ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

Cap QCO THIAGO JOSÉ LANA DE PAULA DIAS

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO NO EB: IDENTIFICANDO A ADERÊNCIA DA CARTILHA EMERGENCIAL DE SIC DIANTE DA NORMA ABNT NBR ISO/IEC 27002:2013

Rio de Janeiro
2016

Cap QCO THIAGO JOSÉ LANA DE PAULA DIAS

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO NO EB: IDENTIFICANDO A ADERÊNCIA DA CARTILHA EMERGENCIAL DE SIC DIANTE DA NORMA ABNT NBR ISO/IEC 27002:2013

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares
.

Orientador: Maj QCO Anderson Barros Torres

Rio de Janeiro
2016

Cap QCO THIAGO JOSÉ LANA DE PAULA DIAS

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO NO EB: IDENTIFICANDO A ADERÊNCIA DA CARTILHA EMERGENCIAL DE SIC DIANTE DA NORMA ABNT NBR ISO/IEC 27002:2013

Trabalho de Conclusão de Curso apresentado à Escola de Formação Complementar do Exército / Escola de Aperfeiçoamento de Oficiais como requisito parcial para a obtenção do Grau Especialização em Ciências Militares
.

Aprovado em

COMISSÃO DE AVALIAÇÃO

_____
Maj QCO ANDERSON BARROS **TORRES** – Presidente
Escola de Formação Complementar do Exército

_____
Cap QCO MAXLI BARROSO **CAMPOS** – Membro
Escola de Formação Complementar do Exército

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO NO EB: IDENTIFICANDO A ADERÊNCIA DA CARTILHA EMERGENCIAL DE SIC DIANTE DA NORMA ABNT NBR ISO/IEC 27002:2013

THIAGO JOSÉ LANA DE PAULA DIAS

RESUMO

A intensa utilização da tecnologia da informação e comunicações (TIC) pelas Forças Armadas (FA) em todo o mundo criou uma nova dimensão de combate no campo de batalha, a cibernética. A TIC é utilizada como instrumento viabilizador para uma maior eficiência dos trabalhos desenvolvidos pelo Exército Brasileiro (EB), tanto em áreas meio como finalísticas, de modo a influenciar as atividades militares em seus diferentes níveis: operacional, tático e estratégico.

Representantes militares e civis demonstram grande preocupação quanto à necessidade de auditar e controlar seus ambientes de TIC, devido à grande abrangência de sua utilização, a fim de garantirem o necessário nível de serviço (NS) de suas infraestruturas e serviços. O EB atribui ao Sistema de Telemática do Exército (SisTEx) a execução das atividades de auditoria de segurança de tecnologia da informação e comunicações.

Atualmente, o EB, através dos Centros de Telemáticas (CT) e Centros de Telemática de Área (CTA), realiza auditorias baseando seus processos através das Instruções Reguladoras sobre Auditoria de Segurança de Sistemas de Informação (IRASEG/IR 13-09) e elaborando suas listas de verificação através dos procedimentos de controle existentes na Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações (CESTIC), publicada pela Portaria nº 72 de 21 de novembro de 2011, do Comandante do Exército.

Os controles de segurança da informação no meio civil foram reunidos através de publicações de normas técnicas elaboradas por organizações notoriamente reconhecidas pelas suas capacidades técnicas. Internacionalmente temos a *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC) que elaboraram em conjunto uma norma contendo um código de boas práticas para controles de segurança da informação, a norma ISO/IEC 27002:2013. Essa mesma norma foi traduzida nacionalmente pela Associação Brasileira de Normas Técnicas (ABNT) produzindo a ABNT NBR ISO/IEC 27002:2013.

É notória a relevância do assunto relativo à auditoria de segurança de TIC nos meios militares e civis, devido à dependência de suas atividades em relação aos serviços e infraestruturas de TIC. Dessa maneira, é imprescindível deter o controle sobre o grau de proteção destinada à TIC, por meio de auditorias que garantam a possibilidade de mitigação de riscos e garantam os necessários NS. Neste cenário, o objetivo deste trabalho consiste em identificar e aplicar método de boa prática nos processos de Auditoria em Segurança da Informação, alinhado com as normas e legislações do Exército Brasileiro, comparando os procedimentos de controle da CESTIC e o que é recomendado pela ABNT NBR ISO/IEC 27002:2013.

Palavras-chave: Auditorias, segurança da informação, ABNT, ISO/IEC 27002:2013.

ABSTRACT

The intensive use of information and communications technology (ICT) by the Armed Forces (AF) throughout the world has created a new dimension of combat on the battlefield, cybernetics. ICT is used as an enabler for greater efficiency of the work developed by the Brazilian Army (EB) in both areas means as purposive, in order to influence the military activities at different levels: operational, tactical and strategic.

Military and civilian representatives have shown great concern about the need to audit and control their ICT environments, due to the wide scope of its use, in order to ensure the necessary level of service (NS) of its infrastructure and services. The EB attaches to Telematic Army System (TASys) implementation of information and communications technology security audit activities.

Currently, the EB through the Telematic Centres (CT) and Centers Area Telematics (CTA), conducts audits based its processes through the Regulatory Instructions on Audit of Information Systems Security (IRASEG / IR 13-09) and drafting their checklists through existing control

procedures in the Emergency Handbook of Information and Communications Technology Security (CESTIC), published by Ordinance No. 72 of November 21, 2011, the Army Commander.

Information security controls in civil means were gathered through technical standards publications produced by notoriously recognized for their technical capabilities organizations. Internationally we have the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) that worked together on a standard having a code of practice for information security controls, ISO / IEC 27002 standard: 2013. The Brazilian Association of Technical Standards (ABNT) producing the ISO/IEC 27002 translated this same standard nationally: 2013.

It is evident the relevance of the subject on the ICT security audit in the military and civilian, due to the dependence of their activities to the mandatory use of ICT services and infrastructure. Thus, it is essential to retain control over the degree of protection intended for ICT through audits to ensure the possibility of mitigating risks and ensuring the NS. In this scenario, the goal of this work is to identify and implement method of good practice in the process of Auditing Information Security, aligned with the rules and laws of the Brazilian Army, comparing the CESTIC control procedures and what the NBR ISO/IEC 27002:2013 recommends.

Keywords: Information security, audit, risk.

AUDITORIAS DE SEGURANÇA DA INFORMAÇÃO NO EB: IDENTIFICANDO A ADERÊNCIA DA CARTILHA EMERGENCIAL DE SIC DIANTE DA NORMA ABNT NBR ISO/IEC 27002:2013

1. INTRODUÇÃO

A intensa utilização da tecnologia da informação e comunicações (TIC) pelas Forças Armadas (FA) em todo o mundo criou uma nova dimensão de guerra, a cibernética[5]. A TIC é utilizada como instrumento viabilizador de uma maior eficiência dos trabalhos desenvolvidos pelo Exército Brasileiro (EB), tanto em áreas meio como finalísticas, de modo a influenciar as atividades militares em seus diferentes níveis: tático, operacional e estratégico.

Os setores militar e civil demonstram preocupação quanto à necessidade de auditar e controlar seus ambientes de TIC, devido à grande abrangência de sua utilização, a fim de garantirem o necessário nível de serviço (NS) de suas infraestruturas e serviços. Devido a isso, o EB atribui ao Sistema de Telemática do Exército (SisTEx) a execução das atividades de auditoria de segurança de tecnologia da informação e comunicações[5]. Esse Sistema é composto pelo Centro Integrado de Telemática do Exército (CITEx), que é um órgão de apoio setorial diretamente subordinado ao Departamento de Ciência e Tecnologia do Exército (DCT), e tem como atribuição estabelecer, manter e operar o sistema de informática e comunicações de interesse do Sistema de Comando e Controle do Exército (SC^2Ex) em seu nível estratégico. Esse Centro atua regionalmente através dos seus CTA e CT que são organizações executoras das auditorias de segurança da

informação e comunicações em suas OM de área, realizadas por meio de visitas de orientações técnicas (VOT) organizadas anualmente, as quais geram relatórios que são enviados ao escalão superior.

