Aplicabilidade da Norma ABNT NBR ISO/IEC 27002 em uma Empresa de Médio Porte

Yan S. Rocha[1], Eliomar A. de Lima[2]

[1]Instituto de Informática – Universidade Federal de Goiás (UFG)
Câmpus Samambaia, CEP 74690-900 – Goiânia, GO – Brasil

[2] Instituto de Informática – Universidade Federal de Goiás (UFG)
Câmpus Samambaia, CEP 74690-900 – Goiânia, GO – Brasil

{yanrocha,eliomar}@inf.ufg.br

Abstract. *In the face of constant changes and cyber threats, information and information assets become a fundamental and extremely valuable asset for many companies, determining their competitiveness. In order to ensure that the information is not with unauthorized persons, nor corrupted or even inaccessible, it is necessary to invest in confidentiality, integrity, and availability, which are the pillars of information security. In this sense, this paper approaches this theme through a case study involving the evaluation of information security in a medium-sized company under the protection of ISO / IEC 27002: 2013. The study revealed a picture full of nonconformities that allowed to raise hypotheses for future studies.*

Resumo. *Diante de constantes mudanças e ameaças cibernéticas, a informação e os ativos informacionais tornam-se um bem fundamental e extremamente valioso para muitas empresas, determinando a competitividade entre elas. Visando assegurar que as informações não estejam com pessoas desautorizadas, não sejam corrompidas ou mesmo inacessíveis, faz-se necessário investir em confidencialidade, integridade e disponibilidade, que são os pilares da segurança da informação. Nesse sentido, este trabalho aborda essa temática por meio de um estudo de caso envolvendo a avaliação de segurança da informação em uma empresa de médio porte sob o amparo da Norma ABNT NBR ISO/IEC 27002:2013. O estudo revelou um quadro repleto de não conformidades que permitiram levantar hipóteses para estudos futuros.*

1. Introdução

A importância dada à informação no século 21 produz implicações e desencadeia uma série de novas situações, representando grande poder a quem detém informações privilegiadas, críticas e/ou sensíveis a determinado contexto e ao mesmo tempo consegue subsidiar a tomada de decisão e a resolução de problemas corporativos.

O mundo dos negócios, imbricado no superlativismo cibernético, está sob ameaça de fenômenos e circunstâncias produzidas em meio a um cenário de grande volatilidade, incertezas, complexidades e ambiguidades. A informação passa a ser um ativo cobiçado devido ao seu grau de revelação do estado de coisas que caracteriza determinado objeto, entidade ou sistema, necessitando que as organizações se mantenham atualizadas para garantir a correta tomada de decisões estratégicas. Segundo Barbosa [1997 p.52] o processo de busca e utilização de informações externas subsidiam decisões estratégicas.

Os avanços tecnológicos, por seu turno, são necessários para que haja maior eficácia na captação, processamento, armazenamento e disponibilização das informações pertinentes. Sem a utilização da tecnologia e seus recursos, é extremamente difícil uma empresa continuar atuando satisfatoriamente no nicho que atua. É nesse contexto que é desejável o uso e aplicação de sistemas de informação para gerenciar toda a demanda de informação gerada. Segundo Turban, Mclean e Wetherbe [2004], sistemas de informação são responsáveis por coletar, armazenar, recuperar e disseminar informações pra fins específicos. Para Laudon [1999], as informações coletadas fazem parte da análise do processo decisório em organizações.

Nos últimos anos, com o advento e popularização da Internet, o acesso a informação fica cada vez mais fácil, tornando a competitividade entre as empresas cada vez maior. Do mesmo modo, potencializam-se os riscos relacionados à segurança da informação, tornando a necessidade de proteção das informações uma preocupação recorrente.

Considerada chave e parte da estratégia da organização, a segurança da informação se torna cada vez mais necessária para a proteção de informações e ativos informacionais. Para Beal [2005 p.71 *apud* Santos and Silva 2012] a segurança da informação é "o processo de proteger a informação das ameaças para garantir a sua integridade, disponibilidade e confidencialidade".

