Information Security Management in the Brazilian second Center for Integrated Air Defense and Air Traffic Control

Gestão de Segurança da Informação no Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo Brasileiro

Tairone Falheiros do Nascimento[1], Rodrigo Franklin Frogeri[2], Liz Áurea Prado[3]

[1]Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA II) – Curitiba – PR – Brasil. Centro Universitário do Sul de Minas – UNISMG – Varginha – MG – Brasil.
[2] Departamento de Pesquisa - Centro Universitário do Sul de Minas – UNISMG – Varginha – MG – Brasil. Programa de Pós-Graduação em Sistemas de Informação e Gestão do Conhecimento - Universidade FUMEC – Belo Horizonte – MG - Brasil
[3] Departamento de Pesquisa - Centro Universitário do Sul de Minas – UNISMG – Varginha – MG – Brasil. Centro Federal de Educação Tecnológica de Minas Gerais – CEFETMG – Varginha – MG – Brasil.

taironetfn@cindacta2.gov.br, rodrigo.frogeri@professor.unis.edu.br, liz.prado@professor.unis.edu.br

Abstract. *The violation of principles such as confidentiality, integrity and availability of information, basic attributes of Information Security (IS), can affect business continuity and productivity and development organizations. Thus, the information security should be a subject of great relevance for organizations of Aeronautics Command (COMAER). In this sense, this study aimed to assess the compliance level of Information Security of the Second Center for Integrated Air Defense and Air Traffic Control (CINDACTA II) in relation to COMAER and Federal Public Administration publications, as well as the degree of CINDACTA II adherence for NBR 27002:2013 recommendations. The research was characterized as applied and descriptive about the objective. It was adopted the hypothetical-deductive method by means the documentary research and survey techniques. As to the problem approach was qualitative and quantitative. The study was carried out with five managers responsible for information security and 57 IT users in the CINDACTA II. We concluded that the CINDACTA II Information Security management is at a level that meets the requirements of NBR 27002:2013, as well as the publications of COMAER and Federal Public Administration. We observed similarities in IS practices between military and civil organizations, allowing us to infer that cultural issues, values and beliefs of the organizational environment influence information security.*

Resumo. *A violação de princípios como a confidencialidade, integridade e disponibilidade da informação, atributos básicos da Segurança da Informação (SI),*

pode afetar a continuidade de negócios e a produtividade e desenvolvimento de organizações. Destarte, a SI deve ser um assunto de grande relevância para as Organizações do Comando da Aeronáutica (COMAER). Nesse sentido, esta pesquisa pretendeu avaliar o nível de conformidade da SI do Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA II) em relação às publicações no âmbito do COMAER e da Administração Pública Federal, bem como o grau de aderência do CINDACTA II às recomendações da norma NBR 27002:2013. A pesquisa caracterizou-se como aplicada e quanto ao objetivo descritiva. Adotou-se o método hipotético-dedutivo por meio das técnicas de pesquisa documental e survey. Quanto à abordagem do problema foi de natureza qualitativa e quantitativa. O estudo foi realizado com cinco gestores responsáveis pela Segurança da Informação e 57 usuários em TI do CINDACTA II. Ao final do estudo, concluiu-se que a gestão de Segurança da Informação do CINDACTA II encontra-se em um nível que atende aos requisitos da norma NBR 27002:2013, bem como às publicações do COMAER e da Administração Pública Federal. Observou-se semelhanças nas práticas em SI entre organizações militares e civis, permitindo inferir que questões culturais, valores e crenças do ambiente organizacional influenciam na segurança da informação.

1. Introdução

A crescente evolução tecnológica possibilita maior acesso às informações, bem como aumenta a capacidade de armazenamento de dados. Em contrapartida, permite uma maior exposição desses dados às ameaças que podem comprometer a confidencialidade, integridade e disponibilidade das informações.

As organizações vêm utilizando grandes servidores de armazenamento localizados em ambientes fisicamente seguros e protegidos logicamente por senha, criptografia, *firewall*, antivírus e outros artifícios tecnológicos, com o objetivo de dificultar o acesso não autorizado aos recintos onde as informações são processadas e armazenadas. Discute-se que a preocupação da segurança o ativo informação não deve ser somente com a infraestrutura física e lógica, mas, especialmente com as pessoas que manipulam as informações de uma organização. A implementação de regras, normas e políticas que padronizem as ações dos usuários da informação é tão importante quanto o desenvolvimento de meios sofisticados para mantê-la protegida (FONTES, 2006). Quanto a este aspecto, nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas Políticas de Segurança da Informação (PSI), que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais, de infraestrutura e logística, além dos recursos humanos (MARCIANO, 2006).

Nesse sentido, no âmbito da Administração Pública Federal (APF), a informação é um ativo valioso e assim, deve ser adequadamente tratada, armazenada e protegida (BRASIL, 2016). Três características são básicas para a Segurança da Informação (SI): confidencialidade, disponibilidade e integridade. Um Sistema de Gestão de Segurança da Informação (SGSI) objetiva preservar tais princípios por meio da aplicação de um processo de gestão de riscos, fornecendo confiança às partes interessadas de que os riscos são adequadamente geridos (NBR 27001, 2013). Dessa forma, é notório que a violação da tríade da Segurança da Informação (SI) - confidencialidade, integridade e

disponibilidade - pode prejudicar ou até mesmo inviabilizar as atividades fim de uma organização.

O Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA II) é uma Organização Militar (OM), subordinada ao grande comando do Departamento de Controle do Espaço Aéreo (DECEA), que tem como missão institucional "garantir a vigilância e o controle da circulação aérea geral, bem como conduzir as aeronaves que têm por missão manter a integridade e a soberania do espaço aéreo brasileiro, na área de sua responsabilidade" (CINDACTA II, 2017, p. 1). O CINDACTA II é responsável pelo espaço aéreo de todo o Sul e parte do Centro-oeste Brasileiro, tornando-se fundamental a preocupação com os requisitos de SI em um sistema crítico como o controle do tráfego aéreo (PIZZO; CUGNASCA, 2010).

As Organizações que envolvem o Comando da Aeronáutica (COMAER) devem tratar a GSI como um assunto de grande relevância (BRASIL, 2017), direcionando, assim, a seguinte pergunta de pesquisa: qual o nível de conformidade em SI do CINDACTA II em relação às publicações no âmbito do COMAER e da Administração Pública Federal, bem como o grau de aderência do CINDACTA II às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013? O objetivo geral do estudo foi avaliar o nível de conformidade da segurança da informação do CINDACTA II em relação às publicações no âmbito do COMAER e da Administração Pública Federal, bem como o grau de aderência do CINDACTA II às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013.