O EB prioriza os trabalhos de Defesa Cibernética[5], o que acarreta na necessidade de se implantar métodos e técnicas de auditoria de Segurança da Informação (SI), tanto baseados em conhecimentos tácitos de profissionais do EB, quanto observando normas elaboradas por organismos normatizadores de reconhecida capacidade técnica[4].

O Ministério da Defesa (MD) define políticas relacionadas à segurança da informação (SI) através da elaboração da Política Nacional de Defesa (PND) e Estratégia nacional de Defesa (END)[6]. Esses documentos determinam que sejam implantados e aperfeiçoados procedimentos que visem garantir os requisitos necessários e relacionados à SI, com a finalidade de proteger estruturas estratégicas que se utilizam de tecnologia da informação e comunicação, incluindo o seu pronto reestabelecimento face a algum incidente[6]. Para isso é necessária a realização de auditorias que permitam determinar o grau de proteção e controle destinados à SI de TIC.

O Departamento de Ciência e Tecnologia do EB (DCT) recebeu da PND a atribuição de desenvolver soluções inovadoras sobre consciência situacional[6], enquadrando-se nessa previsão a necessidade da manutenção do conhecimento sobre os procedimentos de controle de SI aplicados às OM do EB, executados através de auditorias realizadas pelas suas OM de telemática. Para a realização dessas auditorias, o DCT elaborou a Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações (CESTIC)[2,3], como fonte inicial e básica de procedimentos de controle de SI a serem abordados em auditorias, e as Instruções Reguladoras sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro (IRASEG – IR 13-09)[4], publicada pela Portaria nº 003-DCT, de 31 de janeiro de 2007, na qual prevê a realização de auditorias de Controles Técnicos-Normativos, baseadas em normas publicadas, por exemplo, pela Associação Brasileira de Normas Técnicas – ABNT[4].

A CESTIC foi elaborada em caráter emergencial, contendo poucos controles, e utilizando como fonte de conhecimento apenas a experiência profissional de seus elaboradores[3]. Com isso é perceptível a deficiência da aplicação de controles de SI

que observem boas práticas nacionais e internacionais externas ao EB, como as publicadas pela ABNT. Isso acarreta em uma limitada percepção sobre a situação da SI nas OM do EB.

A Cartilha possui procedimentos de controle obrigatórios que devem ser implementados pelas OM do EB[3]. Esses procedimentos são divididos nas seguintes categorias: regras básicas de segurança computacional aos Comandantes de OM, computadores da OM, rede da OM, página de Internet da OM, incidentes de segurança, telefonia e videoconferência na OM, e proteção contra spam[3]. Esses procedimentos de controle são utilizados para a realização de Auditorias de Segurança da Informação (ASI), pelas Organizações Militares de Telemática do EB (OM de telemática do EB).

Tendo como base as fontes bibliográficas supramencionadas, serão apresentadas as análises comparativas entre os controles de SI de TIC, aplicados atualmente pelas OM de telemática do EB, e os controles de SI recomendados pelo código de boas práticas da norma ABNT NBR ISO/IEC 27002:2013[1]. Através dessa análise será possível obter uma visão sobre os Controles (CO), Objetivos de Controle (OC) e Seções de controle da norma da ABNT evidenciados e implantados em diferentes níveis, e outros que não foram evidenciados representando as atuais deficiências.

Assim, no intuito de verificar os procedimentos de controle aplicados através de auditorias de SI de TIC, com relação às boas práticas normativas externas ao EB, foi formulado o seguinte problema:

As auditorias que utilizam os procedimentos de CO de SI existentes na CESTIC, são suficientes para fornecer a necessária visão e gestão de riscos de SI de TIC, quando comparadas aos procedimentos de CO recomendados pela norma ABNT NBR ISO/IEC 27002:2013?

A resposta a tal questionamento possibilitará inferir em qual patamar o EB se encontra, em comparação a auditorias que utilizam boas práticas de controles de SI de TIC externa ao EB, e com isso melhorar seus processos e evoluir sua capacidade operativa.

O Tema sobre a aplicação de métodos e técnicas de boas práticas em auditorias de SI foi escolhido pois possibilita analisar a situação atual e propor melhorias na aplicação de novos controles de SI, e com isso, melhorar a gestão e

mitigação de riscos de SI. Os controles de SI implementados pelas auditorias de TIC são importantes devido à grande dependência das OM do EB na utilização da TIC como meio de aumentar a efetividade de seus trabalhos, tanto administrativos quanto diretamente executados nas diversas atividades fim.

O aperfeiçoamento da gestão de SI pelas OM contribuirá para uma melhor gestão de riscos que garantirá uma maior proteção contra ameaças e mitigação de vulnerabilidades, impactando direta e positivamente em uma melhor disponibilidade dos serviços que a TIC suporta e agregando valor à atividade fim das OM.

Sendo assim, é de suma importância o resultado deste estudo, com enfoque na solução do problema citado, pois caso contrário, os diversos serviços e infraestruturas de TIC do EB permanecerão vulneráveis frente às ameaças internas e externas. Neste cenário, o objetivo desse trabalho consiste em identificar e aplicar método de boa prática relacionados aos processos de Auditoria em Segurança da Informação, alinhados com as normas e legislações do Exército Brasileiro, a fim de destacar as deficiências nos procedimentos de controle da CESTIC com relação aos controles recomendados pela ABNT NBR ISO/IEC 27002:2013. Essas deficiências serão verificadas através dos seguintes objetivos específicos: enquadrar os procedimentos de controle da CESTIC nos controles recomendados pela norma da ABNT; apresentar os controles da norma da ABNT que não são implementados na CESTIC demonstrando deficiências; apresentar os objetivos de controle da norma da ABNT que não são implementados na CESTIC demonstrando deficiências; e apresentar as Seções de controle da norma da ABNT que não são implementadas pela CESTIC demonstrando deficiências.

2. METODOLOGIA

Foi utilizada a metodologia científica através da forma de abordagem na modalidade quantitativa, na qual foram realizados cálculos estatísticos que tornaram possível verificar as diferenças de procedimentos de CO aplicados pela CESTIC e os CO recomendados pela norma ABNT NBR ISO/IEC 27002:2013, tornando possível a verificação das deficiências de CO não implementados nas auditorias de SI de TIC do EB, com base nas boas práticas de organismos normativos externo.

A trajetória desenvolvida pela presente pesquisa bibliográfica teve seu início na revisão teórica do assunto, através de consulta bibliográfica a portarias e instruções

reguladoras do EB[2,3,4], do Estado Maior Conjunto das Forças Armadas[5], do MD[6], e à norma técnica ABNT NBR ISO/IEC 27002:2013[1].

O presente estudo abrange uma população de normas sobre SI vigentes no EB, cada uma com suas finalidades específicas. O estudo foi limitado particularmente a obtenção de amostra de procedimentos de Controles (CO) de SI, existentes na norma CESTIC, utilizada pelas OM de telemática do EB, a fim de enquadrá-los e compará-los às Seções, Objetivos de Controle (OC) e Controles (CO) recomendados pela norma ABNT NBR ISO/IEC 27002:2013. Com isso será possível verificar as atuais deficiências na aplicação de CO de SI de TIC no EB, com base nas melhores práticas da normativa externa ao EB.

Com relação às variáveis envolvidas no estudo, as "**auditorias de SI com base na CESTIC**" apresentam-se como variável dependente pois o seu aperfeiçoamento ocorrerá através da verificação da divergência e convergência de seus procedimentos de CO e os CO recomendados pela variável independente "**norma ABNT NBR ISO/IEC 27002:2013**", que ao serem utilizados, corrigirão as deficiências das auditorias de SI de TIC atuais.

