APPLICATION OF THE NBR ISO/IEC 27002 STANDARD FOR MEET THE CIVIL FRAMEWORK OF THE INTERNET AND THE GENERAL LAW OF DATA PROTECTION APLICAÇÃO DA NORMA NBR ISO/IEC 27002 PARA ATENDIMENTO DO MARCO CIVIL DA INTERNET E DA LGPD

Abstract
Due to the growing offer of services through digital media, the Brazilian public sector needs to guarantee the protection of citizens' data. The objective of this work is to analyze how the implementation of ABNT NBR ISO/IEC 27002:2013 controls can assist the public sector to meet the requirements of current legislation considering the analysis of the requirements of the Civil Framework of the Internet and General Law of Data Protection. Therefore, exploratory research was used with analysis based on bibliographic research of the relevant laws and regulations. The verified results allowed the identification of the main controls of the NBR ISO/IEC 27002:2013 standard that meet the requirements of the current legislation, as well as the main aspects that can serve as a subsidy for public organizations to see value in the adoption and implementation of Information Security Management System (ISMS) based on the ISO/IEC 27000 series.

Keywords: Information Security Management, Civil Framework of the Internet, General Law of Data Protection.

Resumo
Em razão da oferta crescente de serviços por meios digitais, o setor público brasileiro necessita garantir a proteção dos dados dos cidadãos. O objetivo deste trabalho é analisar como a implementação dos controles da norma ABNT NBR ISO/IEC 27002:2013 pode auxiliar o setor público para atendimento aos requisitos da legislação vigente, considerando-se a análise dos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais. Para tanto, realizou-se pesquisa exploratória cuja análise foi baseada em pesquisa bibliográfica das legislações e normas pertinentes. Os resultados verificados permitiram a identificação dos principais controles da norma NBR ISO/IEC 27002:2013 que atendem aos requisitos da legislação vigente, bem como dos principais aspectos que podem servir de subsídio para que organizações públicas possam enxergar valor na adoção e implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na série ISO/IEC 27000.

Palavras-chave: Gestão da Segurança da Informação, Marco Civil da Internet, Lei Geral de Proteção de Dados Pessoais.

1. INTRODUÇÃO

O setor público brasileiro tem se modernizado e cada vez mais oferecido serviços ao cidadão nas diversas esferas de governo, seja no nível federal, estadual ou municipal (Braga, Alves, Figueiredo & Santos, 2008). A administração pública tem se transformado, evoluindo de um modelo liberalizante para uma administração prestadora, que se caracteriza por atuar como provedora de bens e serviços aos cidadãos e ao conjunto da sociedade, no sentido de prover o bem-estar social, e ao mesmo tempo infraestrutural, pois desenvolve tarefas de direção, como no setor privado, focando no planejamento e na ordenação da configuração social (Neto, 2017).

A partir do conceito de Governo Eletrônico (e-Gov), que é a prestação de serviços disponibilizada pelo governo ao conjunto da sociedade por meio do uso da Tecnologia da Informação (Vieira, 2018), e cuja implantação teve início a partir do Grupo de Trabalho Interministerial instituído pela Portaria da Casa Civil da Presidência da República nº 23 de 12 de maio de 2000, diversos serviços têm sido oferecidos desde a esfera federal até a municipal, passando por autarquias e demais órgãos da administração direta e indireta (Zaganelli & Miranda, 2017; Vieira, 2018). Em consonância com estes fatos, o Art. 2° do Decreto s/n° de 2011 estabeleceu como propósito aumentar a transparência, aprimorar a governança pública, ampliar o acesso às informações públicas, prevenir e combater a corrupção, melhorar a prestação de serviços públicos e da eficiência administrativa e fortalecer a integridade pública (Zaganelli & Miranda, 2017).

Como exemplos de serviços públicos podemos citar a possibilidade do cidadão consultar informações sobre serviços em seu município, desde a disponibilidade e localização de equipamentos públicos, bem como a pesquisa de débitos municipais como IPTU (Imposto Predial e Territorial Urbano) e ISS (Imposto sobre Serviços). Na esfera estadual podemos destacar os serviços do Judiciário como Tribunais de Justiça, Ministério Público e Defensoria Pública, que permitem ao cidadão demandar serviços de forma eletrônica a partir de um computador ou mesmo de um aparelho celular com acesso à Internet, ou ainda na esfera federal, com a possibilidade, por exemplo, de se pesquisar a aplicação dos recursos públicos por meio do Portal da Transparência, onde estão detalhados os projetos e a origem dos recursos financeiros a serem aplicados nas mais diversas demandas incluídas no orçamento (Figueiredo & Santos, 2013). No poder legislativo, em particular, a Tecnologia da Informação tem sido usada para apoiar as iniciativas de processo digital, onde a tramitação e publicação de documentos deixa de ser física em papel e passa a ser digital (Braga, 2007; Soares, Barros & Faraj, 2008).

Com o advento do Governo Eletrônico (e-Gov) e a dependência cada vez maior do setor público por ferramentas de sistemas de informação, garantir a segurança da informação tem se tornado uma necessidade constante (Hwang, Li, Shen & Chu, 2004; Araújo, 2012), e para a proteção do conjunto de informações gerido pela organização é necessário um aparato composto por pessoas, processos e tecnologias (Silva & Albuquerque, 2018), de tal forma que o desafio passa a ser então em como implementar as melhores práticas de segurança da informação que atendam a legislação atinente e os marcos regulatórios e que sejam aderentes às particularidades e dinâmica do setor público (Braga et al., 2008).

Para contribuir com esta temática, este trabalho procura identificar os controles da norma NBR ISO/IEC 27002:2013 presentes em um Sistema de Gestão de Segurança da Informação (SGSI) que possam atender às diretrizes do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais (LGPD) dentro do setor público, notadamente no que diz respeito aos dados dos cidadãos, de tal forma que o entendimento e a aplicação das melhores práticas de segurança da informação estejam alinhadas à regulamentação vigente

e possam atender e se possível exceder as expectativas das organizações públicas (e privadas).

Alguns trabalhos correlatos foram encontrados na literatura, como por exemplo, Araújo (2009), Jardim (2013), Bueno, Ikuno, Araújo, Moreira e Melo (2015), Souza, Arima, Oliveira, Akabane e Galegale (2016) e Gonçalves e Varella (2018), no entanto, não foi encontrado nenhum trabalho mais específico que mapeasse os controles da norma NBR ISO/IEC 27002:2013 aos requisitos legais da legislação vigente, em especial no tratamento dos dados de cidadãos na esfera pública, configurando-se assim lacuna para a presente pesquisa, o que justifica este artigo.

Nesse contexto, o problema percebido na literatura é que a aplicação de mecanismos de segurança da informação na gestão pública presentes na série de normas de segurança da informação ISO/IEC 27000, ou mais especificamente, a norma NBR ISO/IEC 27002:2013, tem sido pouco explorada. Assim sendo, o objetivo deste trabalho é analisar como a implementação dos controles da norma ABNT NBR ISO/IEC 27002:2013 pode auxiliar o setor público para atendimento aos requisitos da legislação vigente, considerando-se a análise dos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais.

