EXÉRCITO BRASILEIRO
ESCOLA DE FORMAÇÃO COMPLEMENTAR DO EXÉRCITO
Curso de Gestão e Assessoramento de Estado-Maior - CGAEM

Ten Cel Int Guilherme Keese Diogo Campos

ANÁLISE EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO E SUAS CONSEQUÊNCIAS EM ÓRGÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Salvador
2020

Ten Cel Int Guilherme Keese Diogo Campos

ANÁLISE EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO E SUAS CONSEQUÊNCIAS EM ÓRGÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Centro Universitário do Sul de Minas – UNIS-MG como requisito parcial para a obtenção do Grau Especialização de Gestão em Administração Pública.

.

Orientadora: Profa. Dra. Liz Aurea Prado

Salvador
2020

Ten Cel Int Guilherme Keese Diogo Campos

ANÁLISE EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO E SUAS CONSEQUÊNCIAS EM ÓRGÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Centro Universitário do Sul de Minas – UNIS-MG como requisito parcial para a obtenção do Grau Especialização de Gestão em Administração Pública.
.

Aprovado em 05 de agosto de 2020.

COMISSÃO DE AVALIAÇÃO

_____
Prof. Dr. Rodrigo Franklin Frogeri
UNIS

_____
Profa. Ma. Lívia da Silva Ciacci – Membro 1
UNIS

_____
Prof. Me. Antonio de Biaso Junior – Membro 2
UNIS

GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM UM ÓRGÃO DA ADMINISTRAÇÃO PÚBLICA FEDERAL: estudo de caso no Exército Brasileiro

INFORMATION SECURITY MANAGEMENT IN A FEDERAL PUBLIC ADMINISTRATION ORGANIZATION: case study in the Brazilian Army

Guilherme Keese Diogo Campos[1]
Liz Aurea Prado [2]

RESUMO

O Comando Militar da Amazônia (CMA) tem a missão de, em tempo de paz, participar na dissuasão de ameaças aos interesses nacionais; e, em situação de guerra ou conflito externo, conduzir em sua área de responsabilidade, a campanha militar para derrotar o inimigo que agredir ou ameaçar a soberania, a integridade territorial, o patrimônio e os interesses vitais do Brasil. O Exército Brasileiro pode ser observado como um órgão de elevada importância devido as suas missões e informações que circulam e são produzidas, diariamente por suas instalações. O descumprimento de princípios básicos da Segurança da Informação (SI) pode impactar diretamente na produtividade e no desenvolvimento de uma organização. Nesse contexto, este estudo teve como objetivo analisar o grau de aderência da Base Administrativa do Comando Militar da Amazônia às recomendações de Segurança da Informação (SI) da norma ABNT NBR ISO/IEC 27002:2013. Este intento foi conseguido por meio de um estudo de caso na Base Administrativa (BAdm) do CMA. Adotou-se uma abordagem qualitativa e quantitativa. A abordagem qualitativa utilizou a análise documental e a quantitativa técnicas de estatística descritiva e análise de *cluster*. Concluiu-se, por fim, que existe uma aderência satisfatória da norma NBR ISO/IEC 27002:2013 pela organização, embora haja necessidade de aperfeiçoamento de práticas de SI, e que as legislações das organizações militares estão de acordo com as civis e possibilitam práticas semelhantes com as demais instituições.

Palavras-chave: Comando Militar da Amazônia. Exército Brasileiro. Gestão da Segurança da Informação. ISO/IEC 27002. Segurança da Informação.

ABSTRACT

The Amazon Military Command (AMC) has the mission of, in peacetime, participate in deterring threats to the national interests; and, in the event of war or external conflict, guide in its area of responsibility the military campaign to defeat the enemy who assaults or threatens Brazil's sovereignty, territorial integrity, heritage and vital interests. The Brazilian Army also works as an important organization due to its missions and daily information produced inside its facilities. The failure to comply with basic Information Security (IS) principles can directly affect the organization's productivity and development. Thus, this paper aimed to analyze the

1 Pós-graduando em Gestão em Administração Pública pelo Centro Universitário do Sul de Minas. E-mail: guilhermekeese@homail.com.
2 Mestre em Administração. Especialista em Desenvolvimento de Aplicativos para Dispositivos Móveis. Graduada em Análise e Desenvolvimento de Sistemas. E-mail: liz.prado@professor.unis.edu.br.

maturity level of the Administrative Base of the AMC to the recommendations of IS and its compliance with ABNT NBR ISO / IEC 27002: 2013 norm. This objective has been achieved through the case study, focusing on the Administrative Base of the AMC. This research has chosen a qualitative and quantitative approach: the qualitative approach used documental analysis and the quantitative approach, descriptive statistics techniques and cluster analysis. Finally, it's been concluded that there is a satisfactory observance of the NBR ISO / IEC 27002: 2013 standard by the organization, although there is a need for improvement of IS practices, and the military organizations regulations are in agreement with the civilian rules and allow similar practices with other institutions.

Keywords: Amazon Military Command. Brazilian Army. Information Security Management. ISO / IEC 27002. Information Security.

1 INTRODUÇÃO

Segurança da Informação é um assunto que cresce de importância nos órgãos da Administração Pública, uma vez que existe um constante aumento das redes de computadores e suas conexões (LYRA, 2015). A possibilidade de ataques e invasões nas estruturas de Tecnologia da Informação e Comunicação (TIC) e todos seus ativos demandam um zelo permanente dos membros que compõe a organização.