Para atingir o objetivo proposto, o estudo se baseou no método hipotético-dedutivo. Utilizou-se abordagens quantitativa e qualitativa aplicadas por meio de estatística descritiva e análise documental. O estudo foi dividido em quatro tópicos, além desta introdução: o tópico seguinte trata os fundamentos teóricos que suportam a pesquisa; o tópico três apresenta a metodologia aplicada na pesquisa; o tópico quatro discorre sobre as análises e discussões; e o cinco, as considerações finais. Este trabalho é uma versão ampliada do estudo de mesmo título apresentado no IV Simpósio Mineiro de Gestão, Educação, Comunicação e Tecnologia da Informação – SIMGETI (NASCIMENTO; FROGERI; PRADO, 2018).

2. Referencial teórico

Este capítulo discorre sobre os principais conceitos relacionados à Gestão de Segurança da Informação (GSI), sendo composto por quatro seções: (2.1) Ciclo de Vida da Informação, (2.2) Segurança da Informação, (2.3) Gestão de Segurança da Informação e (2.4) ABNT NBR ISO/IEC 27002:2013.

2.1 Ciclo de Vida da Informação

Segundo Cassarro (1999, p. 35), a informação pode ser definida como "um fato, um evento, um comunicado". McGarry (1999, p. 4) afirma que a informação pode ser "a matéria prima da qual se extrai o conhecimento". Davenport (2000) expande o conceito de informação de Cassarro (1999), relacionando a definição de informação com dado e conhecimento, conforme Quadro 1.

Quadro 1. Dados, informações e conhecimento

Dados	Informação	Conhecimento
Simples observações sobre o estado do mundo	Dados dotados de relevância e propósito	Informação valiosa da mente humana; Inclui reflexão, síntese, contexto
Facilmente estruturado	Requer unidade de análise	De difícil estruturação
Facilmente obtido por máquinas	Exige consenso em relação ao significado	De difícil captura em máquinas
Frequentemente quantificado	Exige necessariamente a medição humana	Frequentemente tácito
Facilmente transferível		De difícil transferência

Fonte: Adaptado de Davenport (2000, p. 18).

Conforme Baltzan e Phillips (2012), os dados são fatos brutos que descrevem um evento, enquanto informação é o produto da conversão dos dados em um contexto significativo e útil. Portanto, pode-se afirmar que o processo de construção do conhecimento envolve o dado que é o elemento básico ou matéria-prima, o qual organizado de forma lógica cria a informação, que por sua vez, ao ser interpretada, gera o conhecimento (DAVENPORT, 2000).

Sêmola (2014, p. 39) afirma que "a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa". Neste sentido, no âmbito da Administração Pública Federal (APF), a informação é um ativo valioso e, assim, deve ser adequadamente tratada, armazenada e protegida (BRASIL, 2016). Ativo é "todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada, os equipamentos em que é manuseada, transportada e descartada" (SÊMOLA, 2014, p. 45).

A informação, como um ativo organizacional, também possui um ciclo de vida natural. Para Sêmola (2014, p. 9) "o ciclo de vida da informação é composto e identificado pelos momentos vividos pela informação que a coloca em risco". Isso ocorre quando os ativos físicos, tecnológicos e humanos fazem uso da informação, nos processos da empresa que a mantém funcionando. São identificados por este autor quatro momentos em que é necessário manter a atenção, pois são ameaças à SI, são eles: manuseio – quando a informação é criada e manipulada; armazenamento – quando a informação é armazenada (pode ser em papel ou em meios magnéticos); transporte – quando a informação é transportada (seja por conversas telefônicas, por fax, ou ainda, por e-mail); e descarte – quando a informação é descartada, seja quando um papel é descartado em uma lixeira, ou ao eliminar arquivos eletrônicos.

Assim, pode-se reconhecer a necessidade de proteção do ativo informação, em virtude da sua importância para os processos de negócios de qualquer organização, bem como que tal proteção deve existir em todos os estágios/ciclos da vida da informação (NBR 27002, 2013).

2.2 Segurança da Informação

A realidade das ameaças à SI tem sido reportada aos Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança (CERT) de vários países. No Brasil, o CERT.br é a organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. De acordo com esta organização, o total de notificações em 2015 foi de 722.205, número muito superior ao ano de 2010 (142.844). O número cresce exponencialmente desde 1999, ano em que se iniciou o levantamento, e que contou com apenas 3.107 incidentes reportados. O ano de 2014 mostrou-se o ano com a maior ocorrência de incidentes, num total de 1.047.031 incidentes registrados (CERT.br, 2017).

Diante deste cenário, percebe-se uma necessidade do desenvolvimento de políticas que possam gerir e mitigar essas ameaças. A NBR 27002 (2013) trata da Gestão da Segurança da Informação (GSI) que tem como função estabelecer estratégias para gerir riscos e definir controles adequados de forma a garantir a integridade, confiabilidade e disponibilidade das informações organizacionais.

O Decreto 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação (PSI) nos órgãos e nas entidades da APF no artigo 2º define a SI como "proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito […]". A Instrução Normativa nº 01 conceitua a Segurança da Informação e Comunicações (SIC) como "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações"; e considera que as informações são ativos valiosos para a eficiente prestação dos serviços públicos no âmbito da APF. Assim, pode-se definir SI como a área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos.

Verifica-se, portanto, que a manutenção das propriedades da informação, tais como, disponibilidade, integridade, confidencialidade e autenticidade está intimamente relacionada ao conceito de SI e se constitui em objetivo a ser atingido para a preservação da informação face aos diversos tipos de ameaças que se apresentam.

Diante do exposto, estabeleceu-se a seguinte hipótese: H_1. o CINDACTA II estabelece e implementa políticas, planos e normas visando atender seus requisitos de SI de acordo com o que está preconizado na legislação e normatização em vigor.

2.3 Gestão de Segurança da Informação

Segundo a NBR 27002 (2013, p. 10), a SI é "alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware"*.

O Sistema de Gestão de Segurança da Informação (SGSI), visa prover um modelo de gestão, dentro de uma perspectiva estratégica da organização, para estabelecer, implementar, manter e melhorar continuamente os controles de segurança e garantir que os controles sejam adequados para proteger os ativos de informação (NBR 27001, 2013).

A importância na implantação de um SGSI é permitir à organização identificar os pontos vulneráveis e as falhas nos sistemas que deverão ser corrigidos. Para isso é imprescindível que o SGSI tenha o patrocínio do nível estratégico da organização e se possível do departamento jurídico, que deverá conferir sua legitimidade.

Ainda de acordo com as orientações da norma, o SGSI deve embasar-se em um ciclo de melhoria contínua baseado no ciclo "*Plan-Do-Check-Act*" (PDCA), conforme apresentado na Figura 1. O objetivo do ciclo PDCA é minimizar o impacto de um incidente pelo uso adequado das seguintes ações: *plan* (planejar) - estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização; *do* (fazer) - implementar e operar a política, controles, processos e procedimentos do SGSI; *check* (checar) - avaliar e, quando aplicável, medir o desempenho de um processo frente a política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção; e *act* (agir) - executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI (NBR 27001, 2006).