Para que a segurança da informação seja garantida, inúmeras abordagens e práticas são recomendadas na literatura técnica-especializada, incluindo precauções que devem ser tomadas. Análises de riscos, por exemplo, são ações necessárias para mitigar situações que podem ser prejudiciais a organização, identificando assim a possibilidade de ameaças. Quando mapeadas as ameaças, um apontamento de soluções cabíveis é realizado visando minimizar o risco. De acordo com Furnell e Thomson [2009], os usuários são identificados como grande ameaça na implantação de práticas e procedimentos de segurança da informação.

Para Oliveira [2001 p.43 apud Spanceski 2004],

> Nenhuma área da informática é tão apreciada como a segurança da informação, todo processo de segurança inicia e tem seu término em um ser humano. Segurança não é uma questão técnica, mas uma questão gerencial e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários. Mas, uma ameaça também pode ser considerada todo e qualquer indício de acontecimentos desfavoráveis, sobre um ativo ou pessoa.

As organizações, em geral, planejam ou criam normas de segurança da informação sem considerar as pessoas, o que dificulta a elaboração e a regulamentação, podendo levar a um resultado ineficiente ou inexequível [LORENS 2007].

Em meio aos desafios e incompreensões existentes para a adoção de medidas e práticas de segurança da informação no meio corporativo, o objetivo deste trabalho é propor hipóteses a partir da avaliação de segurança da informação em uma organização de médio porte que atua no segmento de prestação de serviços em tecnologia da informação, à luz dos requisitos e controles preconizados na Norma NBR ISO/IEC 27002:2013 [ABNT ISO 27002 2013], a qual prevê boas práticas de controles de segurança da informação.

Os conceitos e requisitos especificados na norma ABNT ISO 27002 [2013] são basilares para avaliação pretendida, haja vista a possibilidade de implantação de um sistema de gestão de segurança da informação no contexto organizacional, bem como identificação e mitigação de ameaças. Para tanto, o estudo inicia-se com a identificação das principais

necessidades da organização, buscando reconhecer riscos de segurança da informação, tendo em vista os ativos de maior relevância, face aos objetivos estratégicos estabelecidos. Em seguida, uma análise ampla dos processos e práticas que remetem à segurança da informação é empreendida, em conformidade com os objetivos de controle da norma ABNT ISO 27002 [2013]. Por fim, o resultado alcançado produz subsídios para a definição de hipóteses reveladas a partir de uma visão geral acerca dos pontos críticos associados à garantia e manutenção da segurança da informação corporativa.

2. Segurança da Informação à luz da Norma ABNT ISO 27002

Segundo a norma ABNT NBR ISO/IEC 27002:2013 [ABNT ISO 27002 2013], para se alcançar o que pode ser considerado "Segurança da Informação", faz-se necessária a "implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware". Para tanto, "estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização são atendidos".

Essa norma [ibid.] também recomenda que:

> "O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.".

A norma ABNT ISO 27002 [2013] define como Ativo "objeto de ameaças, tanto acidentais como deliberadas, enquanto que os processos, sistemas, redes e pessoas têm vulnerabilidades inerentes".

A definição e classificação da informação é um requisito mandatório para determinação do nível de proteção das informações. Devido à ocorrência de incidentes de segurança nas empresas, as informações e os ativos informacionais carecem cada vez mais de proteção. Esta requer a implantação de medidas de segurança da informação que vai além de tecnologias computacionais, de modo a assegurar suas propriedades. Para Bunker [2012], embora exista uma grande quantidade de tecnologias da informação destinadas à proteção e segurança dos ativos de informação, não é suficiente para assegurar a efetividade dos mecanismos e instrumentos de segurança da informação.

Os grandes pilares de segurança da informação, conforme preceitua a norma ABNT ISO 27002 [2013], são:

- Confidencialidade – garante que a informação só será acessada por pessoas autorizadas.
- Integridade – garante que a informação alcance seu destino sem algum tipo de modificação.
- Disponibilidade – garante que informações solicitadas devem estar disponíveis para acesso a qualquer momento, de acordo com a requisição do usuário.

