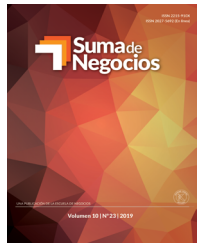
SUMA DE NEGOCIOS, 10(23), 89-99, Julio-Diciembre 2019, ISSN 2215-910X Doi: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2

SUMA DE NEGOCIOS



Artigo de pesquisa

A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos

Fabrício Pelloso Piurcosky[1], *Marcelo Aparecido Costa*[2], *Rodrigo Franklin Frogeri*[3] y *Cristina Lelis Leal Calegario*[4]

[1] *Doutorando em Administração pela Universidade Federal de Lavras - UFLA. Professor no Centro Universitário do Sul de Minas – UNIS-MG, Minas Gerais, Brasil. Correio eletrônico: fabricio@unis.edu.br. ORCID: 0000-0001-5458-5129.*

[2] *Especialista em Cibersegurança e Perícia Forense Computacional pelo Centro Universitário do Sul de Minas - UNISMG. Correio eletrônico: marcelo_ac16@hotmail.com. ORCID: 0000-0002-4941-6029.*

[3] *Doutorando em Sistemas de Informação e Gestão do Conhecimento pela Universidade FUMEC. Professor no Centro Universitário do Sul de Minas – UNIS-MG, Minas Gerais, Brasil. Correio eletrônico: rodrigo.frogeri@professor.unis.edu.br. ORCID: 0000-0002-7545-7529.*

[4] *Doutora em Agricultura e Economia Aplicada. Professora na Universidade Federal de Lavras – UFLA. Minas Gerais - Lavras, Brasil. Correio eletrônico: ccalegario@ufla.br. ORCID: 0000-0003-2579-8744.*

INFORMAÇÃO SOBRE O ARTIGO

Recebido a 14 de março de 2019
Aceito a 3 de junho de 2019
Online a 17 de junho de 2019

Códigos JEL:
M1, M15, M3 y M38

Palavras-chave
Privacidade,
Segurança da Informação,
NBR ISO/IEC 27001,
NBR ISO/IEC 27002,
Gestão de TI

RESUMO

Este estudo tem como objetivo descrever e compreender a realidade de organizações brasileiras quanto à adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). Tal abordagem se justifica mediante regulamentações estabelecidas pelo Estado brasileiro para a manipulação, tratamento e armazenamento de dados pessoais por organizações. Nesse sentido, discute-se a capacidade das organizações de atender aos marcos regulatórios estabelecidos pela LGPD (Lei no 13.709/2018). Para alcançar o intento proposto, o estudo está fundamentado na NBR ISO/IEC 27001, NBR ISO/IEC 27002 e na Lei no 13.709/2018. Quanto ao objetivo, a pesquisa é descritiva com abordagem qualitativa e realizada por meio de estudo de casos múltiplos. Os dados foram coletados via entrevistas semiestruturadas com sete profissionais responsáveis pela coleta, manipulação ou armazenamento de dados de empresas de diferentes portes. O estudo foi realizado dois meses (out/2018) após sanção da LGPD pela Presidência da República do Brasil, caracterizando-se como do tipo corte transversal. O estudo demonstrou que as empresas não estão preparadas para atender aos marcos regulatórios estabelecidos pela LGPD, urgindo por consideráveis mudanças técnicas e de gestão nas áreas de tecnologia da informação e segurança da informação

The General Law for Protecting Personal Data in Brazilian Enterprises: An Analysis of Multiple Cases

Keywords:
Privacy,
Information security,
NBR ISO/IEC 27001,
NBR ISO/IEC 27002,
IT Management.

ABSTRACT

This study aims to describe and understand the reality of Brazilian organizations in terms of compliance with the General Law on the Protection of Personal Data (LGPD). Such an approach is justified by the regulations established by the Brazilian State for the manipulation, processing and storage of personal data by organizations. In this sense, the capacity of organizations to meet the regulatory frameworks established by the LGPD (Law No. 13.709/2018) is discussed. In order to achieve the proposed intent, the study is based on NBR ISO/IEC 27001, NBR ISO/IEC 27002 and Law No. 13.709/2018. As for the

objective, the research is descriptive with a qualitative approach and conducted through multiple case studies. The data were collected via semi-structured interviews with seven professionals responsible for the collection, manipulation or storage of data from companies of different sizes. The study was conducted two months (Oct/2018) after the sanction of the LGPD by the presidency of the Brazilian Republic, characterized as a cross-sectional type. The study showed that the companies are not prepared to meet the regulatory frameworks established by the LGPD, requiring considerable technical and management changes in the areas of Information Technology and Information Security.

Introdução

Informações pessoais estão cada vez mais vulneráveis na atual economia digital, especialmente nas redes sociais e nos cadastros de organizações que atuam virtualmente. Limitar o acesso aos dados pessoais por parte de terceiros depende muitas vezes do usuário, mas tem considerável influência da organização proprietária da rede social para manter a segurança do titular da informação. Entre os anos de 2014 a 2018, a empresa Cambridge Analytica obteve dados de perfis de usuários da rede social Facebook nos Estados Unidos e no Reino Unido, com o objetivo de influenciar eleitores em campanhas políticas. As informações obtidas foram coletadas por meio de testes de personalidade na própria página da rede social, sendo possível traçar o perfil das pessoas por meio de páginas curtidas e postagens realizadas. Mediante análise do comportamento do usuário na rede social, seria possível direcionar propagandas eleitorais de acordo com o perfil da pessoa.

O caso do Facebook gerou uma comoção mundial quanto às responsabilidades das organizações no tratamento e disponibilização de dados pessoais. Com o objetivo de melhorar a segurança da informação para os titulares dos dados foi criado, em 2016, pela União Europeia (UE), o Regulamento Geral de Proteção de Dados (RGPD), sendo aplicada aos países que fazem parte da UE no ano de 2018.

O objetivo da RGPD é fornecer mais segurança para as pessoas em relação ao tratamento dos seus dados pessoais, estabelecendo um conjunto de princípios. A RGPD deixa claro que os titulares dos dados têm total direito sobre suas informações, dando a eles mais controle e, às empresas, responsabilidades. Segundo a RGPD, proteger os direitos fundamentais como a liberdade e a privacidade é um grande passo para a proteção de dados pessoais. Seguindo os princípios da RGPD, foi criada no Brasil a Lei nº 13.709 de 14 de agosto de 2018 ou Lei Geral de Proteção de Dados Pessoais (LGPD), que busca controlar a forma com que as empresas coletam e usam os dados pessoais que têm em seu poder. A lei objetiva se adequar à era digital, em que os dados são trafegados e comercializados sem o devido consentimento dos titulares das informações, cerceando os princípios da liberdade e privacidade.

