Conformidade com a norma ABNT ISO/IEC 27001-2006: um estudo de caso sobre a implementação de Sistema de Gestão da Segurança da Informação

COMPLIANCE WITH ABNT ISO/IEC 27001-2006: A CASE STUDY ON THE IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

Salomão Neves Filho
salomaaoneves2@gmail.com
http://lattes.cnpq.br/5105457957975964
https://orcid.org/0009-0003-8763-438X
Mestre em Ciência da Informação pela Universidade Federal da Paraíba (UFPB), especialista em Gestão de Pessoas pelo Centro Universitário de João Pessoa (UNIPÊ) e graduado em Administração pela UFPB. Atualmente, é facilitador de dinâmica de grupo pelo Centro de Dinâmica de Grupo e Relações Humanas de Recife.

Sânderson Lopes Dorneles
sanderson.dorneles@gmail.com
http://lattes.cnpq.br/5413452412570612
https://orcid.org/0000-0002-3888-2841
Mestre em Ciência da Informação pela Universidade Federal de Pernambuco (UFPE), especialista em Arquivo e Patrimônio pela Universidade Salgado de Oliveira e bacharel em Arquivologia pela Universidade Federal de Santa Maria (UFSM). Atualmente, é professor do curso de Arquivologia da Universidade Estadual da Paraíba (UEPB) e arquivista do Instituto Federal da Paraíba (IFPB).

Submetido: 25 set. 2024
Publicado: 02 nov. 2024

RESUMO
Os modelos de gestão das organizações têm passado principalmente a partir de 1990, por fortes processos de inovação tecnológica, impulsionados pelo aceleramento da globalização. Executivos e gestores necessitam de soluções rápidas diante de um mundo cada vez mais globalizado. Neste contexto, a Gestão da Segurança da Informação, a qual exerce um papel extremamente importante no ambiente organizacional, está voltada a proteger a informação das constantes ameaças digitais do ambiente externo. Esta pesquisa tem como objetivo verificar a conformidade de um supermercado com os requisitos da norma 27001 da Associação Brasileira de Normas Técnicas do ano de 2006, especialmente no que tange à existência, à implementação de um Sistema de Gestão da Segurança da Informação e à Política de Segurança da Informação. A pesquisa se caracteriza como descritiva com estudo de caso e abordagem qualitativa. Os instrumentos de coleta de dados foram um questionário aplicado junto à Gerência de Tecnologia da Informação e um *checklist* aplicado à Coordenação de Recursos Humanos do supermercado objeto de estudo. Os resultados apontam que, apesar do supermercado adotar algumas ações de prevenção, não foi encontrado uma Política de Segurança da Informação, como também a ausência de um Sistema de Gestão da Segurança da Informação, conforme estabelece a referida norma nos itens A.5 e A.8. Para tanto, sugere-se à direção do supermercado, inserir em seu planejamento estratégico uma Política de Segurança da Informação, e tornar o supermercado menos vulnerável os ataques digitais vindos do ambiente externo.
PALAVRAS-CHAVE: Política de Segurança da Informação; Sistema de Gestão de Segurança da Informação; norma técnica.

ABSTRACT
Since the 1990s, the management models of organizations have undergone strong processes of technological innovation, driven by the acceleration of globalization. Executives and managers need quick solutions in the face of an increasingly globalized world. In this context, Information Security Management, which plays an extremely important role in the organizational environment, is geared towards protecting information from the constant digital threats of the external environment. This research aims to verify the compliance of a supermarket with the requirements of standard 27001 of the Brazilian Association of Technical Standards of 2006, especially with regard to the existence and implementation of an Information Security Management System and Information Security Policy. The research is characterized as descriptive with a case study and qualitative approach. The data collection instruments were a questionnaire applied to the Information Technology Manager and a checklist applied to the Human Resources Coordinator of the supermarket under study. The results show that, although the supermarket adopts some preventative actions, it was not found to have an Information Security Policy, nor was it found to have an Information Security Management System, as established by the aforementioned standard in items A.5 and A.8. To this end, it is suggested that the supermarket's management include an Information Security Policy in its strategic planning, and make the supermarket less vulnerable to digital attacks from the external environment.
KEYWORDS: Information Security Policy; Information Security Management System; technical standard.

1 INTRODUÇÃO

Os modelos de gestão nas organizações passaram, principalmente a partir da década de 1990, por intensos processos de inovação tecnológica, impulsionados pela aceleração da globalização. Esse cenário exige que gestores e executivos desenvolvam soluções rápidas para alavancar a competitividade e o sucesso empresarial. Nesse contexto, a Gestão da Segurança da Informação destaca-se pelo seu papel fundamental no ambiente organizacional, sendo a sua principal função proteger as informações contra ameaças à integridade, à disponibilidade e à confidencialidade. Além disso, é responsabilidade dessa gestão zelar pela segurança e pela proteção do ambiente informacional (Mascarenhas Neto; Araújo, 2019). Santos e Baldini Filho (2013) destacam que a proteção eficaz das informações contra ameaças externas está diretamente relacionada à implementação de políticas, aos processos e às normas que sustentam a Gestão da Segurança da Informação.