A variável "**auditorias de SI com base na CESTIC**" deve ser entendida como uma série de procedimentos de CO de SI de TIC utilizados atualmente pelas OM de telemática do EB, na realização de auditorias anuais.

Para a presente pesquisa, a variável "**norma ABNT NBR ISO/IEC 27002:2013**" deve ser entendida como um código de boas práticas expressado em CO de SI de TIC, enquadrados em OC, que por sua vez são agrupados em Seções dessa Norma. Esses CO são recomendados como boa prática na implantação de procedimentos de gestão de SI verificáveis através de auditorias.

Por fim, foi operacionalizada a análise dos dados obtidos, sendo os mesmos submetidos a um tratamento estatístico e criticados, externa e internamente, antes de serem tabulados e apresentados de forma clara, objetiva e sintética.

3. RESULTADOS E DISCUSSÃO

De maneira geral, a pesquisa bibliográfica possibilitou:

- Descrever o momento histórico, motivadores e objetivos para a criação CESTIC;

- Descrever e analisar o objetivo, a estrutura e os procedimentos de SI de TIC da CESTIC, utilizados para extrair diretrizes de verificações para auditorias;
- Descrever e analisar quais são os objetivos e benefícios na norma ABNT NBR ISO/IEC 27002:2013;
- Descrever e analisar a estrutura da norma ABNT NBR ISO/IEC 27002:2013 com relação aos seus itens de segurança em TIC;
- Realizar os enquadramentos dos procedimentos de CO de TIC da CESTIC, com a relação aos CO, OC e as Seções de CO da norma ABNT NBR ISO/IEC 27002:2013;
- Descrever e analisar a possível existência de procedimentos de CO de TIC da CESTIC, que não se enquadram nos CO, OC e Seções da norma ABNT NBR ISO/IEC 27002:2013, obtendo-se os eventuais casos específicos de CO do EB;
- Descrever e analisar os CO, OC e Seções da norma ABNT NBR ISO/IEC 27002:2013 que não são implementados através dos procedimentos de CO de TIC da CESTIC, obtendo-se as atuais deficiências de CO do EB; e
- Descrever e analisar os CO, OC e Seções da norma ABNT NBR ISO/IEC 27002:2013 que são evidenciados e implementados pelos procedimentos de CO de auditoria de SI de TIC da CESTIC, obtendo-se as atuais possíveis convergências com a norma da ABNT.

A CESTIC destinou-se a implantar procedimentos de segurança considerados básicos, com custo reduzido e baixa complexidade de implantação[3]. Esses procedimentos de segurança definidos são enquadrados em Seções. Eles são atualmente utilizados na elaboração de listas de verificação utilizadas em auditorias de SI de TIC pelas OM de telemática do EB.

Essa Cartilha foi elaborada por integrantes do SisTEx que utilizaram os seus conhecimentos desenvolvidos ao longo de suas carreiras para o estabelecimento de procedimentos de CO de SI de TIC, formando um documento com a seleção das melhores práticas de um determinado grupo[3]. Não há em seu conteúdo menção formal da utilização de normas externas ao EB referente às boas práticas nacionais ou internacionais sobre o assunto, evidenciando a possível existência de lacunas e fragilidade de procedimentos e controles.

Em sua estrutura são abordadas seções que listam procedimentos de SI de TIC a serem implantados por todas as OM do EB[3]. As seções são as seguintes:

- Regras Básicas de Segurança Computacional aos CMT OM;
- Computadores da OM;
- Rede da OM;
- Página de Internet da OM;
- Incidentes de Segurança;
- Telefonia e Videoconferência na OM; e
- Proteção contra SPAM.

Outra norma atinente à auditoria de SI de TIC são as Instruções Reguladoras sobre Auditoria de Segurança de Sistemas de Informação (IRASEG/IR 13-09)[4], que têm por finalidade regular as condições para a implantação de um processo de auditoria no EB, e com isso contribuir para o estabelecimento de doutrinas relacionadas ao tema. Essa doutrina contribui para a elaboração do planejamento e execução de auditorias, bem como orienta os Comandantes, Chefes e Diretores sobre o assunto.

A IRASEG estabelece diversos tipos de CO, entre eles o controle técnico-normativo, o qual se refere à utilização de normas externas ao EB como fonte de conhecimento para a elaboração de listas de verificação para auditorias[4]. Nacionalmente a ABNT publicou a norma ABNT NBR ISO/IEC 27002:2013, uma tradução da norma internacional publicada pela ISO/IEC 27002:2013[1]. A Instrução Reguladora reconhece a aplicabilidade de normas elaboradas pela ABNT ou por organismo normativo internacional caso não exista uma norma equivalente no país[4].

Uma das etapas de uma auditoria corresponde à escolha dos controles que serão posteriormente verificados, priorizados e avaliados, a fim de proporcionar a análise, a visão e a gestão de riscos de SI de TIC[4].

A norma ABNT NBR ISO/IEC 27002:2013 foi publicada com a finalidade de reunir e recomendar boas práticas de gestão de SI, através da seleção, implementação e gerenciamento de seus CO recomendados. Esses CO foram extraídos de diversos ambientes reais de riscos originados de organizações com diversos perfis[1].

Visando um melhor entendimento dos dados colhidos, será realizada a apresentação e discussão dos mesmos de maneira isolada evitando, assim, uma generalização das respostas dadas.

O primeiro ponto levantado na pesquisa diz respeito aos enquadramentos dos procedimentos de CO previstos na CESTIC nos CO de segurança listados na norma ABNT NBR ISO/IEC 27002:2013. A pesar de a CESTIC não mencionar formalmente a referência a essa norma externa ao EB, ela apresenta correlações de seus procedimentos de CO de SI com alguns poucos CO estabelecidos pela norma da ABNT. Em alguns casos, verificou-se a existência de mais de um procedimento de CO da CESTIC vinculados a um único CO da norma da ABNT (N:1), e na maioria dos casos, são evidenciados CO da norma da ABNT possuidores de um único procedimento previsto na CESTIC (1:1). Foi percebido, ainda, que a maioria dos CO da norma da ABNT não possuem procedimentos de CO de SI previstos na CESTIC (N:0). Esses enquadramentos podem ser observados no quadro, nas tabelas e gráficos de frequência apresentados a seguir:

Enquadramentos dos procedimentos de CO da CESTIC nos CO da Norma ABNT NBR ISO/IEC 27002:2013

CO da Norma da ABNT	Quantidade de procedimentos de CO da CESTIC evidenciados
5.1.1 Políticas para segurança da informação	0
5.1.2 Análise crítica das políticas para segurança da informação	0
6.1.1. Responsabilidade e papéis pela segurança da informação	2
6.1.2 Segregação de funções	0
6.1.3 Contato com autoridades	0
6.1.4 Contato com grupos especiais	0
6.1.5 Segurança da informação no gerenciamento de projetos	0
6.2.1. Política para uso de dispositivo móvel	4
6.2.2 Trabalho remoto	0
7.1.1 Seleção	0
7.1.2 Termos e condições de contratação	0
7.2.1 Responsabilidades da direção	0
7.2.2. Conscientização, educação, e treinamento em segurança da informação	1
7.2.3 Processo disciplinar	0
7.3.1 Responsabilidades pelo encerramento ou mudança da contratação	0
8.1.1 Inventário dos ativos	0