Segundo estabelecido pelo Estado brasileiro, a Lei nº 13.709 entrará em vigor a partir de fevereiro de 2020, obrigando as organizações a se adaptarem às regulamentações propostas até a data definida. Nesse sentido, este estudo tem como objetivo descrever e compreender a realidade de organizações brasileiras quanto a adequação à LGPD. O trabalho foi norteado pela seguinte pergunta de pesquisa: Como as organizações do sul de Minas Gerais estão se adequando à LGPD? Quanto ao objetivo, o estudo tem caráter descritivo, por objetivar a descrição da realidade das empresas estudadas quanto a adequação à LGPD. Quanto à abordagem metodológica, o estudo é qualitativo com um raciocínio científico indutivo. Os dados foram coletados por meio da técnica de estudo de casos múltiplos e entrevistas semiestruturadas a sete profissionais responsáveis pela coleta, manipulação ou armazenamento de dados pessoais.

Referencial teórico

O referencial teórico do estudo está estruturado em três seções. A primeira seção discorre sobre princípios de Segurança da Informação, seguido pelo Regulamento Geral de Proteção de Dados da UE e, por fim, é apresentada a LGPD, que trata sobre a proteção de dados pessoais no Brasil.

Princípios de Segurança da Informação

Lyra (2015) define *informação* como um conjunto de dados que são tratados e organizados para representar um significado ou sentido em um determinado contexto. A informação dotada de significado passa a ter valor para organizações e pessoas. Nesse sentido, os princípios da Segurança da Informação (SI) objetivam assegurar a proteção das informações contra acessos não autorizados (confidencialidade), manter a disponibilidade, ser íntegra e autêntica em seus devidos fins (integridade). Lyra (2015) complementa que o bem mais precioso das empresas são seus bancos de dados, local de armazenamento dos dados em formato bruto e fonte das informações da empresa. Ziraba e Okolo (2018) consideram a informação como a base da vantagem competitiva na atual economia; contudo, a posse de informações de terceiros pode representar grande ameaça para as organizações e para a privacidade de clientes e funcionários. Os autores argumentam que a formulação de políticas associadas às tecnologias da informação (TI) é uma das melhores maneiras de garantir padrões e procedimentos de TI eficazes, que

protegem os recursos de TI organizacionais e controlam o compartilhamento de informações (Ziraba & Okolo, 2018).

Nesse contexto, a SI tem considerável importância para negócios do setor público ou privado. As organizações aplicam práticas de SI para reduzir os riscos associados ao tráfego de informações em formato digital. Para que essas práticas alcancem os seus objetivos é necessário que um conjunto de controles sejam implementados, desde políticas internas e externas à organização até a aplicação de funcionalidades em *softwares* e *hardwares*. De acordo com a Associação Brasileira de Normas Técnicas (ABNT) em referência à Norma Brasileira (NBR) ISO/IEC 27002, os controles em SI, quando executados de maneira correta, garantirão que os objetivos dos negócios da organização e a segurança da informação sejam atendidos (NBR ISO/IEC 27002, 2013).

Para Ghafir, Saleem, Hammoudeh, Faour, Prenosil, Jaf e Baker (2018), o fator humano é o principal desafio para a implantação de boas práticas de segurança da informação na organização. Observa-se a necessidade de procedimentos para o tratamento e o armazenamento das informação com o objetivo de proteção contra a divulgação e o acesso não autorizados (NBR ISO/IEC 27002, 2013).

Confidencialidade, integridade e disponibilidade

A segurança da informação é fundamentada pelos conceitos de *confidencialidade*, *integridade* e *disponibilidade* da informação (NBR ISO/IEC 27002, 2013). Beal (2005) define *confidencialidade* como a "garantia de que o acesso à informação é restrito aos seus usuários legítimos" (p. 10). O sigilo atribuído à informação deve ser garantido, sendo possível classificá-lo de acordo com o valor da informação para a organização ou sob aspectos normativos (Sêmola, 2014).

A partir do momento que os dados são inseridos no banco de dados da organização, inicia-se o processo de confidencialidade. A NBR ISO/IEC 27002 (2013) recomenda que "acordos de confidencialidade e de não divulgação considerem os requisitos para proteger as informações confidenciais, usando termos de que são obrigados do ponto de vista legal" (NBR ISO/IEC 27002, 2013, p. 12).

Sêmola (2014) define uma *informação íntegra* como aquela que está da mesma forma ou condição de quando foi disponibilizada pelo proprietário. É responsabilidade da organização protegê-la contra alterações indevidas, intencionais ou acidentais. O princípio da *integridade* se aplica a esta situação de forma a garantir a não adulteração da informação armazenada por um terceiro.

O princípio da *disponibilidade* deve garantir que a informação e recursos associados estejam disponíveis de forma imediata, independente da finalidade (Beal, 2005). A indisponibilidade da informação quando necessária pode inviabilizar a sua utilidade (Lyra, 2015).

Para Nascimento, Frogeri e Prado (2018):

> A manutenção das propriedades da informação, tais como: disponibilidade, integridade, confidencialidade e autenticidade está intimamente relacionada ao conceito de SI e se constitui em objetivo a ser atingido para a preservação da informação face aos diversos tipos de ameaças que se apresentam. (p. 8)

A autenticidade na identificação do usuário de um sistema computacional deve ser pessoal, única e associada a três princípios: algo que o usuário sabe, algo que o usuário é e algo que o usuário tem. A utilização de pelo menos dois desses princípios podem garantir um nível de autenticidade maior, prevenindo falhas em SI (Roratto & Dias, 2014).

Normas e política de segurança da informação

A política de segurança da informação tem como objetivo orientar e coordenar as ações na organização de acordo com suas regras de negócios, leis e regulamentações (NBR ISO/IEC 27002, 2013). Uma política de SI pode ser vista como um guia de procedimentos para proteger os dados que a organização tem em seu poder e a forma de sua utilização. Uma boa política de SI necessita de uma boa gestão e envolvimento da alta administração da organização, de forma que haja conscientização e comunicação da política para todos os usuários em todos os níveis hierárquicos (NBR ISO/IEC 27002, 2013).

A NBR ISO/IEC 27002 (2013) determina que a organização deve "assegurar a conscientização dos usuários e responsabilidades pela segurança da informação" (p. 19). No âmbito da gestão de mudanças em práticas organizacionais, a NBR ISO/IEC 27001 (2006) sugere que a alta administração da organização deve se comprometer na criação de planos de contingências para assegurar que todo pessoal responsável direto pelas mudanças tenham competência necessária para executar as tarefas estabelecidas (NBR ISO/IEC 27001, 2006).