A Norma ABNT ISO 27002 [2013] tem como objetivo

> Fornecer diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, implementação e o gerenciamento de controles, levando em

> consideração os ambientes de risco da segurança da informação da organização.

Encontra-se distribuída em 14 seções de controles de segurança da informação, totalizando 35 objetivos de controles e 114 controles [*ibid.*] e está circunscrita na família de normas ABNT NBR ISO/IEC 27000, que trata da gestão de segurança da informação.

3. Metodologia

Com o objetivo de mapear e analisar a real situação de uma organização quanto ao cumprimento dos preceitos de segurança da informação, utilizando como parâmetro os 35 objetivos de controle da norma ABNT ISO 27002 [2013], um estudo de caso simples foi empreendido no âmbito de uma empresa, tomando como base a observação das práticas corporativas que contribuem positiva ou negativamente para a gestão de segurança da informação.

O estudo iniciou-se com uma breve pesquisa bibliográfica para balizar a aplicação da ABNT ISO 27002 [2013], buscando a compreensão de suas definições e requisitos. Em seguida, escolheu-se de forma deliberada uma organização de médio porte que atua no segmento de prestação de serviços em tecnologia da informação, com aproximadamente 90 colaboradores diretos, situada na cidade de Goiânia. Nesse contexto organizacional foi promovido um diagnóstico com base na medição do nível de maturidade de cada prática adotada em termos de controles previstos na norma ABNT NBR ISO/IEC 27002:2013. O processo observacional e de análise e discussão consumiu um tempo de aproximadamente 10 meses, concluído no primeiro semestre de 2018.

Para contemplar a avaliação das seções previstas na norma ABNT ISO 27002 [2013], pontos focais na empresa foram selecionados para poder responder as questões propostas no instrumento de coleta, produzindo artefatos de registro de acompanhamento, contendo o preenchimento de checklists de requisitos. Além de anotar o grau de maturidade, que varia de 0 (não existe) a 2 (definido), os artefatos refletiram as seções daquela norma. Por fim, as análises foram feitas considerando todo o arcabouço informacional e os critérios de avaliação adotados.

Cada artefato produzido consistia de uma série de perguntas diretas, correspondendo ao instrumento de coleta principal, com as respectivas respostas, apresentando o seguinte gabarito:

- ‘SIM’, ‘NÃO’ e ‘NÃO SE APLICA (NA)’, para cada controle avaliado;
- breve resumo de controles que possam suportar, ou já suportam, o controle levantado;
- breve resumo das dificuldades/impossibilidades que possam vir a atender, ou já atendem o requisito;
- se existe ou não a intenção/projeto de implantar uma política/controle sobre o que foi questionado, caso não o tenha;
- o nível de maturidade daquele controle, o qual é classificado como 0 para ‘Não Existe’, 1 para ‘Inicial’ e 2 para ‘Definido’.

4. Resultado e Discussão

O grau de maturidade mapeado no checklist está centrado no diagnóstico dos controles associados aos objetivos de controle previstos na ABNT ISO 27002 [2013]. O grau de maturidade é atribuído de acordo com as respostas obtidas em cada domínio. Ao final é contabilizada a quantidade de cada nível e essa informação é incluída na planilha ‘Nível de Maturidade’, como ilustrado na Figura 1.

Domínios de Segurança de Informação	Total de Perguntas	Nível de Maturidade			
		Não se aplica	0 - Não existente	1 - Inicial	2 - Definido
Seção 5 - Política de Segurança	32				
Seção 6 - Organização da Segurança da Informação	33				
Seção 7 - Segurança em recursos humanos	33				
Seção 8 - Gestão de ativos	44				
Seção 9 - Controle de acesso	66				
Seção 10 - Criptografia	21				
Seção 11 - Segurança física e do ambiente	88				
Seção 12 - Segurança nas operações	92				
Seção 13 - Segurança nas comunicações	34				
Seção 14 - Aquisição, desenvolvimento e manutenção de sistemas	59				
Seção 15 - Relacionamento na cadeia de suprimento	57				
Seção 16 - Gestão de incidentes de segurança da informação	33				
Seção 17 - Aspectos da segurança da informação na gestão da continuidade do negócio	12				
Seção 18 - Conformidade	40				

Figura 1. Nível de Maturidade [Adaptado de ABNT ISO 27002 2013]

Com a obtenção de todas as respostas, pode-se classificar o nível de maturidade de cada seção, mapeando assim de forma ampla as principais conformidades (e não conformidades) em segurança da informação naquela organização.