A cada ano, as estruturas da Administração Pública aumentam as suas redes de computadores e parques tecnológicos devido à intensa necessidade de obtenção e de troca de informações. Segundo Lyra (2015), o avanço das TICs embora facilite o trabalho dos servidores, implica num aumento de vulnerabilidades que devem ser superadas pela instituição. Com isso, aumenta a necessidade de se prover e manter a segurança das informações da organização em oposição ao crescimento significativo de ataques cibernéticos nos mais diversos setores.

Segundo o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), há a necessidade de se orientar e garantir a condução de políticas de segurança já existentes ou a serem implementadas devido a constante necessidade de garantir e melhorar a Segurança da Informação (SI) dos órgãos da Administração Pública Federal.

O Comando Militar da Amazônia (CMA) tem a missão de: em tempo de paz, participar na dissuasão de ameaças aos interesses nacionais; e, em situação de guerra ou conflito externo, conduzir em sua área de responsabilidade, a campanha militar para derrotar o inimigo que agredir ou ameaçar a soberania, a integridade territorial, o patrimônio e os interesses vitais do Brasil. Além disso, a fim de contribuir para a garantia da lei e da ordem e dos poderes constitucionais, o Exército deve manter-se em condições de ser empregado em sua área de responsabilidade, em situação emergencial e temporária, depois de esgotados os instrumentos destinados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, conforme relacionados no Art. 144 da Constituição Federal. Constitui-se, assim, num órgão de elevada importância devido suas missões e informações que circulam e são produzidas, diariamente, por suas instalações.

De acordo com a ISO/IEC 27002:2013, a informação é um ativo que, como qualquer outro ativo é importante, é essencial para os negócios de uma organização, e deve ser adequadamente protegida. Nesse contexto, o aperfeiçoamento e respeito às normas da SI parece ser um desafio, uma vez que exige um alto grau de comprometimento da direção, assimilação e aperfeiçoamento dos servidores, além de ser um processo demorado e contínuo.

Lyra (2015) considera que para as pessoas estarem aptas a identificarem situações de risco, precisam ser treinadas e estimuladas a desenvolver a cultura da SI, identificando quais

informações devem ser protegidas e como. Ocorre que as Unidades Militares que compõe o CMA possuem uma alta rotatividade, uma vez que seus militares permanecem na guarnição, em média, 2 (dois) anos. Tal fato, dificulta o aperfeiçoamento e investimento da cultura de SI dentro da organização.

Utilizando os conceitos da Norma ABNT NBR ISO/IEC 27002:2013, desenvolvida para servir de referência e/ou orientação para as organizações na seleção e implementação de controles de SI, pode-se medir o grau de aderência de uma organização à norma, levando em consideração os seus ambientes de risco de segurança da informação específicos.

Diante disso, torna-se necessário analisar como se encontra a Gestão de Segurança de Informação do CMA frente aos riscos nos ativos de informação do órgão e, consequentemente, ações para conscientizar todos da importância da Segurança da Informação. Para isso, foi determinado como unidade de observação a Base Administrativa (BAdm) do CMA.

Tal abordagem se faz necessária, diante da segurança nos ativos de informação que o Comando Militar da Amazônia necessita para continuar exercendo sua missão junto ao Exército Brasileiro e da necessidade de se proteger todos os dados de alta confidencialidade produzidos e recebidos em relação à Região Amazônica e todas as operações que nela acontecem.

É importante ressaltar a contribuição desse trabalho para o Exército Brasileiro, pois o resultado dessa pesquisa permitirá que o Comando Militar da Amazônia, avalie a necessidade de avançar nos estudos e desenvolva uma gestão mais sólida de Segurança da Informação.

A finalidade desta pesquisa é analisar o grau de aderência da Base Administrativa do Comando Militar da Amazônia às recomendações de Segurança da Informação (SI) da norma ABNT NBR ISO/IEC 27002:2013. A pergunta de pesquisa que norteou o estudo foi a seguinte: qual o grau de aderência da Base Administrativa do Comando Militar da Amazônia às recomendações de Segurança da Informação (SI) da norma ABNT NBR ISO/IEC 27002:2013?

Este intento foi conseguido por meio de um estudo de caso na Base Administrativa (BAdm) do CMA. Adotou-se uma abordagem qualitativa e quantitativa. A abordagem qualitativa foi realizada por meio de análise documental e etnografia; a análise quantitativa se baseou em técnicas de estatística descritiva e análise de *cluster*. Os dados foram coletados por meio de questionário eletrônico e contou com um total de 31 respostas válidas.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação no Exército Brasileiro

Dentro de uma Unidade Militar, a informação deve ser tratada como patrimônio a ser protegido e preservado em todo o seu ciclo de vida, constituindo-se num recurso vital. Todas as informações produzidas e manuseadas no âmbito do Exército Brasileiro (EB) devem ser tratadas para garantir a disponibilidade, integridade, confidencialidade e autenticidade. A proteção e a preservação da informação institucional do EB são consideradas um patrimônio e sua eficácia depende, também, da eficiência no emprego dos recursos de TI (IG-01.014, 2014).