Sob um aspecto técnico da SI, Ferreira e Araújo (2008) asseguram que a segurança em tecnologia pode ser entendida por dois princípios: segurança lógica e segurança física, em que ambas têm um papel importante para garantir a proteção dos ativos da organização. A segurança física tem como principal objetivo impedir o acesso não autorizado em áreas críticas da organização (NBR ISO/IEC 27002, 2013). Carneiro (2002) refere-se à segurança lógica como a segurança no modo como os softwares são usados, configurados, desenvolvidos e executados. A segurança lógica está tanto associada a software quanto a ativos de rede e suas configurações lógicas (NBR ISO/IEC 27002, 2013).

A NBR ISO/IEC 27001 (2006), considera que a gestão da segurança da informação deve se preocupar com a minimização de riscos associados a um incidente (NBR ISO/IEC 27001, 2006). Beal (2005) define *incidente* como um "evento com consequências negativas resultante de um ataque bem-sucedido" (p. 15). Pode-se exemplificar incidentes na área de SI, como: dados incorretos armazenados num sistema, inundação que danifica equipamentos em uma central de dados (*datacenter*) ou o pagamento indevido em decorrência de erro na inclusão de dados no sistema financeiro de uma organização, entre outros. Tais incidentes podem não se concretizar caso haja uma gestão eficiente dos riscos para que eles aconteçam (NBR ISO/IEC 27001, 2006). Para Addington e Manrod (2019), o controle deve ser o primeiro passo

para que a organização minimize as chances de incidentes em SI. Organizações com equipes pequenas em TI e processos imaturos podem ter benefícios associados à SI com a automação e controles rigorosos (Addington & Manrod, 2019).

A NBR ISO/IEC 27001 (2006) trata ainda da comunicação de eventos associados a incidentes em SI. Sugere-se que todos os funcionários, fornecedores e terceiros tenham conhecimento dos procedimentos para notificação de eventos que possam gerar impactos à segurança da informação da organização. Nesse sentido, treinamento constante, políticas internas e externas à organização e canais de comunicação são práticas que podem reduzir o impacto de incidentes em SI.

Regulamento Geral de Proteção de Dados (RGPD)

O regulamento da UE 2016/679 que trata da proteção de dados pessoais considera que ter direito sobre os próprios dados e garantia de proteção aos mesmos é um princípio fundamental na atual economia digital, pois "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (União Europeia, 2016, p. 3). Nesse sentido, a UE criou o Regulamento Geral de Proteção de Dados (RGPD) para proteger a manipulação de dados pessoais por empresas de diversos segmentos de mercado (União Europeia, 2016). Nos países da UE, o regulamento está implementado desde o dia 25 de maio de 2018.

O regulamento da UE se fundamentou no princípio do consentimento. Para que o consentimento seja válido, deverá existir uma declaração escrita, ou em formato eletrônico, ou uma declaração oral registrada pelo titular do dado. A empresa deverá ter um responsável pelo tratamento dos dados pessoais, que ficará responsável por se adequar ao regulamento e responder por eventuais incidentes em SI às autoridades de controle[1] (União Europeia, 2016). Lovell e Foy (2018), argumentam que a RGPD exige que os dados pessoais sejam tratados de forma legal, equitativa e transparente. O recolhimento de dados pessoais por parte de organizações deve ser para fins específicos, explícitos e legítimos e não devem ser utilizados de forma incompatível com essa finalidade. O tratamento de dados pessoais deve ser adequado, pertinente, não deve ser armazenado por mais tempo do que o necessário e deve ser mantido em segurança (Lovell & Foy, 2018).

O RGPD estabelece que alguns dados são considerados sensíveis, especialmente aqueles que tratam sobre a origem racial ou étnica, opiniões políticas, religiosas, filosóficas, dados genéticos, informações associadas à saúde ou orientação sexual (União Europeia, 2016). A portabilidade também está disposta no regulamento, prevendo a transferência dos dados de uma empresa para a outra com o consentimento do titular dos dados. Acredita-se que esse procedimento pode facilitar tanto para a nova organização em obter os dados quanto para o titular em não precisar se deslocar até a nova empresa.

[1] Autoridade pública independente criada por um estado membro da UE, responsável por controlar e verificar o cumprimento do regulamento.

O RGPD proíbe a troca de informações entre organizações sem o consentimento do titular dos dados (União Europeia, 2016). Quaisquer danos com os dados pessoais dos titulares ficam a cargo do responsável pelo tratamento dos dados. Em caso de os titulares dos dados identificarem que seus direitos foram violados, as autoridades de controle serão acionadas e, se confirmada a violação, esse organismo poderá solicitar que a empresa indenize o titular (União Europeia, 2016).

Em complemento ao princípio do consentimento, o RGPD busca exigir das organizações o respeito à privacidade durante a concepção de sistemas computacionais. O objetivo é reduzir riscos relativos ao tratamento dos dados. O RGPD considera o princípio do risco como valioso para assegurar o direito e a liberdade dos titulares de dados, adotando uma abordagem orientada pelo risco na proteção dos dados pessoais (Lambrinoudakis, 2018). Sob uma outra perspectiva associada à privacidade de informações, Borden, Mooney, Taylor e Sharkey (2019) discutem que o RGPD "sufoca" a prática de compartilhamento de informações em tempo real sobre ameaças de segurança da informação, podendo aumentar as chances de que ataques sejam bem-sucedidos. Um compartilhamento eficaz de informações entre organizações do mesmo ramo de negócios pode minimizar riscos, uma vez que um agente de ameaças ativo poderá ter apenas uma oportunidade de atacar um sistema com sucesso (Borden et al., 2019).

O RGPD não traz somente implicações regulamentares e necessidade por mudanças em processos no tratamento das informações por parte das organizações. Banakar, Shah, Shastri, Wasserman e Chidambaram (2019) discutem os aspectos técnicos que o RGPD impõe aos sistemas computacionais, como: criptografia, monitoramento, *logs* (rastreabilidade dos dados), armazenamento de dados em formatos distintos e controle de deleção. Essas características implicam diretamente nos sistemas de armazenamento de dados e sistemas de informação das organizações, podendo aumentar o seu custo de aquisição, manutenção e gestão (Banakar et al., 2019).