Enquadramentos dos procedimentos de CO da CESTIC nos CO da Norma ABNT NBR ISO/IEC 27002:2013	
CO da Norma da ABNT	**Quantidade de procedimentos de CO da CESTIC evidenciados**
8.1.2 Proprietário dos ativos	0
8.1.3 Uso aceitável dos ativos	0
8.1.4 Devolução de ativos	0
8.2.1 Classificação da informação	0
8.2.2 Rótulos e tratamento da informação	0
8.2.3 Tratamento dos ativos	0
8.3.1 Gerenciamento de mídias removíveis	0
8.3.2 Descarte de mídias	0
8.3.3 Transferência física de mídias	0
9.1.1 Política de controle de acesso	0
9.1.2. Acesso às redes e aos serviços de rede	5
9.2.1 Registro e cancelamento de usuário	1
9.2.2 Provisionamento para acesso de usuário	0
9.2.3 Gerenciamento de direitos de acesso privilegiados	0
9.2.4 Gerenciamento da informação de autenticação secreta de usuários	0
9.2.5 Análise crítica dos direitos de acesso de usuário	0
9.2.6 Retirada ou ajuste de direitos de acesso	0
9.3.1 Uso da informação de autenticação secreta	1
9.4.1 Restrição de acesso à informação	0
9.4.2. Procedimentos seguros de entrada no sistema (log-on)	1
9.4.3 Sistema de gerenciamento de senha	0
9.4.4 Uso de programas utilitários privilegiados	0
9.4.5 Controle de acesso ao código-fonte de programas	0
10.1.1. Política para o uso de controles criptográficos	1
10.1.2 Gerenciamento de chaves	0
11.1.1 Perímetro de segurança física	0
11.1.2 Controles de entrada física	0
11.1.3 Segurança em escritórios, salas e instalações	0
11.1.4 Proteção contra ameaças externas e do meio-ambiente	0
11.1.5 Trabalhando em áreas seguras	0
11.1.6 Áreas de entrega e de carregamento	0
11.2.1. Escolha do local e proteção do equipamento	1
11.2.2 Utilidades	0
11.2.3. Segurança do cabeamento	1
11.2.4. Manutenção dos equipamentos	1
11.2.5. Remoção de ativos	1

Enquadramentos dos procedimentos de CO da CESTIC nos CO da Norma ABNT NBR ISO/IEC 27002:2013	
CO da Norma da ABNT	**Quantidade de procedimentos de CO da CESTIC evidenciados**
11.2.6 Segurança de equipamentos e ativos fora das dependências da organização	0
11.2.7. Reutilização e alienação segura de equipamentos	1
11.2.8 Equipamento de usuário sem monitoração	0
11.2.9 Política de mesa limpa e tela limpa	0
12.1.1 Documentação dos procedimentos de operação	0
12.1.2 Gestão de mudanças	0
12.1.3 Gestão de capacidade	0
12.1.4 Separação dos ambientes de desenvolvimento, teste e de produção	0
12.2.1. Controles contra códigos maliciosos	1
12.3.1 Cópias de segurança das informações	0
12.4.1 Registros de eventos	0
12.4.2 Proteção das informações dos registros de eventos (logs)	0
12.4.3 Registros de eventos (log) de administrador e operador	0
12.4.4 Sincronização dos relógios	0
12.5.1 Instalação de software nos sistemas operacionais	1
12.6.1 Gestão de vulnerabilidades técnicas	0
12.6.2. Restrições quanto à instalação de software	1
12.7.1 Controles de auditoria de sistemas de informação	0
13.1.1 Controles de redes	0
13.1.2 Segurança dos serviços de rede	0
13.1.3 Segregação de redes	0
13.2.1. Políticas e procedimentos para a transferência de informações	4
13.2.2 Acordos para transferência de informações	0
13.2.3. Mensagens eletrônicas	1
13.2.4 Acordos de confidencialidade e não divulgação	0
14.1.1 Análise e especificação dos requisitos de segurança da informação	0
14.1.2 Serviços de aplicação seguros em redes públicas	0
14.1.3 Protegendo as transações nos aplicativos de serviços	0
14.2.1. Política de desenvolvimento seguro	2
14.2.2 Procedimentos para controle de mudanças de sistemas	0
14.2.3 Análise crítica técnica das aplicações após mudanças nas plataformas operacionais	0
14.2.4 Restrições sobre mudanças em pacotes de Software	0
14.2.5 Princípios para projetar sistemas seguros	0
14.2.6 Ambiente seguro para desenvolvimento	0
14.2.7 Desenvolvimento terceirizado	0

Enquadramentos dos procedimentos de CO da CESTIC nos CO da Norma ABNT NBR ISO/IEC 27002:2013	
CO da Norma da ABNT	**Quantidade de procedimentos de CO da CESTIC evidenciados**
14.2.8. Teste de segurança do sistema	1
14.2.9 Teste de aceitação de sistemas	0
14.3.1 Proteção dos dados para teste	0
15.1.1 Política de segurança da informação no relacionamento com os fornecedores	0
15.1.2 Identificando segurança da informação nos acordos com fornecedores	0
15.1.3 Cadeia de suprimento na tecnologia da comunicação e informação	0
15.2.1 Monitoramento e análise crítica de serviços com fornecedores	0
15.2.2 Gerenciamento de mudanças para serviços com fornecedores	0
16.1.1 Responsabilidades e procedimentos	0
16.1.2 Notificação de eventos de segurança da informação	0
16.1.3 Notificando fragilidades de segurança da informação	0
16.1.4 Avaliação e decisão dos eventos de segurança da informação	0
16.1.5. Resposta aos incidentes de segurança da informação	1
16.1.6 Aprendendo com os incidentes de segurança da informação	0
16.1.7 Coleta de evidências	0
17.1.1 Planejando a continuidade da segurança da informação	0
17.1.2 Implementando a continuidade da segurança da informação	0
17.1.3 Verificação, análise crítica e avaliação da continuidade da segurança da informação	0
17.2.1 Disponibilidade dos recursos de processamento da informação	0
18.1.1 Identificação da legislação aplicável e de requisitos contratuais	0
18.1.2 Direitos de propriedade intelectual	0
18.1.3 Proteção de registros	0
18.1.4 Proteção e privacidade de informações de identificação pessoal	0
18.1.5 Regulamentação de controles de criptografia	0
18.2.1 Análise crítica independente da segurança da informação	0
18.2.2. Conformidade com as políticas e procedimentos de segurança da informação	1
18.2.3 Análise crítica da conformidade técnica	0
SOMA DOS CO DA NORMA DA ABNT NÃO EVIDENCIADOS	**92 / 81%**
SOMA DOS CO DA NORMA DA ABNT EVIDENCIADOS	**22 / 19%**

Quadro 1 – Enquadramentos dos procedimentos de CO da CESTIC nos CO da Norma NBR ISO/IEC 27002:2013

Tabela 1 – Rol de resultados referentes à quantidade de procedimentos CO da CESTIC vinculados a cada um dos CO da norma da ABNT

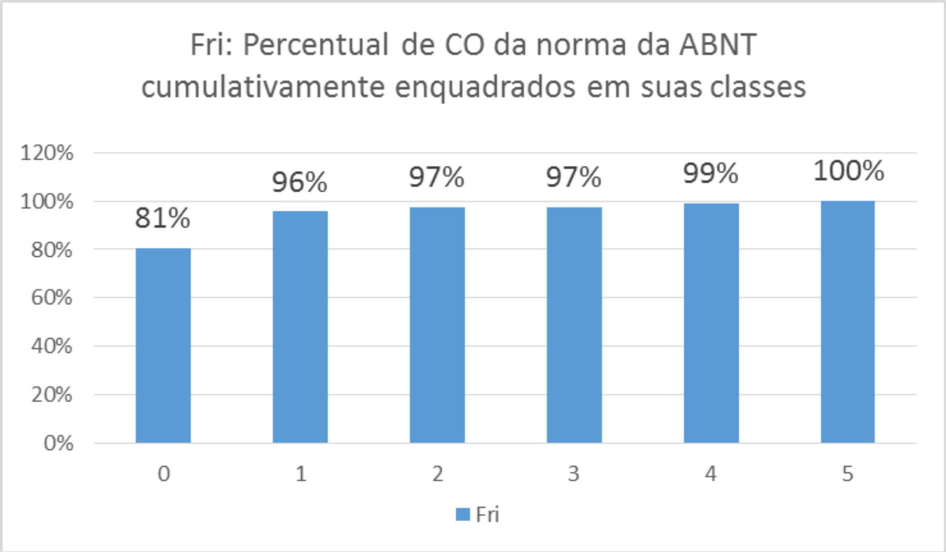
Rol de resultados referentes à quantidade de procedimentos CO da CESTIC vinculados a cada um dos CO da norma da ABNT
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0 ,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,2,2,4,4,5