A existência de ameaças, vulnerabilidades e riscos é inerente ao emprego e acesso às informações, num contexto de uma crescente informatização de atividades e processos organizacionais. Sendo que o sucesso das ações de Segurança da Informação (SI) depende, fundamentalmente, da conscientização do público interno, da capacitação científico-tecnológica dos recursos humanos envolvidos, da qualidade das soluções adotadas e da SI contra ameaças internas e externas (IG-01.014, 2014).

A SI tem como objetivo proporcionar harmonia e ajustes das ações de SI a serem adotadas no EB, com as ações estabelecidas nas demais instituições, mantendo sempre o foco nas especificidades da Força. As diretrizes gerais buscam guiar todos os procedimentos de SI em todas as Organizações Militares (OM) do EB e demais publicações sobre o tema e

demonstram o comprometimento e a visão do Alto Comando do EB em relação à SI (BRASIL, 2011).

As Instruções Gerais (IG) relacionadas à SI na esfera do Exército Brasileiro (EB) têm por finalidade orientar o planejamento e a execução das ações relacionadas a este tema. Sua criação é composta, nas suas referências, de documentos normativos sobre SI vigentes no âmbito do Ministério da Defesa (MD), bem como outras publicações de interesse na esfera da Administração Pública Federal (APF) (BRASIL, 2014).

A gestão de SI deve ser o elemento norteador para a tomada de decisões em relação a todas as ações de SI. Toda a cadeia hierárquica do EB, empresas prestadoras de serviços, terceiros e partes interessadas deverão ser sensibilizadas a respeito da importância de SI para a Força e, assim, promover atitudes favoráveis referentes ao tema. Dessa forma, em todas as OM do EB deverão ser realizadas instruções de sensibilização, conscientização e capacitação para formação e fortalecimento da cultura de SI (IG-01.014, 2014).

Dessa forma, o EB publicou em 1 de agosto de 2014, no Boletim do Exército Nº 13, a Portaria Nº 803, de 30 de julho de 2014, aprovando as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro. O documento referência 17 outras normas, incluindo a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados; a Medida Provisória nº 2.200-2, de 24 de agosto de 2001 - Institui a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil; 4 (quatro) Decretos da APF; 3 (três) Instruções Normativas do GSI/PR; duas Portarias Normativas do Ministério da Defesa; 3 (três) Portarias do Comandante do Exército; Manual de Campanha MC 30-3 - Ramo Contra Inteligência e ABNT NBR ISO/IEC 27001:2013.

2.2 Norma ABNT NBR ISO/IEC 27002:2013

A norma ABNT NBR ISO/IEC 27002:2013 tem como propósito servir como referência na implementação e desenvolvimento de um Sistema de Gestão de Segurança da Informação (SGSI) para organizações e empresas, considerando os riscos de negócios e definindo controles que servirão de parâmetros avaliações de riscos.

Ao todo são 18 capítulos, sendo que serão abordados os 14 referentes às seções de controles de Segurança da Informação, sendo que cada seção define um ou mais objetivos de controle. Conforme a norma preconiza, não há relação da ordem em que os capítulos são apresentados com suas respectivas importâncias, podendo ser aplicados de acordo com a necessidade e a avaliação de cada órgão (NBR 27002, 2013).

A norma ABNT NBR ISO/IEC 27002:2013 não possui o condão de esgotar as necessidades de todas as empresas, cabendo aos entes envolvidos realizarem as adaptações necessárias. Cada organização deve avaliar quais objetivos de negócios serão abordados pelos controles apresentados e quais as novas demandas devem ser desenvolvidas para diminuir ou eliminar os riscos aos ativos da organização.

De acordo com a norma, as Políticas de Segurança das Informações (PSI) devem estabelecer a abordagem da organização para gerenciar os objetivos de segurança das informações, contemplando requisitos de estratégia do negócio, regulamentações e ameaças da SI. A PSI deve definir a SI, estabelecendo seus princípios e objetivos, atribuições de responsabilidades e exceções, estabelecendo ainda um intervalo para revisão da mesma.

A Organização da Segurança das Informações estabelece a estrutura de gerenciamento, controle e operação da SI, identificando os ativos e processos de SI, definindo os responsáveis e suas atribuições.

No caso da Segurança em Recursos Humanos (SRH), a norma cita que deve assegurar a seleção adequada dos recursos humanos, com vistas às suas referências pessoais e profissionais, incluindo uma verificação destas e de sua documentação. As responsabilidades

devem ser claras e sempre praticadas, existindo um processo disciplinar formal e bem difundido, de forma a coibir violações da SI. No caso de encerramento ou mudança da contratação, especial atenção deve ser dada à proteção dos interesses da organização.

Os ativos de Informação e os recursos de processamento desta devem ser identificados e inventariados, sendo estabelecidos responsáveis pela sua estruturação e manutenção, tratando da qualificação do seu ciclo de vida. Deve ser estabelecido nível de proteção adequada à informação, prevenindo ainda a divulgação, modificação, remoção ou destruição das informações de forma não autorizada.

A Política de Controle de Acesso visa detalhar com rigor o limite de acesso, físico e lógico, à informação, devido aos riscos de SI associado. Observando que uma das formas para se proteger a confidencialidade, autenticidade e/ou a integridade da informação é através da utilização da criptografia. Soma-se, nesse contexto, a segurança física e do ambiente com o propósito de evitar a admissão de pessoas não autorizadas e danos dolosos ou não aos ativos de informação da organização. Os acessos físicos devem ser limitados e definidos para prevenir as informações sensíveis.