Ziegler, Evequoz e Huamani (2019) complementam os argumentos de Banakar et al. (2019) ao considerarem que a intenção da RGPD não é impedir a exploração de dados pessoais, mas assegurar que essa exploração seja feita de acordo com a aprovação dos titulares dos dados. Contudo, Ziegler et al. (2019) concordam com Banakar et al. (2019) ao observarem que essas práticas possuem um impacto direto nas atividades de negócios e consideráveis efeitos nos Sistemas Gerenciadores de Banco de Dados (SGBDs) das organizações. Nesse sentido, Ziegler et al. (2019) estabelecem cinco efeitos do RGPD nos SGBD, a saber: i) gestão de riscos: deve-se avaliar o risco de exposição às sanções e penalidades relacionadas com o RGPD; ii) titular e controle dos direitos dos dados: os SGBD devem ser projetados com os titulares dos dados no núcleo do modelo, inclusive em termos de transações econômicas; iii) consistência de propósito: o consentimento informado prévio deve ser específico e uma empresa não pode usar os dados coletados além da finalidade anunciada no momento em que o envolvido deu o consentimento; as organizações terão que prever o uso dos dados e preparar

formulações claras; (iv) transferência de dados para terceiros: as organizações deverão, claramente, mapear, gerir, monitorar e controlar a forma como processam e partilham dados; as empresas deverão adaptar os processos internos a essas funções adicionais; (v) transferência transfronteiriça: os SGBD deverão levar em conta a territorialidade do processamento e transferência de dados. Isso exigirá que as sociedades globais separem e segreguem o processamento de dados provenientes de residentes europeus de processos de dados em países que não são reconhecidos como "países adequados".

O regulamento criado pela UE pode ser considerado um marco para a proteção dos dados pessoais, sendo utilizado como base para a adequação das legislações de vários países, inclusive o Brasil. Discute-se a seguir a proposição brasileira para a proteção de dados pessoais.

Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira

Com base no RGPD da União Europeia, foi aprovada no Brasil no dia 14 de agosto de 2018 a Lei nº 13.709, que dispõe:

> Sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (Medida Provisória nº 869, p.1)

A LGPD (Lei nº 13.709) foi fundamentada nos princípios do respeito à privacidade, liberdade de expressão, de informação, de comunicação e de opinião; não violação da intimidade, honra e imagem; livre iniciativa, livre concorrência e defesa do consumidor e, principalmente, os direitos humanos (Lei n. 13.709, 2008). A LGPD não se aplica ao tratamento de dados pessoais realizado por pessoa natural com fins exclusivamente particular e não econômicos; realizados para fins exclusivamente jornalísticos, artísticos ou acadêmicos; segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais; ou provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD (Lei n. 13.709, 2008).

Está previsto na LGPD, o princípio do consentimento. Entende-se por *consentimento* a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (Medida Provisória n° 869, 2019, p. 1). O titular dos dados pessoais tem o direito de obter da organização a relação dos seus dados armazenados. Também pode solicitar correções em dados incompletos ou desatualizados; bloqueio ou eliminação de dados desnecessários ou tratados em desconformidade com a legislação vigente; portabilidade dos dados com a devida aprovação; e a revogação de consentimento (Lei n. 13.709, 2008). As empresas deverão definir responsáveis pelo tratamento dos dados pessoais, sendo essa a pessoa ou grupo de pessoas responsáveis por responder às solicitações de ordem pessoal ou governamental (Lei n. 13.709, 2008).

Os responsáveis pelo tratamento de dados, junto com a empresa, deverão formular novas políticas para se adequarem à Lei, estabelecendo novas condições para a organização em relação ao seu regimento de funcionamento, procedimentos, incluindo termos para reclamação e petições dos titulares dos dados, além de implementações de normas de segurança, padrões técnicos, obrigações específicas para os envolvidos no tratamento de dados, ações educativas para seus empregados e supervisão de riscos do negócio e outros aspectos relacionados ao tratamento de dados pessoais (Lei n. 13.709, 2008).

A lei entra em vigor após decorridos 18 (dezoito) meses de sua publicação oficial em fevereiro de 2020 (Lei n. 13.709, 2008). O não cumprimento da lei coloca as empresas sujeitas a punições administrativas (Lei n. 13.709, 2008). Essas punições vão desde advertência até multa associada ao faturamento da organização. Caso seja advertida, a organização terá um prazo para se adequar. As punições iniciam com multas em valor fixo pré-determinado até multas diárias, relativa a 2% do faturamento da empresa, limitada ao total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração (Lei n. 13.709, 2008).

Para que seja possibilitado a defesa do infrator, serão analisados alguns parâmetros e critérios, como a gravidade e a natureza das infrações e dos direitos pessoais afetados, boa-fé, vantagem competitiva pretendida com a infração, condição econômica, reincidência, avaliação do dano, cooperação com as entidades, e planejamento na adoção das boas práticas de governanças para se adequar à lei (Lei n. 13.709, 2008).

Do que foi proposto pelo RGPD da União Europeia no Brasil, foi vetada a criação da Autoridade de Controle que seria responsável para fiscalizar o cumprimento da lei. No dia 7 de maio de 2019, a Medida Provisória (MP) 869/2018 que tratava da criação da Autoridade Nacional de Proteção de Dados (ANPD), que regulará a (LGPD) no Brasil foi aprovada pela comissão mista da Câmara dos Deputados brasileira (Medida Provisória n° 869, 2019).

A medida define, dentre outros mecanismos de governança da ANPD, a sua forma de composição: serão 21 membros, sendo cinco representantes indicados pelo Poder Executivo, três pela sociedade civil, três por instituições científicas, três pelo setor produtivo, um pelo Senado, um pela Câmara dos Deputados, um pelo Conselho Nacional de Justiça, um pelo Conselho Nacional do Ministério Público, um pelo Comitê Gestor da Internet, um por empresários e um por trabalhadores (Medida Provisória n° 869, 2019).

Metodologia

Quanto ao objetivo, o estudo teve um caráter descritivo com abordagem qualitativa e um raciocínio científico indutivo. Os dados foram coletados à luz da técnica de estudo de casos múltiplos. Para Yin (2015), um estudo de casos múltiplos possui três fases, a saber: i) definição e planejamento:

desenvolve-se a teoria e, na sequência, os casos são selecionados e concomitantemente o protocolo de coleta de dados é definido; ii) preparação, coleta e análise: os casos selecionados são conduzidos sequencialmente e para cada um dos casos é desenvolvido um relatório individual; iii) análise e conclusão: os resultados dos casos são cruzados para posterior modificação da teoria, desenvolvimento de implicações políticas e escrita do relatório com os resultados cruzados.

Os casos do estudo foram selecionados de acordo com a acessibilidade dos autores às organizações e por questões de disponibilidade dos entrevistados. Para a coleta de dados foi utilizada a técnica de entrevista semiestruturada, analisadas por meio da análise de conteúdo. Bardin (2011) considera que a análise de conteúdo possui três fases fundamentais, fases: pré-análise, exploração do material e tratamento dos resultados (inferência e a interpretação). A primeira fase trata da organização dos dados para análise e são definidos indicadores que orientarão a análise. A segunda fase, exploração, objetiva agrupar os dados em classes/categorias de análise, de modo a facilitar a adequação dos dados coletados aos construtos e objetivo estabelecido na pesquisa. A terceira fase, tratamento/análise dos resultados, realiza-se inferências e interpretações dos corpos textuais.