A título de ilustração, o escore obtido nas duas primeiras seções está representado nas Figuras 2 e 3. A primeira Seção analisada foi a '*Seção 5 – Política de segurança da informação*', na qual foi realizado um total de 32 perguntas e apenas duas tiveram respostas 'SIM', como mostra a Figura 2. As perguntas que resultaram nessas respostas foram: '*A direção apoia as diretrizes deste documento?*' e '*A organização adota práticas de Backup?*'.

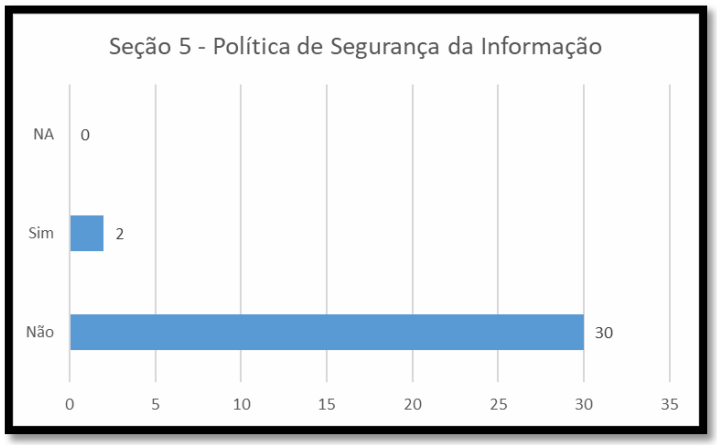

Figura 2. Respostas quanto aos controles da Seção 05 – ABNT ISO 27002

A predominância de respostas '*Não atende'* aos controles da Seção 05 é agravada pela inexistência de uma Política de Segurança da Informação. Em seguida analisou-se a '*Seção 06 – Organização da Segurança da Informação*', cujo resultado está sintetizado na Figura 3.

As demais seções passaram pelo mesmo processo de avaliação, culminando com o diagnóstico de maturidade sintetizado na Figura 4. Vale ressaltar que os níveis de maturidade obtidos refletem o estágio atual em termos de práticas adotadas por parte dos colaboradores, das medidas de controle empregadas e/ou institucionalizadas, bem como os hábitos e costumes que caracterizam a cultura de segurança da informação no âmbito da unidade de análise.

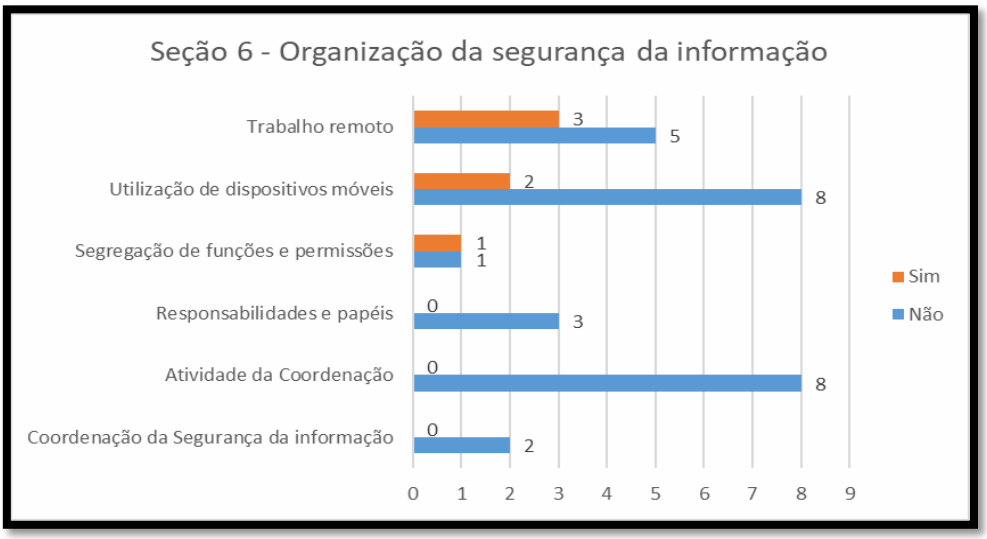

Figura 3. Respostas quanto aos controles da Seção 06 – ABNT ISO 27002 [2013]