Este trabalho foi organizado da seguinte forma: após uma breve introdução desta seção 1, na seção 2 é apresentado uma revisão da literatura sobre os aspectos pertinentes da segurança da informação notadamente na gestão pública. Ademais, na seção 3, é descrita a metodologia de pesquisa aplicada no trabalho. Na seção 4, é exibida a análise dos resultados e finalmente, na última seção, expõem-se as considerações finais da pesquisa.

2 REFERENCIAL TEÓRICO

2.1 Gestão da Segurança da Informação

De acordo com a NBR ISO/IEC 38500:2018, a Governança Corporativa é o sistema pelo qual as organizações são direcionadas e controladas, e a Governança Corporativa de Tecnologia da Informação (TI) é o sistema pelo qual o uso atual e futuro da TI é dirigido e controlado, o que significa avaliar e direcionar o uso da TI para dar suporte à organização e monitorar o seu uso para realizar planos. Inclui a estratégia e as políticas de uso da TI dentro da organização (NBR ISO/IEC 38500:2018; Marques, 2007; Leal & Camuri, 2008).

Para o Information Technology Governance Institute (ITGI) e a Information Systems Audit and Control Association (ISACA), a “Governança de TI é responsabilidade do conselho de administração e da gerência executiva. É parte integrante da governança corporativa e consiste em estruturas e processos de liderança e organizacionais que asseguram que a TI da organização sustente e amplie as estratégias e objetivos da organização” (ITGI, 2003).

Como a Tecnologia da Informação é usada como ferramenta fundamental em todos os processos administrativos, seja da iniciativa privada, seja da iniciativa pública, um de seus aspectos mais importantes é quanto à segurança da informação (Canongia & Mandarino, 2009).

Um sistema dito seguro e que é aderente aos preceitos de segurança da informação é todo aquele composto por pessoas, processos e tecnologia e que tem a capacidade de fornecer informações íntegras a todo usuário devidamente autenticado e autorizado no momento em que elas são solicitadas, sempre por meio de requisições válidas, identificadas e rastreáveis, impedindo que terceiros não autorizados interceptem, observem ou alterem estas mesmas informações (Marciano, 2006; Siqueira, 2012).

A informação é um tipo de ativo (NBR ISO/IEC 27005:2019), que por sua vez possui algum tipo de vulnerabilidade, que é uma fraqueza que pode ser potencialmente explorada

por uma ou mais ameaças. Em outras palavras, as vulnerabilidades são os elementos que, uma vez expostos e explorados pelas ameaças, afetam a confidencialidade, a integridade e a disponibilidade dos ativos (Marciano, 2006).

Em consequência disso, todo ativo tem um risco associado, que é a probabilidade de que as ameaças explorem as vulnerabilidades e comprometam os ativos (Sêmola, 2003).

O pilar de implementação de um Sistema de Gestão de Segurança da Informação (SGSI) é a tríade pessoas, processos e tecnologia. Não há como pensar a segurança da informação dentro das organizações sem levar em consideração estes três componentes (Fontes, 2012; Silva & Albuquerque, 2018).

De acordo com o National Institute of Standards and Technology (NIST), Segurança da Informação é a "proteção de informações e sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de garantir a confidencialidade, integridade e disponibilidade" (Nieles, Dempsey & Pillitteri, 2017).

A confidencialidade, integridade e disponibilidade também são conhecidas como Tríade da Segurança (Stallings & Brown, 2017). A confidencialidade garante que os dados ficarão protegidos contra divulgação não autorizada, incluindo meios para proteger a privacidade pessoal e informações proprietárias. A integridade, por sua vez, assegura que os dados ficarão protegidos contra modificação ou destruição indevida e garante o não-repúdio e a autenticidade da informação. Por fim, a disponibilidade é a garantia de acesso e uso oportuno e confiável de informações a qualquer usuário autorizado a utilizá-lo (Nieles et al, 2017).

O Hexagrama Parkeriano (Parkerian Hexad), proposto por Donn B. Parker, expandiu os atributos da Tríade de Segurança, definindo a autenticidade como sendo a verificação da veracidade quanto à alegação de origem ou autoria de um dado documento ou informação, que poderia ser aferida com o uso de assinatura digital, por exemplo; a posse ou controle, que é quando o dado, informação ou sistema está na posse de quem o controla ou utiliza; e a utilidade, que diz respeito ao proveito que o usuário pode fazer de dados, informações ou sistemas (Reid & Gilbert, 2010).

A NBR ISO/IEC 27001:2013 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A sua adoção deve ser uma decisão estratégica da organização (Laureano; Moraes, 2005). O estabelecimento e a implementação do SGSI de uma organização são influenciados por: suas necessidades e objetivos; requisitos de segurança; processos organizacionais; e tamanho e estrutura da organização (Associação Brasileira de Normas Técnica, 2013a).

A NBR ISO/IEC 27002:2013 em particular estabelece os objetivos de controle e os controles que devem ser usados em alinhamento com o processo de tratamento de riscos de segurança da informação. Ao todo são 14 (quatorze) categorias, por onde estão distribuídos 35 (trinta e cinco) objetivos de controle que contêm, em conjunto, 114 (cento e quatorze) controles no total.

2.2 Gestão da Segurança da Informação no Setor Público

A norma NBR ISO/IEC 27002:2013, presente na série NBR ISO/IEC 27000 que trata dos aspectos de segurança da informação, foi projetada para que as organizações, tanto públicas como privadas, a usem como uma referência na seleção de controles dentro do processo de implementação de um Sistema de Gestão de Segurança da Informação (SGSI) (Associação Brasileira de Normas Técnica, 2013b).

A International Organization for Standardization (ISO) propôs uma norma, a ISO/IEC 27012, que especifica as técnicas de segurança e diretrizes de sistemas de

gerenciamento de segurança da informação para organizações da administração pública e governo eletrônico, mas ela foi cancelada em 2009 (Szmit, M & Szmit A, 2015).

Uma forma de melhorar a interação entre o cidadão e o governo, bem como melhorar a oferta de bens e serviços aos cidadãos e ainda ampliar o acesso às informações de interesse público com vistas a aumentar a transparência é com a adoção de sistemas de informação que deem sustentação às diversas modalidades de prestação de serviços à sociedade (Figueiredo & Santos, 2013).

Há de se destacar também que as diversas iniciativas de e-Gov, que por padrão usam sistemas de informação para dar sustentação à prestação dos serviços, podem ou não armazenar informações sensíveis, como por exemplo dados dos cidadãos e informações governamentais que exijam um certo grau de confidencialidade. E a partir do momento em que estas informações passam a ter valor para a organização pública, elas passam a requerer algum grau de proteção (NBR ISO/IEC 27005:2019).

A informação gera conhecimento e é fundamental nas organizações (Silva & Albuquerque, 2018), e o processo de gestão da informação é importante pois fornece e mantém constantes o fluxo informacional nas organizações (Araújo, 2009).