Os dados foram coletados dois meses (out/2018) após a aprovação da LGPD, configurando o estudo como do tipo corte transversal. Parte das entrevistas foram realizadas via mídia eletrônica Skype e Discord (3), e parte presencialmente (4).

Segundo Gil (2002), as entrevistas permitem uma maior flexibilidade e maior imersão no fenômeno estudado por parte do pesquisador, podendo assumir diversas formas no seu decorrer. Gil (2002) considera que uma entrevista pode ser caracterizada como informal, focalizada, parcialmente estruturada ou totalmente estruturada. A entrevista informal se distingue da simples conversação apenas por ter como objetivo básico a coleta de dados. A entrevista é focalizada quando, embora livre, enfoca tema bem específico, cabendo ao entrevistador esforçar-se para que o entrevistado retorne ao assunto após alguma digressão. Pode ser parcialmente estruturada, quando é guiada por relação de pontos de interesse que o entrevistador vai explorando ao longo de seu curso. Pode ser, ainda, totalmente estruturada quando se desenvolve a partir de relação fixa de perguntas (Gil, 2002, p.117).

A composição dos construtos deste estudo teve como base o trabalho de Freitas e Silva (2018), princípios da NBR ISO/IEC 27002 e especificações da LGPD brasileira. A Tabela 1 destaca os construtos utilizados na pesquisa.

O roteiro de entrevista contou com 36 questionamentos que foram distribuídos entre dados sócio demográficos dos respondentes, características da organização e construtos elencados na Tabela 1. Sete empresas de diferentes ramos de negócio e tamanho compuseram os casos analisados.

Tabela 1 - Relação entre o construto analisado e a literatura

Construto	Referência
Compreensão do conceito de segurança da informação	NBR ISO/IEC 27002:2005 – Item 0.1
Compreensão do conceito de proteção de dados	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 0.1
Responsabilidades e práticas de proteção de dados aplicadas pela organização	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 6
Princípios de gestão da segurança da informação	NBR ISO/IEC 27002:2005 – Item 5
Conhecimento da LEI Nº 13.709, de 14 de agosto de 2018	LEI Nº 13.709 DE AGOSTO DE 2018
Consentimento	LEI Nº 13.709 DE AGOSTO DE 2018 – Capítulo II
Princípios de tratamento dos dados pessoais	LEI Nº 13.709 DE AGOSTO DE 2018 – Capítulo II
Segurança física e do ambiente	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 9
Segurança em recursos humanos	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 8
Direito dos titulares dos dados	(Freitas & Mira, 2018); LEI Nº 13.709 DE AGOSTO DE 2018 – Capítulo III
Encarregado da proteção de dados	(Freitas & Mira, 2018); LEI Nº 13.709 DE AGOSTO DE 2018 – Capítulo IV
Contratos	LEI Nº 13.709 DE AGOSTO DE 2018 – Capítulo VI
Controle de acesso	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 11
Capacitação dos funcionários para adequação à lei	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 14
Responsabilidade do responsável pelo tratamento dos dados pessoais	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 15
Gestão de incidentes em segurança da informação	(Freitas & Mira, 2018); NBR ISO/IEC 27002:2005 – Item 13

Fonte: Desenvolvida pelos autores (2019).

Análises e discussões

Segundo o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas - SEBRAE (2014), a classificação das empresas brasileiras é feita em dois grupos de atividade, sendo um grupo de Indústria e outro para Comércio e Serviços, conforme Tabela 2.

Tabela 2 - Classificação pelo setor da empresa e número de funcionários

Indústria			Comércio e Serviços		
Pequena	**Média**	**Grande**	**Pequena**	**Média**	**Grande**
20 a 99	100 a 499	>= 500	10 a 49	50 a 99	>= 100

Nota. Sebrae (2014, p. 23).

A Tabela 3 apresenta as características das organizações em que o estudo foi realizado e a sua classificação, conforme Tabela 2. As empresas foram identificadas pela letra "E", seguido por um número sequencial. A mesma ordem foi adotada para os entrevistados vinculados a cada empresa (Tabela 4).

Observa-se que cinco empresas são classificadas como de grande porte, uma de médio porte e outra pequena. Todas as organizações estão situadas no Sul de Minas Gerais e pertencem a ramos de atividades distintos.

A empresa E1 foi fundada na cidade de Boa Esperança, MG, com a construção de um pequeno abatedouro de animais de corte. Hoje, a empresa E1 se considera capaz de atender, não só os municípios da região, mas também outras regiões de Minas Gerais e estados brasileiros. A empresa E2 tem mais de 30 anos de experiência nos ramos de atacado e distribuição. Possui mais de três mil itens disponíveis para comercialização e nove mil clientes ativos, e tornou-se assim referência regional no segmento. Atualmente, além do atacado e distribuição, E2 opera nas áreas de logística, incorporadora e agropecuária. A empresa E3 foi fundada em 1963, com a união de produtores rurais da cidade de Boa Esperança, MG, com o objetivo de obter alternativas para a valorização da produção e maior rentabilidade em suas atividades. A empresa E3 atua nos segmentos de café, leite, milho e soja, atendendo a mais de 4756 associados ativos, em que 90% desses associados trabalham em regime de agricultura familiar com a adoção de práticas de sustentabilidade.

E4 foi fundada em 1968 na cidade de Nepomuceno, MG, é considerada uma das maiores empresas de avicultura de postura da América Latina e tem como objetivo a criação de aves para a produção de ovos, a exploração agropecuária e a comercialização de seus produtos. É também a primeira e única empresa em Minas Gerais a realizar o processamento de ovos; oferece às indústrias alimentícias, ovos pasteurizados e desidratados, desenvolvidos por meio de moderna tecnologia.

A empresa E5 atua com atividades de consultoria e assessoramento jurídico do Poder Executivo. E5 possui unidades jurídicas localizadas em todo o país, e se encontra em franco crescimento. E6 foi fundada em 1972 com atividades associadas ao tratamento psiquiátrico e psicológico, mantendo esse tipo de serviço até o início de 1994. Em 1998, inaugurou um Pronto Atendimento 24 horas, um serviço estruturado para atendimento de casos de urgência e emergência. Em 2012, E6 se tornou o primeiro hospital 100% próprio da operadora de planos saúde em que estava vinculada. A empresa é considerada um dos maiores grupos administrativos no ramo de planos de saúde da cidade de Varginha e da região. A empresa E7 é uma multinacional com origem holandesa. Tem mais de um século de história e conta com mais de 37000 funcionários em 100 países diferentes. Possui mais de 450 produtos e serviços. A unidade da cidade de Varginha, MG produz equipamentos médicos como raios x, ressonância magnética e tomografia.