A organização não possui nenhum procedimento ou prática definida que diz respeito às Seções '*Seção 8 – Gestão de ativos*', '*Seção 10 – Criptografia*' e '*Seção 15 – Relacionamento na cadeia de suprimentos*'. Por outro lado, a '*Seção 11 – Segurança física e do ambiente*' e '*Seção 12 – Segurança nas operações*' foram as que mais tiveram representatividade quanto ao nível de maturidade '*Inicial'*. As demais seções se se limitaram há poucos controles no nível '*Inicial*', conforme ilustrado na Figura 4.

O nível de maturidade '*Inicial'* sugere que a empresa possui algumas práticas de uso nas diretrizes abordadas, mas, não necessariamente dispõe de políticas específicas para implementá-las. Por fim, há controles que não se aplicam à organização observada, a exemplo do que ocorre com algumas diretrizes contidas na '*Seção 11 – Segurança física e do ambiente*', '*Seção 12 – Segurança nas operações*' e '*Seção 18 – Conformidade*'.

Observou-se também que, apesar de ser uma empresa de médio porte e com taxas de crescimento crescentes nos últimos anos, não existia uma preocupação iminente quanto às ameaças até então identificadas, seja porque não havia orçamento previsto para segurança da informação, seja porque ainda não há nenhuma prática no nível de maturidade '*definido'*.

A sensação de falta de consciência e incompreensão por parte dos colaboradores da empresa pode ser percebida quando o termo segurança da informação é constantemente confundido com "segurança do ambiente", "segurança elétrica", ou mesmo "segurança corporativa".

