que atua na área da Saúde e Segurança do Trabalho, no Rio Grande do Sul. As ações e mudanças realizadas na instituição, são realizadas de acordo com as novas normas vigentes, a fim de proteger todos os dados pessoais sensíveis envolvidos no dia a dia de trabalho da organização. Consequentemente, não é possível estender os resultados e ações implementadas para outras organizações. Dessa forma, o estudo realizado se limita no fato de ser apenas realizado em uma única empresa.

3.6 ASPECTOS ÉTICOS

A etapa do procedimento de coleta de dados consiste em um questionário online aplicado aos membros do Comitê. Através disso, é imprescindível que os aspectos éticos sejam respeitados. Para tal, foi disponibilizado aos respondentes o Termo de Consentimento Livre e

Esclarecido (TCLE), a fim de atender os aspectos éticos da instituição de ensino e sanar qualquer dúvida sobre o estudo proposto, no qual pode ser verificado no Apêndice B.

O TCLE disponibilizado pelos pesquisadores, segue todos os princípios éticos da Resolução 196/96 do Conselho Nacional de Saúde, na qual regulamenta sobre ética na pesquisa com seres humanos.

Ademais, ficou esclarecido que todas as informações utilizadas são apenas para fins acadêmicos, podendo os pesquisados desistirem da participação a qualquer momento durante o andamento do estudo, sem qualquer penalização.

Após a finalização da pesquisa acadêmica, os dados dos entrevistados serão mantidos por cinco anos na sala da professora orientadora, na qual está localizada no seguinte endereço: Avenida Roraima, nº 1000, no bairro Camobi, no município de Santa Maria - RS, sob o CEP nº 97.105-900, no prédio 74C, Centro de Ciências Sociais e Humanas, Departamento de Ciências Contábeis (DCC), sala nº 4337. Após cinco anos, os dados serão completamente destruídos.

4 ANÁLISE DOS DADOS

A empresa objeto deste estudo, atua no segmento de saúde e segurança do trabalho, na cidade de Santa Maria/RS. A instituição tem 22 anos de existência e nasceu dentro de uma outra empresa da área da saúde. A missão é promover soluções inteligentes para os clientes e experiências positivas, baseados no modelo Disney.

Para Silva e Vicente (2019), a marca Disney sempre esteve vinculada a uma visão de magia e de encantamento de clientes, onde ela faz com que o indivíduo sinta a transformação de sonho em realidade, com inovação e criatividade e, acima de tudo, uma garantia de excelência de serviço. Walt Disney dizia que "você pode sonhar, criar, projetar e construir o lugar mais maravilhoso do mundo, mas é preciso pessoas para tornar o sonho realidade" (SILVA; VICENTE, 2019, p. 71), trazendo que é o papel das pessoas alcançar a qualidade de processos e a excelência dos serviços.

A companhia Disney age firmemente na busca da excelência e da qualidade total em seus serviços. O seu segredo está na atenção aos detalhes, nos quais a maioria das organizações acaba não concentrando seus esforços (SILVA; VICENTE, 2019). A partir disso, a instituição adotou a visão de ser reconhecida por aquilo que acredita e faz, tendo como seus valores a ética, o respeito e a valorização das pessoas.

Situada no centro da cidade de Santa Maria/RS, a empresa realiza, anualmente, mais de 50 mil atendimentos, entre exames clínicos e laboratoriais. Possui uma carteira ativa de mil clientes, que são atendidos por nove técnicos profissionais em segurança do trabalho e dois médicos do trabalho. A equipe conta com mais de 40 colaboradores diretos e indiretos, atendendo todo Brasil através da rede de credenciados.

A medicina do trabalho é uma especialidade cujo objetivo é atuar na prevenção de doenças do exercício profissional e controle de riscos ambientais. Além disso, está relacionada às normas do governo que as organizações precisam seguir no investimento da saúde do trabalhador.

De modo geral, o objetivo da medicina do Trabalho é atuar na prevenção de doenças às quais os assalariados estão vulneráveis no contexto de suas atividades profissionais. O médico atua aplicando um programa de proteção, ou seja, o Programa de Controle Médico de Saúde Ocupacional (PCMSO), de acordo com cada área de atuação do trabalhador na empresa. O médico do trabalho também monitora a saúde do trabalhador solicitando a realização de exames em intervalos regulares de acordo com a função do colaborador. Além disso, o objetivo da saúde ocupacional é conciliar as demandas do mercado sem colocar em risco a saúde dos

colaboradores, bem como extinguir as responsabilidades e limitações dessas figuras profissionais.

Com base na atividade da empresa, nota-se que o segmento em que ela atua possui a execução de procedimentos e operações envolvendo dados sensíveis, o ponto chave da Lei Geral de Proteção de Dados Pessoais. Com isso, a instituição criou um Comitê de LGPD, para verificar seus processos e adequar-se à legislação.

A adoção de boas práticas de proteção de dados pessoais, que demonstram o espírito e a cultura da organização, e a existência de políticas que têm o objetivo de proteger os dados pessoais, garante aos titulares de dados o exercício de todos os seus direitos. Para dar transparência sobre a proteção de dados pessoais, aqui serão revistas as políticas de privacidade da organização e entender como esta organização se comporta quando o assunto é proteger dados pessoais.

Em abril de 2023, a empresa adquiriu a plataforma DPOnet um *software* que auxilia na implantação da LGPD nas instituições. Uma plataforma de *software* inovadora que ajuda empresas a cumprirem a lei com mais leveza, comodidade e custo acessível, abrangendo, três níveis distintos: jurídico, infraestrutura e tecnologia, governança e cultura.

A plataforma conta com cursos segmentados para diretores, líderes de departamento e representantes. Todos realizam o treinamento inicial, que contempla os conceitos fundamentais sobre a LGPD. Em seguida, é feita a formação oficial do Comitê de LGPD da empresa, este que realizou o treinamento completo e fez as ações.

A DPOnet conta com advogados especializados em LGPD, profissionais de TI e de processos, com *expertise* em metodologias ágeis e normas internacionais de qualidade e segurança da informação.

O treinamento é 100% *online*, com vídeos e pequenas explicações, que facilitam o entendimento. Nesse quesito, o controle interno, tem suma importância no auxílio às adequações, já que este mapeia todos os processos internos da instituição. O Comitê possui encontros semanais, onde realizam as atividades em conjunto e discutem as ações e resultados.

4.1 PRÁTICAS DE GESTÃO VOLTADAS À PROTEÇÃO DE DADOS

A primeira parte do treinamento é a teoria, compreender o que é a LGPD e os impactos dentro da instituição. O treinamento foi dividido em três partes: curso para o representante, curso para a diretoria e curso aos líderes de departamento, que é de fato o Comitê. O

representante é o CEO, a diretoria é a supervisão geral, que acompanha e supervisiona as movimentações do Comitê.