A informação, quando utilizada estrategicamente pelas organizações, é um fator determinante para o sucesso, mas, se mal gerida, pode comprometer o ambiente corporativo. Araújo (2016) enfatiza a importância da informação como um insumo essencial, ressaltando que, se for especializada desde sua origem até seu uso, está apta a completar todo o ciclo de vida, mesmo diante de eventuais problemas no processo, como dificuldades no uso ou circulação devido ao volume físico.

Atualmente, existem diversas normas nacionais e internacionais que tratam da Segurança da Informação, orientando atividades que visam tornar os sistemas mais seguros. Destacam-se, em particular, as normas da *International Organization for Standardization* (ISO) / *International Electrotechnical Commission* (IEC) da família 27000 e as versões brasileiras da Associação Brasileira de Normas Técnicas (ABNT) (Santos; Baldini Filho, 2013).

Nesse contexto, suscita-se a seguinte questão problema de pesquisa: Como uma organização implementa e gerencia um Sistema de Gestão da Segurança da

Informação (SGSI) conforme os requisitos da norma ABNT ISO/IEC 27001 (ABNT, 2006)?

Sendo assim, esta pesquisa tem como objetivo verificar a conformidade de um supermercado com os requisitos da norma ABNT ISO/IEC 27001 (ABNT, 2006), especialmente, no que tange à existência, à implementação de um Sistema de Gestão da Segurança da Informação (SGSI) e à Política de Segurança da Informação. Como objetivos específicos, busca-se avaliar o nível de conformidade do supermercado com os requisitos da norma ABNT ISO/IEC 27001 (ABNT, 2006) no que diz respeito à Segurança da Informação; identificar vulnerabilidades e falhas nos processos de gestão da Segurança da Informação do supermercado, tanto no setor de Tecnologia da Informação (TI) quanto no de Recursos Humanos; e analisar o nível de conscientização dos colaboradores sobre a Política de Segurança da Informação, a fim de sugestões de melhorias nas práticas de segurança e no treinamento de colaboradores.

O supermercado em questão está localizado em João Pessoa, Paraíba, e foi inaugurado no ano de 2019. Sua diretoria é composta por Presidente, Diretor Comercial e Diretor Administrativo. A comunicação entre os colaboradores é feita por grupos de *WhatsApp*, de ouvidoria e de pesquisas de clima organizacional. O processo seletivo é realizado tanto internamente quanto, externamente, utilizando-se a rede social *Instagram*, o Sistema Nacional de Emprego (SINE) e um *site* de vagas. Atualmente, a empresa conta com 80 colaboradores.

O setor supermercadista brasileiro tem crescido aceleradamente desde o final dos anos 1990 até as últimas décadas do século XXI, impulsionado pela globalização de produtos e de serviços. Isso elevou o consumidor de mero espectador a protagonista, permitindo-lhe maior liberdade de escolha sobre os produtos de consumo. O Brasil tem se destacado em investimentos em alta tecnologia no setor, posicionando-se entre os países que mais investem em redes de supermercados de médio e de grande porte. Segundo Gobacklog (2020), entre as 500 maiores empresas do setor hipermercadista no Brasil, a média de faturamento por loja foi de 34 milhões em 2018, evidenciando o esforço dessas organizações em acompanhar as mudanças digitais em um mercado altamente competitivo. Entretanto, Mascarenhas Neto e Araújo (2019) alertam que, embora os recursos tecnológicos e as ferramentas de comunicação instantânea aumentem a produtividade e resolvam problemas, muitas organizações ainda negligenciam as vulnerabilidades e ameaças a que estão expostas.

Nesse cenário, o setor de Recursos Humanos das redes de supermercados desempenha uma dupla missão. Primeiramente, deve se alinhar com a alta administração e a Gerência de Tecnologia da Informação para promover a disseminação da Política de Segurança da Informação entre os colaboradores. Em segundo lugar, se houver interesse em certificações, é responsabilidade do RH garantir o cumprimento dos requisitos do Sistema de Gestão da Segurança da Informação, com especial atenção à Norma ABNT ISO/IEC 27001 (ABNT, 2006), no que tange à segurança dos Recursos Humanos.

2 MARCO TEÓRICO CONCEITUAL

Como base para o referencial teórico, está estruturado em quatro cenários principais. O primeiro cenário aborda a gestão da informação no contexto corporativo. O segundo traz a Segurança da Informação, com ênfase nas políticas organizacionais relacionadas. No terceiro, apresenta um panorama sobre a norma ABNT ISO/IEC 27001 (ABNT, 2006), que estabelece diretrizes para a Gestão da

Segurança da Informação em organizações. Por fim, o quarto cenário cita a legislação brasileira referente à Segurança da Informação.

2.1 A INFORMAÇÃO NO AMBIENTE CORPORATIVO

Não é de hoje que a informação no ambiente das organizações vem sendo pesquisada, a partir notadamente dos anos 1980 ou mesmo no terceiro milênio. Diversos autores da comunidade acadêmica, em particular, os vinculados com a Ciência da Informação, vem se debruçando a fim de disseminar aquela que tem sido responsável não só pelo desenvolvimento de novas tecnologias, mas ao fenômeno que se propagou, nas mais diversas civilizações.