Tabela 2 – Definição das classes de frequência do rol da tabela 1

Classes (k)	**Amplitude total (AT)**	**Amplitude de classe (h)**
7	6	1

Tabela 3 – Quantidade de CO da norma da ABNT agrupados nas classes que informam a quantidade de procedimentos de CO da CESTIC que evidenciaram cada um dos CO da norma da ABNT

Quantidade de CO da norma da ABNT agrupados nas classes que informam a quantidade de procedimentos de CO que evidenciaram cada um dos CO da norma da ABNT				
Quantidade de procedimentos de CO da CESTIC	**fi**	**fri**	**Fi**	**Fri**
0	92	81%	92	81%
1	17	15%	109	96%
2	2	2%	111	97%
3	0	0%	111	97%
4	2	2%	113	99%
5	1	1%	114	100%



Gáfico 1 – Percentual de CO da norma da ABNT cumulativamente enquadrados em suas classes de frequências

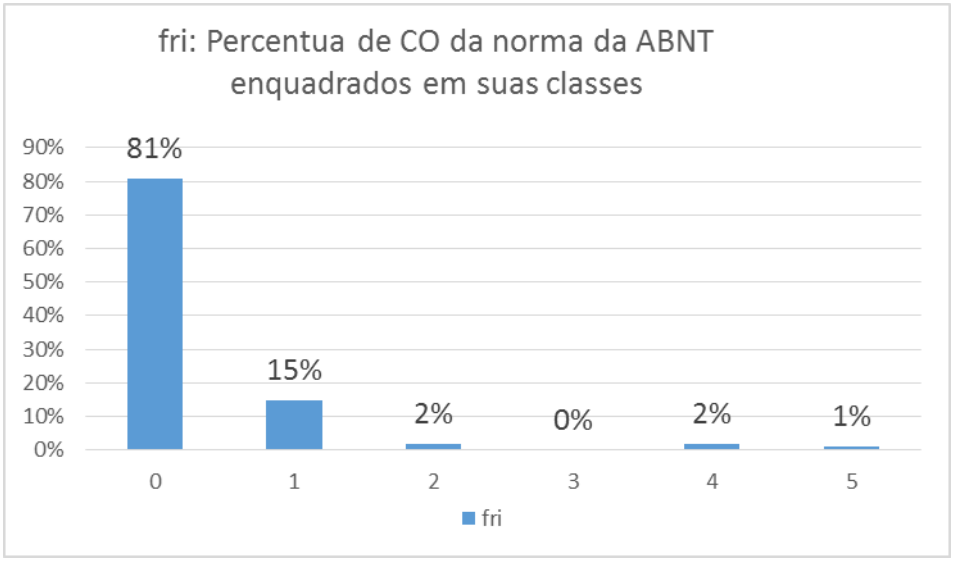


Gráfico 2 – Percentual de CO da norma da ABNT enquadrados em suas classes de frequência

Percebe-se que 15% dos CO evidenciados da norma da ABNT possuem somente um procedimento de CO previsto na CESTIC (1:1). Há dois CO evidenciados da norma da ABNT que possuem dois procedimentos de CO previstos na CESTIC (2:2), o que corresponde a 2% de todos os CO evidenciados. Há, ainda, 2% de CO evidenciados da norma da ABNT, que possuem quatro procedimentos de CO (2:4), e apenas 1% contendo cinco procedimentos CO da CESTIC (1:5). Por fim, fica constatado que 81% dos CO da norma da ABNT não possuem nenhum procedimento de CO evidenciado por procedimentos de CO da CESTIC. Esse valor indica uma grande deficiência relacionada à aplicação de CO de SI considerados como boas práticas pela norma da ABNT, e representa as atuais áreas de CO não verificadas pelas auditorias de SI de TIC. É interessante também destacar os CO da norma da ABNT mais evidenciados, devido à maior quantidade de procedimentos de CO da CESTIC vinculados a eles: 6.2. Dispositivos móveis e trabalhos remotos e 14.2. Segurança em processos de desenvolvimento e suporte com quatro procedimentos cada, e os CO 9.1. Requisitos do negócio para controle de acesso, 13.2. Transferência de informação com cinco procedimentos cada.

Outro aspecto abordado foi o estudo do percentual de CO da norma da ABNT evidenciados e não evidenciados por procedimentos de CO da CESTIC, mas desta vez, agrupados em seus respectivos OC previstos na norma da ABNT. Com isso, foi possível obter a visão sobre o nível de implementação desses OC recomendados, através da verificação da quantidade de CO evidenciados e a quantidade de CO previstos na norma.

Enquadramentos dos CO da norma da ABNT nos seus OC e as suas quantidades de CO evidenciados

OC da norma da ABNT	Quantidade de CO evidenciados na CESTIC	Quantidade total de CO do OC da norma da ABNT	% de CO evidenciados do OC da norma da ABNT	% de CO não evidenciados do OC da norma da ABNT
5.1. Orientação da direção para segurança da informação	0	2	0%	100%
6.1. Organização interna	1	5	20%	80%
6.2. Dispositivos móveis e trabalhos remotos	1	2	50%	50%
7.1. Antes da contratação	0	2	0%	100%
7.2. Responsabilidades da direção	1	3	33%	67%
7.3. Encerramento e mudança da contratação	0	1	0%	100%
8.1. Responsabilidade pelos ativos	0	4	0%	100%
8.2. Classificação da informação	0	3	0%	100%
8.3. Tratamento de mídias	0	3	0%	100%
9.1. Requisitos do negócio para controle de acesso	1	2	50%	50%
9.2. Gerenciamento de acesso do usuário	1	6	17%	83%
9.3. Responsabilidades dos usuários	1	1	100%	0%
9.4. Controle de acesso ao sistema e à aplicação	1	5	20%	80%
10.1.Controles criptográficos	1	2	50%	50%
11.1 Áreas seguras	0	6	0%	100%
11.2. Equipamentos	5	9	56%	44%
12.1. Responsabilidades e procedimentos operacionais	0	4	0%	100%
12.2. Proteção contra códigos maliciosos	1	1	100%	0%
12.3. Cópias de segurança	0	1	0%	100%
12.4. Registros e monitoramento	0	4	0%	100%
12.5. Controle de software operacional	1	1	100%	0%
12.6. Gestão de vulnerabilidades técnicas	1	2	50%	50%
12.7. Considerações quanto à auditoria de sistemas de informação	0	1	0%	100%
13.1. Gerenciamento da segurança em redes	0	3	0%	100%
13.2. Transferência de informação	2	4	50%	50%
14.1. Requisitos de segurança de sistemas de informação	0	3	0%	100%
14.2. Segurança em processos de desenvolvimento e suporte	2	9	22%	78%
14.3. Dados para teste	0	1	0%	100%

Enquadramentos dos CO da norma da ABNT nos seus OC e as suas quantidades de CO evidenciados				
OC da norma da ABNT	**Quantidade de CO evidenciados na CESTIC**	**Quantidade total de CO do OC da norma da ABNT**	**% de CO evidenciados do OC da norma da ABNT**	**% de CO não evidenciados do OC da norma da ABNT**
15.1. Segurança da informação na cadeia de suprimento	0	3	0%	100%
15.2. Gerenciamento da entrega do serviço do fornecedor	0	2	0%	100%
16.1. Gestão de incidentes de segurança da informação e melhorias	1	7	14%	86%
17.1. Continuidade da segurança da informação	0	3	0%	100%
17.2. Redundâncias	0	1	0%	100%
18.1. Conformidade com requisitos legais e contratuais	0	5	0%	100%
18.2. Análise crítica da segurança da informação	1	3	33%	67%
SOMA	**22**	**114**	**19%**	**81%**