A Tabela 4 destaca os dados sócio demográficos dos entrevistados, sendo a maioria atuante no setor de tecnologia da informação (TI) com cargo de decisão e manipulação direta dos dados organizacionais; outros dois entrevistados estão vinculados ao setor administrativo, escolhidos pela organização para o tratamento dos dados em formato digital devido a inexistência de um setor de TI na empresa.

Tabela 3 - Identificação das empresas

Id.	Porte	Cidade/UF	Setor	Número de funcionários	Ramo de Atividade
E1	Média	Boa Esperança/MG	Indústria e Comércio	100	Frigorífico e Comércio
E2	Grande	Boa Esperança/MG	Comércio e Serviços	230	Atacado Distribuidor e Logística
E3	Grande	Boa Esperança/MG	Comércio e Serviços	500	Agronegócio
E4	Grande	Nepomuceno/MG	Indústria e Comércio	1000	Agroindústria
E5	Pequena	Varginha/MG	Serviços	49	Advocacia
E6	Grande	Varginha/MG	Serviços	500	Hospitalar
E7	Grande	Varginha/MG	Indústria	450*	Eletroeletrônico

*A empresa E7 é uma multinacional, mas o estudo analisou apenas a Unidade de Varginha – MG.
Fonte: Desenvolvida pelos autores (2019).

Tabela 4 - Identificação dos entrevistados

Id.	Cargo	Idade	Gênero	Formação acadêmica
E1	Assistente Financeiro	24	Feminino	Ciências contábeis
E2	Gerente de TI	34	Masculino	Análise e desenvolvimento de sistemas
E3	Gerente de TI	47	Masculino	Ciência da computação
E4	Analista de Suporte TI	27	Masculino	Sistemas de informação
E5	Analista de Suporte TI	23	Masculino	Ciência da computação
E6	Analista de Sistemas TI	28	Masculino	Ciência da computação
E7	Assistente Administrativo	24	Feminino	Engenharia de produção

Fonte. Desenvolvida pelos autores (2019).

A faixa etária média dos entrevistados é de 29 anos. Todos possuem graduação e a maioria tem formação acadêmica no campo de tecnologia da informação (Bacharelado em Ciência da Computação). A maioria dos entrevistados (5) são do gênero masculino e dois são do gênero feminino. Os cargos predominantes entre os entrevistados são de Gerente de TI (2) e Analista de Suporte de TI (2).

Na Tabela 5 são apresentados os resultados quantitativos em relação aos construtos pré-estabelecidos na pesquisa.

Quanto ao construto princípios de gestão de segurança da informação, foi possível observar que mais da metade das empresas não possui uma política de segurança da informação definida. A NBR ISO/IEC 27001 considera que um dos primeiros passos para a gestão da segurança da informação é o estabelecimento de uma política que irá regulamentar as práticas em SI da organização.

Quanto à compreensão da Lei nº 13.709, observou-se um considerável desconhecimento da lei e de seus princípios e alguns entrevistados não sabiam da sua existência, como revela os fragmentos a seguir. “Não, eu ouvi falar sobre ela “LGPD”, mais ainda não sei o que ela está tratando” (E6). “Não, hoje a gente não trabalha com políticas de segurança ainda, hoje a gente está melhorando essas questões de segurança, mas não trabalhamos com nenhum termo ainda” (E1).

Sobre o fator principal que a Lei nº 13.709 trata, o consentimento entre a empresa e a pessoa, apenas uma única empresa informou que teve consentimento em relação aos dados que tem em seu poder. As demais empresas (6) alegaram que, devido a mudanças de gestão e sistemas, perderam o controle dos dados e não souberam dizer a forma como eles foram recolhidos. Algumas empresas (3) informaram que pelo fato de não trabalharem diretamente com pessoas físicas, mas com pessoas jurídicas (organizações governamentais), eles não sabem como os dados foram coletados, como é observado nos fragmentos a seguir. “Não, a gente não trabalha com pessoas física, a gente trabalha com INSS

Tabela 5 - Adequação das respostas quanto aos construtos - análise quantitativa

Construtos	Aplica	Aplica parcialmente	Não aplica
Princípios de gestão da segurança da informação	43%	-	57%
Compreensão do conceito de proteção de dados e da Lei nº 13.709	29%	29%	43%
Responsabilidades e práticas de proteção de dados aplicadas pela organização	14%	57%	29%
Princípios de tratamento dos dados	100%	-	-
Segurança física e do ambiente	29%	43%	29%
Segurança em recursos humanos	14%	57%	29%
Direito dos titulares dos dados	-	-	100%
Encarregado da proteção de dados	43%	-	57%
Contratos	-	-	100%
Controle de acesso	86%	14%	-
Formação	29%	71%	-
Responsabilidade do responsável do tratamento	43%	-	57%
Gestão de incidentes de segurança da informação	-	-	100%

Fonte: Desenvolvida pelos autores (2019).

— Instituto Nacional do Seguro Social, IBAMA — Instituto Brasileiro do Meio Ambiente, a gente não sabe como esses dados foram coletados" (E5).

> Levando em consideração o tratamento que a gente tem com os dados é muito difícil ter o consentimento, as vezes pela organização tratar de muito dinheiro, informação que não pode ser dada, dados que não podem ser passados, pode até ser que tenha, que eles têm uma política maior, mas de verdade eu acho que não é tão rigoroso igual a lei pode vir a trazer. (E7)

Considerando os princípios de tratamento dos dados propostos na Lei nº 13.709, os entrevistados (7) foram enfáticos em dizer que os dados recolhidos são realmente necessários para as finalidades propostas, conforme estrato. "Os dados que a gente coleta hoje, pelo sistema a gente define quais são obrigatórios para facilitar para o pessoal na hora da coleta não pegar informações fora do padrão, fora do que a gente precisa" (E6).

Segundo a NBR ISO/IEC 27002, deve haver uma segurança mínima no processo de coleta e armazenamento de dados. Argumenta-se que práticas de segurança da informação na coleta de dados pessoais podem ser aplicadas como contraprova em casos de "vazamento" de dados. Frente a isso, observou-se que grande parte das empresas (6) faz o uso de recursos de segurança da informação para a coleta de dados, contudo, não para a finalidade proposta na Lei nº 13.709. Os relatos evidenciaram que não há um local seguro para a coleta dos dados e, em alguns casos, a coleta é realizada por uma pessoa fora do ambiente empresarial. "A coleta de dados é direto com o cliente, pelo vendedor, ele anda com seu *smartphone* onde os cadastros já são lançados direto em nossos servidores" (E2). "No local da coleta não, mas quando é feito o cadastro a gente tira uma foto dele para vincular a ficha na hora do cadastro, mas ele saindo da sala, temos monitoramento em todo o ambiente da empresa" (E3).