> Dentro de um contexto histórico, evidenciou-se, nas mais diversas civilizações, a preocupação eminente de salvaguardar as informações. Por exemplo, na China antiga, a linguagem escrita era reservada a membros pertencentes à classe superior que exerciam o direito de aprender a ler e a escrever. Essa mesma civilização utilizava duas formas distintas de registrar suas informações, conforme seu grau de importância: a escrita demótica, utilizada para os assuntos do cotidiano, e a hieroglífica, mais complexa e formada por desenhos e símbolos, era usada para informações consideradas restritas a um grupo de pessoas (Mascarenhas Neto; Araújo, 2019 p. 14).

Para Barbosa (2008), o desenvolvimento das Tecnologias de Informação e Comunicação se propagou a tal ponto de ser inegável e ao mesmo tempo irreversível o ser humano não possua celulares, *tablets* e outros aparelhos de comunicação, fruto da disseminação da informação tanto para as pessoas, quanto para as organizações.

> Devido a sua crescente importância para as organizações contemporâneas, a informação e o conhecimento, tem merecido, cada vez mais, a atenção de gestores, de profissionais e pesquisadores. O contínuo desenvolvimento das tecnologias da informação e comunicação (TICs) tem potencializado a produção e disseminação de informações em escalas inimagináveis há pouco tempo atrás. É inegável que as redes de comunicação, que hoje em dia integram não apenas computadores pessoais, mas também telefones celulares e diversos outros aparelhos, tem sido incorporados, de forma irreversível, nos mais diversos aspectos dos afazeres humanos. Do lado da demanda, tanto para as pessoas quanto para as organizações, a obtenção e uso da informação tornam-se cada vez mais, processos críticos para o seu desempenho (Barbosa, 2008, p. 02).

Na visão de Santos e Baldini Filho (2013), a informação significa valor para a sociedade, sejam nas organizações públicas ou privadas. Contudo, o crescimento das vulnerabilidades e das ameaças aos sistemas de informação aflorou a necessidade da implantação de ações para proteção do patrimônio digital das organizações. A ABNT ISO/IEC 27002 (ABNT, 2005) trata a informação como um ativo muito importante, e por este motivo, precisa ser protegida, sendo indispensável no mundo dos negócios. Com o crescente volume da interconectividade, a informação passa a ficar totalmente exposta a vários tipos de vulnerabilidade.

2.2 A SEGURANÇA DA INFORMAÇÃO E SUA POLÍTICA NAS ORGANIZAÇÕES

A Segurança da Informação pode ser entendida como um conjunto de procedimentos que venham a intervir na sua preservação, no intuito de blindar as

organizações aos riscos de ameaças cibernéticas as quais ficam expostas diariamente. Segundo a ABNT ISO/IEC 17799 (ABNT, 2005), a Segurança da Informação está alicerçada em proteger a informação de ameaças constantes, para poder garantir o sucesso e ao mesmo tempo poder emergir novos investimentos e oportunidades do negócio.

> A Segurança da Informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio (ABNT ISO/IEC 17799, 2005, p. 9.).

O Tribunal de Contas da União – TCU (2013) define que a Segurança da Informação tem como objetivo garantir a integridade, a confidencialidade, a autenticidade e a disponibilidade das informações processadas, sejam de instituições públicas ou privadas; essas garantias estão diretamente relacionadas a controles de acesso.

A Política de Segurança da Informação deve ser tratada como área estratégica da organização, percorrendo um paralelo constante com a alta direção. Para ser implantada, faz-se necessário um planejamento organizacional com o aval do corpo gestor (diretores e gerentes).

Segundo o Tribunal de Contas da União (2013), a Política de Segurança da Informação não deve ficar apenas na Tecnologia da Informação, e sim, totalmente incorporada com a missão e com a visão e as metas da organização. O seu conteúdo varia muito da tipologia de cada empresa e de sua área de atuação. Abaixo, relacionamos alguns tópicos que o TCU (2013) considera indispensável para o bom desempenho da Política de Segurança da Informação:

- definição e disseminação na organização;
- declaração que conste o apoio da alta administração;
- definição das responsabilidades na gestão da Segurança da Informação;
- análise da gestão de riscos;
- conformidade com os sistemas computacionais com a Política de Segurança da Informação;
- políticas de controle de acesso a recursos e sistemas;
- procedimentos de detecção de vírus;
- consequências de violação de normas;
- direitos de propriedade (de produção, software, normas legais)
- plano de treinamento em Segurança da Informação.

Sendo assim, a implementação de uma Política de Segurança da Informação eficaz depende diretamente de um alinhamento estratégico entre a alta direção e os demais setores da organização. Além disso, é fundamental que essa política esteja completamente integrada aos objetivos e à cultura institucional, conforme destacado pelo Tribunal de Contas da União (2013). A inclusão de tópicos essenciais como a gestão de riscos, o controle de acesso, e a conformidade com normas legais, reforça a necessidade de um planejamento minucioso e contínuo, que assegure tanto a proteção dos ativos informacionais quanto à conformidade com as exigências legais e operacionais da organização.