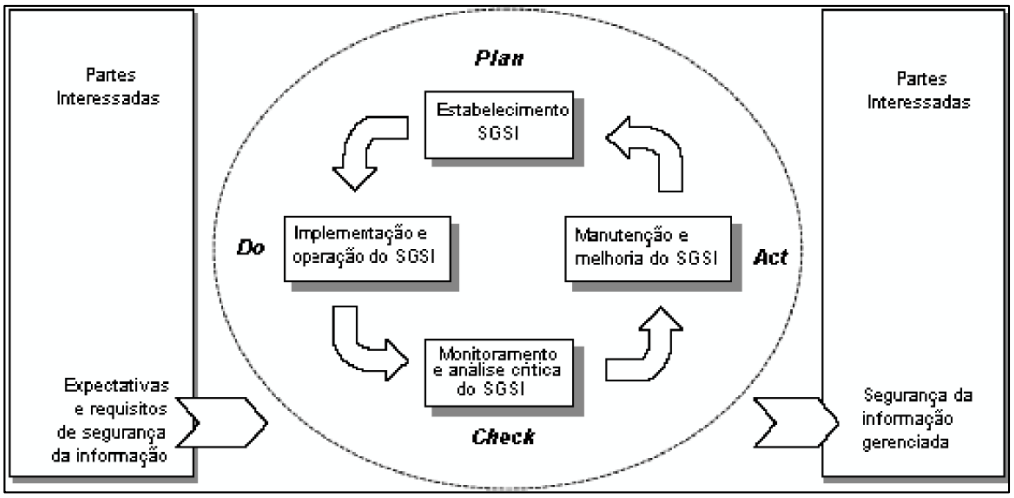

Figura 1 - Modelo PDCA aplicado aos processos do SGSI

Fonte: Adaptado da NBR 27001 (2006, p. 6).

O modelo PDCA para um planejamento de GSI destaca como elementos de entrada e saída do ciclo as partes interessadas (*stakeholders*), sendo estes elementos fundamentais no estabelecimento de um sistema de gestão em segurança da informação.

Nesse sentido, a seguinte hipótese foi estabelecida: H_2. usuários com a real percepção de que são parte fundamental na garantia da inviolabilidade da informação são pontos fortes na efetividade da gestão da Segurança da Informação.

2.4 ABNT NBR ISO/IEC 27002:2013

A norma ABNT NBR ISO/IEC 27002:2013 foi elaborada para especificar os requisitos para o estabelecimento, implementação, operacionalização, monitoração, revisão, manutenção e melhoria de um SGSI. Considera os riscos de negócio de uma organização, por meio da definição de controles que podem ser utilizados para atender aos requisitos identificados por meio da análise/avaliação de riscos (NBR 27002, 2013).

A norma possui 18 capítulos, sendo 14 deles referentes às seções de controles de segurança da informação, divididas em 35 objetivos de controle e 114 controles aplicáveis à segurança da informação (NBR 27002, 2013). Conforme estabelece a norma, tais controles de segurança precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando demandado, para garantir em linhas operacionais de decisão (nível de arquitetura) que os objetivos de negócio e da segurança da organização sejam atendidos (NBR 27002, 2013).

Assim, a norma apresenta um conjunto de controles que pode ser implementado para atender aos requisitos de segurança da organização. Em geral, esses requisitos devem ser levantados em uma etapa prévia por meio de técnicas como a análise e avaliação de riscos. A norma ABNT NBR ISO/IEC 27002:2013 não atende a todas as demandas organizacionais e prevê que adaptações ou novos controles possam ser utilizados além dos que são recomendados.

Destarte, o caminho para alcançar a SI passa por identificar quais controles são necessários para mitigar os riscos associados aos ativos da organização. Uma forma de fazer isso é identificar quais objetivos de negócios e de SI são atendidos pelos controles já adotados e quais ações ainda precisam ser adotadas, tendo em vista a realidade da organização. Destarte, estabeleceu-se a seguinte hipótese: H_3. o CINDACTA II implementa os controles de segurança indicados na norma ABNT NBR ISO/IEC 27002:2013.

3. MATERIAL E MÉTODO

Este estudo teve como objetivo geral avaliar o nível de conformidade da SI do CINDACTA II em relação às publicações no âmbito do COMAER e da Administração Pública Federal, bem como o grau de aderência do CINDACTA II às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013.

Para alcançar o objetivo estabelecido três hipóteses foram estabelecidas e serão confirmadas ou refutadas ao término desta pesquisa. Os seguintes objetivos específicos foram estabelecidos em relação a cada hipótese: O_1. verificar se os instrumentos normativos internos do CINDACTA II sobre SI estão em conformidade com o que está preconizado na legislação e normatização em vigor; O_2. avaliar a percepção ou conhecimento acerca da SI dos usuários em TI da Organização em estudo. O_3. verificar o grau de aderência do CINDACTA II em relação às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013.

De acordo com Marconi e Lakatos (2003, p.155), a pesquisa é “um procedimento formal, com método de pensamento reflexivo, que requer um tratamento científico e se constitui no caminho para conhecer a realidade ou para descobrir verdades parciais”. Para Gil (2002, p. 17), a pesquisa é “desenvolvida mediante o

concurso dos conhecimentos disponíveis e a utilização cuidadosa de métodos, técnicas e outros procedimentos científicos". Para atingir os objetivos propostos, o estudo se baseou no método hipotético-dedutivo. Segundo Prodanov e Freitas (2013, p. 32) tal método "inicia-se com um problema ou uma lacuna no conhecimento científico, passando pela formulação de hipóteses e por um processo de inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese".

Em relação a seu objetivo, a pesquisa é de caráter descritivo, e quanto à abordagem do problema é classificada como de natureza qualitativa e quantitativa. Os dados do estudo foram obtidos por meio de pesquisa documental e *survey*. A coleta dos dados ocorreu em três etapas: (i) a primeira etapa foi realizada mediante pesquisa documental relativa às normas e regulamentos utilizados ou produzidos pela Organização em relação a segurança da informação; (ii) a segunda etapa foi realizada por meio da aplicação de questionário fechado em escala *Likert* de quatro pontos (sim; sim, porém ...; não; não se aplica) aos gestores de TI da Organização. O questionário elaborado baseou-se na proposta de Sêmola (2014) sendo que a pontuação máxima a ser obtida é de 118 pontos. O autor afirma que tal instrumento auxilia gestores em TI a perceber o grau de aderência da Organização em relação às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013. Sêmola (2014) realizou orientações aos gestores em relação a três possíveis faixas de pontuação obtidas no referido questionário, conforme Quadros 2, 3 e 4.

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).