Uma forma de gerir a informação é por meio da utilização da Tecnologia da Informação e Comunicação (TIC), e dada a sua importância, o Ministério do Planejamento, Orçamento e Gestão elaborou um documento intitulado e-Ping, que trata sobre Padrões de Interoperabilidade de Governo Eletrônico no Governo Federal e estabelece as condições de interação com os demais poderes e esferas de governo e com a sociedade em geral, e a Portaria SLTI/MP nº 5, de 14 de julho de 2005, tornou a sua adoção obrigatória (Araújo, 2012).

De acordo com Silva e Albuquerque (2018), muitas organizações públicas e privadas investem em tecnologia e pessoas, mas negligenciam os processos e a formação de uma cultura organizacional de segurança da informação, sem o quais não se podem alcançar plenamente a proteção da informação.

A Portaria nº 34, de 5 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, e que instituiu o Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, definiu Infraestruturas Críticas da Informação como o "subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade" e Ativos de Informação como os "meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso" (Canongia & Mandarino, 2009).

Assim, a segurança da informação visa proteger os ativos sob o ponto de vista da Confidencialidade, Integridade e Disponibilidade, e para tal deve lançar mão de Tecnologias, Processos e Pessoas para alcançar este objetivo (Fontes, 2012; Silva & Albuquerque, 2018). Como as pessoas são o elo mais fraco e ao mesmo tempo o mais importante da corrente de segurança, adotar uma política de segurança adequada pode ajudar o órgão público a implementar da melhor maneira possível os controles e protocolos com vistas a proteger seus ativos (Silva, 2010). No entanto, devem ser observadas, obrigatoriamente, a legislação vigente e os marcos regulatórios, bem como as normas técnicas inerentes ao assunto (Associação Brasileira de Normas Técnica, 2013a).

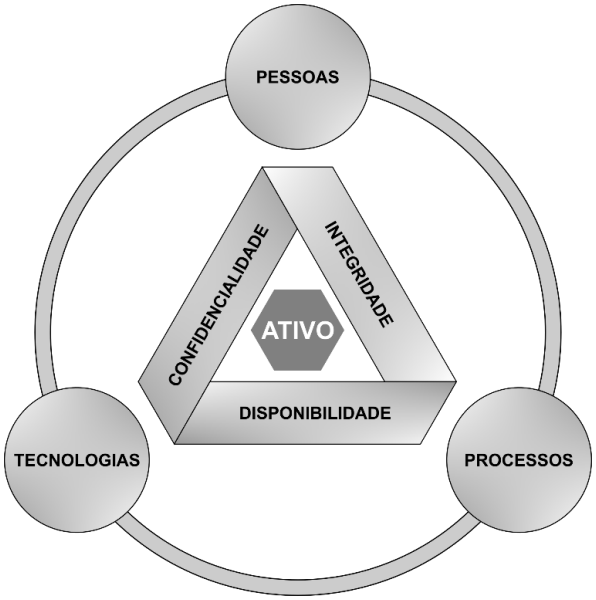

Figura 1 - Diagrama do processo de Segurança da Informação (elaborado pelo autor)

A norma NBR ISO/IEC 27002:2013 destaca que a segurança da informação pode ser alcançada se forem implementados um conjunto adequado de controles, políticas, processos, procedimentos, estrutura organizacional e tecnologias de *software* e *hardware* que suportem estas funções (Souza et al., 2016; Silva & Albuquerque, 2018).

A segurança da informação, que pode ser caracterizada pelo tripé confidencialidade, integridade e disponibilidade (Stallings & Brown, 2018), encontra respaldo de aplicabilidade no setor público não só na série NBR ISO/IEC 27000, como também na Lei nº 12.527 de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI), e que dispõe "sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações" (Araújo, 2012). Esta lei também tem como principal diretriz o princípio da publicidade dos atos da administração pública, sendo o sigilo a exceção (Jardim, 2013; Araújo, 2012).

Sendo a informação um ativo importante que tem valor para organização e que está sujeito a ameaças, sejam elas acidentais ou deliberadas (Associação Brasileira de Normas Técnica, 2013b), é necessário observar que a mesma deve ser classificada para se verificar quais níveis de proteção que devem ser aplicados (Araújo, 2012).

Segundo a NBR ISO/IEC 27002:2013, a classificação da informação é muito importante pois assegura que a mesma receberá um nível adequado de proteção que esteja de acordo com a sua importância para a organização, que é medida a partir de parâmetros como o seu valor intrínseco, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada. No que diz respeito ao setor público, o Decreto nº 7.845, de 14 de novembro de 2012, que dispõe sobre o Núcleo de Segurança e Credenciamento, regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo Federal.

Sendo então a informação importante para a organização e esta ser representada por um ativo, é conveniente que o mesmo tenha um proprietário que seja responsável por qualificar o seu ciclo de vida. O proprietário do ativo deve ser responsável pelo seu inventário e assegurar-se de que o ativo tem a devida classificação e proteção. O proprietário ainda deve ser responsável por analisar periodicamente as classificações e restrições ao

acesso aos ativos, bem como dar um tratamento adequado quando o ativo é excluído ou destruído (Associação Brasileira de Normas Técnica, 2013b).

Da mesma forma, o Decreto nº 7.845 de 14 de novembro de 2012, em seu Art. 2º, estabelece o gestor de segurança e credenciamento como "responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle" (Decreto n. 7.845, 2012).

Por sua vez, a Lei nº 12.965, de 23 de abril de 2014, também conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres no uso da Internet no âmbito do território brasileiro, com vistas principalmente aos direitos fundamentais como o princípio da neutralidade de rede, que em outras palavras significa que os provedores não podem segregar os serviços de conexão com base no tipo de dado trafegado (Zaganelli & Miranda, 2017), de modo a assegurar direitos e liberdades dos usuários, pois esta legislação visa proteger a liberdade de expressão, a privacidade, a proteção dos dados e a cidadania e participação no mundo digital (Santos & Araujo, 2017).

No que diz respeito aos dados pessoais dos usuários, que podem ser definidos como o acúmulo de fatos e acontecimentos que formam a personalidade de cada indivíduo (Souza, 2018), e que se relacionam com uma pessoa natural identificada ou identificável (Lei n. 13.709, 2018; Agostinelli, 2018), a Lei nº 13.709 de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), visa proteger situações que dizem respeito exclusivamente a operações que envolvam o tratamento de dados pessoais, assim descritos em seu Art. 5º, Inciso X, ou seja, "coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (Lei n. 13.709, 2018; Mulholland, 2018).

Os dados pessoais podem ser classificados como públicos ou privados, e entende-se como dado público aquele que não está sob sigilo (Agostinelli, 2018). Por sua vez, os dados privados referem-se a vida privada do indivíduo (Agostinelli, 2018), e a LGPD classifica como dados (privados) sensíveis aqueles referentes à ideologia, religião ou crença, origem racial, saúde ou vida sexual (Raminelli & Rodegheri, 2016).

Sendo os dados pessoais de um indivíduo um ativo que pode ser objeto de uma política de segurança da informação, pode-se adotar os controles da norma NBR ISO/IEC 27002:2013 pertinentes a este ativo específico, já que a NBR ISO/IEC 27005:2019 estabelece que os ativos podem ser de vários tipos.