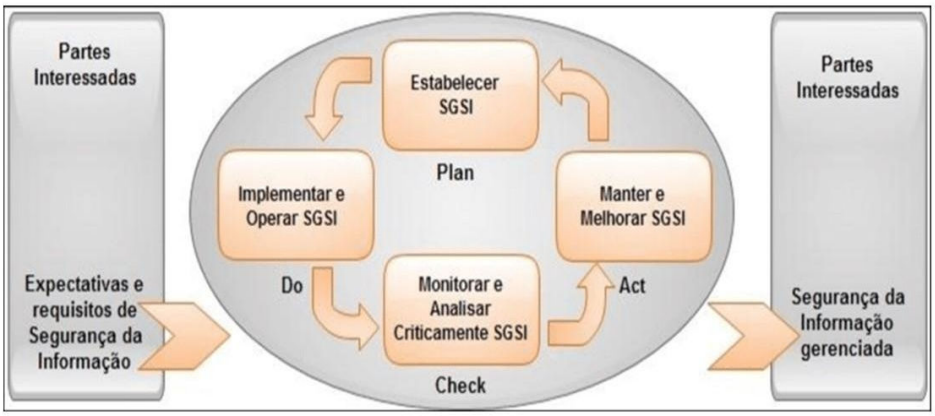
2.3 NORMA ABNT ISO/IEC 27001:2006 E O SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A Associação Brasileira de Normas Técnicas (ABNT) implantou uma série de normas que abrangem a Segurança da Informação. A série de normas ficaram conhecidas como família ISO 27000 e abrangem a adoção de políticas de Segurança da Informação, como também a implantação de Sistemas de Gestão da Segurança da Informação nas organizações. Esta pesquisa tomou por base o arcabouço teórico da ABNT ISO/IEC 27001 (ABNT, 2006), a qual trata da implantação de um Sistema de Gestão da Segurança da Informação (SGSI).

Essa norma tem como objetivo principal definir requisitos para a implementação, a operação, o monitoramento, a análise crítica, a manutenção e a melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI), documentado no contexto dos riscos inerentes aos negócios da organização. Como também adota o modelo *Plan, Do, Check, Act* (PDCA) que, em português, significa Planejar, Fazer, Checar, Agir, para assim estabelecer todos os passos que as organizações devem tomar, ao decidirem implantar um SGSI.

De acordo com Mendes *et al.* (2013), a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) deve estar alinhada à estrutura organizacional, às prioridades estratégicas e às necessidades específicas da organização. Além disso, o SGSI precisa ser flexível e adequado à complexidade dos problemas de segurança que surgirem, de modo que questões menos complexas possam ser tratadas com soluções igualmente simples. Esses aspectos são relatados e demonstrados na Figura 1 por Mendes *et al.* (2013):

Figura 1: Ciclo PDCA no SGSI



Fonte: Mendes *et al.* (2013).

A imagem representa o ciclo PDCA e é aplicado à gestão de um Sistema de Gestão de Segurança da Informação (SGSI).

O ciclo inicia com a fase de Planejar (*Plan*), na qual se estabelece o SGSI, definindo políticas, objetivos e processos para garantir a Segurança da Informação, em conformidade com as expectativas e requisitos das partes interessadas. Em seguida, Fazer (*Do*), quando se implementa e opera a política, os controles, os processos e os procedimentos do SGSI; Checar (*Check*) o desempenho do SGSI é monitorado e analisado criticamente para medir o desempenho de um processo frente à política, aos objetivos e à experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção. Por fim, na fase de Agir (*Act*), são realizadas melhorias no sistema com base nas análises, garantindo a continuidade e a

evolução da Segurança da Informação.

Nas laterais da imagem, são destacadas as partes interessadas, que fornecem os requisitos iniciais, e o resultado final do ciclo, que é a Segurança da Informação gerenciada de maneira eficaz.

2.4 LEGISLAÇÃO BRASILEIRA DE SEGURANÇA DA INFORMAÇÃO

Ao longo de sua trajetória, a Segurança da Informação e os Sistemas de Gestão da Segurança da Informação têm sido respaldados não apenas pelas normas da Associação Brasileira de Normas Técnicas, mas também por dispositivos da legislação brasileira, incluindo decretos, leis, normativas e diretrizes do Gabinete de Segurança Institucional da Presidência da República.

Dentro da evolução histórica da Segurança da Informação no Brasil, verifica-se no Quadro 1 alguns dos atos normativos de extrema importância, que clarificam, a guarda, o sigilo e a proteção dos dados, principalmente voltados para a Segurança da Informação nas organizações.