Todos os cursos trataram sobre os conceitos da LGPD. O curso da pessoa nomeada como representante, que é a responsável por liderar a implementação e a manutenção da LGPD, conta com o suporte das demais partes envolvidas. A adequação tem a seguinte ordem:

a) implementação: treinamento, sugestões de questionários, sugestões de processos, portal Privacidade & Você - publicar o Selo no *site*, no e-mail, nas redes sociais e impresso e revisar os questionários e processos sugeridos;
b) manutenção: registros de melhoria contínua;
c) manutenção: relatório de impacto à proteção de dados;
d) manutenção: registro e comunicação de incidentes;
e) manutenção: atualização de políticas;
f) manutenção: atendimento aos titulares e à ANPD;
g) manutenção: treinamentos e cultura;
h) manutenção: manutenção de processos;
i) manutenção: acompanhamento de processos sugeridos;
j) manutenção: atualização de contratos e termos;
k) manutenção: acompanhamento de novas questões (dados obtidos na plataforma DPOnet).

A organização realizou a conscientização de ao menos seus colaboradores-chave (diretoria, gestores ou líderes de departamento) sobre o tema da proteção de dados pessoais, ou seja, promoveu o treinamento/curso, para a compreensão da matéria e início de uma nova cultura de proteção de dados pessoais. O comitê é formado por oito membros, tendo um presidente e vice-presidente eleitos, que são os responsáveis por coordenar todos os encontros e pautas a serem discutidas.

Nos primeiros encontros, o comitê montou e aprovou o Regulamento Interno do Comitê de Proteção de Dados Pessoais, tendo como premissas básicas, sob responsabilidade a:

a) criação de políticas em geral, para a empresa e para departamentos específicos;
b) auxílio para identificar atividades que envolvam o tratamento com dados pessoais e orientar o menor risco possível para a sua prática;
c) auxílio e realização de atividades de educação e cultura;
d) análise de problemas envolvendo produtos e serviços;
e) apoio em caso de incidentes de dados pessoais;
f) auxílio na manutenção de todo o programa de gestão da proteção de dados pessoais;

g) realizar a manutenção do engajamento e conscientização das partes interessadas e de todos os setores da organização em relação à proteção de dados pessoais;
h) manter todos os setores cientes dos indicadores e *status* do programa de gestão de proteção de dados pessoais e principais ações em andamento;
i) avaliar e opinar previamente quanto às medidas de segurança e mitigação de riscos de novos projetos (projetos de execução) que envolvam tratamento de dados pessoais com altos riscos;
j) gerir internamente o programa de gestão de proteção de dados pessoais;
k) realizar ações contínuas junto aos colaboradores, parceiros, prestadores de serviços e cooperados para conscientização acerca da Lei geral de proteção de dados pessoais;
l) realizar treinamentos contínuos de todos os setores e colaboradores da organização;
m) enviar representantes em eventos relacionados com sua finalidade, desde que com anuência da organização (dados obtidos na plataforma DPOnet).

Uma das primeiras ações práticas foi a implementação do selo Portal Privacidade & Você, estabelecendo assim o canal de comunicação com os titulares de dados e com a ANPD. O selo foi adquirido através do *software*. Logo após a conclusão do treinamento sobre conceitos fundamentais, o comitê realizou um evento sobre LGPD a toda empresa. O evento teve como objetivo criar uma cultura de proteção e privacidade de dados pessoais. Além disso, passou a usar vídeos na disseminação de conteúdos para manter vivo o tema. Todas as ações realizadas pelo comitê, bem como seus encontros são registrados em ata, contendo a assinatura de todos os membros. As reuniões, debates e documentos do Comitê são confidenciais e só podem ser acessados por seus respectivos membros, ou terceiros devidamente autorizados para tal, mediante documentação da vista dada, desta forma, não foi possível conhecer e analisar todos os assuntos tratados e registrados em ata.

4.1 INFRAESTRUTURA E TECNOLOGIA

O Quadro 1 representa as medidas sobre o tema infraestrutura e tecnologia pertinentes ao objeto do estudo. A numeração está de acordo com os itens pertinentes a empresa, demais tópicos não foram abordados.

Quadro 1 - Infraestrutura e tecnologia- plataforma DPOnet

Item	Título
4	Descarte de mídias.
7	Acesso às redes e aos serviços de rede.
8	Registro e cancelamento de usuário.
11	Gerenciamento da informação de autenticação secreta de usuários.
14	Uso da informação de autenticação secreta.
24	Segurança em escritórios, salas e instalações.
26	Trabalhando em áreas seguras.
28	Localização e proteção do equipamento.
34	Cópias de segurança das informações.
35	Controles contra malware.
39	Sincronização dos relógios.
40	Instalação de software nos sistemas operacionais.
41	Gestão de vulnerabilidades técnica
42	Restrições quanto à instalação de software.
43	Controles de auditoria de sistemas de informação.
48	Acordos de confidencialidade e não divulgação.
50	Serviços de aplicação seguros sobre redes públicas.
51	Protegendo as transações nos aplicativos de serviços.
53	Restrições sobre mudanças em pacotes de software.
56	Teste de segurança do sistema.
58	Proteção dos dados para teste.
59	Disponibilidade dos recursos de processamento da informação.

Fonte: Elaborado pela autora (2023) com dados da plataforma DPOnet.

O Quadro 1 apresenta os tópicos de infraestrutura e tecnologia revisados na instituição pelo comitê. Em se tratando da relevância do tema, cada um destes itens precisou ser revisto e criado um plano de ação.

O Art. 46, da Lei nº 13.709/2018 destaca:

> 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 (BRASIL, 2018a).

O operador obriga-se a cumprir o tratamento dos dados dentro das finalidades específicas definidas pelo responsável pelo tratamento, limitando ao mínimo a quantidade de dados pessoais recolhidos, o tempo de tratamento, o prazo de conservação e a acessibilidade. Por exemplo, esta medida deverá garantir que nem todos os utilizadores das informações tenham acesso ilimitado e indefinido aos dados pessoais tratados pela empresa (DUARTE; DOMENICONI JUNIOR; EBOLI, 2022).

Sendo assim, a empresa deve adotar medidas de segurança com a finalidade de garantir a proteção dos dados pessoais contra acessos não autorizados, situações acidentais, ou até mesmo ilícitas. Com base nos itens a serem cumpridos, a empresa adotou as seguintes medidas, com base nos planos de ações. Desta forma, o Quadro 2, apresenta as medidas propostas pelo comitê para sanar os itens pertinentes a instituição.

Quadro 2 - Medidas de infraestrutura e tecnologia- Comitê de LGPD

(continua)

Item	Título	Medidas
4	Descarte de mídias.	As mídias são descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais, por meio do protocolo de descarte.
7	Acesso às redes e aos serviços de rede.	Os usuários somente recebem acesso às redes e aos serviços de rede que tenham sido especificamente autorizados a usar, a TI e a supervisão geral liberam os acessos de acordo com a função.
8	Registro e cancelamento de usuário.	Um processo formal de registro e cancelamento de usuário é implementado para permitir a atribuição dos direitos de acesso. Feito na admissão e demissão do colaborador, por meio do manual do usuário.
11	Gerenciamento da informação de autenticação secreta de usuários.	A concessão de informação de autenticação secreta é controlada por meio de um processo de gerenciamento formal.
14	Uso da informação de autenticação secreta.	Os usuários são orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta.
24	Segurança em escritórios, salas e instalações.	É projetada e aplicada segurança física para escritórios, salas e instalações.
26	Trabalhando em áreas seguras.	São projetados e aplicados procedimentos para o trabalho em áreas seguras.
28	Localização e proteção do equipamento.	Os equipamentos são protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizadas.