Assim, torna-se um desafio para a Administração Pública atender às regras de transparência e publicidade exigidas pela chamada Lei de Acesso à Informação e ao mesmo tempo respeitar as restrições quanto à confidencialidade da informação no caso de grandes bases de dados que apresentam informações sensíveis de usuários e de demais cidadãos (Gonçalves & Varella, 2018).

Alguns trabalhos correlatos foram encontrados na literatura, como por exemplo, o trabalho de Araújo (2009), que tratou sobre o mapeamento da segurança dos ativos de conhecimento que eram prioritários nos processos de gestão de segurança da informação e de gestão do conhecimento do Serviço Federal de Processamento de Dados (Serpro).

Outro trabalho, o de Jardim (2013), tratou sobre os aspectos relativos à implantação da Lei nº 12.527, de 18 de novembro de 2011, também conhecida como Lei de Acesso à Informação (LAI), principalmente do ponto de vista arquivístico, uma vez que os documentos públicos são considerados ativos de informação e, portanto, demandam proteção. Estes documentos podem ainda, eventualmente, referir-se a dados de cidadãos que podem ou não estarem protegidos por sigilo.

O trabalho de Bueno et al. (2015), por sua vez, apresentou uma metodologia de gestão de riscos, denominada MGR, aplicada ao Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.

Um trabalho mais recente, o de Souza et al. (2016), estudou como a gestão de riscos de segurança da informação se apresentava numa instituição pública federal de ensino superior, o Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP), para verificar se os requisitos de segurança da informação eram vistos como prioritários e se estavam sendo aplicados.

Outro trabalho recente, o de Gonçalves e Varella (2018), também deu sua contribuição ao discutir os desafios da administração pública na disponibilização de dados de cidadãos, atendendo, ao mesmo tempo, as regras de transparência e publicidade da Lei de Acesso à Informação e as restrições quanto à sua confidencialidade.

2.3 Marco Civil da Internet

O Capítulo II do Marco Civil da Internet, que trata dos direitos e garantias dos usuários, estabelece em seu Art. 7º, entre outras coisas, a inviolabilidade da intimidade e da vida privada; a inviolabilidade e sigilo do fluxo de suas comunicações pela internet; informações claras e completas constantes dos contratos de prestação de serviços; o não fornecimento a terceiros de seus dados pessoais; e informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades a que se propõem (Lei n. 12.965, 2014).

No Capítulo III, que trata da provisão de conexão e de aplicações de Internet, o Art. 10º presente na Seção II, que trata da proteção aos registros, aos dados pessoais e às comunicações privadas, estabelece, entre outras coisas, que a guarda e a disponibilização dos dados pessoais e do conteúdo de comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas (Lei n. 12.965, 2014). Nesta mesma seção, o Art. 11º estabelece que em qualquer operação de coleta, armazenamento, guarda e tratamento de dados pessoais, a legislação brasileira e os direitos à privacidade e à proteção dos dados pessoais deverão ser respeitados (Lei n. 12.965, 2014).

2.4 Lei Geral de Proteção de Dados Pessoais

Os Art. 5º e 12º da Lei Geral de Proteção de Dados Pessoais (LGPD) definem dado pessoal como qualquer informação que identifique ou possa identificar uma pessoa física ou natural (Lei n. 13.709, 2018).

Ainda de acordo com a LGPD, em seu Art. 23º, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (BRASIL, 2018). Em seu Art. 37º, a Lei estabelece que os agentes de tratamento devem manter registro das operações de tratamento de dados pessoais que realizarem, e em seu Art. 47º que estes mesmos agentes ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei (Lei n. 13.709, 2018).

A LGPD também define em seu Art. 5º como agentes de tratamento o controlador e o operador, que são, respectivamente, a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; e a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (Lei n. 13.709, 2018). Por último tem-se a figura do encarregado, que segundo o Art. 5º da LGPD é a "pessoa indicada pelo controlador para

atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) ", conforme redação dada pela Medida Provisória nº 869, de 2018 (Lei n. 13.709, 2018).

Uma vez identificado o ativo, dá-se início ao seu tratamento. A LGPD, em seu Art. 5º, estabelece que o tratamento de dados pessoais envolve toda operação que se refira a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Lei n. 13.709, 2018).

A LGPD estabelece o acesso aos dados pessoais dos usuários em algumas situações. Em seu Art. 18º garante que o titular dos dados pessoais tem direito a obter do controlador o acesso aos dados em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição. Em seu Art. 13º, permite que os órgãos de pesquisa poderão ter acesso a bases de dados pessoais para realização de estudos em saúde pública. Estes dados deverão ser tratados exclusivamente dentro do órgão e usados exclusivamente para a finalidade a que se destina, usando, sempre que possível, a anonimização ou pseudonimização dos dados (Lei n. 13.709, 2018).

Por fim, a LGPD, em seu Art. 46º, atribui aos agentes de tratamento a responsabilidade em adotar as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados (Lei n. 13.709, 2018). A LGPD prevê tratamento especial quando da transferência de dados para terceiros, em especial quando se trata de transferência internacional de dados, conforme descrito no Art. 33º da referida lei (Lei n. 13.709, 2018).

É importante destacar que a LGPD, em seu Art. 33º, estabelece que só é permitida a transferência internacional de dados pessoais nos casos em que o destinatário sejam países ou organismos internacionais que proporcionem grau de proteção equivalente ou quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos (Lei n. 13.709, 2018).

Como os sistemas de informação são baseados em tecnologias da informação e comunicação que dão sustentação à coleta, tratamento e armazenamento de dados, a LGPD em ser Art. 49º estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança (Lei n. 13.709, 2018).

Quanto à gestão de incidentes de segurança da informação, a LGPD em seu Art. 48º estabelece que "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares" (Lei n. 13.709, 2018).

3 METODOLOGIA

Esta pesquisa classifica-se como de natureza exploratória e descritiva, com abordagem qualitativa, executada a partir da análise de pesquisa bibliográfica e documental, tendo como base principalmente normas técnicas que permitam a aplicação das melhores práticas e a legislação vigente de caráter mandatório (Dalfovo, Lana & Silveira, 2008; Gerhardt & Silveira, 2009).

A pesquisa qualitativa foi aplicada neste trabalho, pois na área de segurança da informação o setor privado tem se mostrado mais ágil, ao passo que o setor público possui características que engessam de certa forma a adoção e adequação de novos processos e tecnologias. Assim, a pesquisa qualitativa permitiu entender como estas particularidades

inerentes ao setor público impactam na correta adoção e implementação de políticas de segurança da informação com o objetivo de proteger seus ativos (Gerhardt & Silveira, 2009).

A pesquisa exploratória executada neste trabalho permitiu um maior entendimento do problema, visto as particularidades inerentes ao setor público que não necessariamente podem ser replicadas do setor privado (Gerhardt & Silveira, 2009), tendo se baseado em ampla pesquisa bibliográfica (Dalfovo, Lana & Silveira, 2008). A pesquisa não se restringiu somente aos aspectos de Tecnologia da Informação e de Segurança da Informação, mas principalmente no que diz respeito à legislação atinente e pertinente, em especial o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD).

Como referencial de aplicação do Sistema de Gerenciamento de Segurança da Informação (SGSI) foram analisados os controles da NBR ISO/IEC 27002:2013, tida como referência na aplicação das melhores práticas de proteção e controle dos ativos de segurança da informação, tanto no setor público quanto privado.