Quadro 2 – Enquadramentos dos CO da norma da ABNT nos seus OC e as suas quantidades de CO evidenciados na CESTIC

Tabela 4 – Rol de resultados com o percentual de CO evidenciados na CESTIC para cada OC da norma da ABNT

Rol de resultados com o percentual de CO evidenciados na CESTIC para cada OC da norma da ABNT
0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,0%,14%,17%,20%,20%,22%, 33%,33%,50%, 50%,50%,50%, 50, 56%, 100%, 100% e 100%

Tabela 5 – Obtenção das classes de frequência do rol da tabela 4

Classes (k)	Amplitude total (AT)	Amplitude de classe (h)
6	100	17

Tabela 6 – Quantidade de OC evidenciados da norma da ABNT agrupados nas classes que informam a faixa percentual de CO evidenciados/implementados

Quantidade de OC evidenciados da norma da ABNT agrupados nas classes que informam a faixa percentual de CO evidenciados/implementados				
% de CO evidenciados/implementados previstos para o OC	**fi**	**fri**	**Fi**	**Fri**
0% - 16%	20	57%	20	57%

Quantidade de OC evidenciados da norma da ABNT agrupados nas classes que informam a faixa percentual de CO evidenciados/implementados

% de CO evidenciados/implementados previstos para o OC	fi	fri	Fi	Fri
17% - 33%	6	17%	26	74%
34% - 50%	5	14%	31	89%
51% - 67%	1	3%	32	91%
68% - 84%	0	0%	32	91%
85% - 100%	3	9%	35	100%

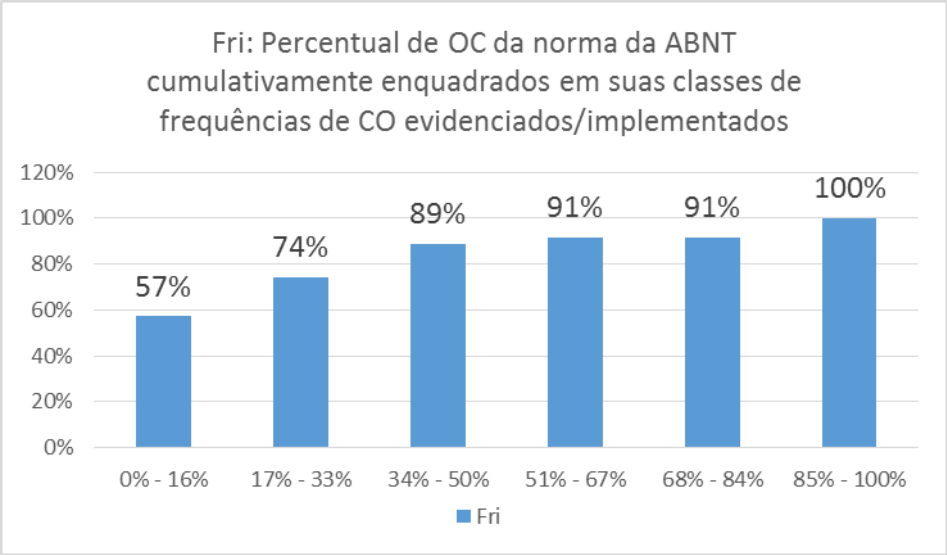


Gráfico 3 – Percentual de OC da norma da ABNT cumulativamente enquadrados em suas classes de frequências de CO evidenciados/implementados

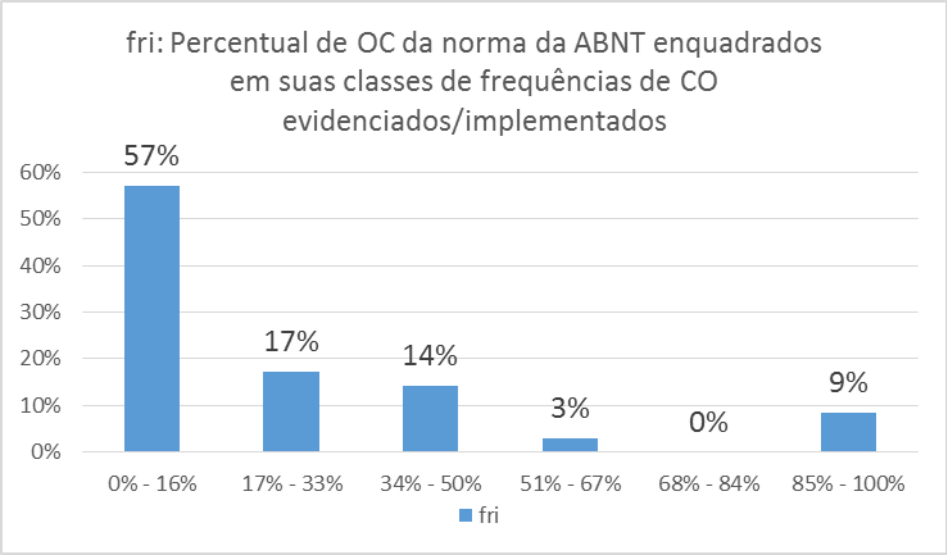


Gráfico 4 – Percentual de OC da norma da ABNT cumulativamente enquadrados em suas classes de frequências de CO evidenciados/implementados

Com relação aos valores relacionados aos OC da norma da ABNT que possuem até 16% dos seus CO previstos implementados, 95% deles não possuem CO implementados (54% do total de OC da norma da ABNT) e um OC possui 14% de seus CO previstos implementados. Essa primeira classe de frequência corresponde a 57% de todos os OC recomendados pela norma da ABNT, e representam a classe de maior deficiência de OC de SI de TIC das atuais auditorias realizadas. Em seguida, temos um grupo de OC correspondente a 17% do total previsto na norma da ABNT, que possui de 17 a 33% de seus CO previstos implementados pela CESTIC, ou seja, essa é mais uma classe de frequência que representa uma pequena quantidade de CO previstos implementados. A classe de frequência seguinte correspondente a 14% do total previsto na norma da ABNT que implementa de 34 a 50% de seus CO previstos na norma, existindo, ainda, mais um grupo com um baixo percentual de implementação, mas, dessa vez, mais próxima da metade recomendada. É perceptível que 89% dos OC previstos na norma ABNT NBR ISO/IEC 27002:2013 possuem nenhuma, fraca ou mediana implementação de seus CO recomendados previstos, o que corresponde a uma grande deficiência na verificação da SI de TIC nas auditorias executadas pelas OM de telemática do EB, quando comparadas ao código de boas práticas da ABNT. 11% dos OC da norma da ABNT tiveram o percentual acima de 50% de seus CO implementados na CESTIC. Desses, o OC 11.2. Equipamentos obteve 56% de implementação e os 9.3. Responsabilidades dos usuários, 12.2. Proteção contra códigos maliciosos e 12.5. Controle de software operacional tiveram 100% de seus CO previstos evidenciados na CESTIC.

Com relação as quais Seções da norma da ABNT são implementadas na CESTIC, é possível analisá-las através das evidências de atendimento aos OC implantados e analisados anteriormente. A análise da relação entre OC implementados na CESTIC e as Seções de controle previstas na norma da ABNT podem ser observadas a seguir.