(conclusão)

Item	Título	Medidas
34	Cópias de segurança das informações.	Cópias de segurança das informações, softwares e das imagens do sistema são efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.
35	Controles contra malware.	São implementados controles de detecção, prevenção e recuperação para proteger contra malware, combinados com um adequado programa de conscientização do usuário.
39	Sincronização dos relógios.	Os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, são sincronizados com uma fonte de tempo precisa.
40	Instalação de software nos sistemas operacionais.	Procedimentos para controlar a instalação de software em sistemas operacionais são implementados, como o desencorajamento e estão limitados às mudanças necessárias, e todas as mudanças são estritamente controladas pela direção e TI.
41	Gestão de vulnerabilidades técnica	Informações sobre vulnerabilidades técnicas dos sistemas de informação em uso são obtidas em tempo hábil; a exposição da organização a estas vulnerabilidades deve ser avaliada e são tomadas as medidas apropriadas para lidar com os riscos associados.
42	Restrições quanto à instalação de software.	Regras definindo critérios para a instalação de software pelos usuários são estabelecidas e implementadas pela TI.
43	Controles de auditoria de sistemas de informação.	As atividades e requisitos de auditoria envolvendo a verificação nos sistemas operacionais são cuidadosamente planejados e acordados para minimizar a interrupção nos processos do negócio.
48	Acordos de confidencialidade e não divulgação.	Os requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação são identificados, analisados criticamente e documentados, no manual do colaborador.
50	Serviços de aplicação seguros sobre redes públicas.	As informações são apenas na rede privada, não envolvendo as redes públicas.
51	Protegendo as transações nos aplicativos de serviços.	Informações envolvidas em transações nos aplicativos de serviços são protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
53	Restrições sobre mudanças em pacotes de software.	Modificações em pacotes de software são desencorajadas e estão limitadas às mudanças necessárias, e todas as mudanças são estritamente controladas pela direção e TI.
56	Teste de segurança do sistema.	Testes de funcionalidade de segurança são realizados durante o desenvolvimento de sistemas pela TI.
58	Proteção dos dados para teste.	Os dados de teste são selecionados com cuidado, protegidos e controlados, conforme os critérios da TI.
59	Disponibilidade dos recursos de processamento da informação.	Os recursos de processamento da informação são implementados com redundância suficiente para atender aos requisitos de disponibilidade, de acordo com os critérios da TI.

Fonte: Elaborado pela autora (2023) com dados da plataforma DPOnet.

Diante das medidas expostas, todas as mudanças, realizadas pela TI buscam implementar novos padrões de segurança, políticas de privacidade e *cookies*, sempre prezando pela clareza e transparência. Ressaltando a importância deste setor neste aspecto, pois diversos processos que são suscetíveis a exposição de dados, passam pelo sistema utilizado. Em uma entrevista realizada com o responsável técnico pela TI, ele explicou as ações realizadas diariamente no controle de invasões. Em vinte anos, nenhuma tentativa de invasão teve sucesso, além disso, há um *backup* diário que é armazenado em três diferentes locais na nuvem, sendo uma delas nos Estados Unidos.

Na entrevista, o responsável ao ser questionado sobre as medidas para proteção de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas quando há o trânsito de informações em rede públicas, foi pontuado que jamais utiliza-se outra rede a não ser a privada, nenhuma rede pública é utilizada. Ainda, é realizado diariamente uma varredura para coletar informações sobre vulnerabilidades técnicas dos sistemas utilizados. Conforme o responsável "há testes regulares das funcionalidades de segurança dos sistemas, desenvolvidos internamente ou terceirizados, para assegurar que a aplicação trabalha".

Foi realizado o levantamento de equipamentos periféricos. A partir dele, montou-se um vídeo sobre a colocação e utilização de senhas seguras, tanto para os computadores, como celulares e *IPADs* da instituição. Além disso, criaram-se dois protocolos, um de descarte de equipamentos e outro de utilização, no caso da utilização de dosímetros e *notebooks* em visitas técnicas. Tendo em vista a preocupação com o armazenamento correto dos equipamentos e de arquivos contendo informações pessoais, foi montado uma nova sala de arquivos, com acesso somente a pessoas autorizadas.

O novo manual do colaborador, que é entregue no primeiro dia de trabalho, recebeu a autorização de tratamento de dados, onde ao entrar, o colaborador deverá estar de acordo com tratativas de seus dados. Além disso, o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Somado a isso, deverá seguir as normas previstas na Lei nº 13.709/2018. Também neste momento, é dado ao funcionário suas credenciais.

Em relação a segurança em escritórios, salas e instalações, foi refeita toda a parte de monitoramento por câmeras, contemplando uma área maior e tendo um acompanhamento diário pela supervisão.

Como exemplo de plano de ação realizada pelo Comitê, cita-se o plano do item 7 referente ao acesso às redes e aos serviços de rede. O método 5W2H reúne um conjunto de questionamentos voltados para a organização e planejamento de procedimentos estruturados

em encaminhamentos mais diretos. Por conta disso, é frequentemente aplicado no gerenciamento de organizações que buscam o alcance de uma melhoria contínua de processos, dessa forma, ele foi utilizado nos planos de ações.

A numeração do plano se dá em virtude de a escolha ser o item 7, correspondente à numeração a qual é pertinente à instituição.

Plano de ação 02

- **O que fazer?**

  Ajustar e mapear os acessos às redes e sistemas de cada usuário.

- **Por que fazer?**

Para que se tenha o devido controle dos acessos às redes, evitando o acesso a informações confidenciais e a dados pessoais a pessoas não autorizadas.

- **Onde fazer?**

  Nos acessos às redes.

- **Quem vai fazer?**

  Presidente do comitê e supervisão geral.

- **Quanto vai custar?**

  Sem custo.

- **Situação?**

  Finalizado (dados obtidos da empresa objeto do estudo).

Na execução deste plano de ação, foi necessário acessar o sistema utilizado e verificar todos os acessos, além da rede interna. Com base nas informações colhidas, montou-se uma planilha de controle de acessos necessários para cada função. Este controle auxiliará na contratação de novos colaboradores, já deixando tanto a rede, quanto o sistema com os acessos necessários para atuar.

Cada um dos itens mencionados acima, possui um plano de ação objetivo para manter as informações seguras.

4.2 JURÍDICO

Na organização existem diversas áreas por onde as informações circulam e são manipuladas. Assim, a primeira tarefa da LGPD jurídico é conhecer toda a estrutura do fluxo de informação empresarial, ou seja, saber os processos internos e os sistemas envolvidos.