Uma vez analisados os controles da referida norma, estes foram confrontados com as diretrizes apontadas pelo Marco Civil da Internet e pela LGPD. Na sequência foi criado um quadro analítico no qual foram destacados os controles que atendem aos requisitos da legislação vigente.

A análise de equivalência consistiu em avaliar cada artigo do Marco Civil da Internet e da LGPD, buscando assim verificar se haviam controles da NBR ISO/IEC 27002:2013 que pudessem dar suporte às exigências das referidas leis. Para tanto, vale ressaltar que foram considerados apenas os aspectos das duas legislações que dissessem respeito somente à proteção de dados de cidadãos.

4 ANÁLISE DOS RESULTADOS

4.1 Categorias da Norma NBR ISO/IEC 27002:2013

A NBR ISO/IEC 27002:2013 possui 114 (cento e quatorze) controles distribuídos por 14 (quatorze) categorias. O Quadro 1 apresenta as categorias presentes na norma distribuídos um por linha, com o nome da categoria na primeira coluna e uma breve descrição na segunda coluna. Nas terceira e quarta colunas há um indicativo se aquela categoria possui controles que ajudam ou não tanto organizações públicas como privadas a atenderem aos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais (LGPD).

Quadro 1 – Correspondência das categorias da NBR ISO/IEC 27002:2013 com o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD)

Categoria	Descrição da Categoria	Indicativo de Atendimento	
		Marco Civil da Internet	LGPD
A.5	Políticas de segurança da informação	---	Sim
A.6	Organização da segurança da informação	---	Sim
A.7	Segurança em recursos humanos	---	---
A.8	Gestão de ativos	Sim	Sim
A.9	Controle de acesso	---	Sim
A.10	Criptografia	---	---
A.11	Segurança física e do ambiente	---	---
A.12	Segurança nas operações	---	---
A.13	Segurança nas comunicações	Sim	Sim
A.14	Aquisição, desenvolvimento e manutenção de sistemas	---	Sim
A.15	Relacionamento na cadeia de suprimento	---	---
A.16	Gestão de incidentes de segurança da informação	---	Sim
A.17	Aspectos da segurança da informação na gestão da continuidade do negócio	---	---
A.18	Conformidade	Sim	Sim

Fonte: dados da pesquisa.

No Quadro 1, verifica-se que das quatorze categorias da NBR ISO/IEC 27002:2013, três possuem algum controle que atende o Marco Civil da Internet e oito à Lei Geral de Proteção de Dados Pessoais (LGPD). No entanto, isso não significa necessariamente que as demais categorias não possuam controles que possam ser usados em maior ou menor grau para atender aos requisitos destas leis.

O que se procura mostrar com o Quadro 1 é que as organizações que adotam as boas práticas da referida norma já possuem alguma base para atender a legislação e regulamentações obrigatórias. E como apontavam Laureano e Moraes (2005), é importante que as organizações adotem as regulamentações do mercado em que atuam. No entanto, Silva e Albuquerque (2018) asseveravam que para a adoção de uma política de segurança da informação havia a necessidade de uma mudança cultural na organização.

Enquanto o Quadro 1 mostra uma visão macro da NBR ISO/IEC 27002:2013, ao listar somente suas categorias, na próxima seção serão descritos com mais detalhes os controles das categorias selecionadas, o que culminará com o Quadro 2, que mostrará os controles da referida norma que atendem as Leis em análise neste trabalho.

4.2 Controles da Norma NBR ISO/IEC 27002:2013

Os controles da norma NBR ISO/IEC 27002:2013 seguem a seguinte diretriz: cada categoria, numerada de A.5 a A.18, possui um ou mais objetivos de controle declarando o que se espera que seja alcançado, que por sua vez possuem um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle em questão (NBR ISO/IEC 27002:2013).

A começar pelo controle 5.5.1, que faz parte da Categoria A.5 (ver Quadro 1) e do Objetivo de Controle 5.1, um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. Entre outras coisas, esta política deve contemplar requisitos oriundos de regulamentações e legislação vigente.

No controle 6.1.1 da mesma norma, todas as responsabilidades pela segurança da informação devem ser definidas e atribuídas (Associação Brasileira de Normas Técnica, 2013b).

A figura do encarregado, previsto na LGPD, encontra equivalente na NBR ISO/IEC 27002:2013 no controle 6.1.3, que sugere que contatos apropriados com autoridades relevantes devem ser estabelecidos e mantidos.

A NBR ISO/IEC 27002:2013 trata da Gestão dos Ativos na categoria A.8, por meio de dois objetivos de controle: o 8.1, que trata da responsabilidade pelos ativos, e o 8.2, que trata da classificação da informação.

Dentro do objetivo de controle 8.1, o controle 8.1.1, que trata do inventário dos ativos, sugere que a organização deve identificar os ativos relevantes no ciclo de vida da informação e documente a sua importância. De acordo com a referida norma, o ciclo de vida da informação inclui a criação, o processamento, o armazenamento, a transmissão, a exclusão e a sua destruição (Associação Brasileira de Normas Técnica, 2013b).

O controle 8.1.2, que trata do proprietário dos ativos, sugere que os ativos mantidos no inventário tenham um proprietário. Neste caso, é importante destacar que o proprietário não é o dono da informação, mas sim o responsável pelo seu tratamento. O dono ou proprietário no sentido literal da palavra seria o titular do dado pessoal, que é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, conforme descrito no Art. 5º da LGPD. O proprietário, conforme descrito na norma, seria o agente de tratamento (Lei n. 13.709, 2018).

Outro controle importante é o 8.1.3, que trata do uso aceitável dos ativos, e sugere que as regras para o uso aceitável das informações sejam identificadas, documentadas e implementadas. Neste caso a LGPD é bastante clara em seu Art. 6º, ao estabelecer que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios de finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (Lei n. 13.709, 2018).

Dentro do objetivo de controle 8.2, o controle 8.2.1, que trata da classificação da informação, sugere que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade. Este mesmo controle sugere que o proprietário do ativo, neste caso o agente de tratamento, seja o responsável por sua classificação (Associação Brasileira de Normas Técnica, 2013b).

De acordo com a NBR ISO/IEC 27002:2013, é a partir da classificação da informação que se pode iniciar o tratamento dos ativos, conforme descrito no controle 8.2.3, que sugere que o tratamento dos ativos seja desenvolvido e implementado de acordo com o esquema de classificação da informação adotado.

A LGPD, em seu Art. 46º, atribui aos agentes de tratamento a responsabilidade em adotar as medidas de segurança aptas a proteger os dados pessoais de acessos não autorizados (Lei n. 13.709, 2018), e isto pode ser alcançado por meio do controle 9.1.1, que trata da política de controle de acesso. Este controle sugere que uma política de controle de acesso deva ser estabelecida, documentada e analisada criticamente a intervalos regulares. A norma estabelece também que é de responsabilidade do proprietário do ativo, neste caso o agente de tratamento, o estabelecimento de regras de controle de acesso, de direitos de acesso e de restrições (Associação Brasileira de Normas Técnica, 2013b).