O questionário foi disponibilizado em meio impresso e aplicado aos gestores responsáveis pela SI do CINDACTA II – oficiais e civis assemelhados pertencentes à Seção de Segurança da Informação (CSSI) e às Seções pertencentes à Subdivisão de Tecnologia da Informação (TTI) da Organização – totalizando sete profissionais; desses, cinco participaram da pesquisa. Um total de 14 temas e 59 questões compuseram o instrumento de levantamento de dados desta etapa, seguindo as recomendações de Sêmola (2014). O Quadro 5 apresenta os temas abordados no instrumento de avaliação da SI na perspectiva dos gestores em TI.

Quadro 5. Temas abordados para avaliação da SI na perspectiva dos gestores em SI

Tema abordado	**Quantidade de questões***
Políticas de segurança da informação	1
Organização da segurança da informação	6
Segurança em recursos humanos	4
Gestão de ativos	4
Controle de acesso	6
Criptografia	2
Segurança física do ambiente	6
Segurança nas operações	9
Segurança nas comunicações	5
Aquisição, desenvolvimento e manutenção de sistemas	6
Relacionamento na cadeia de suprimento	3
Gestão de incidentes de segurança da informação	2
Aspectos da segurança da informação na gestão da continuidade do negócio	2
Conformidade	3

Fonte: Desenvolvido pelos autores (2017).

*Os instrumentos de pesquisa utilizados neste estudo foram fornecidos aos avaliadores e estão disponíveis sob solicitação dos interessados.

A terceira etapa se deu por intermédio da aplicação de questionário eletrônico aos usuários em TI da Organização. As questões do questionário foram elaboradas com a finalidade de abordar os doze temas da área de SI preconizados na NBR ISO/IEC 27002:2013 (Quadro 6). A escolha dos temas está relacionada ao papel (atitude, comportamento e conhecimento) que os usuários em TI desempenham a favor ou não da SI na Organização.

Quadro 6. Temas abordados para avaliação da SI na perspectiva dos usuários

Tema abordado	Quantidade de questões
Uso do antivírus	2
Utilização do *firewall*	2
Senhas	4
Partilha de senhas	2
Bloqueio do computador	2
Equipamentos de armazenamento externo	2
Cópias de segurança	3
Correio eletrônico	4
Encriptação da informação	3
Conhecimento do usuário	7
Papel do usuário na Segurança da Informação	6
Campanha de educação e conscientização	2

Fonte: Desenvolvido pelos autores (2017).

*Os instrumentos de pesquisa utilizados neste estudo foram fornecidos aos avaliadores e estão disponíveis sob solicitação dos interessados.

Os temas abordados estão relacionados aos tópicos nove (Controle de Acesso) e treze (Segurança nas comunicações) da norma NBR ISO/IEC 27002:2013 e totalizaram 39 questões, apresentados em escala *Likert* de cinco pontos (discordo totalmente a concordo totalmente). Um total de 74 pessoas foram convidadas para participar da terceira etapa do estudo, sendo que 57 participaram. A amostra do estudo envolveu militares e civis vinculados ao CINDACTA II que fazem uso diário dos recursos computacionais da OM. O convite foi realizado por meio eletrônico (e-mail corporativo). Descartou-se da amostra ocupantes dos cargos de gestão. Um total de 17 convidados não participaram da pesquisa.

4. Resultados e análises

Os resultados da pesquisa são apresentados em três etapas. Na primeira etapa são destacados os resultados da pesquisa documental. Na sequência, os resultados obtidos do questionário aplicado aos gestores em TI. Em seguida, os resultados do questionário aplicado aos usuários em TI.

4.1. Análises e discussões - pesquisa documental

Para a pesquisa documental, realizou-se uma análise criteriosa das documentações existentes acerca da Segurança da Informação e aplicáveis ao CINDACTA II. Constatou-se que toda documentação normativa relacionada a SI, elaborada ou revisada no âmbito do CINDACTA II, encontra-se em consonância com as publicações do COMAER, bem como da APF e demais instrumentos de teor legal afetos ao tema, conforme Quadro 7.

Quadro 7. Documentação sobre SI elaboradas pelo CINDACTA II

Documento	Assunto	**Propósito**
Norma Padrão de Ação (NPA) 406	Funcionamento, Organização e Operação da Subdivisão de Tecnologia da Informação (TTI) e suas Seções	Regular o funcionamento e organização da Subdivisão de Tecnologia da Informação (TTI) e suas Seções subordinadas, pertencentes à Divisão Técnica do CINDACTA II.
NPA 460	Padronização de Ações em Tecnologia da Informação	Definir os procedimentos para utilização dos recursos de Tecnologia da Informação (TI) aplicados nas atividades administrativas do CINDACTA II.
NPA 461	Elaboração do Plano de Tecnologia da Informação do CINDACTA II	Estabelecer as diretrizes aplicáveis à elaboração e revisão do Plano Diretor de Tecnologia da Informação (PDTI) do CINDACTA II, dotando o Centro de um planejamento visando propor, coordenar e articular as estratégicas e investimentos na área de Tecnologia da Informação (TI), em conformidade com a missão da Organização.
NPA 463	Padronização de Ações em Informática Operacionais	Definir procedimentos para utilização dos recursos de Tecnologia da Informação (TI) diretamente aplicados nas atividades operacionais do CINDACTA II.
NPA 464	Política de Uso da Internet	Normatizar o uso apropriado do acesso à Internet através dos recursos de Tecnologia da Informação (TI) do CINDACTA II, PACT e Destacamentos subordinados.
NPA 465	Procedimentos para Implantação, Controle e Manutenção de Equipamentos de Informática e Sistemas Administrativos	Estabelecer os procedimentos para a implantação, controle e manutenção dos equipamentos de informática, bem como de sistemas administrativos, cuja responsabilidade é da Subdivisão de Tecnologia da Informação (TTI), através da Seção de Informática Administrativa (TIAd) do CINDACTA II.
NPA 466	Funcionamento do Comitê Gestor de Tecnologia da Informação do CINDACTA II	Estabelecer as diretrizes aplicáveis ao funcionamento do Comitê de Tecnologia da Informação do CINDACTA II (CGTI/CINDACTA II), visando dotar a Organização de uma instância deliberativa para propor, coordenar e articular as estratégias e investimentos na área de Tecnologia da Informação (TI), em conformidade com a missão da Organização.
NPA 467	Política de Segurança da Informação do CINDACTA II	Estabelecer a Política de Segurança da Informação no âmbito do CINDACTA II para a correta utilização dos recursos de Tecnologia da Informação (TI).

Fonte: Desenvolvido pelos autores (2017).

Do exposto, foi possível confirmar a hipótese H_1. a Organização estabelece e implementa políticas, planos e normas visando a atender seus requisitos de Segurança da Informação de acordo com o que está preconizado na legislação e normatização em vigor.