Com base nas instruções do treinamento, o Quadro 3 representa as questões pertinentes e aplicáveis à instituição, com suas medidas já estabelecidas no tocante a área jurídica. A

numeração apresentada nos itens se refere aos elementos pertinentes à instituição, não sendo necessário todos os sugeridos pela DPOnet.

Quadro 3 - Jurídico

Item	Título	Medidas
1	Requisito LGPD/Avaliação de Impacto.	A organização promove a avaliação de impacto à proteção de dados pessoais em relação às suas atividades de tratamento.
21	Requisito LGPD/ Consentimento.	A organização coleta ou garante que seja coletado o consentimento dos responsáveis dos menores e prevê em seus instrumentos (como contratos, termos de uso e política de privacidade) a coleta desse consentimento de forma destacada, específica, transparente e informada.
22	Requisito LGPD/Direito dos titulares.	A organização fornece de maneira clara a identidade e os detalhes de contato do controlador ou seu representante para o titular dos dados.
24	Requisito LGPD/Coleta e Processamento de Dados Pessoais.	A organização informa, explicitamente, ao titular de dados em seus instrumentos (como contratos, termos de uso, políticas de privacidade) as finalidades para as quais os dados pessoais são e/ou serão tratados.
25	Requisito LGPD/Direito dos titulares.	A organização informa aos titulares de dados as finalidades do tratamento para as quais os dados pessoais são tratados e também a hipótese da Lei geral de proteção de dados pessoais (Arts. 7º e 11) que autoriza o tratamento.
26	Requisito LGPD/Direito dos titulares.	A organização informa aos titulares de dados o período para o qual os dados pessoais serão armazenados ou, se isso não for possível, os critérios usados para determinar esse período.
29	Requisito LGPD/ Consentimento.	A organização, em seus instrumentos (como contratos, termos de uso e políticas de privacidade) colhe o consentimento do titular de dados no formato escrito, deixando explícito e em um texto de fácil compreensão o fato de estar colhendo o consentimento.
32	Requisito LGPD/Coleta e Processamento de Dados Pessoais.	A organização conta com instrumentos que regulam a proteção de dados pessoais de modo a estabelecer acordos em relação às atividades de tratamento entre controlador e operador.
36	Requisito LGPD/Contratos.	A organização, como operadora, adota contratos com os controladores que estabelecem as regras em relação ao tratamento dos dados pessoais.
72	Legítimo interesse.	Para as atividades de tratamento de dados pessoais (processos) que têm como base legal o legítimo interesse do controlador ou de terceiros, a organização adota um procedimento que permite ao titular de dados dizer que não deseja que seus dados pessoais continuem a ser tratados (direito ao "*opt-out*").

Fonte: Elaborado pela autora (2023) com dados da plataforma DPOnet.

Baseado nos itens relevantes selecionados, referentes ao tema jurídico, o comitê desenvolveu ações em conjunto com a direção. Nos contratos de prestação de serviços, estando de acordo com os itens 22, 24, 25, 26, 29, 32, 36 e 72, houve a inclusão das cláusulas 20 a 26.2 sobre "Tratamento de Dados". Um dos principais itens desta inclusão, é o inciso 21, que obriga

o contratado a esclarecer aos destinatários de seus serviços, que os dados que fornecem são sensíveis, cuja utilização depende da observância de regras já fixadas.

De acordo com o que foi explicado acima, o exemplo de plano de ação jurídico referente aos itens supracitados, aborda o item 24 que trata o requisito LGPD/Coleta e Processamento de Dados Pessoais.

A numeração 41 do plano de ação se dá em virtude de a numeração ser correspondente a numeração dos itens pertinentes a instituição, não seguindo a numeração numérica.

Plano de ação 41

- **O que fazer?**

Incluir no contrato o item Tratamento de dados, que deverá deixar explícitas as obrigações em face dos dados pessoais, e o asseguramento do livre acesso às informações prestadas pela contratada, bem como sua transparência.

- **Por que fazer?**

A organização precisa informar, explicitamente, ao titular de dados em seus instrumentos (como contratos, termos de uso, políticas de privacidade) as finalidades para as quais os dados pessoais são e/ou serão tratados.

- **Onde fazer?**

  Nos contratos e nas negociações.

- **Quem vai fazer?**

  Setor financeiro e supervisão geral. Revisão pelo advogado da empresa.

- **Quanto vai custar?**

  Sem custo.

- **Situação?**

  Finalizado (dados obtidos da empresa objeto do estudo).

Esta ação foi realizada de forma conjunta entre financeiro, supervisão geral e departamento jurídico. O setor jurídico aprovou o texto, porém com ressalvas, cada um dos itens propostos precisa de fato estar sendo realizado pela instituição, para que não haja dúvidas quanto ao tratamento adequado dos dados. Além disso, propôs que o contrato fosse revisado com mais frequência, em virtude das constantes mudanças.

Em conformidade ao item 01, o comitê semanalmente se reúne no tocante às questões de mudanças que estão sendo feitas, além disso, é conversado e deixado um parecer à direção sobre os impactos de uma eventual nova atividade, que possa impactar no tratamento de dados pessoais.

Além dos clientes registrados e que possuem contratos de prestação de serviço com a empresa, há a possibilidade de realizar atendimentos clínicos e laboratoriais sem ser cliente de carteira da instituição. Nesses atendimentos particulares de consultas e exames, não há contrato de prestação de serviços, sendo apenas mencionado no Atestado de Saúde Ocupacional (ASO), a segurança do tratamento de dados. Com base nisso, criou-se um protocolo de dados pessoais, com a menção aos menores de idade, exposto no item 21, para a população em geral que deseja consultar de maneira avulsa.

Por fim, de acordo com o entrevistado, todo e qualquer documento jurídico será revisado, para garantir a conformidade das cláusulas com a LGPD, inclusive com adesão à política de confidencialidade.

4.3 GOVERNANÇA E CULTURA

O Quadro 4 representa as medidas sobre o tema governança e cultura pertinentes ao objeto do estudo. A numeração está de acordo com os itens pertinentes à empresa, demais tópicos não foram abordados, por não serem relacionados à instituição.

Quadro 4 - Governança e cultura

(continua)

Item	Título	Medida
2	Responsabilidades pelo encerramento ou mudança da contratação.	As responsabilidades e obrigações pela segurança da informação que permaneçam válidas após um encerramento ou mudança da contratação são definidas, comunicadas aos funcionários ou partes externas e cumpridas.
6	Política para o uso de dispositivo móvel.	Uma política e medidas que apoiam a segurança da informação são adotadas para gerenciar os riscos decorrentes do uso de dispositivos móveis.
16	Seleção.	Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e à classificação das informações a serem acessadas.
19	Devolução de ativos.	Todos os funcionários e partes externas devolvem todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

(conclusão)

Item	Título	Medida
22	Reutilização e/ou descarte seguro de equipamentos.	Todos os equipamentos que contêm mídias de armazenamento de dados são examinados antes da reutilização, para assegurar que todos os dados

		sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança.
23	Política de mesa limpa e tela limpa.	São adotadas políticas de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação.
46	Direitos de propriedade intelectual.	Procedimentos apropriados são implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual e sobre o uso de produtos de software proprietários.
59	Processo disciplinar.	Existe um processo disciplinar formal, implantado e comunicado, para tomar ações contra funcionários que tenham cometido uma violação de segurança da informação.
61	Validação de terceiros.	A organização tem um procedimento interno para validar os seus fornecedores e parceiros comerciais, que permite verificar se contam com um nível razoável de maturidade em proteção de dados pessoais, considerando o cumprimento de medidas fundamentais, jurídicas e de segurança dos dados pessoais.