A Segurança nas operações possui como objetivo a garantia do uso correto dos recursos de processamento da informação e a organização e divulgação dos procedimentos de operação para todos os servidores interessados. Já a Segurança nas comunicações enseja a proteção das informações em redes e dos recursos de processamento da informação que as apoiam, conforme nos traz a norma. Todos os acessos devem ser controlados a fim de se proteger todos os serviços conectados à rede.

No caso da aquisição, desenvolvimento e manutenção de sistemas, todas as áreas afetas devem ser englobadas pela SI em seus processos. Toda implementação de sistemas de informação que geram suporte aos negócios devem ser tratados com atenção. Assim, importante destacar que o relacionamento na cadeia de suprimento baseia-se num acordo prévio entre a organização e o fornecedor, de maneira que haja a garantia da proteção dos ativos da organização que são acessados pelos fornecedores.

Destaca-se, na gestão de incidentes de Segurança da Informação, a necessidade de envolvimento de todos os servidores, fornecedores e terceiros à respeito dos procedimentos relativos a segurança dos ativos na organização. Qualquer vulnerabilidade e ocorrência de Segurança da Informação devem ser reportados, permitindo a correta e oportuna tomada de decisão do gestor.

Ressalta-se nos aspectos da Segurança da Informação na gestão da continuidade do negócio, o objetivo de evitar a solução de continuidade das atividades do negócio e resguardar os processos contra falhas, minimizando possíveis danos aos ativos da informação. E, por fim, ainda visando a diminuição de danos, destaca-se que a Conformidade possui como escopo impedir infrações das leis, estatutos e normas, bem como de outros requisitos de Segurança da Informação. Um dos seus aspectos importantes é a contratação de consultorias independentes para a verificação da aderência às normas.

3 MATERIAL E MÉTODO

A pesquisa identifica-se quanto à finalidade como aplicada, uma vez que segundo Marconi e Lakatos (2002) esse tipo de pesquisa "caracteriza-se por seu interesse prático, isto é, que os resultados sejam aplicados ou utilizados, imediatamente, na solução de problemas que ocorrem na realidade".

Em relação aos objetivos, a pesquisa é descritiva, pois de acordo com Gil (2010) a pesquisa descritiva "tem como objetivo descrever fatos observados, as características de determinadas populações ou fenômenos. Uma de suas peculiaridades está na utilização de técnicas padronizadas de coleta de dados, tais como o questionário e a observação sistemática".

Quanto aos procedimentos, a pesquisa caracteriza-se como estudo de caso. Para Yin (2010, p. 25) "o estudo de caso não necessita conter uma interpretação completa ou exata dos eventos atuais. Ao contrário, a finalidade do "estudo de caso" é estabelecer uma estrutura para discussão e debate entre os estudantes".

No que concerne à natureza, a pesquisa caracteriza-se como qualitativa, quanto a análise documental e aplicação da estratégia de etnografia para a coleta de dados. O estudo é quantitativo por mensurar, por meio de estatística descritiva e uma escala percentual, o nível de maturidade em GSI da Base Administrativa do Comando Militar da Amazônia.

Segundo Gil (2010), o uso da estatística descritiva visa reconhecer e entender os dados gerando informações relevantes. Através dela, sintetiza-se valores de natureza semelhantes e obtém-se uma visão do todo, apresentando os resultados através de gráficos, de tabelas e de medidas descritivas.

Já Marconi (2002) apresenta a análise de cluster como um conjunto de técnicas estatísticas com a finalidade agrupar objetos de acordo com suas peculiaridades, formando grupos ou conglomerados homogêneos.

A unidade de observação utilizada como evidência foi a Base Administrativa do Comando Militar da Amazônia, organização militar do Exército Brasileiro localizada na cidade de Manaus, Amazonas. Nela se concentram a maioria de todos os procedimentos administrativos desse Grande Comando (englobando sete Unidades Militares com características diferentes), principalmente os relacionados às aquisições, licitações, recebimento de material, controle patrimonial, dentre outros.

Na primeira etapa da coleta de dados foi feita uma análise documental que consistiu em uma pesquisa das normas existentes no órgão que pudessem implantar, determinar ou mesmo dar suporte às práticas de Segurança da Informação no órgão. Foi feita, ainda, uma seleção de toda a bibliografia pertinente ao tema. Posteriormente, uma leitura minuciosa de todos os textos selecionados e seleção da metodologia a ser utilizada. Nessa fase da revisão bibliográfica foram verificados a Segurança da Informação no Exército Brasileiro e a Norma ABNT NBR ISO/IEC 27002:2013.

Segundo Mattos e Castro (2011), para se obter uma descrição detalhada e completa a respeito de um determinado grupo de pessoas e, também, um maior entendimento do que eless fazem, deve-se utilizar a base metodológica da etnografia. Dessa forma, possibilita-se maiores reflexões e atitudes nas práticas que envolvem a unidade de observação.

Dessa forma, a coleta de dados foi desenvolvida através da observação se há conformidade das atividades desenvolvidas pelos servidores com as legislações pertinentes, utilizando a experiência e conversas informais com os militares que trabalham e são diretamente responsáveis pelo gerenciamento de TI no Órgão. Além disso, houve a observação direta de várias situações em algumas áreas da Base Administrativa.