Na seção seguinte discute-se os resultados do questionário aplicado aos gestores de TI da organização em estudo.

4.2. Análises e discussões - gestores em TI

O Quadro 8 apresenta os resultados do questionário aplicado aos gestores em TI da Organização. Objetivou-se verificar o grau de aderência do CINDACTA II em relação às recomendações da norma ABNT NBR ISO/IEC 27002:2013.

Quadro 8 – Grau de aderência à NBR 27002:2013

Domínio		Pontuação						Aderência (%)
	Qtde perguntas	Respondentes					Organização	
		1	2	3	4	5		
1. Políticas de segurança da informação	1	1	2	2	2	2	1,8	90
2. Organização da segurança da informação	6	9	8	9	9	9	8,8	73
3. Segurança em recursos humanos	4	6	5	3	6	7	5,4	68
4. Gestão de ativos	4	6	6	6	7	7	6,4	80
5. Controle de acesso	6	12	12	12	12	12	12	100
6. Criptografia	2	3	3	1	2	3	2,4	60
7. Segurança física e do ambiente	6	7	8	11	12	12	10	83
8. Segurança nas operações	9	11	6	7	10	10	8,8	49
9. Segurança nas comunicações	5	8	7	6	10	10	8,2	82
10. Aquisição, desenvolvimento e manutenção de sistemas	6	8	1	2	5	5	4,2	35
11. Relacionamento na cadeia de suprimento	3	2	0	0	3	4	1,8	30
12. Gestão de incidentes de segurança da informação	2	4	3	4	4	4	3,8	95
13. Aspectos da segurança da informação na gestão da continuidade do negócio	2	4	1	3	3	4	3	75
14. Conformidade	3	0	2	1	5	4	2,4	40
Total	**59**	**81**	**64**	**67**	**90**	**93**	**79**	**67**

Fonte: Dados da pesquisa (2017).

Perante o exposto, foi constatado que a Organização atingiu a pontuação de 79 e o grau de aderência de 67% e se encontra na faixa 1, conforme escala definida por Sêmola (2014). É importante destacar que oito domínios constam na faixa 1 (Quadro 2), são eles: A5 – Controle de acesso (100%); A12 – Gestão de incidentes de segurança da informação (95%); A1 – Políticas de segurança da informação (90%); A7 – Segurança física e do ambiente (83%); A9 – Segurança nas comunicações (82%); A4 – Gestão de ativos (80%); A13 – Aspectos da segurança da informação na gestão da continuidade do negócio (75%); e A2 – Organização da segurança da informação (73%).

Ademais, cinco domínios constam na faixa 2 (Quadro 3), são eles: A3 – Segurança em recursos humanos (68%); A6 – Criptografia (60%); A8 – Segurança nas operações (49%); A14 – Conformidade (40%); e A10 – Aquisição, desenvolvimento e manutenção de sistemas (35%).

Por fim, somente o domínio A11 – Relacionamento na cadeia de suprimento (30%) consta na faixa 3 (Quadro 4). Diante dos resultados, a hipótese H_2, a Organização implementa os controles de segurança preconizados na norma ABNT NBR ISO/IEC 27002:2013 foi parcialmente confirmada, tendo em vista que o grau de aderência da Organização às recomendações da norma ficou em 67%.

Observou-se pelo resultado apresentado no item conformidade, que tem com objetivo garantir que a SI esteja implementada e seja operada de acordo com as políticas e procedimentos da organização, certa divergência com a avaliação das documentações existentes na organização. A aderência de 40% pode indicar que as normas existem, contudo, podem não ser efetivamente seguidas ou não estejam amplamente implementadas. A menor pontuação observada (30%) ocorreu para o tema "relacionamento na cadeia de suprimentos", que tem como objetivo garantir a proteção dos ativos da organização que são acessados pelos fornecedores. A baixa pontuação pode indicar uma preocupação maior da instituição pela segurança interna e desconsiderar aspectos de SI já vigentes a terceiros. A norma NBR ISO/IEC 27002:2013 preconiza que os mesmos controles em SI aplicados internamente na organização devem se estender a prestadores de serviço e/ou fornecedores.

O tema aquisição, desenvolvimento e manutenção de sistemas, que visa garantir que a SI seja parte integrante de todo o ciclo de vida dos sistemas de informação, incluindo os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas também se apresentou com uma pontuação abaixo de 40%. Apesar de inferências mais profundas sobre o resultado não serem possíveis por uma análise quantitativa, o baixo resultado pode indicar ausência de alinhamento entre os setores de desenvolvimento e de SI, uma vez que há normas vigentes (NPA 465) para tratar do tema.

Destaca-se como resultados positivos os temas: controle de acesso (100%), gestão de segurança da informação (95%) e política de segurança da informação (90%). Tais resultados podem indicar que a organização tem controles internos documentados e, em grande parte, estão implementados com considerável eficiência.

Finalmente, tendo em vista a melhoria do grau da aderência da Organização em relação às recomendações de SI da norma, sugere-se a adoção das seguintes ações: (i) revisar, periodicamente o documento de política de segurança da informação, bem como os documentos originados a partir dela, tais como normas e orientações; a fim de manter a SI na Organização em níveis desejáveis de confiabilidade; (ii) atualizar o inventário dos recursos de informação (ativos) disponíveis na OM; e (iii) treinar os usuários em TI para que sejam capazes de identificar e notificar fragilidades em SI.

Com o objetivo de aprofundar na compreensão dos aspectos de SI da organização, analisou-se a perspectiva dos usuários em TI.

4.3. Análises e discussões - usuários em TI

Em relação ao grau de escolaridade dos respondentes, constatou-se que 96,5% tem formação superior. Entre as 57 respostas, 87,7% são do sexo masculino e 12,3% são do sexo feminino; no que concerne ao tempo na Organização, 35,1% possuem

tempo entre 2 e 5 anos, 28,1% possuem tempo entre 5 e 10 anos, 19,3% possuem tempo menor que 2 anos, 12,3% possuem tempo acima de 15 anos e 5,3% possuem tempo entre 10 e 15 anos. No tocante à função desempenhada pelos respondentes na OM, 42,1% são chefes de seção, 17,5% são adjuntos de seção, 15,8% são chefes de subdivisão, 12,3 desempenham sua função com auxiliares, 7% são comandantes, subcomandantes ou chefe de divisão e 5,3% são adjuntos de divisão.

A seguir, buscou-se avaliar a percepção dos usuários em TI da Organização sobre as boas práticas em SI. A Tabela 1 apresenta os percentuais de concordância total em relação aos temas analisados, de acordo com a NBR ISO/IEC 27002:2013.