A LGPD prevê em seu Art. 33º tratamento especial para a transferência de dados para terceiros (Lei n. 13.709, 2018), e o Marco Civil da Internet, em seu Art. 22º, prevê que o fornecimento de registros de conexão ou de registros de acesso a aplicações de Internet somente poderão ser realizados por meio de ordem judicial (Lei n. 12.965, 2014).

A NBR ISO/IEC 27002:2013 prevê no objetivo de controle 13.2, que trata da transferência de informação, a manutenção dos aspectos de segurança da informação dos dados que são transferidos para quaisquer entidades externas.

O controle 13.2.1, que trata das políticas e procedimentos para transferência de informações, sugere que políticas, procedimentos e controles de transferências formais sejam estabelecidos para proteger a transferência de informações. Outro controle, o 13.2.2, que trata de acordos para transferência de informações, sugere que acordos para transferência segura de informações do negócio entre a organização e as partes externas sejam estabelecidos (Associação Brasileira de Normas Técnica, 2013b).

Já o controle 13.2.4, que trata de acordos de confidencialidade e não divulgação, sugere que os requisitos para confidencialidade ou acordos de não divulgação para a proteção da informação sejam identificados, analisados criticamente e documentados (Associação Brasileira de Normas Técnica, 2013b).

A LGPD, em ser Art. 49º, estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança (Lei n. 13.709, 2018). Tal requisito encontra respaldo no controle 14.1.1, que trata da análise e especificação dos requisitos de segurança da informação, e que sugere que "os requisitos relacionados à segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes" (Associação Brasileira de Normas Técnica, 2013b).

A gestão de incidentes de segurança da informação, prevista na LGPD em seu Art. 48º, pode ser atendida por meio do controle 16.1.2, que trata da notificação de eventos de segurança da informação, sugere que tais eventos sejam relatados o mais rapidamente possível por meio dos canais de gestão, e segundo o controle 16.1.5, que trata da resposta aos incidentes de segurança da informação, sejam reportados de acordo com procedimentos documentados. Esta comunicação deve ser feita a um ponto de contato definido ou para partes externas, neste caso, a Autoridade Nacional de Proteção de Dados (ANPD) (Associação Brasileira de Normas Técnica, 2013b; Lei n. 13.709, 2018).

O objetivo de controle 18.1, que trata da conformidade com requisitos legais e contratuais, tem por objetivo "evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança" (Associação Brasileira de Normas Técnica, 2013b). Em seu controle 18.1.1, que trata da identificação da legislação aplicável e de requisitos contratuais, é exposto que todos os requisitos legislativos estatutários, regulamentares e contratuais pertinentes sejam explicitamente identificados (Associação Brasileira de Normas Técnica, 2013b).

Como o agente de tratamento deve manter o registro das operações de tratamento de dados, conforme explicitado no Art. 37º da LGPD (Lei n. 13.709, 2018), a NBR ISO/IEC 27002:2013 apoia este requisito por meio do controle 18.1.3, que trata da proteção de registros, e que sugere que os registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada. Este controle também pode ser usado para atender ao Art. 13º do Marco Civil da Internet, que estabelece que cabe ao administrador de sistema manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança pelo prazo estabelecido em Lei (Lei n. 12.965, 2014).

Por fim, tanto a lei do Marco Civil da Internet quanto a LGPD estabelecem o direito do cidadão à privacidade (Lei n. 12.965, 2014; Lei n. 13.709, 2018), que é atendida na NBR ISO/IEC 27002:2013 por meio do controle 18.1.4, que trata da proteção e privacidade de informações de identificação pessoal, e que sugere que "a privacidade e a proteção das informações de identificação pessoal sejam asseguradas conforme requerido por legislação

e regulamentação pertinente", ou seja, a norma indica que a lei vigente no país deve ser usada para garantir tal requisito.

No Quadro 2 é listado um resumo dos controles da NBR ISO/IEC 27002:2013 que atendem o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais. Verifica-se que dos cento e quatorze controles presentes na norma, oito atendem o Marco Civil da Internet, ou seja, 7%. Por sua vez, dezessete controles atendem a Lei Geral de Proteção de Dados Pessoais (LGPD), ou seja, 15%.

Quadro 2 - Quadro resumo dos controles da NBR ISO/IEC 27002:2013 que atendem ao Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais (LGPD)

Categoria	**Controles**	**Indicativo de Atendimento**	
		Marco Civil da Internet	**LGPD**
A.5 - Políticas de segurança da informação			
	5.1.1 Políticas para segurança da informação	---	Sim
A.6 - Organização da segurança da informação			
	6.1.1 Responsabilidades e papéis pela segurança da informação	---	Sim
	6.1.3 Contato com autoridades	---	Sim
A.8 - Gestão de ativos			
	8.1.1 Inventário dos ativos	---	Sim
	8.1.2 Proprietário dos ativos	---	Sim
	8.1.3 Uso aceitável dos ativos	Sim	Sim
	8.2.1 Classificação da informação	---	Sim
	8.2.3 Tratamento dos ativos	Sim	Sim
A.9 - Controle de acesso			
	9.1.1 Política de controle de acesso	---	Sim
A.13 - Segurança nas comunicações			
	13.2.1 Políticas e procedimentos para transferência de informações	Sim	Sim
	13.2.2 Acordos para transferência de informações	Sim	Sim
	13.2.4 Acordos de confidencialidade e não divulgação	Sim	---
A.14 - Aquisição, desenvolvimento e manutenção de sistemas			
	14.1.1 Análise e especificação dos requisitos de segurança da informação	---	Sim
A.16 - Gestão de incidentes de segurança da informação			
	16.1.2 Notificação de eventos de segurança da informação	---	Sim
	16.1.5 Resposta aos incidentes de segurança da informação	---	Sim
A.18 - Conformidade			
	18.1.1 Identificação da legislação aplicável e de requisitos contratuais	Sim	Sim
	18.1.3 Proteção de registros	Sim	Sim
	18.1.4 Proteção e privacidade de informações de identificação pessoal	Sim	Sim

Fonte: dados da pesquisa.

Como se pode verificar, nem todos os controles da norma podem ser mapeados diretamente a todos os requisitos do Marco Civil da Internet ou da Lei Geral de Proteção de Dados Pessoais e vice-versa, pois ela é projetada para que as organizações, sejam elas públicas ou privadas, a usem como uma referência na seleção de controles durante o processo

de estabelecimento e implementação de um Sistema de Gestão da Segurança da Informação (SGSI) (Associação Brasileira de Normas Técnica, 2013b). Mas isso não pode ser visto como uma restrição para a adoção de um SGSI, pois como asseverava Laureano e Moraes (2005), é importante que as organizações adotem as regulamentações do mercado em que atuam, pois, a adoção de políticas de segurança da informação proporciona às organizações transparência e credibilidade.

Ainda que a norma não contemple todos os requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, a NBR ISO/IEC 27002:2013 esclarece que os controles necessários podem ser selecionados desta norma ou então novos controles podem ser projetados para atender às necessidades específicas e particulares da organização, como bem alertava Gonçalves e Varella (2018) sobre a necessidade de se avaliar os mecanismos de controle a serem adotados.