Fonte: Elaborado pela autora (2023) com dados da plataforma DPOnet.

A governança corporativa, como um modelo organizacional, se torna uma estratégia de gestão, onde fortalecem as formas de comportamento, tendo o seu relacionamento com todos os públicos envolvidos na organização. Nesse sentido, exige-se que a pessoa principalmente a gestão e os líderes tenham um esforço consciente para mudar hábitos, crenças e tradições normativas. Para Lopes, Valentim e Fadel (2014, p. 274), a cultura possui o papel determinante para a formação de valores organizacionais. Em especial, os valores organizacionais em relação à informação são extremamente importantes para a Governança Corporativa, pois indicam a forma que seus colaboradores lidam com a informação, alterando e ajustando a relação das pessoas em relação ao compartilhamento, divulgação e uso da informação.

Diante disto, a Cultura Organizacional é, de maneira clara, um conjunto de hábitos, crenças e artefatos que são vividos e compartilhados entre elementos de um mesmo grupo, onde esses conjuntos de hábitos, crenças e costumes são peças chaves para favorecer a implantação dos princípios da Governança Corporativa, justamente pela implantação de seus elementos na vivência da organização (ALVES, 2023).

Em consequência, o item 23, referente a política de mesa limpa e tela limpa, trata-se de um exemplo claro de criação de hábito, onde a organização deve adotar uma política de mesa limpa, para garantir que as mesas estejam livres de documentos e dispositivos como *pendrives*, *HDs* externos, em momentos e ambientes adequados, com o objetivo de evitar expor informações a terceiros. Além disso, também adota uma política de tela limpa, para

computadores e outros dispositivos semelhantes, para garantir que as telas não sejam alvo de olhares curiosos ou acesso sem autorização.

De acordo com o que foi explicado acima, o exemplo de plano de ação referente aos itens supracitados, aborda o item 23.

Ressaltando, a numeração dos planos de ações não estão sendo organizados pela numeração padrão, pois eles são realizados de acordo com os itens pertinentes a instituição.

Plano de ação 23 - Governança e Cultura

- **O que fazer?**

Na reunião do comitê será realizado às normativas a serem seguidas por todos os membros da empresa. A presidente reunirá as normas e irá apresentar a toda a equipe na reunião geral, além disso, um dos integrantes do comitê, passará um vídeo explicativo de como bloquear o seu computador e criar um login para um visitante.

- **Por que fazer?**

Todos precisam estar cientes das normativas criadas pelo comitê de LGPD, devendo cumprir com as regras para que todos os dados estejam protegidos.

- **Onde fazer?**

  Na sala de reunião.

- **Quem vai fazer?**

  A presidente e um integrante do comitê.

- **Quanto vai custar?**

  Sem custo.

- **Situação?**

  Finalizado (dados obtidos da empresa objeto do estudo).

Foi realizado um encontro com todos os colaboradores para apresentar as normativas do tratamento de dados da empresa. Diante das mudanças propostas, houve um visível interesse dos colaboradores em conhecer mais o trabalho do comitê, bem como querer fazer parte.

Levando isso em consideração, logo após, o não cumprimento das medidas impostas pelo comitê, pode ser interligado ao item 59, que refere-se ao processo disciplinar, onde a própria instituição deixa claro na sua documentação, como no contrato de trabalho e no manual do colaborador, quais são as ações disciplinares a serem tomadas a quem tenha cometido uma violação de segurança da informação, inclusive dados pessoais. O mesmo procedimento é descrito no regimento interno do comitê de LGPD.

5 CONCLUSÕES E RECOMENDAÇÕES

Este capítulo apresenta as conclusões do estudo de caso, a partir das evidências obtidas, além de recomendações para estudos futuros.

5.1 CONCLUSÕES

Este estudo teve por objetivo analisar se as práticas de gestão e proteção de dados, atualmente utilizadas por uma organização, são suficientes e adequadas para cumprir com os requisitos mínimos que são previstos na LGPD. Dessa forma, pode-se avaliar os efeitos e as mudanças ocorridas na organização, realizadas por um comitê e sua direção, com o auxílio de uma plataforma especializada em adequação à legislação de proteção de dados. Para responder ao objetivo do estudo, realizou-se um estudo de caso, com a coleta e exploração de informações qualitativas, coletadas a partir de eventos reais, através de entrevistas e da observação sistemática.

Ademais, buscou-se através da leitura, buscar referências na literatura e na legislação, afim de alinhar a teoria e a prática com o sistema. Nesse sentido, tendo em vista que a legislação sobre a proteção de dados pessoais é recente, muito ainda se discute sobre o que são dados pessoais sensíveis e a penalidade sobre o descumprimento e o vazamento dessas informações. A ANPD começou somente agora, cerca de cinco anos após a Lei nº 13.709/2018 ser publicada, a aplicar multas pela inobservância das normas. Adicionalmente, buscou-se investigar os principais pontos de contato dentro da instituição, onde ocorrem o manuseio das informações sensíveis, sua gravidade, a natureza das infrações e dos direitos pessoais afetados, bem como a condição econômica do infrator, o grau do dano causado, a cooperação do infrator na resolução e a adoção de política de boas práticas de governança para a adoção de medidas corretivas.

Em relação ao segundo objetivo específico da pesquisa, que buscou identificar e mapear as práticas de gestão voltadas à proteção de dados, implementadas pela organização, verificou-se que a instituição precisou implementar novos protocolos, realizar mudanças nos acessos disponíveis no sistema e rede interna, além de adequar um novo espaço físico para guardar arquivos, como documentos, contratos, laudos e exames clínicos. Nesse aspecto, diante das ações realizadas, a instituição, atualmente, possui práticas de gestão de proteção de dados, suficientes e adequadas em conformidade com as normas previstas na legislação.

Assim, respondendo ao terceiro objetivo específico da pesquisa, que buscou analisar a adoção de práticas de gestão e proteção de dados, que garantam o cumprimento dos requisitos

mínimos exigidos pela lei e que estão de acordo com o sistema implementado, verificou-se que apenas a instituição precisou modificar alguns processos. Constatou-se que no âmbito jurídico, precisou-se incluir as cláusulas de proteção de dados, deixando claro aos titulares de dados, as finalidades do tratamento para as quais são tratados. Da mesma forma, aplicaram-se mudanças na infraestrutura e tecnologia, como o descarte correto e protocolado dos equipamentos, testes regulares da funcionalidade do sistema. Estas evidências revelam que não houve apenas a adoção de uma única ação em um determinado departamento da organização, mas sim, uma completa revisão nos processos internos para proporcionar melhorias tanto na parte da legislação, quanto no próprio desempenho organizacional.