Foi aplicado um questionário de múltipla escolha em escala *Likert* de quatro pontos (sim; sim, porém ...; não; não se aplica) submetido aos militares integrantes da unidade de

observação, com o objetivo de mensurar a percepção de SI nos servidores e sua aplicabilidade efetiva no Órgão.

A população para aplicação do questionário e a quantidade de respostas obtidas estão consolidados na Tabela 1.

Tabela 1 - Quantidade de respostas ao questionário aplicado

Público-alvo	População	Respostas	%
Oficiais	19	19 (*)	100 %
Praças	54	12 (**)	22,22 %

(*) 1 Coronel, 3 Tententes-Coronéis, 1 Major, 5 Capitães e 9 Tenentes
(**) 5 Subtenentes e 7 Sargentos.
Fonte: Desenvolvido pelos autores (2019).

O cálculo da confiabilidade dos resultados em relação ao tamanho da população (73) indicou um índice confiabilidade dos resultados próximos de 90% (margem de erro de 11%). O Quadro 1 indica os tópicos abordados na pesquisa de SI, aplicada aos servidores da BAdm.

Quadro 1. Temas abordados para avaliação da SI na perspectiva dos servidores da BAdm

Tópicos abordados	Quantidade de perguntas
1. Políticas de Segurança da Informação	1
2. Organização da Segurança da Informação	6
3. Segurança em recursos humanos	4
4. Gestão de ativos	4
5. Controle de acesso	5
6. Criptografia	2
7. Segurança física e do ambiente	6
8. Segurança nas operações	9
9. Segurança nas comunicações	5
10. Aquisição, desenvolvimento e manutenção de sistemas	6
11. Relacionamento na cadeia de suprimento	3
12. Gestão de incidentes de Segurança da Informação	2
13. Aspectos da Segurança da Informação na gestão da continuidade do negócio	2
14. Conformidade	3

Fonte: Desenvolvido pelos autores (2019).

O questionário para levantamento dos dados se baseou no estudo de Nascimento, Frogeri e Prado (2019). Os autores organizaram um questionário com base na ISO/IEC 27002 e no estudo de Sêmola (2014). Os Quadros 2, 3, e 4 apresentam a estrutura de pontuação sugerida por Sêmola (2014).

Quadro 2. Orientações da faixa 1 (pontuação / aderência).

Resultado entre 78-118 / Grau de aderência 66% - 100%
Parabéns! Sua empresa deve estar em destaque em seu segmento de mercado por causa da abrangência dos controles de segurança que aplica ao negócio. Apesar de não podermos ver a uniformidade das ações, distribuídas pelos 14 domínios, podemos dizer que sua empresa está conscientizada da importância da segurança

para a saúde dos negócios. A situação estará ainda melhor se todas as ações e controles aplicados tiverem sido decididos com base em uma análise de riscos integrada e sob a gestão de um Security Officer.

Fonte: Adaptado de Sêmola (2014).

Quadro 3. Orientações da faixa 2 (pontuação / aderência).

Resultado entre 39-77 / Grau de aderência 33% - 65%
Atenção! Esse resultado pode ter sido alcançado de diversas formas. Sua empresa pode ter adotado quase a totalidade dos controles, mas a maioria dos quesitos pode estar defasada, desatualizada ou inativa, o que demonstra bom nível de consciência, mas também deficiência na estrutura de gestão ou falta de fôlego financeiro para subsidiar os recursos de administração. Poderia, ainda, ter uma parcela representativa dos controles em ordem, deixando os demais inoperantes ou mesmo inexistentes. Diante disso, é conveniente alertarmos para a grande possibilidade de evolução, bem como a possibilidade de estagnação e de redução tendenciosa do nível de segurança por falta de orientação. Mais uma vez, a ausência de uma análise de riscos pode ser a causa para a desorientação dos investimentos e a dificuldade de priorização das atividades.

Fonte: Adaptado de Sêmola (2014).

Quadro 4. Orientações da faixa 3 (pontuação / aderência).

Resultado entre 0-38 / Grau de aderência 0% - 32%
Cuidado! A situação não é confortável para a empresa. A Segurança da Informação não está sendo tratada como prioridade, e a pontuação indica ausência ou ineficácia de muitos dos controles recomendados pela norma. As causas podem ser o desconhecimento dos riscos e a falta de sensibilização dos executivos e da alta administração. Arrisco dizer que seu segmento de mercado não vive um momento muito competitivo ou que a segurança não seja vista por seus clientes como um fator crítico de sucesso por causa da natureza de sua atividade. Outra hipótese é que devem estar ocorrendo ações isoladas — de um departamento ou de outro — que, apesar de louváveis, não distribuem uniformemente a segurança e acabam por minimizar o aumento do nível de segurança do negócio. Apesar de tudo, não é hora de desanimar. Sempre há tempo de reverter a situação. Comece com uma análise de riscos e boa sorte.

Fonte: Adaptado de Sêmola (2014).

Os resultados do questionário aplicado foram organizados, sintetizados e apresentados graficamente para melhor compreensão das questões pesquisadas.

4 ANÁLISES E DISCUSSÕES

Os resultados da pesquisa são apresentados em duas fases. Na primeira fase está o resultado da pesquisa documental e, em seguida, são exibidos os resultados obtidos do questionário aplicado aos servidores da Base Administrativa do CMA.