Também não se espera que a NBR ISO/IEC 27002:2013 atenda totalmente as Leis em análise neste trabalho, pois a norma alerta que nem todos os controles e diretrizes contidos nela podem ser aplicados e orienta que controles adicionais e recomendações externas a ela devam ser consideradas, pois em suma, a norma deve ser usada como ponto de partida para o desenvolvimento de diretrizes específicas para a organização (Associação Brasileira de Normas Técnica, 2013b).

Há de se destacar também que a norma não contempla o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais no que diz respeito à aplicação de penalidades e multas àqueles que infringem seus dispositivos legais, pois esta é uma prerrogativa dos entes públicos que fiscalizam a sua aplicação.

Para contemplar estas lacunas, entraram em vigor novas normas, a NBR ISO/IEC 27701:2019, que "especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI)", e que estende os requisitos das normas NBR ISO/IEC 27001 e NBR ISO/IEC 27002 para incluir a gestão da privacidade dentro das organizações, e a NBR ISO/IEC 29100:2020, que "especifica uma terminologia comum de privacidade; especifica os atores e os seus papéis no tratamento de dados pessoais (DP); descreve considerações de salvaguarda de privacidade; e fornece referências para princípios conhecidos de privacidade para tecnologia da informação" (Associação Brasileira de Normas Técnica, 2019; Associação Brasileira de Normas Técnica, 2018).

Enquanto o Quadro 1 mostrava uma visão macro da NBR ISO/IEC 27002:2013, ao listar somente suas categorias, o Quadro 2 mostrou em detalhes os controles da referida norma que atendem as Leis em análise neste trabalho.

Assim, pode-se chegar à conclusão de que a adoção e implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na norma NBR ISO/IEC 27002:2013 poderá ajudar as organizações públicas (e privadas) a atenderem aos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais, a exemplo do que apontava Bueno et al. (2015), ao exemplificar que a série ISO/IEC 27000 é base para iniciativas na Administração Pública Federal para implementação de um modelo para análise, avaliação e aceitação de riscos de segurança da informação, pois como bem escreveu Souza (2016), a segurança da informação é agenda estratégica no setor público, uma vez que existem leis e normas que tratam de sua aplicação e cuja observância é obrigatória.

5 CONSIDERAÇÕES FINAIS

Este trabalho se propôs a analisar como a implementação dos controles da norma ABNT NBR ISO/IEC 27002:2013 pode auxiliar o setor público para atendimento aos requisitos da legislação vigente, considerando-se a análise dos requisitos do Marco Civil da

Internet e da Lei Geral de Proteção de Dados Pessoais. Após confrontação da norma com as referidas leis, verificou-se que dos 114 controles presentes na norma, oito atendem ao Marco Civil da Internet, ou seja, 7%. Por sua vez, dezessete controles atendem a Lei Geral de Proteção de Dados Pessoais (LGPD), ou seja, 15%.

Os principais resultados encontrados foram que tanto o Marco Civil da Internet quanto a Lei Geral de Proteção de Dados Pessoais encontram respaldo na norma NBR ISO/IEC 27002:2013, de modo que as organizações, sejam elas públicas ou privadas, podem beneficiar-se caso já tenham dispendido esforços para implantação da referida norma. Dessa forma, verificou-se que a adoção e implementação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado na série ISO/IEC 27000 poderá ajudar as organizações a atenderem os requisitos destas Leis. Além disso, abre-se também uma oportunidade para que novos controles sejam desenvolvidos e incorporados ao SGSI da organização.

Como contribuição deste trabalho, acredita-se que os resultados encontrados possam servir de subsídio para que as organizações enxerguem maior valor na adoção e implementação de um SGSI baseado na série ISO/IEC 27000. Em especial, num SGSI a ser implementado que considere a aplicação da norma NBR ISO/IEC 27002:2013, que dispõe de controles de segurança da informação amplamente aceitos e tidos como aderentes às melhores práticas. Isto porque estes controles podem permitir que sejam atendidos diversos requisitos do Marco Civil da Internet e da Lei Geral de Proteção de Dados Pessoais.

A Lei Geral de Proteção de Dados Pessoais (LGPD), que nasceu da Medida Provisória nº 869 de 27 de dezembro de 2018 e que foi aprovada como Projeto de Lei de Conversão pelo Congresso Nacional antes de seguir para sanção da Presidência da República, encontra-se no período de *vacatio legis*. Ou seja, a LGPD foi promulgada, mas ainda não entrou em vigor, o que significa que muitas organizações estão procurando adequar-se a esta nova realidade.

Para trabalhos futuros, propõe-se ampliar o escopo desta pesquisa discutindo novos controles que podem ser desenvolvidos e incorporados a um Sistema de Gestão de Segurança da Informação (SGSI). Isto permitirá também a criação de Sistema de Gestão de Privacidade da Informação (SGPI), com o objetivo de atender ao Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, além de outras leis que possam vir a serem promulgadas.

REFERÊNCIAS

Agostinelli, J. (2018). A Importância da Lei Geral de Proteção de Dados Pessoais no Ambiente Online. Anais do Encontro Toledo de Iniciação Científica Prof. Dr. Sebastião Jorge Chammé - Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente, v. 14, n. 14

Araújo, W. J. A. (2009). Segurança do Conhecimento nas Práticas da Gestão da Segurança da Informação e da Gestão do Conhecimento. Tese (Doutorado em Ciência da Informação). Brasília, Universidade de Brasília

Araújo, W. J. A. (2012). Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal. Informação & Sociedade: Estudos, 22, 13-24. Número Especial

Associação Brasileira de Normas Técnicas. (2020). *Tecnologia da informação – Técnicas de segurança – Estrutura de Privacidade* (NBR ISO/IEC 29100:2020). Rio de Janeiro. https://www.abntcatalogo.com.br/norma.aspx?ID=438365

Associação Brasileira de Normas Técnicas. (2019a). *Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes* (NBR ISO/IEC 27701:2019). https://www.abntcatalogo.com.br/norma.aspx?ID=437612

Associação Brasileira de Normas Técnicas. (2019b). *Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação* (NBR ISO/IEC 27005:2019). Rio de Janeiro. https://www.abntcatalogo.com.br/norma.aspx?ID=429058

Associação Brasileira de Normas Técnicas. (2018). *Tecnologia da informação – Governança da TI para a organização* (NBR ISO/IEC 38500:2018). https://www.abntcatalogo.com.br/norma.aspx?ID=408943

Associação Brasileira de Normas Técnicas. (2013a). *Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos* (NBR ISO/IEC 27001:2013). https://www.abntcatalogo.com.br/norma.aspx?ID=306580

Associação Brasileira de Normas Técnicas. (2013b). *Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação* (NBR ISO/IEC 27002:2013). https://www.abntcatalogo.com.br/norma.aspx?ID=306582

Neto, E. B. (2017, jan/abr). Transformações do Estado e a Administração Pública no século XXI. *Revista de Investigações Constitucionais*, Curitiba, v.4, n.1, p. 207-225