Por fim, como ponto de melhoria e sugestões para a instituição, a organização deve elencar os responsáveis pelas ações, tendo uma supervisão das atividades, para que não ocorra nenhum erro de processo interno, ocasionando alguma interferência no tratamento de dados, deixando vulnerável o acesso às informações, descumprindo os direitos fundamentais como a liberdade e a privacidade e até mesmo sobrecarregando algum colaborador. Além disso, sugere-se realizar semestralmente um encontro com todos os colaboradores, reafirmando a adoção de práticas de gestão e proteção de dados, para que todos tenham consciência da importância atribuída à proteção dos dados e para que as práticas sejam revistas, caso seja necessário, também deverão ser atualizadas ou até mesmo, que sejam criadas novas práticas.

Nessa perspectiva, o Regimento Interno do comitê, por si só traz ações que devem se tornar rotina, como mencionado anteriormente, repassar as informações e buscar a conscientização das partes interessadas, de todos os setores da organização em relação à proteção de dados pessoais e gerar engajamento. Em síntese, manter todos os setores cientes dos indicadores e *status* do programa de gestão de proteção de dados pessoais e principais ações em andamento.

Nessa linha, também contribui criar estratégias preventivas através dos riscos avaliados, com a infraestrutura e os processos que formam a base do sistema de controle interno. Assim dizendo, ter um levantamento e formalização de falhas, nos processos para que se obtenha relatórios quantitativos e qualitativos das causas e frequências destas falhas, a gravidade e os efeitos destas ocorrências, bem como elas podem ser detectadas. Do mesmo modo, também devem se atentar à estrutura firmada pela entidade, onde haja uma definição do controle do ambiente com padrões, políticas, mecanismos e normas internas são exemplos de atividades de controle, que são as manifestações das estratégias de gerenciamento de riscos da organização. Visando identificar, prevenir e/ou monitorar riscos, as atividades de controle devem ser

incorporadas a todo e qualquer setor da instituição, visto que todos devem seguir os preceitos da LGPD.

A comunicação sustenta todo o sistema de controle, seja por meio de relatórios ou pelo compartilhamento de ações, dessa forma, a instituição necessita realizar medições, avaliações e auditorias contínuas, que por sua vez, auxiliarão na avaliação do desempenho nesta área. Ter um controle do risco é um processo interativo e, para melhorar continuamente os controles, a organização deve avaliar a eficácia dos mesmos e aprender com os seus próprios esforços.

5.2 RECOMENDAÇÕES A ESTUDOS FUTUROS

Como oportunidades de pesquisa para realização de estudos futuros, sugere-se a aplicação deste estudo em outros segmentos do mercado, bem como a implementação de sistemas e/ou treinamentos de adequação a LGPD. Devido ao crescente enfoque sobre a temática de proteção de dados, há amplas possibilidades da aplicação do estudo em diferentes organizações (considerando seus diferentes portes e segmentos de atuação), de modo a se avaliar os processos e ações de cada organização a manter os dados protegidos e os impactos do não cumprimento da Lei nº 13.709/2018.

Do mesmo modo, indica-se a avaliação das práticas de gestão e proteção de dados, em forma de pesquisas qualitativas, que busquem evidenciar subsídios não percebidos mediante o estudo de caso, aprofundando tais observações. Adicionalmente, este estudo investigou os processos e ações de adequação de uma única empresa, que atua no segmento que lida diretamente com dados sensíveis. A aplicação de multas pela ANPD, está trazendo novos serviços e produtos ao mercado, afim de tornar a adequação a LGPD mais acessível, além dos impactos do não cumprimento da norma, dessa forma, tais questões constituem-se oportunidades para a realização de novos estudos.

REFERÊNCIAS

ALMEIDA, M. C. **Auditoria**: um curso moderno e completo. 8. ed. São Paulo: Atlas, 2012.

ALMEIDA, M. C. **Auditoria**: um curso moderno e completo: textos, exemplos e exercícios resolvidos. 7. ed. São Paulo: Atlas, 2010. 517 p.

ALVES, C. V. O. C. **A relação entre Governança Corporativa, Cultura Organizacional e Competência em Informação para a construção de conhecimento em organizações familiares**. 2023. 236 f. Dissertação (Mestrado em Mídia e Tecnologia) - Universidade Estadual Paulista Júlio de Mesquita Filho, Bauru, 2023.

BARRETO JUNIOR, I. F.; FAUSTINO, A. Aplicativos de serviços para saúde e proteção dos dados pessoais de usuários. **Revista Jurídica**, Curitiba, v. 1, n. 54, p. 292-316, 2019.

BOENTE, A.; BRAGA, G. P. **Metodologia científica contemporânea**: para universitários e pesquisadores. Rio de Janeiro: Brasport, 2004.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 abr. 2023.

BRASIL. **Lei nº 13.787, de 27 de dezembro de 2018**. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm. Acesso em: 05 jun. 2023.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 05 jun. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília: ANPD, 2022a. Disponível em: . Acesso em: 26 abr. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. Autoridade Nacional de Proteção de Dados. Coordenação-Geral de Fiscalização. **Processo Administrativo Sancionador nº 00261.000489/2022-62**. Brasília: MJSP, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/2022-62-dou-imprensa-nacional.pdf. Acesso em: 23 jul. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Planejamento Estratégico ANPD 2021-2023**. Brasília, 04 jul. 2022b. https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/planejamento-estrategico-anpd-2021-2023. Acesso em: 22 jul. 2023.

BRITO, M. F. B. **A importância do sistema integrado de gestão empresarial para as organizações**. 2017. 61 f. Dissertação (Mestrado em Gestão) - Universidade de Coimbra, Coimbra, 2017.

CELIDONIO, T.; NEVES, P. S.; DONÁ, C. M. Metodologia para mapeamento dos requisitos listados na LGPD (Lei Geral de Proteção de Dados do Brasil número 13.709/18) e sua adequação perante a lei em uma instituição financeira - Um estudo de caso. **Brazilian Journal of Business**, São José dos Pinhais, v. 2, n. 4, p. 3626-3648, 2020.

CERVO, A. L.; BERVIAN, P. A.; DA SILVA, R. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

COCURULLO, A. **Gestão de riscos corporativos**: riscos alinhados com algumas ferramentas de gestão: um estudo de caso no setor de celulose e papel. 3. ed. São Paulo: 2004.

CONSELHO DA UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de outubro de 1995**. Relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Luxemburgo: Parlamento Europeu, 1995. Disponível em: https://www.conjur.com.br/dl/di/diretiva-europeia.pdf. Acesso em: 15 jul. 2023.