Tabela 1. Resumo dos resultados que avaliaram a percepção dos usuários em TI sobre boas práticas em SI na organização

Tema	**%**
Campanha de educação e conscientização	**66,5**
Comportamento do usuário acerca do tratamento dado ao descarte das informações sigilosas.	65,0
Em relação ao projeto de se criar um portal no sítio interno da organização (portal intraer) para disseminação de assuntos referentes à SI	66,7
O usuário ao detectar algum tipo de anomalia no seu computador comunica o ocorrido ao responsável pela GSI da organização.	67,0
Opinião a favor da criação de campanhas educativas de conscientização de temas referentes à SI.	61,4
Os usuários, conscientes do seu papel na SI, buscam se manter atualizados sobre os assuntos inerentes ao tema.	43,9
Um usuário em TI orientaria outro usuário sobre os procedimentos corretos diante de uma situação de quebra das regras de SI na organização.	94,7
Conhecimento do usuário	**83,3**
Conhecimento da adoção pela organização das políticas de controle de acesso aos recursos computacionais.	94,7
Conhecimento da adoção pela organização de procedimentos para detectar e punir violações à SI.	86,0
Entendimento de que a informação é um ativo da organização e, portanto, deve ser preservada.	68,4
Pleno conhecimento da importância que os sistemas operacionais das estações de trabalho, bem como os aplicativos estejam sempre atualizados e com os patches mais recentes instalados.	84,2
Cópias de segurança	**45,6**
Desconhecimento de que a organização adota procedimentos para manter a informação sempre disponível.	36,8
Efetua cópias de segurança.	80,7
Nunca efetuaram cópias de segurança.	19,3

Correio eletrônico	**42,2**
Desconhecem a importância da análise do assunto do e-mail antes de abri-lo.	14,1
Nunca abrem, executam ou leem os arquivos anexados em e-mails recebidos de fontes desconhecidas.	79,0
Nunca utilizaram e-mail corporativo para tratar de assuntos pessoais.	72,0
Utilizam computadores de outras pessoas para acessar contas de correio eletrônico e similares.	3,5
Encriptação da informação	**58,8**
Não enviam dados confidenciais por meio eletrônico.	96,5
Verificação se uma informação confidencial enviada por meio eletrônico foi transmitida de forma protegida.	21,1
Equipamentos de armazenamento externo	**40,4**
Usuários que não consideram prudente a utilização de armazenamento externo de terceiros no próprio computador.	40,4
Papel do usuário na Segurança da Informação	**72,6**
Cumprimento das normas de SI pelos usuários em TI	82,5
Importância da PSI.	91,2
Nunca o usuário instalou um programa obtido na internet no computador da organização.	70,9
Percepção do usuário sobre o seu papel na SI da organização.	45,6
Senhas	**63,6**
Importância da alteração periódica da senha de acesso aos recursos computacionais	96,5
Não compartilhamento de senhas com outras pessoas na Organização.	89,5
Prática dos usuários em realizar alteração periódica da senha.	10,5
Utilização da mesma senha para acessar diferentes serviços	57,9
Uso do antivírus	**49,9**
Atualização automática do sistema de antivírus	70,0
Varredura com antivírus de dispositivos de armazenamento externo.	29,8
Utilização do firewall	**67,1**

Conhecimento que os computadores da Organização possuem firewall.	67,0
Consciência por parte dos usuários de que que a garantia da SI não está atrelada somente ao fato da existência de antivírus e firewall.	67,2
Bloqueio do computador	**58,1**
Compreensão por parte do usuário de que há risco em deixar o computador logado quando se afastam do mesmo.	67,0
Usuários que sempre bloqueiam o computador quando estão ausentes.	49,1
Total	**61,5**

Fonte: Dados da pesquisa (2017).

*O percentual do nível de concordância corresponde à concordância máxima atribuída pelos respondentes (concordo totalmente).

Destacou-se na Tabela 1, os temas com os maiores (acima de 70%) percentuais e as práticas com os menores (menor que 30%) percentuais. O tema "conhecimento do usuário sobre as políticas e normas em segurança da informação vigentes na organização" obteve a maior média de concordância (83,3%). A expressiva maioria dos usuários (94,7%) afirmou ter conhecimento da adoção pela Organização das políticas de controle de acesso aos recursos computacionais. Cerca de 86% dos usuários declaram ter conhecimento da adoção pela Organização de procedimentos para detectar e punir violações à SI. Para 68,4% dos usuários há um entendimento de que a informação é um ativo da organização e, portanto, deve ser preservada. Em relação ao conhecimento, por pare dos usuários, da importância de se manter atualizado os sistemas operacionais das estações de trabalho, bem como os aplicativos instalados, 84,2% dos pesquisados declaram pleno conhecimento.

O tema com o segundo maior percentual foi o "papel do usuário na segurança da informação" (72,6%). Em relação ao ambiente organizacional, no tocante ao cumprimento das normas de SI pelos usuários em TI, foi constatado que somente 17,5% discordavam que os usuários em TI cumprem as normas de SI. Considerando que a PSI é a principal norma de TI de uma Organização, verificou-se que 91,2% dos respondentes concordam totalmente da importância da PSI, e somente 3,5 % discordaram totalmente. Em relação à percepção do usuário sobre o seu papel na SI da Organização. Foi constatado que 45,6% responderam concordo totalmente, 45,6% concordo em parte e que apenas 8,8 % não sabem que atuam diretamente/indiretamente com a SI. Apesar de a Organização adotar privilégios de acesso e permissão aos recursos computacionais, buscou-se averiguar o comportamento do usuário acerca da instalação de programas "baixados" da internet, sendo constatado que a maioria dos usuários (70,9%) afirma nunca ter realizado a instalação de *softwares* que tinham como origem a internet.

Ao serem analisadas as práticas em SI com os menores percentuais, destacou-se as seguintes: prática dos usuários em realizar alteração periódica da senha (10,5); desconhecem a importância da análise do assunto do e-mail antes de abri-lo (14,1%); nunca efetuaram cópias de segurança (19,3%); verificação se uma informação confidencial enviada por meio eletrônico foi transmitida de forma protegida (21,1); e varredura com antivírus de dispositivos de armazenamento externo (29,8%).

As análises permitiram observar que a grande maioria dos respondentes (96,5%) concordam com a importância da alteração periódica da senha de acesso aos recursos computacionais. Contudo, 10,5% dos usuários nunca realizaram a referida mudança.

Cerca de 72% dos respondentes nunca utilizam o *e-mail* corporativo para tratar de assuntos pessoais e 79% dos usuários nunca abrem, executam ou leem os arquivos anexados em *e-mail* recebidos de desconhecidos. Os resultados evidenciaram que 14,1% dos usuários desconhecem a importância da análise do assunto do *e-mail* antes de abri-lo.