Quadro 1: Evolução histórica da Segurança da Informação no Brasil

Nº	ANO	ATO NORMATIVO	DESCRIÇÃO
1	1988	Art. 5º, Inciso XXXIII da Constituição Federal, de 5 de outubro de 1988 (Brasil, 1988)	Reforça o princípio da transparência pública e a responsabilidade dos órgãos públicos no fornecimento de informações, exceto quando for necessário o sigilo em casos que envolvem a segurança do Estado e da sociedade.
2	2002	Decreto nº 4.553, de 27 de dezembro de 2002	Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado. **Obs.:** Revogado pelo Decreto nº 7.845/2012.
3	2011	Lei nº 12.527, de 18 de novembro de 2011 (Brasil, 2011)	Regula o acesso à informação (Lei de Acesso à Informação).
4	2012	Decreto nº 7.845, de 14 de novembro de 2012 (Brasil, 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.
5	2014	Lei nº 12.965, de 23 de abril de 2014 (Brasil, 2014)	Lei do Marco Civil na Internet, estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.
6	2018	Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018)	Lei Geral de Proteção de Dados para proteger os direitos fundamentais de liberdade e de privacidade.
7	2020	Decreto nº 10.222, de 5 de fevereiro de 2020 (Brasil, 2020)	Aprova a estratégia Nacional de Segurança Cibernética
9	2021	Decreto nº 10.641, de 2 de março de 2021 (Brasil, 2021)	Altera o decreto que institui a Política Nacional de Segurança da Informação
10	2022	Medida Provisória nº 1.124, de 13 de junho de 2022 (Brasil, 2022a)	Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados, em autarquia de natureza especial e transforma cargos em comissão. **Obs.:** Convertida na Lei nº 14.460/2022.
11	2022	Lei nº 14.460, de 25 de outubro de 2022 (Brasil, 2022b)	Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019.

Fonte: Elaborado pelos autores (2023).

No quadro, é destacada a evolução das normas brasileiras relacionadas à transparência, proteção de dados e segurança digital. Desde a Constituição de 1988, que garante o direito de acesso à informação, até a Lei Geral de Proteção de Dados (LGPD) de 2018. O Brasil tem avançado na regulamentação do acesso à informação pública, na proteção da privacidade dos cidadãos e no fortalecimento da segurança cibernética. Medidas como o Marco Civil da Internet em 2014 e decretos que estabelecem estratégias de segurança digital reforçam o compromisso do país com a governança digital e a proteção de dados.

3 PERCURSO METODOLÓGICO

Quanto ao tipo de pesquisa, este estudo enquadra-se como descritivo e baseado em um estudo de caso, alinhando-se aos objetivos propostos do presente estudo. A pesquisa descritiva visa a retratar as práticas e os procedimentos adotados para a Gestão da Segurança da Informação em um supermercado.

Conforme Gil (2009, p. 42), "[...] as pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou manifestação ou, então, o estabelecimento de relações entre variáveis". Nesse sentido, o estudo tem como foco descrever o grau de conformidade da organização com os requisitos da norma ABNT ISO/IEC 27001 (ABNT, 2006), com especial atenção à implementação de um Sistema de Gestão da Segurança da Informação (SGSI) e à Política de Segurança da Informação.

A pesquisa busca identificar falhas e vulnerabilidades nos setores de Tecnologia da Informação (TI) e Recursos Humanos (RH), além de avaliar o nível de conscientização dos colaboradores em relação às suas responsabilidades e à gestão de riscos.

O estudo de caso, por sua vez, caracteriza-se pela exploração aprofundada de um contexto específico, permitindo uma análise detalhada das práticas e dos desafios enfrentados pela organização. Segundo Gil (2009, p. 54), o estudo de caso oferece as seguintes vantagens:

> a) explora situações da vida real cujos limites não estão claramente definidos;
> b) preserva a unidade do objeto de estudo;
> c) descreve o contexto no qual a investigação é realizada;
> d) permite a formulação de hipóteses ou o desenvolvimento de teorias; e
> e) explica as variáveis causais de fenômenos complexos, para os quais levantamentos e experimentos não são adequados.

Dessa forma, a combinação da pesquisa descritiva com o estudo de caso proporciona uma visão ampla e detalhada do cumprimento da norma ABNT ISO/IEC 27001 (ABNT, 2006), além de permitir a identificação de melhorias na gestão da Segurança da Informação.

No que se refere a abordagem, esta pesquisa configura-se como qualitativa, pelo fato de não ser necessário dados numéricos, pois a pesquisa qualitativa é fundamentada no conhecimento de como se comporta determinado grupo social. Minayo (2016) relata que a pesquisa qualitativa não responde a dados quantitativos, estando alicerçada na dinamicidade e na motivação de como se apresenta determinado grupo social, justamente porque no universo do ser humano, existe um mundo de relações e representações.

Para o levantamento de dados, foram elaborados dois instrumentos baseados

na ABNT ISO/IEC 27001 (ABNT, 2006). Esses instrumentos consistem em um questionário, respondido por um analista de Tecnologia da Informação (TI), a fim de identificar a Política de Segurança da Informação do supermercado (Apêndice A), e um *checklist* com nove questões, respondido pela Coordenadora de Recursos Humanos do supermercado (Apêndice B). É importante destacar que tanto o *checklist* quanto o questionário buscaram verificar se o supermercado possui uma Política de Segurança da Informação, bem como um Sistema de Gestão da Segurança da Informação.

4 ANÁLISE E DISCUSSÃO DOS RESULTADOS: QUESTIONÁRIO APLICADO AO ANALISTA DE TECNOLOGIA DA INFORMAÇÃO

O questionário contou com oito perguntas que foram baseadas no Anexo A, item A.5, relativa à Política de Segurança da Informação da ABNT ISO/IEC 27001 (ABNT, 2006). O intento deste questionário foi detectar ou não a existência de um Sistema de Gestão da Segurança da Informação, conforme o que preestabelece a ABNT ISO/IEC 27001 (ABNT, 2006) como também evidenciar se o supermercado possui uma Política de Segurança da Informação.