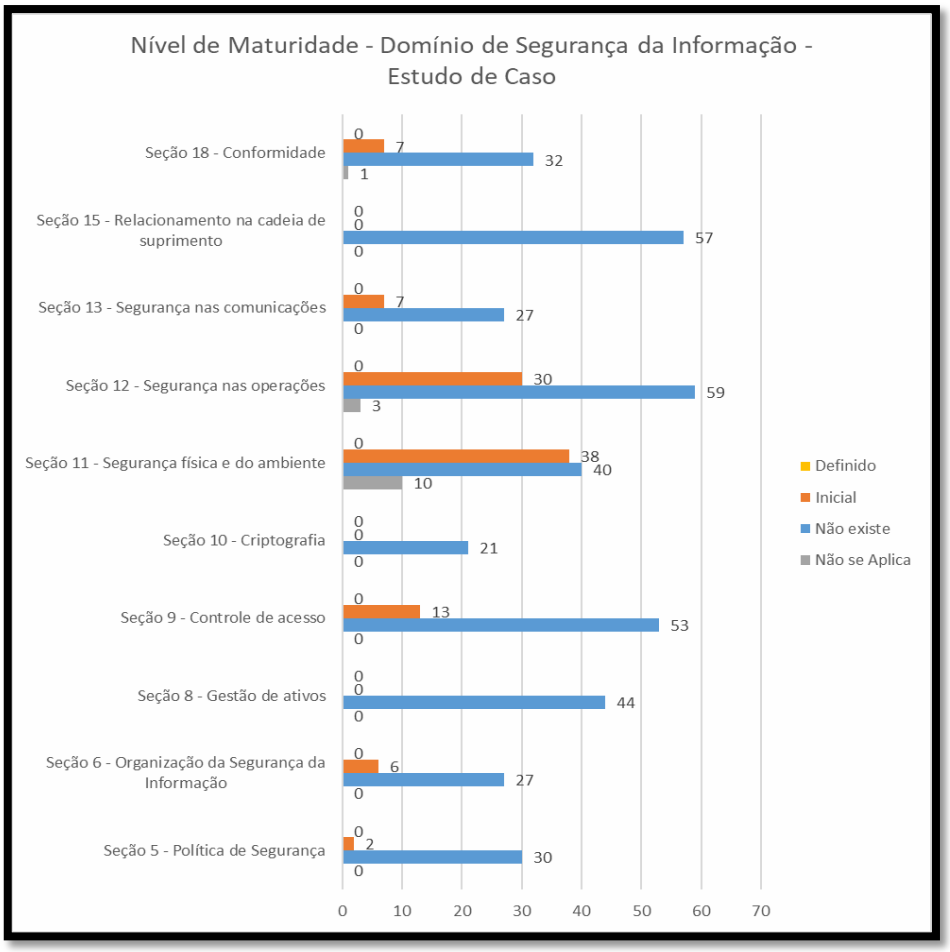

Figura 4. Nível de Maturidade – Estudo de caso [O Autor 2018]

4.1. Discussão

A avaliação das práticas e das medidas adotadas no âmbito da organização estudada, à luz dos controles recomendados pela ABNT ISO 27002 [2013], permitiu revelar um quadro de graves inconformidades, vulnerabilidades e incompreensões no que tange à segurança da informação.

Considerando que a função básica da área de segurança da informação é a proteção dos ativos de informação, por meio da minimização dos riscos a níveis aceitáveis [FERREIRA AND ARAÚJO 2008] e considerando que as impressões alcançadas na unidade de análise, fruto das observações participante e da aplicação dos instrumentos de coleta junto aos pontos focais da organização, permitiu elucidar o estado de coisas que orbitam os sistemas e as tecnologias de informação, uma série de conjecturas pode ser extraída, ainda que a confirmação esteja fora da alçada deste estudo:

- a implementação de controles por meio de processos para a proteção das informações é uma das formas de prover segurança aos sistemas de informação;
- o passo que antecede qualquer medida de controle de segurança da informação diz respeito à realização da classificação da informação, de modo a proteger as mais críticas;
- é preciso definir papéis, responsabilidades e responsabilização no âmbito da gestão de segurança da informação para iniciar o processo de implantação de segurança da informação na organização;

- os usuários de sistemas de informação tendem a não observar as práticas de segurança da informação por desconhecimento ou desinteresse;
- os profissionais de TI tendem a priorizar medidas associadas exclusivamente a tecnologias da informação.

Ainda que as constatações acerca do nível de maturidade das práticas e controles de segurança da informação estejam condicionadas a um modelo de referência reconhecido e consagrado pela norma ABNT ISO 27002 [2013], assumir as suposições retrocitadas implica na adoção de um modelo de ciclo de vida para implantação de um Sistema de Gestão de Segurança da Informação (SGSI) que contemple as várias fases que devem ser executadas continuadamente para propiciar melhorias e aumento gradativo do nível de maturidade da gestão de segurança da informação. O Quadro 1 apresenta uma proposta de modelo de ciclo de vida para implantar o SGSI, inspirada na norma ABNT NBR ISO/IEC 27001:2013, que trata da estruturação de um SGSI.

Quadro 1. Ciclo de Vida para Implantação do SGSI

Fase I - Plan	Fase II - Do	Fase III - Check	Fase IV - Act
○ Estruturação do SGSI ○ Plano Diretor de Segurança ○ Diagnóstico de Segurança ○ Avaliação, Tratamento dos Riscos e Seleção dos Controles de Segurança ○ Declaração de Aplicabilidade (*Statement of Applicability*)	○ Política Corporativa de Segurança da Informação ○ Classificação da Informação ○ Plano de Continuidade dos Negócios e de TI ○ Treinamento e Conscientização ○ Implementação dos Controles Especificados na Declaração de Aplicabilidade	○ Monitoração dos Controles de Segurança ○ Gestão de Incidentes ○ Revisão do nível de risco residual ○ Auditoria Interna do SGSI	○ Implementação de melhorias ○ Ações Corretivas e Preventivas ○ Comunicação das Ações e Resultados para Alta Administração e Partes Interessadas ○ Assegurar que as Melhorias foram Implementadas e Atenderam as Expectativas

Fonte: Ferreira e Araújo [2008]

O SGSI envolve preliminarmente a identificação de fatores críticos de sucesso e o mapeamento de dificuldades para o processo de implantação da gestão da segurança da informação, com base na experiência da própria organização [FERREIRA E ARAÚJO 2008].