A NBR ISO/IEC 27002 trata o tema capacitação em segurança da informação sugerindo que treinamentos constantes sejam realizados pelas organizações, a fim de orientar os funcionários em práticas que mitiguem ameaças. Sugere-se que após o processo de contratação de um novo funcionário sejam apresentadas as políticas e normas organizacionais vigentes, especialmente aquelas associadas à SI. Observou-se pelos depoimentos que algumas empresas (4) não instruíram seus funcionários nesse sentido, conforme relatos:

> [...] mas ninguém disse que não poderia passar informação. No meu ponto de vista eu estou errado, mas a empresa em nenhum momento chegou para mim e disse que eu não posso passar para pessoas externas...e eu sei que são informações sigilosas, mas fazer o que. (E5)

Considerando o que está previsto na LGPD, em relação aos direitos dos titulares dos dados, observou-se que nenhuma empresa está preparada para as regulamentações estabelecidas. O processo de demissão de funcionários foi observado como o mais preocupante por parte dos entrevistados e, também, o mais polêmico.

> Hoje quando os funcionários são desligados da empresa, a gente mantém o usuário inativo, e nunca exclui, porque tem muita informação que foi ele quem cadastrou e muitas transações que foram feitas por ele, então como que vou apagar o usuário e como vou saber depois quem fez e quem cadastrou as informações, não tem como. (E4)

> Se isso acontecer e tiver que funcionar dessa forma, a partir do momento que eu fizer a portabilidade e vou ter que apagar as informações, é algo que vai ter que ser revisado. Se isso acontecer nosso departamento de TI vai ter que crescer muito, agora vamos esperar para ver, muito interessante isso. (E2)

As organizações alegam precisar das informações de funcionários demitidos no seu banco de dados para fins de balanços contábeis e pela necessidade de portabilidade. Entende-se por *portabilidade* a transferência de dados a outro fornecedor de serviço ou produto (Lei n. 13.709, 2008). De Hert, Papakonstantinou, Malgieri, Beslaye Sanchez (2018) discutem o tema portabilidade na RGDP da UE sob duas perspectivas, a saber: a primeira numa ótica fechada, em que o exercício da portabilidade dos dados está intrinsecamente ligado à retirada ou apagamento de dados do primeiro controlador de dados; e a segunda abordagem denominada "indireta", em que a portabilidade dos dados não implica, automaticamente, o apagamento dos dados pelo primeiro controlador de dados. Sob essa dicotomia, De Hert et al. (2018) argumentam que a abordagem indireta pode proporcionar um cenário de fusão. A portabilidade dos dados pode incentivar a criação de plataformas de serviços interoperáveis. De Hert et al. (2018) defendem a adoção da portabilidade indireta ou extensiva, considerando que a lógica do direito à portabilidade é reforçar os direitos de controle do titular dos dados em benefício próprio e promover oportunidades de inovação por meio do compartilhamento dos dados pessoais entre controladores de forma segura sob o controle constante do titular. A preocupação apontada por E2 e E4 está associada aos cinco princípios de um SGBD observados por Ziegler et al. (2019) diante das regulamentações do RGPD. Observa-se uma necessidade pela remodelagem dos modelos de banco de dados dos sistemas de informação atuais para atender à regulamentação.

Segundo a LGPD, é necessário que cada empresa tenha um encarregado ou responsável pela proteção de dados. Nesse sentido, mais da metade das empresas entrevistadas (5) não possuem pessoal responsável pela proteção de dados, ficando a cargo dos profissionais de TI. As demais empresas (3) possuem um setor responsável para fazer o tratamento dos dados, sendo que em determinada empresa apenas uma pessoa é responsável para realizar todos os processos de tratamento da informação — coleta, processamento, análise, segurança e descarte (Lyra, 2015).

> Eu tenho uma pessoa específica para mexer com a informação, eu não tenho um monte de usuário com permissão para alterar ou incluir...isso hoje é unificado, e na TI mesma coisa, temos restrições, nem todo mundo tem acesso. Eu sei exatamente quais pessoas tem acesso. (E3)

Contratos com terceiros que possuem acesso a dados de clientes da empresa devem ser revisados com a implantação da Lei nº 13.709, principalmente se os titulares dos dados não foram informados de que suas informações poderiam ser acessadas por terceiros. Dentre as organizações pesquisadas (7), nenhuma apresentou um contrato que contemple adequação à Lei nº 13.709.

Com relação ao controle de acesso, observou-se que a maioria das empresas (6) possuem um bom controle de acesso em seus sistemas de informação para garantir a proteção dos dados. Uma das empresas demonstrou fragilidade no controle de acesso aos dados no sistema de informação. Observou-se que os dados não estão restritos a um usuário ou grupo de usuários de um determinado setor, mas qualquer pessoa com acesso ao sistema consegue obter as informações.

As instruções da Lei nº 13.709 associadas ao tratamento dos dados pessoais por parte dos funcionários, na maioria das empresas (5), foram observadas superficialmente. Não foram identificados cuidados com o tratamento de dados pessoais ou preocupação com o vazamento desses dados para terceiros. Em dois casos (2) foram identificadas boas práticas em SI no tratamento de dados de terceiros. Em uma das organizações, as obrigações legais do ramo de atuação (hospitalar) exigem cuidados na divulgação e/ou acesso a informações. A outra organização (E4) utiliza políticas internas de SI para garantir o adequado tratamento dos dados.

O último construto abordado na pesquisa, incidentes de segurança da informação, evidenciou que nenhuma empresa possui ciência sobre o assunto, e nunca informaram os titulares dos dados sobre os incidentes em SI ocorridos. Todas as empresas envolvidas na pesquisa alegaram a ocorrência de incidentes de segurança da informação. Segundo os entrevistados, os incidentes foram divulgados apenas internamente na organização. Os entrevistados alegaram medo na divulgação do incidente, por acreditarem que poderia levar clientes e parceiros à perda de confiança na organização.

Por fim, foi possível observar resultados semelhantes aos de Freitas e Mira (2018), em Portugal com o RGPD, confirmando o desconhecimento dos funcionários e da organização quanto às regulamentações associadas à proteção de dados pessoais e práticas a serem aplicadas para adequação à nova legislação.

Considerações finais

Retomando a pergunta de pesquisa estabelecida para nortear o estudo ("Como as organizações do Sul de Minas Gerais estão se adequando à LGPD?"), podemos considerar que a adequação das organizações do sul de Minas Gerais à Lei nº 13.709 de 14 de agosto de 2018 será um grande desafio, especialmente devido ao curto prazo para que a lei entre em vigor (fevereiro de 2020). O estudo evidenciou que nenhuma organização, entre as pesquisadas, está preparada para atender aos marcos regulatórios da LGPD brasileira. Alguns entrevistados demonstraram certo conhecimento da lei, mas outros não sabiam da sua existência.