Das oito perguntas formuladas, o respondente poderia assinalar um “X” nas respostas de sim, parcialmente, ou não (ver Apêndice A). Foram obtidas uma resposta negativa e sete respostas positivas.

A principal questão (que foi a pergunta número um) se o supermercado possuía um manual explicativo contendo a Política de Segurança da Informação, a qual a resposta foi negativa, já demonstra de alguma forma a fragilidade do supermercado quanto às ameaças cibernéticas do ambiente externo e, ao mesmo tempo, expõe a ausência de conscientização e de normalização que poderia conter em um manual de Política de Segurança da Informação. Isso evidencia também a ausência de um Sistema de Gestão da Segurança da Informação, conforme estabelece a ABNT ISO/IEC 27001 (ABNT, 2006).

As demais perguntas, embora todas as respostas sejam 'sim', apresentam certa repetição. Em particular, chama a atenção o fato das justificativas para as respostas da terceira e quarta perguntas serem idênticas, o que prejudica a percepção do compromisso da Direção do supermercado em preservar e em proteger seus sistemas de TI.

Importante registar que o SGSI do Supermercado é terceirizado, cabendo ao analista de TI a sua monitoração e operacionalidade. Por outro lado, percebe-se pelas respostas da segunda até a oitava questão que o analista de TI e a Direção do supermercado (ao que se apresenta), fazem análise de riscos mensalmente, se preocupam com os acordos de confidencialidade, e se atentam a proteção de senhas, e aos riscos vindos do ambiente externo.

4.1 *CHECKLIST* COM A COORDENAÇÃO DO RECURSOS HUMANOS

Elaborou-se um *checklist*, que foi enviado para ser respondido pela Coordenação de Recursos Humanos (ver Apêndice B). Esse instrumento possibilitou evidenciar ou não, se a área de Recursos Humanos está empenhada em seguir o estabelecido no Anexo 1, item A.8, referente à Segurança em Recursos Humanos da norma ABNT ISO/IEC 27001 (ABNT, 2006), que trata do Sistema de Gestão de Segurança da Informação (SGSI).

O *checklist* foi estruturado com nove questões, divididas em três questões sobre as responsabilidades antes da contratação de pessoal, três questões a respeito das responsabilidades durante a contratação e mais três questões em relação a rescisão do contrato ou mudança na contratação. A respondente teria que marcar com um "X" em sim, parcialmente ou não, e também foi criada uma coluna de observações.

Das nove questões do *checklist*, obtiveram-se cinco respostas como sim e quatro respostas como não.

As respostas positivas evidenciaram:

- que a organização faz avaliação do candidato, analisando o seu currículo e os empregos anteriores;
- caso o empregado cometa erro grave que comprometa a Segurança da Informação da organização, o mesmo sofre uma advertência disciplinar;
- caso o empregado seja desligado, a Coordenação de Recursos Humanos prepara o processo de desligamento, onde são clarificados direitos e deveres;
- que o empregado desligado devolve a organização, farda, equipamentos de proteção individual entre outros ativos;
- que, após o desligamento, é retirado do empregado o seu acesso, seja e-mails, senhas, crachá, bem como o acesso a informações privativas da organização.

As respostas negativas evidenciaram que:

- a organização não possui uma cartilha com a Política de Segurança da Informação conforme preestabelece a ABNT ISO/IEC 27001 (ABNT, 2006), para que o colaborador entenda suas responsabilidades, podendo abrandar os riscos de fraude e roubo;
- o empregado selecionado assina seu contrato de trabalho, porém, desconhece a sua responsabilidade perante a Segurança da Informação;
- a Coordenação de Recursos Humanos não incentiva os empregados a disseminarem a Segurança da Informação, como forma de prevenir ameaças e falhas humanas;
- os empregados não recebem educação continuada referente a suas funções, como não são conscientizados das políticas da organização.

Pelas respostas que foram analisadas no *checklist*, conclui-se que o supermercado, apesar de estabelecer algumas responsabilidades que de certa forma protege a sua Segurança da Informação, o mesmo não atende totalmente o Anexo 1, item A.8, que diz respeito à Segurança em Recursos Humanos da norma ABNT ISO/IEC 27001 (ABNT, 2006), não sendo evidenciada a existência de uma Política de Segurança.

5 CONSIDERAÇÕES FINAIS

As organizações que se destacam e permanecem competitivas no mercado atual encontram na estrutura de suas operações um componente essencial: uma Política de Segurança da Informação robusta. Sem ela, as empresas se tornam vulneráveis a inúmeras ameaças digitais, fato que se reflete no Brasil sendo o quinto país mais afetado por crimes cibernéticos no mundo (iG Tecnologia, 2023).

Diante desse cenário, a Associação Brasileira de Normas Técnicas (ABNT) desempenha um papel crucial, ao promover a certificação das empresas em diversas áreas técnicas, incluindo os sistemas de gestão da Segurança da Informação. A norma ABNT ISO/IEC 27001 (ABNT, 2006), que foi o foco desta pesquisa, estabelece

diretrizes claras para a criação e manutenção de um sistema de segurança eficaz, essencial para mitigar os riscos internos e externos.