5. Considerações Finais

A pesquisa permitiu diagnosticar as práticas e os procedimentos de segurança da informação adotados no âmbito organizacional, em conformidade com objetivos de controle da ABNT ISO 27002 [2013]. A empresa, objeto de análise deste estudo, revelou que os controles observados apresentam predominantemente baixo nível de maturidade, refletindo as vulnerabilidades e ameaças quanto aos preceitos de confidencialidade, integridade e disponibilidade.

Ainda que incipiente, os resultados obtidos sugerem que diversas abordagens e estratégias de implantação são passíveis de serem adotadas naquele contexto, desde que observem minimamente as suposições verificadas nesta pesquisa. Além disso, os artefatos produzidos revelam um quadro de conformidades (e inconformidades) em termos de segurança da informação, que poderão contribuir para a definição da estratégia de implantação de um sistema de gestão de segurança da informação, já que alguns pressupostos devem ser observados para que não haja ambiguidades e interpretações equivocadas por parte dos gestores que estarão à frente desse processo.

Esta pesquisa terá continuidade no escopo do projeto de conclusão de curso do primeiro autor, cujas hipóteses aqui levantadas subsidiarão a nova etapa do trabalho, pautado pelo sistema de gestão de segurança da informação, de modo a ampliar os horizontes de avaliação para a proposta do plano de ação a ser elaborado, levando em consideração aspectos de viabilização da aplicação no contexto corporativo. Nesse sentido, apropriar-se da norma ABNT NBR ISO/IEC 27001:2013 e de outras referências que abordam o sistema de gestão de segurança da informação é um dos requisitos chaves para a sequência do trabalho.

6. Referências

ABNT ISO 27002. (2013). ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR/ISO/IEC 27002:2013 tecnologia da informação – técnicas de segurança – código de prática para controles de segurança da informação.

BARBOSA, R. R. (1997). Monitoração ambiental: uma visão interdisciplinar. Revista de Administração, São Paulo: v.32, n.4, p. 42-53, out./dez.

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

BUNKER, G. (2012). “Technology is not enough: taking a holistic view for information assurance”. In: Information Security Technical Report, (17): 19-25.

FERREIRA, F. N. F.; ARAÚJO, M. T. (2008). Política de Segurança da Informação – Guia Prático para Elaboração e Implementação, Editora Ciência Moderna, Rio de Janeiro.

FURNELL, S.; THOMSON, K. L. (2009). From Culture to disobedience: recognising the varying user acceptance of IT security. Computer Fraud & Security, (2), 5-10.

LAUDON, Kenneth C.; LAUDON, Jane P. (1999). Sistema da Informação com Internet. Rio de Janeiro: LTC.

LORENS, E. M. (2007). Aspectos normativos da Segurança da Informação: um modelo de cadeia de regulamentação, Dissertação de Mestrado, Universidade de Brasília, Brasília-DF, Brasil.

OLIVEIRA, W. (2001). Segurança da Informação. Florianópolis: Visual Books.

SANTOS, D. L. R.; SILVA, R. M. S. (2012). Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001. Trabalho de Segurança de Informação do MCI 2012/2013. Universidade do Porto, Faculdade de Engenharia.

SMITH, A.; JONES, B. (1999). On the complexity of computing. In Advances in Computer Science, pages 555–566. Publishing Press.

SPANCESKI, F. R. (2004). Política de Segurança da Informação: desenvolvimento de um modelo voltado para instituições de ensino. Monografia do Trabalho de Conclusão de Curso em Sistemas de Informação.

TURBAN, E.; MCLEAN, E.; WETHERBE, J. (2004). Tecnologia da informação para gestão. Transformado os negócios da economia digital. [S.l.: s.n.]