Foi realizado um estudo detalhado dos documentos elencados no Quadro 5, sendo constatado que toda documentação normativa relacionada à Segurança da Informação do Comando Militar da Amazônia, encontra-se em conformidade com as publicações da Diretoria de Ciência e Tecnologia do Exército, bem como da APF.

Quadro 5. Documentação sobre SI elaborada pela Diretoria de Ciência e Tecnologia e utilizada no CMA

Documento	Assunto e Objetivo
Decreto n° 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.
Portaria Nº 049-DCT, de 19 de dezembro de 2005.	Aprova as Instruções Reguladoras para Emprego Sistêmico do Serviço de Correio-Eletrônico no Exército Brasileiro - IRESCE (IR 13-06).
Portaria Nº 026-DCT, de 31 de março de 2006.	Aprova as Instruções Reguladoras para Emprego Sistêmico da Informática no Exército Brasileiro - IREMSI (IR 13-07).

Portaria Nº 003-DCT, de 31 de janeiro de 2007.	Aprova as Instruções Reguladoras Sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro - IRASEG (IR 13-09).
Portaria Nº 004-DCT, de 31 de janeiro de 2007.	Aprova as Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro - IRESER (IR 13-15).
Portaria Nº 006-DCT, de 5 de fevereiro de 2007.	Aprova as Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (2ª Edição).
Portaria Nº 011-DCT, de 29 de março de 2010.	Aprova o Plano de Migração para Software Livre no Exército Brasileiro, versão 2010.
Portaria Nº 720, de 21 de novembro de 2011.	Aprova a Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações.
Portaria Nº 803, de 30 de julho de 2014.	Aprova as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro (EB10-IG-01.014) e dá outras providências.
Portaria Nº 1.067, de 8 de setembro de 2014.	Aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 1ª Edição, 2014, e dá outras providências.

Fonte: Desenvolvido pelos autores (2019).

Nota-se que a unidade analisada dispõe de normas, regulamentos e legislações amparando e estimulando a implementação de políticas de Segurança da Informação em consonância com as legislações mais atualizadas em vigor.

A seguir, apresenta-se os resultados da pesquisa realizada nos servidores que compõe a Base Administrativa do CMA.

Verifica-se no Quadro 6 os resultados oriundos do questionário aplicado aos servidores da Base Administrativa do CMA para verificar o grau de aderência dessa unidade de análise em relação às normas da SI.

Quadro 6. Grau de aderência à NBR 27002:2013.

Controles sugeridos pela norma ABNT ISO/IEC 27002:2013	**Quantidade de perguntas**	**Média**	**Aderência (%)**
1.Políticas de Segurança da Informação	1	1,5	**74,2**
2.Organização da Segurança da Informação	6	5,9	49,5
3. Segurança em recursos humanos	4	5,3	65,7
4. Gestão de ativos	4	5,1	64,1
5. Controle de acesso	6	8,0	66,7
6. Criptografia	2	1,5	**37,9**
7. Segurança física e do ambiente	6	6,1	50,5
8. Segurança nas operações	9	9,6	53,6
9. Segurança nas comunicações	5	6,9	**69,3**
10. Aquisição, desenvolvimento e manutenção de sistemas	6	5,2	43,0
11. Relacionamento na cadeia de suprimento	3	3,4	55,9
12. Gestão de incidentes de Segurança da Informação	2	1,5	**38,7**
13. Aspectos da Segurança da Informação na gestão da continuidade do negócio	2	1,9	48,4
14. Conformidade	3	3,0	49,5
Total:	**59**	**64,7**	**54,8**

Fonte: Desenvolvido pelos autores (2019).

O questionário aplicado foi respondido por 31 militares, sendo 19 oficiais e 12 praças. Em relação ao grau de escolaridade dos servidores que responderam à pesquisa, sabe-se que 80,6% têm formação superior. Entre os 31 respondentes, 87,1% são do sexo masculino e 12,9% são do sexo feminino. No que concerne ao tempo na Organização, 19,35% possuem tempo menor que 1 ano, 41,94% possuem tempo entre 1 e 2 anos, 29,03% possuem tempo entre 2 e 3 anos e 9,68% possuem tempo maior que 3 anos. No tocante à função desempenhada pelos respondentes na OM, 32,25% são chefes de seção, 38,70% são adjuntos de seção e 29,05% desempenham suas funções como auxiliares.

O resultado obtido pela Organização é de 64,7 pontos e seu grau de aderência foi de 54,8%. Dessa forma, pode-se aferir que a BAdm se encontra na faixa 2 da escala definida por Sêmola (2014). A divisão das faixas de acordo com os controles sugeridos pela norma ABNT ISO/IEC 27002:2013 são os que se seguem: Faixa 1 – Observa-se 4 (quatro) tipos de controle: Políticas de Segurança da Informação (74%), Segurança em recursos humanos (66%), Controle de acesso (67%) e Segurança nas comunicações (69%); na Faixa 2, por sua vez, enquadrou-se todos os 10 (dez) controles restantes: Organização da Segurança da Informação (49%), Gestão de ativos (64%), Criptografia (38%), Segurança física e do ambiente (51%), Segurança nas operações (54%), Aquisição, desenvolvimento e manutenção de sistemas (43%), Relacionamento na cadeia de suprimento (56%), Gestão de incidentes de Segurança da Informação (39%), Aspectos da Segurança da Informação na gestão da continuidade do negócio (48%) e Conformidade (49%).