A pesquisa desenvolvida visou verificar a conformidade de uma empresa supermercadista com os itens A.5 e A.8 da referida norma, que tratam da Política de Segurança da Informação e da Segurança em Recursos Humanos, respectivamente. Para tanto, foram aplicados instrumentos de coleta de dados, como questionário e *checklist*, que permitiram diagnosticar a ausência de uma política formalizada de Segurança da Informação.

Os resultados demonstraram que, apesar de alguns esforços pontuais para garantir a segurança digital, a ausência de uma Política de Segurança da Informação estruturada expõe o supermercado a vulnerabilidades significativas. Assim, recomenda-se que a direção da empresa inclua em seu planejamento estratégico a criação e implementação de uma política dessa natureza, mesmo que inicialmente não almeje a certificação ISO/IEC 27001. Esse passo fortaleceria a empresa contra ameaças cibernéticas, tornando-a menos suscetível a danos materiais e financeiros.

Esta pesquisa, portanto, contribuiu para a formulação de ferramentas de diagnóstico baseadas na norma ABNT ISO/IEC 27001 (ABNT, 2006), que podem ser aplicadas não só ao setor de supermercados, mas também a outras organizações. A adoção de um Sistema de Gestão da Segurança da Informação permite não só proteger os ativos digitais da empresa, mas também criar uma cultura de segurança entre os colaboradores, minimizando riscos operacionais e maximizando a eficiência organizacional.

REFERÊNCIAS

ARAÚJO, S. G. L. **A dimensão humana no processo de Gestão da Segurança da Informação**: um estudo aplicado à Pró-Reitoria de Gestão de Pessoas da Universidade Federal da Paraíba. Dissertação (Mestrado em Ciência da Informação). João Pessoa: Universidade Federal da Paraíba, 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT ISO/IEC 17799:** 2005 - Tecnologia da informação – Código de prática para a gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**: 2005 - Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão de Segurança da Informação. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: 2006 - Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2006.

BARBOSA, R. R. Gestão da Informação e do Conhecimento: origens, polêmicas e perspectivas. **Informação & Informação**, Londrina, v. 13, n. esp., p. 1-25, 2008. Disponível em: http://www.uel.br/revistas/uel/index.php/informacao/article/view/1843. Acesso em: 12 jan. 2023.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de

1988. **Diário Oficial da União**, Brasília, DF, 05 out. 1988.

BRASIL. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 30 dez. 2002.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. **Diário Oficial da União**, Brasília, DF, 18 nov. 2011.

BRASIL. Decreto n.º 7.845, de 14 de novembro de 2012. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. **Diário Oficial da União**, Brasília, DF, 16 nov. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. **Diário Oficial da União**, Brasília, DF, 06 fev. 2020.

BRASIL. Decreto nº 10.641, de 2 de março de 2021. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. **Diário Oficial da União**, Brasília, DF, 03 mar. 2021.

BRASIL. Medida Provisória nº 1.124, de 13 de junho de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. **Diário Oficial da União**, Brasília, DF, 14 jun. 2022a.

BRASIL. Lei nº 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de julho de 2019. **Diário Oficial da União**, Brasília, DF, 26 out. 2022b.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4. ed. 13 reimpr. São Paulo: Atlas, 2009.

GOBACKLOG. **Varejo supermercadista e perspectiva sobre o crescimento no Brasil**. [*S.l.*]: Gobacklog.com, 2020. Disponível em: https://www.gobacklog.com/varejo-supermercadista. Acesso em: 11 jan. 2023.

IG TECNOLOGIA. **Brasil é o 5º país do mundo mais afetado por crimes cibernéticos**. [*S.l.*]: iG Tecnologia, 2023. Disponível em: https://tecnologia.ig.com.br/2023-04-15/brasil-quinto-pais-mais-afetado-crimes-ciberneticos.html. Acesso em: 29 set. 2024.

MASCARENHAS NETO, P. T.; ARAÚJO, W. J. **Segurança da Informação:** uma visão sistêmica para implantação nas organizações. João Pessoa: Editora da UFPB, 2019.

MENDES, R. R. *et al*. Uma metodologia para implantação de um Sistema de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002. **Revista Principia,** João Pessoa, nº 22, p. 69-80, 2013. Disponível em: https://periodicos.ifpb.edu.br/index.php/principia/article/view/158/128. Acesso em: 16 jan. 2023.

MINAYO, Cecília de Souza. **Pesquisa social**: teoria, método e criatividade. Petrópolis: Vozes, 2016;

SANTOS, V. O. dos; BALDINI FILHO, R. Um modelo de Sistema de Gestão da Segurança da Informação baseado nas normas ABNT NBR ISO/IEC 27001: 2006, 27002:2005 e 27005: 2008. **Revista de Telecomunicações**, [*S.l.*], v. 15, n. 1, p. 1-6, 2013. Disponível em: https://www.inatel.br/revista/busca/288-um-modelo-de-sistema-de-gestao-da-seguranca-da-informacao14301-s147497-1/file. Acesso em: 16 jan. 2023.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Boas práticas em Segurança da Informação**. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2013.