Quanto a encriptação da informação, notou-se que a maioria dos respondentes tem um comportamento que está de acordo com o recomendado pela NBR ISO/IEC 27002:2013, uma vez que não enviam dados confidenciais por meio eletrônico de forma descriptografada (96,5%). No entanto, ao apurar se os mesmos adotam o procedimento de verificar se a informação confidencial foi transmitida de forma protegida, somente 21,1% dos usuários responderam sempre. Esperava-se que os valores fossem mais elevados, uma vez que se trata de informação confidencial.

A análise dos dados coletados permitiu concluir que, de uma forma geral, os usuários em TI apresentam-se como uma proteção para a SI na Organização, pelo fato de assumirem comportamentos e atitudes preconizados na literatura na maioria dos procedimentos de segurança da informação. Esses dados concordam com o estudo de Pimenta e Quaresma (2016), realizado em Portugal com empresas de pequeno, médio e grande porte, em que a principal conclusão dos autores revelou que os usuários constituem uma proteção para a segurança dos sistemas de informação nas organizações.

Como aspectos positivos associados ao conhecimento, comportamento e atitude revelados pelos usuários em TI, destacam-se os seguintes: (i) consideram importantes as atualizações dos sistemas operacionais, bem como dos aplicativos; (ii) consideram que a atualização do antivírus permite uma melhor proteção à estação de trabalho; (iii) utilizam senhas robustas; (iv) consideram importante a periodicidade da alteração da senha de acesso aos recursos computacionais; (v) não partilham ou divulgam as suas senhas com terceiros; (vi) realizam cópias de segurança com regularidade; (vii) não utilizam o *e-mail* corporativo para tratar de assuntos pessoais; (viii) não abrem, leem ou executam os arquivos anexados em *e-mails* que são enviados por desconhecidos; (ix) não passam informações sigilosas por meios de comunicação não confiáveis; (x) conhecem que a Organização possui políticas adequadas para o controle de acesso lógico aos recursos computacionais; (xi) estão cientes que todos os atos praticados têm consequências; (xii) consideram que a PSI da Organização é importante e (xiii) comunicam ao gestor de Segurança da Informação algum tipo de anomalia que ocorra no seu computador.

Como aspectos negativos no conhecimento, comportamento e atitude revelados pelos usuários em TI, os seguintes itens se destacaram: (i) conectam dispositivos de armazenamento externo de terceiros às estações de trabalho; (ii) utilizam a mesma senha para acessar diversos serviços; (iii) não bloqueiam o seu computador quando se ausentam e (iv) desconhecem que diretamente ou indiretamente desempenham um papel importante na segurança da informação da Organização.

Os resultados associados aos aspectos negativos apresentaram certa semelhança ao estudo de Pimenta e Quaresma (2016), em que os comportamentos e atitudes dos usuários considerados negativos em relação a segurança da informação foram os seguintes: (i) a maioria dos usuários de TI já foi infectada por vírus; (ii) optam por senhas fáceis de memorizar, em detrimento das de construção robusta; (iii) utilizam a internet na organização para fins pessoais; (iv) ligam dispositivos de armazenamento externo de outras pessoas aos computadores de trabalho; e (v) não bloqueiam o computador quando se ausentam. Observa-se que as semelhanças nas práticas negativas associadas a segurança da informação entre uma organização militar e empresas de diferentes portes em Portugal se assemelham em atividades do cotidiano, como o bloqueio do equipamento ao se ausentar da estação de trabalho ou na utilização de dispositivos de armazenamento externo de outras pessoas no computador da organização. Contudo, divergências podem ser consideradas. A utilização de serviços (e-mail ou internet) em TI e de recursos computacionais (computadores) da organização para fins pessoais não foi observada na organização militar. Pode-se inferir que fatores culturais, valores e crenças dos usuários em TI influenciam no comportamento associado a segurança da informação, tanto positivamente quanto de forma negativa. Para Fazenda e Fagundes (2014), a cultural local brasileira influencia no estabelecimento de uma cultura orientada pela segurança da informação nas organizações. Grande parte dos usuários têm a ideia de que segurança da informação é "proteger o computador" e não observam o risco associado à troca de informações confidenciais por outros meios como, informações faladas em locais inadequados ou materiais com informações confidenciais descartados de forma incorreta.

Acredita-se que os resultados negativos da SI nas organizações podem ser minimizados por meio de práticas de auditoria e conscientização por parte da gestão em SI da organização, conforme defende a norma NBR ISO/IEC 27002:2013.

Por fim, tendo como base os resultados apontados, destaca-se um conjunto de recomendações a serem seguidas pelos usuários em TI da organização estudada e, acredita-se que sejam aplicáveis a outras instituições governamentais, a saber: (i) utilizar senhas robustas, por meio da construção que conjugue letras maiúsculas/minúsculas, números e caracteres especiais, bem como proceder a sua mudança regularmente e não compartilhá-las com terceiros; (ii) ser cuidadoso na manipulação de arquivos de terceiros, pois podem conter códigos maliciosos; (iii) ser cuidadoso na utilização da Internet e do *e-mail* corporativo, sob pena de poderem ser infectados por algum tipo de *software* malicioso; (iv) ter cuidado com a utilização de dispositivos de armazenamento externo, uma vez que conectar dispositivos externos de terceiros no computador de trabalho representa uma ameaça; (v) efetuar sempre que possível cópia de segurança da informação do computador para o repositório (servidor de arquivo) ou para um dispositivo de armazenamento externo, devendo estes serem guardados em local diferente da localização do computador; (vi) bloquear ou terminar a sessão no seu computador sempre que se ausentar do seu posto de trabalho, mesmo que por pouco tempo; e (vii) seguir as políticas de segurança definidas pela Organização, que têm como objetivo a proteção da informação organizacional.

5. Considerações Finais

É oportuno neste momento retomar a pergunta de pesquisa que direcionou este estudo - qual o nível de conformidade em SI do CINDACTA II em relação às publicações no âmbito do COMAER e da Administração Pública Federal, bem como o grau de aderência do CINDACTA II às recomendações de SI da norma ABNT NBR ISO/IEC 27002:2013? Observamos que, ainda que existam pontos que possam ser aperfeiçoados, a gestão de SI do CINDACTA II se encontra em um nível que atende aos requisitos de segurança atuais da Organização, dadas as suas particularidades e cenário em que está inserida. Identificamos que toda documentação normativa relacionada à SI, elaborada ou revisada no âmbito do CINDACTA II, encontra-se em consonância com as publicações no âmbito do COMAER, da APF e demais instrumentos de teor legal afetos ao tema.

O estudo permitiu identificar que o CINDACTA II possui um grau de aderência mediano em relação às recomendações de SI da norma ABNT ISO/IEC NBR 27002:2013. Com o objetivo de melhorar o grau da aderência da Organização à NBR 27002:2013, sugerimos que a adoção das ações de revisar periodicamente o documento da política de SI, bem como os documentos originados a partir dela, tais como normas e orientações, a fim de manter a SI na Organização em níveis desejáveis de confiabilidade; atualizar o inventário dos recursos de informação (ativos) disponíveis na OM; e treinar os usuários em TI para que sejam capazes de identificar e notificar uma fragilidade de SI.