A maior parte dos resultados, muito embora estejam na faixa 2, conforme analisado anteriormente, evidenciam uma proximidade com o limite inferior dos valores e, consequentemente, uma necessidade de aprimoramento e evolução da gestão de Segurança da Informação. Somente quatro tipos de controle tiveram seus valores estabelecidos na Faixa 1 e, como na análise anterior, é necessário atentar aos baixos valores dos mesmos dentro do intervalo.

Dessa forma, observa-se que o Órgão demonstra uma boa maturidade em Segurança da Informação, porém, necessita de atenção na sua estrutura de gestão, uma vez que o grau de aderência da Organização às recomendações da norma ficou em 55%.

Os resultados mais positivos da pesquisa: Políticas de Segurança da Informação (74%), Segurança em recursos humanos (66%), Controle de acesso (67%) e Segurança nas comunicações (69%), indicam um bom nível de controle interno e uma satisfatória proteção das informações em redes. Parece, também, que há uma boa conscientização e cumprimento dos procedimentos pelos servidores dos procedimentos de Segurança da Informação. Embora abaixo dos 66% preconizados na Faixa 1, a Gestão de Ativos (64%) que visa assegurar que a informação receba um nível adequado de proteção, também teve uma boa avaliação.

Notou-se que a menor pontuação aferida retrata a Gestão de incidentes de Segurança da Informação (39%) e a Criptografia (38%). Isso pode sinalizar uma necessidade de melhor gerenciamento sobre os incidentes de SI, bem como aprimorar os procedimentos para comunicação de fragilidades encontradas.

Outra baixa pontuação foi encontrada no item Aquisição, desenvolvimento e manutenção de sistemas (43%). Essa percepção pode ter sido retratada dessa forma devido a peculiaridade da Organização que possui no 4º Centro de Temática (unidade vizinha ao CMA) seu gerenciamento para desenvolver e realizar manutenções de sistemas.

O item Conformidade se apresentou com resultados semelhantes ao item Organização da Segurança da Informação, ambos com 49%. Estes valores parecem indicar que as normas podem não estar sendo seguidas ou que nem todos os procedimentos estão sendo realizados.

No item Relacionamento da cadeia de suprimento, que visa garantir a proteção dos ativos da organização que são acessados pelos fornecedores, os 56% de aderência obtidos,

parecem indicar uma satisfatória aplicação dos controles internos em SI estendidos a prestadores de serviço e/ou fornecedores.

Por fim, com o objetivo de se aprimorar o grau da aderência da Organização em relação às recomendações de SI da norma, sugere-se a adoção das seguintes ações: (i) dar ampla divulgação das normas e orientações emanadas do escalão superior, atualizando e informando os servidores sobre os corretos procedimentos, a fim de informar e desenvolver o público interno da unidade; (ii) trabalhar a possibilidade de se manter em áreas importantes aqueles servidores que possuem intenção de permanecer na organização militar por mais tempo, a fim de se evitar a solução de continuidade nos processos de SI com a alta rotatividade da guarnição; e (iii) treinar os usuários em TI para que sejam capazes de identificar e notificar fragilidades em SI.

5 CONSIDERAÇÕES FINAIS

Neste momento, é oportuno retornar à pergunta de pesquisa que norteou o estudo: Qual o grau de aderência da Base Administrativa do Comando Militar da Amazônia às recomendações de Segurança da Informação (SI) da norma ABNT NBR ISO/IEC 27002:2013?

Foi possível verificar na BAdm problemas referentes a falta de conhecimento sobre SI e a dificuldade de se aprimorar a gestão de SI. As análises evidenciaram um moderado grau de incipiência em SI do órgão. Um grau moderado de SI pode indicar maior risco às informações e, como sugere Sêmola (2014), a organização pode ter adotado a maior parte dos controles, porém pode ter havido uma desatualização ou defasagem dos quesitos. Isso caracteriza um satisfatório nível de consciência, ao mesmo tempo que sinaliza uma carência na gestão ou mesmo a inexistência de alguns dos controles. Além disso, faz-se necessário observar tanto uma possível evolução, como redução do nível de segurança, baseado na falta de oportuna orientação (Sêmola, 2014).

Demonstrou-se que os integrantes da Base Administrativa necessitam de melhor e maiores informações para seu aprimoramento e consciência em SI. As análises permitiram observar a necessidade por aperfeiçoamento de práticas em Segurança da Informação na instituição, a fim de garantir controles eficazes e menos vulneráveis.

Os resultados da análise dos documentos sugerem a necessidade de criação de normas internas que, além de respeitar a legislação vigente, explique detalhadamente as funções e responsabilidades de todos em fiscalizar, contribuir e aplicar a SI.

O grau de aderência atingido no presente estudo foi classificado como mediano em relação às recomendações de SI da norma ABNT ISO/IEC NBR 27002:2013. Como sugestão para a melhora da classificação de aderência, sugere-se instruções aos servidores, para que estes possam estar sempre familiarizados e atualizados com as normas de SI, além de incorporarem mais atitudes de prevenção e proteção aos ativos de informação; deve-se buscar, ainda, atualização da legislação pertinente a implantação de SI na Unidade e, da mesma forma, todos os documentos decorrentes dela.