APÊNDICE A - QUESTIONÁRIO APLICADO À GERÊNCIA DE TI DO SUPERMERCADO

"SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO ABNT NBR 27001"
QUESTIONÁRIO APLICADO COM O ANALISTA DE TI DE UM SUPERMERCADO LOCALIZADO NA CIDADE DE JOÃO PESSOA
Fonte: ABNT NBR 27001 – A.5.1 – Política de Segurança da Informação

1 – O Supermercado possui uma cartilha ou um manual com a Política de Segurança da Informação, aprovado pela Direção e comunicado a todos os funcionários e partes externas interessadas?
Sim ( ) Parcialmente ( ) Não (X)
Justifique: Toda permissão que o pessoal externo necessite tem que ser avaliada pela empresa especialista em segurança que o supermercado contratou, porém não conheço um manual com a Política de Segurança da Informação.

2 – A Política de Segurança da Informação é analisada criticamente em períodos semanais ou mensais ou quando de mudanças em decorrência de novos processos a fim de assegurar a sua eficácia?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Analisamos Mensalmente, para evitar riscos futuros a empresa e sempre que temos novos processos, para melhorar a eficácia.

3 – A Direção apoia efetivamente a Segurança da Informação no Supermercado, por meio de ações que externem seu comprometimento e direcionando atribuições de forma clara?
Sim (X) Parcialmente ( ) Não ( )
Justifique: A direção foi a primeira a se posicionar a respeito da segurança contratando uma empresa especialista em Segurança da Informação

4 – A Coordenação das atividades de Segurança da Informação, são desenvolvidas por pessoas chaves, com funções e papeis bem definidos?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Temos uma empresa terceirizada especializada para tratar da Segurança da Informação da empresa.

5 – Os acordos de confidencialidade são analisados criticamente, de forma a proteger a Segurança da Informação?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Nossas informações são bem protegida com a política de senha e outros.

6 – Para gerenciar a Segurança da Informação, (seus controles, processos e procedimentos) o Supermercado leva em consideração a análise em intervalos planejados ou quando da existência de mudanças significativas?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Temos um planejamento mensal para melhorar ainda mais a segurança de nossos dados.

7 – Ao lidar com os riscos de processamento da informação vindos do ambiente externo dos negócios, a Segurança da Informação do Supermercado, identifica e faz o controle, antes de conceder o acesso?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Nossa Equipe Analisa as permissões necessárias para cada liberação externo para não comprometer nossa rede.

8 – Os requisitos de Segurança da Informação são identificados e considerados antes de se conceder aos clientes o acesso aos ativos ou as informações do Supermercado?
Sim (X) Parcialmente ( ) Não ( )
Justifique: Para nossos clientes, usamos uma rede a parte para não deixar nossa rede vulnerável e qualquer pessoa fazer uso dela.

APÊNDICE B – QUESTIONÁRIO APLICADO À COORDENAÇÃO DE RECURSOS HUMANOS DO SUPERMERCADO

"SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO ABNT NBR 27001"
QUESTIONÁRIO APLICADO COM A COORDENADORA DE RECURSOS HUMANOS DO SUPERMERCADO LOCALIZADO NA CIDADE DE JOÃO PESSOA
Fonte: ABNT NBR 27001 – A.8 – *CHECKLIST* SEGURANÇA EM RECURSOS HUMANOS

RESPONSABILIDADES ANTES DA CONTRATAÇÃO						
1	Papel da Organização e do empregado	A organização possui uma cartilha com a Política de Segurança da Informação, assim o funcionário entenderá suas responsabilidades, abrandando riscos de fraude e roubo	SIM	PARCIAL-MENTE	NÃO X	OBSERVAÇÕES Não temos cartilha de segurança e sim MANUAL DE CONDUTA
2	Seleção de Candidatos	A organização faz avaliação do candidato, analisando o seu currículo e os empregos anteriores, bem como suas redes sociais e possíveis riscos observados.	X			
3	Condições do contrato de trabalho	Os empregados selecionados concordam e assinam o contrato de trabalho declarando sua responsabilidade e a da organização junto a Segurança da Informação			X	Não temos cartilha de segurança e sim MANUAL DE CONDUTA
RESPONSABILIDADES DURANTE A CONTRATAÇÃO						
1	Responsabilida-de da Direção Respaldada pelo Recursos Humanos e demais Gerências	O Recursos Humanos e os Gerentes, incentivam os empregados a disseminarem a Segurança da Informação, como forma de prevenir ameaças e falhas humanas perante s Segurança da Informação.	SIM	PARCIAL-MENTE	NÃO X	OBSERVAÇÕES
2	Capacitação e educação continuada	Os empregados recebem educação continuada referente as suas funções, bem como são conscientizados das políticas da organização			X	
3	Advertência disciplinar	Caso o empregado cometa erro grave que comprometa a Segurança da Informação da Organização, o mesmo sofre uma "advertência disciplinar"	X			
RESCISÃO DO CONTRATO OU MUDANÇA NA CONTRATAÇÃO						
1	Rescisão do Contrato	Caso o empregado seja desligado, o Recursos Humanos prepara o processo de desligamento, onde são clarificados direitos e deveres.	SIM X	PARCIAL-MENTE	NÃO	OBSERVAÇÕES
2	Devolução de fardamentos, EPIS e outros	O empregado ao ser desligado, devolve a organização, farda, EPIS entre outros ativos.	X			
3	Cancelamento do direito a acesso	Após o seu desligamento, é retirado do empregado o seu acesso, seja email, senhas, crachás bem como o acesso à informações privativas da organização.	X			