De uma forma geral, os usuários em TI do CINDACTA II se apresentaram como uma proteção para a SI na Organização pelo fato de assumirem comportamentos e atitudes corretas na maioria dos procedimentos de SI recomendados por normas internacionais. Assim como preconizado na literatura, o fator humano é o elo mais frágil da segurança da informação, sendo necessário que as práticas do cotidiano dos usuários em TI sejam constantemente avaliadas, revisadas, evoluídas e amplamente divulgadas a todos os interessados.

Por fim, acreditamos que o estudo apresentou contribuições no âmbito acadêmico e organizacional. No âmbito acadêmico, o estudo evidenciou semelhanças nas práticas em SI entre organizações militares e civis, permitindo inferir que questões culturais, valores e crenças do ambiente organizacional influenciam na segurança da informação. No âmbito organizacional, especialmente na esfera das instituições militares, o estudo apresentou uma estrutura metodológica passível de ser replicada em outras organizações militares e direcionar práticas de melhorias.

Mesmo que o estudo tenha seguido práticas metodológicas essenciais ao desenvolvimento de um conhecimento científico, o trabalho possui algumas limitações. A principal limitação ateia-se ao fato de o estudo ter sido realizado em uma única organização militar, o CINDACTA II. Destarte, os resultados e as conclusões não podem ser extrapolados para outras organizações militares do COMAER. Outra limitação está associada à abordagem quantitativa, que inviabilizou inferências mais profundas sobre os resultados.

Como trabalhos futuros sugerimos que o estudo seja replicado em outras organizações militares do COMAER, a fim de se observar o nível de maturidade da

segurança da informação na instituição como um todo. O fator humano pode ser explorado por meio de práticas metodológicas de cunho fenomenológico para compreender as razões do comportamento inadequado dos usuários em TI e identificar possíveis soluções para mitigar as vulnerabilidades organizacionais em razão do comportamento humano. Sugerimos ainda que abordagens qualitativas, realizadas por meio de entrevistas, seguindo a estrutura de levantamento de dados definidas neste estudo, podem apresentar informações não identificadas pelo nosso trabalho.

Referências

BALTZAN, P; PHILLIPS, A. **Sistemas de informação**. Porto Alegre: AMHG, 2012.

BRASIL. **Decreto nº 3.505, 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Portal da Legislação. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d3505.htm>. Acesso em 19 jun. 2016.

_____. **Instrução Normativa Nº 1 de 13.06.2008 do Gabinete de Segurança Institucional da Presidência da República**, Brasília, 2008. Disponível em: <http://www.mct.gov.br/index.php/content/view/72703.html>. Acesso em: 19 abr. 2017.

BRASIL. **Presidência da República. Casa Militar**. Departamento de Segurança da Informação e Comunicações. Guia básico de orientações ao gestor em segurança da informação e comunicações: versão 2.0 – Brasília: Presidência da República, 2016. 92 p.. Disponível em: <http://dsic.planalto.gov.br/documentos/guiagestor.pdf>. Acesso em 23 mar. 2017.

CINDACTA II. **Missão**. Disponível em:<http://www2.fab.mil.br/cindacta2/index.php/missao>. Acesso em: 12 jul. 2017.

CASSARRO, A. C. **Sistemas de informação para tomadas de decisões**. 3. ed. São Paulo: Pioneira, 1999.

CERT.br. **Estatísticas dos incidentes reportados ao CERT.br**. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 23 abr. 2017.

DAVENPORT, Thomas.H. **Ecologia da Informação: porque só a tecnologia não basta para o sucesso na era da informação**. 2. ed. São Paulo: Futura, 2000.

DCA 11-45. **Comando da Aeronáutica**. Concepção estratégica Força Aérea 100. Brasília, 2017. Disponível em: <http://www.fab.mil.br/Download/arquivos/FA100.pdf> Acesso em: 10 jul. 2017.

FAZENDA, R. V.; FAGUNDES, L. L. Análise dos Desafios para Estabelecer e Manter Sistema de Gestão de Segurança da Informação no Cenário Brasileiro. 2014, **Anais...** Goiânia, GO: SBC, 2014. p. 454–463. Disponível em: <https://sol.sbc.org.br/index.php/sbsi/article/view/5831/5729>. Acesso em: 7 ago. 2019.

FONTES, Eduardo. **Segurança da Informação: O usuário faz a diferença**. 1. ed. São Paulo: Saraiva, 2006.

GIL, A.C. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

MARCIANO. J. L. P. **Segurança da Informação – uma abordagem social**. Tese de Doutorado apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília, Brasília, 2006. Disponível em: <http://www.enancib.ppgci.ufba.br/premio/UNB_Marciano.pdf>. Acesso em: 22 abr. 2017.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Fundamentos de metodologia científica*. 7. ed. São Paulo: Editora Atlas, 2003.

MCGARRY, Kevin. **O contexto dinâmico da informação: uma análise introdutória.** 2.ed. Brasília: Briquet de Lemos, 1999.

NASCIMENTO, T. F. DO; FROGERI, R. F.; PRADO, L. Á. Gestão de Segurança da Informação (GSI) no Segundo Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA II). 2018, Varginha, MG: Even3, 2018. p. 1–30. Disponível em: <http://www.even3.com.br/Anais/simgeti/111315-GESTAO-DE-SEGURANCA-DA-INFORMACAO-(GSI)-NO-SEGUNDO-CENTRO-INTEGRADO-DE-DEFESA-AEREA-E-CONTROLE-DE-TRAFEGO-AEREO-(>.

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. Rio de Janeiro, 2006.

_____. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013.** Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2013.

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 27005:2011**. Tecnologia da informação – Técnicas de Segurança – Gestão de riscos de segurança da informação. Rio de Janeiro, 2011.

PIMENTA, A. M. S.; QUARESMA, R. F. C. A *Segurança dos Sistemas de Informação e o Comportamento dos Usuários*. **Journal of Information Systems and Technology Management**, v. 13, n. 3, p. 533-552, 2016. Disponível em: <http://www.scielo.br/pdf/jistm/v13n3/1807-1775-jistm-13-03-0533.pdf>. Acesso em: 21 maio 2017.

PIZZO, Walter Nogueira; CUGNASCA, Paulo Sérgio. Análise de risco de segurança da informação como fator de avaliação de disponibilidade de sistemas críticos de controle do espaço aéreo. **Anais...** Manuaus: [s.n.], 2010.

PRODANOV, Cleber Cristiano; FREITAS, Ernani César de. **Metodologia do Trabalho Científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Feevale, 2013.

SÊMOLA, M. **Gestão da segurança da informação: uma visão executiva**. 2.ed. Rio de Janeiro: Campus, 2014.