Enquadramentos dos OC da norma da ABNT nas Seções de controle e as suas quantidades de OC evidenciados/implementados				
Seções de controle da norma da ABNT	**Quantidade de OC implemen-tados na CESTIC**	**Quantidade total de OC da Seção da norma da ABNT**	**% de OC imple-mentados da norma da ABNT**	**% de OC não implemen tados da norma da ABNT**
5. Políticas para a Segurança da Informação	0	1	0%	100%
6. Organização da Segurança da Informação	2	2	100%	0%
7. Segurança em Recursos Humanos	1	3	33%	67%
8. Gestão de ativos	0	3	0%	100%
9. Controle de Acesso	4	4	100%	0%
10. Criptografia	1	1	100%	0%
11. Segurança Física e do Ambiente	1	2	50%	50%
12. Segurança nas Operações	3	7	43%	57%
13. Segurança nas Comunicações	1	2	50%	50%
14. Aquisição, Desenvolvimento e Manutenção de Sistemas	1	3	33%	67%
15. Relacionamento na Cadeia de Suprimentos	0	2	0%	100%
16. Gestão de Incidentes de Segurança da Informação	1	1	100%	0%
17. Aspectos de Segurança da informação na gestão da Continuidade do Negócio	0	2	0%	100%
18. Conformidade	1	2	50%	50%
SOMA	**16**	**35**	**46%**	**54%**

Quadro 3 – Enquadramentos dos OC da norma da ABNT nas Seções de controle e as suas quantidades de OC evidenciados/implementados

Tabela 7 – Rol de resultados referentes à quantidade percentual de OC evidenciados/implantados para cada uma das Seções de controle

Rol de resultados referente à quantidade percentual de OC evidenciados/implantados para cada uma das Seções de controle
0%,0%,0%,0%,33%,33%,43%,50%,50%,50%,100%,100%,100% e 100%

Tabela 8 – Obtenção das classes de frequência do rol da tabela 7

Classes (k)	**Amplitude total (AT)**	**Amplitude de classe (h)**
5	100	20

Tabela 9 – Quantidade de Seções da norma da ABNT agrupadas nas classes que informam a sua quantidade percentual de OC evidenciados/implementados

Quantidade de Seções da norma da ABNT agrupadas nas classes que informam a sua quantidade percentual de OC evidenciados/implementados

% de OC implantados previstos para a Seção	fi	fri	Fi	Fri
0% - 19%	4	29%	4	29%
20% - 39%	2	13%	6	42%
40% - 59%	4	29%	10	71%
60% - 79%	0	0%	10	71%
80% - 100%	4	29%	14	100%

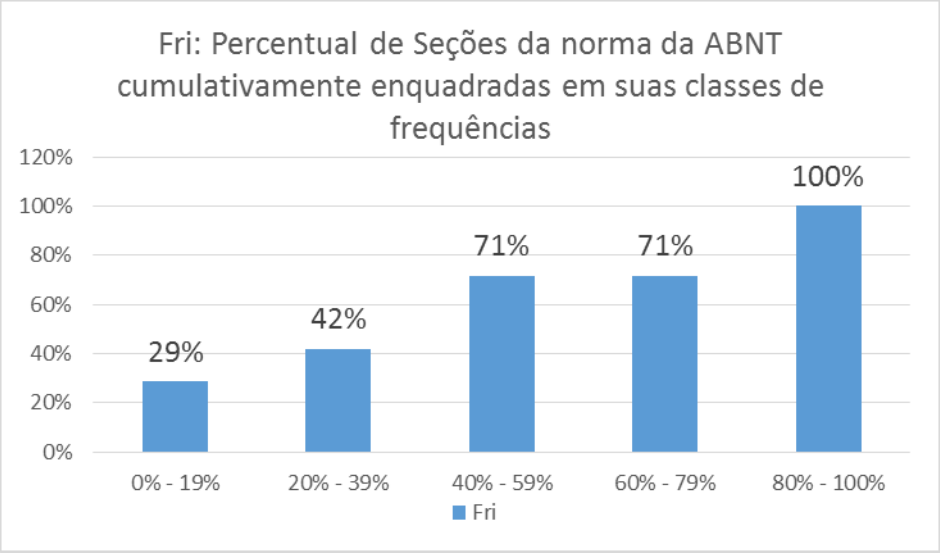


Gráfico 5 – Percentual de Seções da norma da ABNT cumulativamente enquadradas em suas classes de frequência

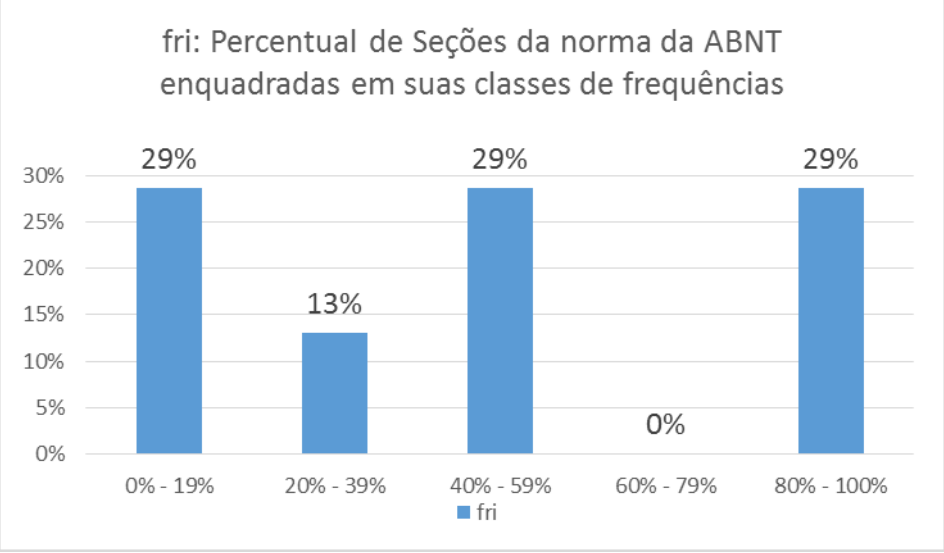


Gráfico 6 – Percentual de Seções da norma da ABNT enquadradas em suas classes de frequência

As três primeiras classes de frequência correspondem a 71% das Seções de controle prevista na norma da ABNT, das quais 29% se referem às Seções de controle que não são implementadas pela CESTIC, pois não há nenhum OC (0%) implementado referente a elas, representando as principais deficiências de implementação das Seções. As Seções não implementadas são: 5. Política para a Segurança da Informação, 8. Gestão de Ativos, 15. Relacionamento na Cadeia de Suprimentos e 17. Aspectos de Segurança da Informação na Gestão da Continuidade do Negócio. Nesse mesmo grupo de 71%, em seguida temos uma classe de frequência correspondente a 13% das Seções da norma da ABNT, que possuem de 20 a 39% de seus OC previstos implementados pela CESTIC, são elas: 6. Segurança e Recursos Humanos, 11. Segurança Física e do Ambiente, 12. Segurança nas Operações, 13. Segurança nas Comunicações, 14. Aquisição, Desenvolvimento e Manutenção de Sistemas e 18. Conformidade. Completando esse grupo de 71%, há a terceira classe de frequência que corresponde a 29% das Seções previstas na norma da ABNT, e que possuem implementados de 40 a 59% de seus OC previstos, indicando o intervalo mediano de implementação. Existe, ainda, a classe de frequência correspondente aos últimos 29% do total de Seções de controle recomendadas pela norma da ABNT, as quais todas elas possuem todos os seus OC implementados (100%).

Cabe relembrar que as Seções de controle foram implementadas em diferentes níveis pela CESTIC, pois na maioria dos casos não tiveram todos os seus OC previstos na norma da ABNT implementados. Por sua vez, também ocorreram implementações de OC em que não ficaram evidenciadas as implantações de todos os seus CO previstos na norma da ABNT. Logo, há variações quanto ao nível de atendimento dos diferentes níveis de recomendações da norma da ABNT. É importante ressaltar, ainda, que os procedimentos de CO da CESTIC foram enquadrados de acordo com as descrições dos CO da norma da ABNT.