Assim, acredita-se que o estudo apresentado contribuiu para demonstrar que as legislações das organizações militares estão de acordo com as civis e possibilitam práticas semelhantes com as demais instituições. As limitações encontradas neste trabalho são relativas ao fato do estudo ter englobado apenas uma unidade militar, muito embora a organização analisada reúna mais seis outras unidades para as atribuições relativas à BAdm. Dessa forma, carece-se de outros estudos para dar suporte as demais organizações do CMA. Além disso, a abordagem quantitativa sobre os resultados não possibilitou deduções mais profundas.

Sugere-se como trabalhos futuros, a possibilidade de se repetir esse estudo em outras unidades militares abrangidas pelo CMA. Dessa forma, poderá se aferir a aderência de outras

organizações e determinar o nível de maturidade em SI nas unidades da região amazônica. O uso de uma pesquisa qualitativa pode fornecer dados mais precisos para identificação de possíveis falhas nos processos de Segurança da Informação, bem como no gerenciamento sobre os incidentes de SI e na comunicação de fragilidades encontradas.

REFERÊNCIAS

BRASIL. Estado-Maior do Exército. Aprova a Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações no Exército Brasileiro e dá outras providências. Portaria Nº 720-DCT, de 21de novembro de 2011. **Boletim do Exército**, Brasília, 2011.

BRASIL. Estado-Maior do Exército. Aprova as Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército Brasileiro e dá outras providências. Portaria Nº 006-DCT, de 05de fevereiro de 2007. **Boletim do Exército**, Brasília, 2.ed. 2007.

BRASIL. Estado-Maior do Exército. Aprova as Instruções Gerais de Segurança da Informação e Comunicações para o Exército Brasileiro e dá outras providências - SIMATEX (EB10-IG-01.014). Portaria Nº 803-EME, de 30 de julho de 2014. **Boletim do Exército**, Brasília, n. 37, 12 set. 2014.

BARBOSA, Aguiar de S. **Avaliação Preliminar dos Níveis de Maturidade dos Controles de Segurança da Informação e Comunicações adotados em Organizações Militares do Exército Brasileiro, de acordo com a Norma ABNT NBR ISO/IEC 27002:2005.** 2009. Monografia (Especialização) - Curso de Especialização em Gestão da Segurança da Informação e Comunicações - CEGSIC / Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília, Brasília. 2009.

BUSINESS CONTINUITY INSTITUTE - BCI. **Good practice guidelines 2008. A management guide to implementing global good practice in business continuity management.** BCI, 2008.

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos de Informação na Organizações.** 1. ed. Atlas, 2005.

COMANDO MILITAR DA AMAZÔNIA. **Missão.** Disponível em: <http://www.cma.eb.mil.br/home/missao-e-valores.html>. Acesso em: 05 nov. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 01/IN01/DSIC/GSIPR - Estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação, no âmbito da Administração Pública Federal, direta e indireta.** [Internet]. Oct 13; 2008. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 02/IN01/DSIC/GSIPR - Metodologia de Gestão de Segurança da Informação** [Internet]. Oct 13; 2008. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 03/IN01/DSIC/GSIPR - Diretrizes para a Elaboração de Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal** [Internet]. Jun 30; 2009. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 11/IN01/DSIC/GSIPR - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação (SIC) nos órgãos ou entidades da Administração Pública Federal; direta e indireta – APF** [Internet]. Oct 2; 2012. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 04/IN01/DSIC/GSIPR - (Revisão 01) - Diretrizes para o processo de Gestão de Riscos de Segurança da Informação - GRSIC nos órgãos e entidades da Administração Pública Federal** [Internet]. Feb 25; 2013. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 17/IN01/DSIC/GSIPR - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF)** [Internet]. Oct 4; 2013. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSIPR. **Norma Complementar 18/IN01/DSIC/GSIPR - Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federa (APF)** [Internet]. Oct 4; 2013. Disponível: http://dsic.planalto.gov.br. Acesso em: 09 set. 2019.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

IMONIANA, Joshua.O. **Auditoria de Sistemas de Informação.** 3. ed. Atlas, 2004.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. 1. ed. Brasília, 2015.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa**. 5 ed. São Paulo: Atlas, 2002.

MATTOS, C. G. L. de; CASTRO, P. A. de. **A abordagem etnográfica na investigação científica.** 2011. Disponível em http://books.scielo.org/id/8fcfr/pdf/mattos-9788578791902-03.pdf. Acesso em: 06 dez. 2019.

NASCIMENTO, T. F. DO; FROGERI, R. F.; PRADO, L. Á. Gestão de Segurança da Informação no Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo Brasileiro. **Revista de Sistemas e Computação**, Salvador, v. 9, n. 1, p. 189-210, jan./jun. 2019.

NBR 27001. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de Segurança da Informação** - Requisitos. 1a. ed. Rio de Janeiro: ABNT, 2006.

NBR 27002. 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**. Rio de Janeiro, 2013.

NBR 27005. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de Segurança da Informação**. 1a. ed. Rio de Janeiro: ABNT, 2008.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão executiva.** Elsevier, 2003.

YIN, Robert. K. **Estudo de Caso: Planejamento e Métodos.** 2. ed. Porto Alegre: Bookman. 2001.