Observamos que todas as empresas necessitarão de consideráveis modificações nos seus processos internos de coleta e armazenamento de dados, além de profundas alterações na gestão em segurança da informação. Os escassos recursos tecnológicos são um limitador para adequação à lei, assim como o desconhecimento das melhores práticas em segurança da informação. Nesse sentido, recomenda-se que as seguintes mudanças sejam aplicadas como passos iniciais para adequação à LGPD: criação de uma política de segurança da informação conforme a regra de negócio da organização; plano de formação com treinamento para os funcionários; definição do responsável pelo tratamento de dados; mudanças no sistema de gestão empresarial (*Enterprise Resource Planning* ou ERP) para adequação aos direitos dos titulares dos dados; e, se possível, utilização de consultorias externas para auxiliar a organização na adequação à LGPD. Dentre as obrigatoriedades estabelecidas pela LGPD, o tema associado ao desligamento/demissão de funcionários e a portabilidade dos dados pessoais foi o mais polêmico e acreditamos que será bastante discutido até a vigência da lei.

O Brasil deu um passo importante para a proteção e privacidade dos dados pessoais, adequando-se às práticas de países desenvolvidos. Nesse sentido, e considerando o prazo para vigência da LGPD, recomendamos para trabalhos futuros a realização de estudos longitudinais a fim de se observar o desenvolvimento e adequação das organizações brasileiras às regulamentações. O Brasil, por ser um país de tamanho continental, pode apresentar consideráveis discrepâncias nos estudos realizados em diferentes regiões do país, podendo ser uma abordagem interessante em novos estudos. Mesmo sendo utilizado princípios metodológicos essenciais a um trabalho dessa natureza, limitações podem ser consideradas. O trabalho se limitou a observar organizações de uma única região do estado de Minas Gerais, impossibilitando que generalizações a nível estadual ou nacional possam ser consideradas.

Agradecimentos

Nós agradecemos o Departamento de Pesquisa do Centro Universitário do Sul de Minas – UNIS-MG, Brasil. Programa de Pós-Graduação em Cibersegurança e Perícia Forense Computacional – UNISMG, Brasil. Universidade Federal de Lavras – UFLA, Brasil.

REFERÊNCIAS

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27001. (2006). *Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos*.

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002. (2013). *Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação*.

Addington, D., & Manrod, M. (2019). Cyber security threats and solutions for the private sector. In *Understanding new security threats*. New York, NY: Routledge.

Banakar, V., Shah, A., Shastri, S., Wasserman, M., & Chidambaram, V. (2019). Analyzing the Impact of GDPR on Storage Systems. In USENIX HotStorage. Recuperado de https://arxiv.org/pdf/1903.04880.pdf

Bardin, L. (2011). *Análise de conteúdo* (1a ed.). São Paulo, SP: Almedina.

Beal, A. (2005). *Segurança da informação : princípios e melhores práticas para a proteção dos ativos de informação nas organizações* (1a ed.). São Paulo, SP: Atlas.

Borden, R., Mooney, J., Taylor, M., & Sharkey, M. (2019). Threat information sharing under GDPR. *Scitech Lawyer, 15*(3), 30-35.

Carneiro, A. (2002). *Introdução à segurança dos sistemas de informação*. Porto, Portugal: FCA.

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law and Security Review, 34*(2), 193–203. https://doi.org/10.1016/j.clsr.2017.10.003

Ferreira, F. N. F., & Araújo, M. T. de. (2008). Política de segurança da informação guia prático para elaboração e implementação. (1st ed.). Rio de Janeiro, RJ: Ciência Moderna.

Freitas, M. da C., & Silva, M. M. da. (2018). GDPR in SMEs. Em *13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1–6). Caceres, Spain: IEEE. https://doi.org/10.23919/CISTI.2018.8399272

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing, 74*(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (4a ed.). São Paulo, SP: Atlas.

Lambrinoudakis, C. (2018). The general data protection regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers. Em *Trust, Privacy and Security in Digital Business* (Vol. 11033). Springer International Publishing. https://doi.org/10.1007/978-3-319-98385-1_1

Lei n. 13.709, de 14 de agosto de 2018 (2008). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). 2008. Brasília, DF. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm#art65

Lovell, M., & Foy, M. A. (2018). General Data Protection Regulation (GDPR). *Bone & Joint 360, 7*(4), 41–42. https://doi.org/10.1302/2048-0105.74.360622

Lyra, M. R. (2015). *Governança da segurança da informação*. Brasília, DF: n.d.

Medida Provisória nº 869, de 2018. (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. (2019). Brasília, DF. Recuperado de https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/135062

Nascimento, T. F. do, Frogeri, R. F., & Prado, L. Á. (2018). Gestão de segurança da informação (GSI) no Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA II). Em *IV Simpósio Mineiro de gestão, educação, comunicação e tecnologia da informação* (pp. 1–30). Varginha, MG: Even3. Recuperado de https://even3.blob.core.windows.net/anais/111315.pdf

Roratto, R., & Dias, E. D. (2014). Security information in production and operations: a study on audit trails in database systems. *Journal of Information Systems and Technology Management, 11*(3), 717–734. https://doi.org/10.4301/S1807-17752014000300010

Serviço Brasileiro de Apoio às Micro e Pequenas Empresas. (2014). Participação das micro e pequenas empresas na economia brasileira. *Bibioteca do SEBRAE*. Brasília, DF: Serviço Brasileiro de Apoio às Micro e Pequenas Empresas – Sebrae. Recuperado de http://www.sebrae.com.br/Sebrae/Portal%20Sebrae/Estudos%20e%20Pesquisas/Participacao%20das%20micro%20e%20pequenas%20empresas.pdf

Sêmola, M. (2014). *Gestão da segurança da informação: uma visão executiva* (2a ed.). Rio de Janeiro, Brasil: Campus.

União Europeia. (2016). Regulamento Geral de Proteção de Dados. *Jornal Oficial da União Europeia*. Recuperado de https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Proteção-Dados.pdf

Yin, R. K. (2015). Estudo de Caso - Planejamento e Métodos. (5a ed.). São Paulo, SP: Bookman.

Ziegler S., Evequoz E., & Huamani A.M.P. (2019) The impact of the European General Data Protection Regulation (GDPR) on future data business models: Toward a new paradigm and business opportunities. Em Aagaard A. (Eds). *Digital business models*. Palgrave Macmillan, Cham, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-13005-3_9

Ziraba, A., & Okolo, C. (2018). *The impact of information technology (IT) policies and strategies to organization's competitive advantage* (1a Ed.). Munich, Germany: GRIN Verlag. Recuperado de https://dl.acm.org/citation.cfm?id=3239838