Braga, L. V., Alves, W. S., Figueiredo, R. M. C. & Santos, R. R. (2008, jan./mar.). O papel do governo eletrônico no fortalecimento da governança do setor público. *Revista do Serviço Público,* Brasília, DF, ano 59, n.1, p.5-21

Braga, S. S. (2007, Junho). Podem as novas tecnologias de informação e comunicação auxiliar na consolidação das democracias? Um estudo sobre a informatização dos órgãos legislativos na América do Sul. *Opinião Pública*, Campinas, v.13, n.1, p.1-50

Bueno, P. M. S., Ikuno, F. S., Araújo, A. S., Lima, J. N. O., Moreira, J. R. M. & Melo, L. A. V. (2015). Uma Iniciativa Para Aprimorar a Gestão de Riscos de Segurança da Informação na Administração Pública Federal. *In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, 15, 2015, Florianópolis. Anais. Florianópolis: Sociedade Brasileira de Computação, p.495-500

Canongia, C. & Mandarino, R. (2009, jul-dez). Segurança cibernética: o desafio da nova Sociedade da Informação. *Parceria Estratégica*. Brasília, DF, v.14, n.29, p.21-46

Dalfovo, M. S., Lana, R. A. & Silveira, A. (2008). Métodos quantitativos e qualitativos: um resgate teórico. *Revista Interdisciplinar Científica Aplicada*, v.2, n.4

Decreto nº 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7845.htm

Figueiredo, V. S. & Santos, W. J. L. (2013). Transparência e controle social na administração pública. *Revista Temas de Administração Pública*, FCL/Ar-Unesp, v.8, n.1

Fontes, E. (2012). *Políticas e Normas para a Segurança da Informação*. Editora Brasport, Rio de Janeiro

Gerhardt, T.E.; Silveira, D.T. (2009). *Métodos de Pesquisa*. Universidade Aberta do Brasil –UAB/UFRGS. Editora da UFRGS, Porto Alegre

Gonçalves, T. C. N. M.; Varella, M. D. (2018). Os desafios da Administração Pública na disponibilização de dados sensíveis. *Revista Direito GV*. v.14, n.2. p.513-536.

Hwang, M. S., Li, C. T.; Shen, J. J., Chu, Y. P. (2004). Challenges in E-Government and Security of Information. *Information & Security. An International Journal*. v.15, n.1, p.9-2

IT Governance Institute (ITGI). (2003). *Board Briefing on IT Governance.* Rolling Meadows, IL, USA.

Jardim, J. M. (2013). A implantação da lei de acesso à informação pública e a gestão da informação arquivística governamental. *Liinc em Revista*, v.9, n.2, p.383-405,

Laureano, M. A. P.; Moraes, P. E. S. (2005). Segurança como estratégia de gestão da informação. *Revista Economia & Tecnologia*, Paraná, v.8, n.3, p.38-44, jan./mar.

Leal, J. M.; Camuri, W. C. (2008). A Governança Corporativa e os Modelos Mundialmente Praticados. *Revista de Ciências Gerenciais*, Rio Claro, v.12, n.15, p.59-74.

Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

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

Marciano, J. L. P. (2006, julho) *Segurança da Informação – uma abordagem social*. Tese (Tese de Doutorado) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, DF

Marques, M. C. C. (2007, Junho). Aplicação dos princípios da governança corporativa ao sector público. *Revista de Administração Contemporânea*, Curitiba, v.11, n.2, p.11-26

Mulholland, C. S. (2018). 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*, v.19, n.3

Nieles M.; Dempsey, K.; Pillitteri, V. Y. (2017). An Introduction to Information Security. *National Institute of Standards and Technology Special Publication*, 800-12 Revision 1

Raminelli, F. P.; Rodegheri, L. B. (2016). A Proteção de Dados Pessoais na Internet no Brasil: Análise de decisões proferidas pelo Supremo Tribunal Federal. *Revista Cadernos do Programa de Pós-Graduação em Direito*. PPGDir/UFRGS

Reid, R. C.; Gilbert, A. H. (2010). Using the Parkerian Hexad to introduce security in an information literacy class. *In 2010 Information Security Curriculum Development Conference (InfoSecCD '10).* ACM, New York, NY, USA, 45-47

Santos, M. C. C. L. & Araujo, M. (2017). O Tempo e o Espaço. Fragmentos do Marco Civil da Internet: Paradigmas de Proteção da Dignidade Humana. *Revista Brasileira de Políticas Públicas*, v.7, n.3, p.160-183

Sêmola, M. (2003). *Gestão da Segurança da Informação – Uma visão executiva*. Editora Campus, Rio de Janeiro

Silva, J. F.; Albuquerque, C. R. S. (2018) Descrição e Modelagem Prática na Construção de uma Política de Segurança da Informação na Secretaria de Educação do Estado de Pernambuco. *Boletim do Tempo Presente*, n.12, p.87-105

Silva, L. F. C. P. (2010). *Gestão de Riscos em Tecnologia da Informação como fator crítico de sucesso na Gestão da Segurança da Informação dos órgãos da Administração Pública Federal: estudo de caso da Empresa Brasileira de Correios e Telégrafos – ECT.* Dissertação (Mestrado em Ciência da Informação) – Faculdade de Economia, Administração e Ciência da Informação e Documentação, Universidade de Brasília, Brasília, DF

Siqueira, A. H. (2012). *Arquitetura da informação: uma proposta para fundamentação e caracterização da disciplina científica*. Tese (Tese de Doutorado) – Faculdade de Ciência da Informação, Universidade de Brasília, Brasília, DF.

Soares, F. M.; Barros; L. M.; Faraj, N. A. (2008). Legimática: A Tecnologia da Informação Aplicada a Qualidade da Produção Legislativa. *Revista da Faculdade de Direito*, UFMG, n.5

Souza, J. G. S., Arima, C. H., Oliveira, R. M. N., Akabane, G. K. & Galegale, N. V. (2016, novembro). Gestão de Riscos de Segurança da Informação numa Instituição Pública Federal: um estudo de caso. *Revista ENIAC Pesquisa*, v.5, n.2, p.240-256

Souza, L. R. M. (2018). Proteção de Dados Pessoais: Estudo Comparado do Regulamento 2016/679 do Parlamento Europeu e Conselho e o Projeto de Lei Brasileiro N. 5.276/2016. *Caderno Virtual da Escola de Direito e Administração Pública do IDP*, v.1, n.41

Stallings, W. & Brown, L. (2018). *Computer Security: Principles and Practice*. Pearson Education, New Jersey, 4th Edition

Szmit, M.; Szmit, A. (2015). Risk Management in NIST and ISO/IEC 27K Information Security Management Standards' Family - a Brief Analysis. *Mechanics Transport Communications*. volume 13, issue 3/1, Poland

Vieira, G. S. (2018, mar). Governo eletrônico brasileiro: ações de integração entre sistemas de governo e sociedade. *Multi-Science Journal*, [S.l.], v.1, n.4, p.24-33

Zaganelli, J. C.; Miranda, W. V. (2017). Marco Civil da Internet e Política Pública de Transparência: Uma Análise da e-Democracia e do Compliance Público. *Revista Brasileira de Políticas Públicas*, Brasília, v.7, n.3, p.633-646.