CONSELHO FEDERAL DE CONTABILIDADE. **NBC TA 315 (R1)**: Identificação e avaliação dos riscos de distorção relevante por meio do entendimento da entidade e do seu ambiente. Brasília: CFC, 2016. Disponível em: https://edisciplinas.usp.br/pluginfile.php/3315387/mod_resource/content/1/NBCTA315%28R1%29.pdf. Acesso em: 30 abr. 2023.

CONSELHO FEDERAL DE MEDICINA. **Código de Ética Médica**. Brasília: CFM, 2019. Disponível em: https://portal.cfm.org.br/images/PDF/cem2019.pdf. Acesso em: 22 abr. 2023.

CONSELHO FEDERAL DE MEDICINA. **Resolução CFM nº 1.638/2002**. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Brasília: CFM, 2002. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2002/1638. Acesso em: 11 jul. 2023.

CONSELHO FEDERAL DE MEDICINA. **LGPD**: a Lei Geral de Proteção de Dados Pessoas e a atuação do profissional da medicina. Brasília: CFM, 2022. Disponível em: https://www.flip3d.com.br/pub/cfm/index9/?numero=38&edicao=5305#page/22. Acesso em: 11 jul. 2023.

COSTA, W. C. **Sistema de controle interno**: estudo em uma empresa pública de concessão de crédito. 2019. 57 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Contábeis) - Universidade Federal da Paraíba, João Pessoa, 2019.

CREPALDI, S. A. **Auditoria contábil**: teoria e prática. 8. ed. São Paulo: Atlas 2013.

CROTTY, M. **The foundations of social research**: meaning and perspective in the research process. London: Sage, 1998.

CRUZ, U. L.; PASSAROTO, M.; THOMAZ JUNIOR, N. O impacto da Lei Geral de Proteção de Dados Pessoais (LGPD) nos escritórios de contabilidade. **ConTexto - Contabilidade em Texto**, Porto Alegre, v. 21, n. 49, p. 30-39, 2021.

CUSTÓDIO, J. J. *et al*. Análise do controle interno no setor de almoxarifado de uma empresa de transporte à luz da metodologia COSO. **Revista de Administração, Contabilidade e Sustentabilidade**, Campina Grande, v. 9, n. 2, p. 1-10, 2019.

DONEDA, D. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DPONET. 2023. Disponível em: https://app.dponet.com.br/. Acesso em: 16 jul. 2023.

DUARTE, E. P.; DOMENICONI JUNIOR, R.; EBOLI, D. LGPD: medidas essenciais de segurança da informação. In: CONGRESSO DE SEGURANÇA DA INFORMAÇÃO, 2., 2022, Americana. **Anais** [...]. Americana: Fatec Seg, 2022.

FACHIN, O. **Fundamentos de metodologia**. 4. ed. São Paulo: Saraiva, 2003.

FIGUEIREDO, J. F. Controle interno nas empresas | Como manter uma gestão de qualidade. **Financial Contabilidade**, Vitória, 10 ago. 2018. Disponível em: https://www.financialnet.com.br/controle-interno-nas-empresas-como-manter-uma-gestao-de-qualidade/. Acesso em: 22 jul. 2023.

FLORIANO, J. C.; LOZECKYI, J. A importância dos instrumentos de controle interno para gestão empresarial. **UNICENTRO - Revista Eletrônica Lato Sensu**, Guarapuava, n. 5, p. 1-8, 2008.

FRANCO, H.; MARRA, E. **Auditoria contábil**. 4. ed. São Paulo: Atlas, 2001.

FUNDAÇÃO BRADESCO. Escola Virtual. **Lei Geral de Proteção de Dados (LGPD)**. 2020. Disponível em: https://www.ev.org.br/cursos/lei-geral-de-protecao-de-dados-lgpd. Acesso em: 10 jul. 2023.

GARCIA, O. P. G.; KINZLER, L.; ROJO, C. A. Análise dos sistemas de controle interno em empresas de pequeno porte. **Revista INTERFACE-UFRN/CCSA**, Natal, v. 11, n. 2, p. 133-153, 2014.

IMONIANA, J. O.; NOHARA, J. J. Cognição da estrutura de controle interno: uma pesquisa exploratória. **Revista de Administração e Contabilidade da Unisinos**, São Leopoldo, v. 2, n. 1, p. 37-46, 2005.

INSTITUTO DOS AUDITORES INTERNOS DO BRASIL. **Normas brasileiras para o exercício da auditoria interna**. 2. ed. São Paulo: Audibra, 1992.

JESUS, V. A. P.; BARBOSA, F. K. Sistema de Gestão Empresarial ERP. **UNILUS Ensino e Pesquisa**, São Paulo, v. 13, n. 30, p. 294, 2016.

LOPES, E. C.; VALENTIM, M. L. P.; FADEL, B. Efeitos da cultura organizacional no desenvolvimento dos modelos de governança corporativa. **Revista FAMECOS**, Porto Alegre, v. 21, n. 1, p. 268-286, jan./abr. 2014.

LOUREIRO, D. P. B. **A importância dos controles internos nas organizações**. 2010. 22 f. Trabalho de Conclusão de Curso (Bacharel em Ciências Contábeis) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010.

LÜDKE, M.; ANDRÉ, M. E. D. A. **Pesquisa em educação**: abordagens qualitativas. São Paulo: EPU, 1986.

MARION, J. C.; DIAS, R.; TRALDI, M. C. **Monografia para os cursos de administração, contabilidade e economia**. São Paulo: Atlas, 2002.

MARQUES, L. N. **O mapeamento do modelo data management maturity (dmm) à Lei Geral de Proteção de Dados (LGPD)**. 2020. 77 f. Trabalho de Conclusão de Curso (Bacharelado em Engenharia da Computação) - Pontifícia Universidade Católica de Goiás, Goiás, Goiânia, 2020.

MAXIMINIANO, A. C. A. **Introdução à administração**. 5. ed. São Paulo: Atlas, 2000.

MILES, M. B.; HUBERMANN, A. M. **Qualitative data analisys**: an expanded soucerbook. 2. ed. Califórnia: Sage, 1994.

MINAYO, M. C. S. (Org.). **O desafio do conhecimento**: pesquisa qualitativa em saúde. 14. ed. Rio de Janeiro: Hucitec, 2014. 408 p.

MONTEIRO, R. P. Análise do sistema de controle interno no Brasil: objetivos, importância e barreiras para sua implantação. **Revista Contemporânea de Contabilidade**, Florianópolis, v. 12, n. 25, p. 159-188, 2015.

MULHOLLAND, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, 2018.

OLIVEIRA, A.; CAMPOS, B.; MACEDO, A. LGPD - Proposta de implementação de melhorias em um escritório de contabilidade na cidade de Macapá/AP: estudo de caso. **Concilium**, [*S. l.*], v. 22, n. 6, p. 39-53, 2022.

OLIVEIRA, G. S. *et al*. Grupo focal: uma técnica de coleta de dados numa investigação qualitativa?. **Cadernos da FUCAMP**, Monte Carmelo, v. 19, n. 41, p. 1-13, 2020.

PINHEIRO, P. P. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018. 2. ed. São Paulo: Saraiva Educação, 2020.

SAMPIERI, R. H.; LUCIO, P. B. **Metodologia de pesquisa**. Porto Alegre: Penso, 2013.

SANCOVSCHI, M. *et al*. Mudanças no sistema de controle interno de uma empresa brasileira do setor elétrico. **Pensar Contábil**, Rio de Janeiro, v. 21, n. 76, p. 4-15, 2019.

SCHERER FILHO, J. L. **Tratamento de Dados em Sistemas de Informações Contábeis a partir da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)**: um estudo de multicaso. 2020. 25 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Contábeis) - Universidade de Caxias do Sul, Caxias do Sul, 2020.

SELLTIZ, C.; WRIGHTSMAN, L. S.; COOK, S. W. **Métodos de pesquisa das relações sociais**. São Paulo: Herder, 1965.

SILVA, J. M. **Controle interno transparência segurança**. 2017. 13 f. Trabalho de Conclusão de Curso (Especialização em Contabilidade Pública) - Universidade do Sul de Santa Catarina, Tubarão, 2017.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 4. ed. Florianópolis: UFSC, 2005. Disponível em: http://tccbiblio.paginas.ufsc.br/files/2010/09/024_Metodologia_de_pesquisa_e_elaboracao_de_teses_e_dissertacoes1.pdf. Acesso em: 30 jun. 2023.

SILVA, A. F.; VICENTE, C. Gestão por propósito no setor público: contribuições do modelo Disney de excelência. *In*: ROCHA, C. G.; DUARTE, M. R. B. (Orgs.). **Administração pública na prática**. Florianópolis: CRA-SC, 2019. p. 65-80.

SILVA, A. H. C.; ABREU, C. L.; COUTO, D. C. F. Evolução do controle interno no setor público: um estudo dos novos normativos emitidos entre 2003-2016. **Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ**, Rio de Janeiro, v. 22, n. 2, p. 20-38, 2017.

SILVA, L. V. *et al*. **Metodologia de pesquisa em administração**: uma abordagem prática. São Leopoldo: Unisinos, 2012.

TEVES, D. M. **A proteção de dados pessoais**: o novo paradigma jurídico. 2019. 170 f. Dissertação (Mestrado em Ciências Econômicas e Empresariais) - Universidade dos Açores, Ponta Delgada, 2019.

UNIVERSIDADE FEDERAL DE SÃO CARLOS. **Metodologia de gestão de riscos**. São Carlos: UFSCar, 2022. Disponível em: https://www.dirc.ufscar.br/riscos/metodologia-de-gestao-de-riscos-ufscar.pdf. Acesso em: 22 abr. 2023.

YIN, R. K. **Case study research**: design and methods. Thousand Oaks: Sage Publications, 2003.

APÊNDICE A - ROTEIRO DA ENTREVISTA COM A TI

Quando é necessário que informações dos serviços de aplicação transitem em redes públicas, são tomadas medidas para protegê-las de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas?

As informações dos registros de eventos (log) e seus recursos são protegidos contra acessos não autorizados e para que NINGUÉM consiga editá-los nem adulterá-los?

As atividades dos administradores e operadores do sistema são registradas, analisadas criticamente a intervalos regulares e protegidas para que NINGUÉM consiga editá-las nem adulterá-las?

É feito um controle de permissão, para que apenas pessoas autorizadas e treinadas possam alterar os softwares presentes nos dispositivos, tanto para atualizações quanto para a instalação de novas aplicações?

Em intervalos regulares, é feita uma varredura para coletar informações sobre vulnerabilidades técnicas dos sistemas utilizados? A exposição da organização a estas vulnerabilidades são avaliadas, em tempo hábil, para se tomar as medidas apropriadas para lidar com os riscos associados?

São realizados testes das funcionalidades de segurança dos sistemas, desenvolvidos internamente ou terceirizados, para assegurar que a aplicação trabalha conforme o esperado?

São tomadas medidas de segurança para a utilização de equipamentos, próprios ou pessoais (em função do trabalho), fora das dependências da organização? Para isso, é levado em conta os diferentes riscos de segurança como danos, furto e espionagem?

A instituição tem critérios, regras, que devem ser considerados antes de os colaboradores instalarem softwares?

A empresa tem controles de detecção, prevenção e recuperação para proteger contra vírus e outros softwares nocivos, e também um adequado programa de conscientização dos colaboradores usuários?

APÊNDICE B - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

UNIVERSIDADE FEDERAL DE SANTA MARIA - UFSM
CENTRO DE CIÊNCIAS SOCIAIS E HUMANAS
CURSO DE CIÊNCIAS CONTÁBEIS

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE)

Graduanda: Bruna Altevogt Libino.
Professora orientadora: Msc. Ana Paula Fraga.

Eu, Bruna Altevogt Libino, responsável pelo trabalho CONTROLE INTERNO COMO UMA FERRAMENTA PARA ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS (LGPD): UM ESTUDO DE CASO, o convido a participar como voluntário deste estudo. Por meio desta pesquisa, pretende-se investigar se as práticas de gestão e proteção de dados em uso pela organização, atualmente, são suficientes e adequadas para atenderem os requisitos mínimos exigidos por lei.

Acreditamos que ela seja importante pois o tema urge, configurando-se uma fonte rica e desafiadora para estudar e pesquisar. Para o desenvolvimento deste estudo será feito: um diagnóstico a respeito das ações e práticas de gestão e proteção de dados, através de um estudo de caso com a elaboração de um questionário com questões fechadas e abertas de caráter subjetivo com seus gestores.

Sua participação constará por meio de um questionário que será enviado por e-mail e *whatsapp*. Sendo sua participação voluntária, você não receberá benefícios financeiros, nem assumirá riscos e/ou danos.

Você tem garantida a possibilidade de não aceitar participar ou de retirar sua permissão a qualquer momento, sem nenhum tipo de prejuízo pela sua decisão.

Durante todo o período da pesquisa você terá a possibilidade de tirar qualquer dúvida ou pedir qualquer outro esclarecimento. Para isso, entre em contato com algum dos pesquisadores ou com o Comitê de Ética em Pesquisa com Seres Humanos.

As informações desta pesquisa serão confidenciais e poderão ser divulgadas em eventos ou publicações, sem a identificação dos voluntários, a não ser entre os responsáveis pelo estudo, sendo assegurado o sigilo sobre sua participação.

Agradeço a sua participação!

Graduanda: Bruna Altevogt Libino (brunaaltevogt@icloud.com).

AUTORIZAÇÃO

Após a leitura deste documento, estou suficientemente informado, ficando claro que minha participação é voluntária e que posso retirar este consentimento a qualquer momento sem penalidades. Estou ciente também dos objetivos da pesquisa, dos procedimentos aos quais serei submetido, dos possíveis danos ou riscos deles provenientes e da garantia de confidencialidade.

Diante do exposto e de espontânea vontade, expresso abaixo minha concordância em participar deste estudo.

Você aceita participar da pesquisa?

( ) Sim

( ) Não

Observação: Caso o respondente marque a opção “Não”, o questionário será desconsiderado.