Assim, percebe-se que o Exército Brasileiro, por meio de suas OM de telemática, necessita complementar suas normas de auditoria de SI de TIC, especificando mais procedimentos de controle extraídos do código de boas práticas da norma ABNT NBR ISO/IEC 27002:2013, a fim de melhorar a sua visão e a gestão de riscos de SI de TIC com relação às diversas OM do EB.

4. CONCLUSÃO

O ambiente atual do EB tem apresentado como principal característica a dependência das áreas meio e finalísticas com relação aos serviços e infraestruturas de tecnologia da informação e comunicações. Essa dependência provém da necessidade de o EB, atuar em seus níveis estratégico, operacional e tático, buscando uma maior eficiência na execução dos trabalhos.

Esse novo ambiente, gerou a necessidade de se aumentar a capacidade do EB e garantir os seus diferentes níveis de serviços de TIC. O aumento dessa capacidade ajuda o EB a se proteger da ocorrência de incidentes, sejam eles comuns, relacionados a sua operação, ou devido à ação intencional inimiga, exigindo um permanente estado de prontidão.

Exemplificando a assertiva acima, podem ser citadas as ações desenvolvidas pelas Organizações Militares de telemática, CT e CTA, que compõem o SisTEx, subordinado ao DCT. Essas ações se resumem na realização anual de auditorias de segurança da informação nas áreas de tecnologia da informação e comunicações, atualmente reguladas quanto ao processo através da IRASEG IR 13-09 e quanto aos procedimentos de CO pela CESTIC.

Condizente com o atual contexto, buscou-se verificar o grau de atendimento das boas práticas em segurança da informação internas do EB, por meio da análise da CESTIC, com relação ao que é recomendado pelo código de boas práticas em segurança da informação externa ao EB, a norma ABNT NBR ISO/IEC 27002:2013. Essa comparação ocorreu através do enquadramento dos procedimentos de segurança da informação impostos pela CESTIC, nos CO recomendados pela norma da ABNT. Em seguida, os CO evidenciados foram relacionados aos seus respectivos OC da mesma norma, verificando-se o grau de sua implementação. Posteriormente, os OC implementados foram associados as suas Seções de controle, também possibilitando verificar o grau de implementação das Seções. Com isso, foi possível verificar a existência de deficiências e os atuais focos de atenção de CO de segurança da informação aplicados.

A análise de tais dados deixou clara a existência de uma lacuna na verificação de aspectos relacionados à segurança da informação na área da tecnologia da informação e comunicações, o que causa uma deficiência na visão e gestão de

riscos de TIC, deixando os serviços e suas infraestruturas vulneráveis às ameaças que exploram vulnerabilidades causando incidentes.

Visando solucionar tal falha torna-se necessária a constituição de um grupo para a revisão da CESTIC e a sua capacitação sobre a norma ABNT NBR ISO/IEC 27002:2013. A norma externa ao EB que deve ser utilizada é a ABNT NBR 27002:2013, pois possui um código de boas práticas sobre segurança da informação consolidado através de boas práticas internacionais em controles de segurança da informação em tecnologia da informação.

A revisão da CESTIC deve contemplar dois focos de melhoria para as auditorias de SI: o primeiro é o aumento do grau da implementação de CO, OC e Seções de controle já evidenciados e implementados na CESTIC. Isso pode ser feito através da máxima utilização das Diretrizes previstas para implementação de CO, de OC, e consequentemente das Seções de controle recomendados pela norma da ABNT; o segundo foco corresponde à implementação de todos os elementos previstos pelo código de boas práticas atualmente inexistentes na CESTIC. Esse último foco citado deve ser considerado como a principal área de melhoria nos processos de auditoria de segurança da informação, pois são lacunas que não estão sendo verificadas e podem estar sendo atualmente exploradas para causar incidentes de SI.

Os integrantes desse grupo de aperfeiçoamento da CESTIC devem figurar como multiplicadores de conhecimento sobre a norma, possibilitando que as auditorias sejam realizadas de forma homogênea, independente da equipe de auditoria, e de acordo com a nova CESTIC.

Além das necessidades de revisão e capacitações supracitadas recomenda-se a elaboração de uma lista de verificação pelo grupo revisor, a fim de buscar a homogeneidade e a devida abrangência das auditorias. Essa padronização baseada na nova cartilha facilita, ainda mais, a consolidação de indicadores gerais e a comparação dos resultados entre as diferentes regiões de auditoria, além de dirimir dificuldades de implementação por parte dos militares capacitados.

A utilização das listas de verificação deve ser considerada uma meta a ser cumprida anualmente e, para isso, deve ser incluída nos Contratos de Objetivos, que são acordados e assinados anualmente entre os diversos escalões superiores e subordinados. Essa ação gera um maior comprometimento dos comandantes, chefes e diretores dos diversos tipos de unidades militares, a dispenderem atenção

ao assunto segurança da informação, através de seus Oficiais de Informática da OM.

Em sequência, às sugestões anteriores recomenda-se criação de uma capacitação específica para as equipes de auditoria com a finalidade de que haja homogeneidade na aplicação da lista de verificação além de facilitar o recebimento de contribuições para o aperfeiçoamento da CESTIC. Pode-se utilizar do Ambiente Virtual de Aprendizagem (AVA) da Diretoria de Ensino e Cultura do Exército (DECEx) como viabilizador dessa capacitação, devido à economia de gastos relacionados às diárias e passagens além de oferecer ao aluno maior flexibilidade nos estudos. Essa maior flexibilidade deve ocorrer em horário de expediente a fim de não prejudicar as responsabilidades particulares dos militares e não tornar essa atividade um ônus. Recomenda-se, ainda, incluir a mesma capacitação realizada pelo grupo revisor no calendário anual de capacitações das OM de telemática do EB. Essa aquisição sendo adquirida de forma centralizada, facilita a elaboração do processo administrativo e padroniza o nível da capacitação oferecida. Com isso, os militares aprenderão sobre os conceitos, vocabulários, aplicações e CO da norma da ABNT, podendo contribuir com maior facilidade e embasamento para o aperfeiçoamento da nova Cartilha.

É recomendável que as capacitações e a execução das auditorias de segurança da informação em TIC devem ser mantidas pelas OM de telemática por possuírem grande capilaridade no território nacional. Isso facilita a implementação das auditorias em um maior número possível de unidades do EB. Contribuindo para uma maior amplitude de cobertura dessas ações de proteção.

Por fim, o último grupo que deve ser capacitado é o formado pelos representantes da área de informática das OM apoiadas pelos CTA e CT. Eles devem possuir o conhecimento adequado sobre a nova Cartilha a fim de implantarem todos os procedimentos de SI previstos, e assim, efetivamente tornarem cada uma das OM um local protegido contra ameaças. É importante que os Centros de Telemática mantenham contato com suas OM apoiadas com o objetivo de ajudar na implantação dos procedimentos e dirimir dificuldades.

Ressalta-se, novamente, que essas ações de melhoria são necessárias devido à tendência do crescimento dos combates relacionados à guerra cibernética no contexto mundial, tornado inevitável o emprego do EB neste complexo ambiente tecnológico, que apenas pode ser vencido através da constante capacitação, ações

inovadoras de aperfeiçoamento das auditorias, valorização dos militares e unidades destinadas a esse fim, cabendo destacar que não são unidades que entregam produtos tangíveis, e sim, intangíveis que visam proteger a continuidade dos serviços e infraestruturas.

Assim, uma Força Terrestre cuja finalidade é contribuir para a garantia da soberania nacional, dos poderes constitucionais, da lei e da ordem, salvaguardando os interesses nacionais, cooperando com o desenvolvimento nacional e o bem-estar social, deve manter intactas, contínuas e sempre disponíveis todos os seus serviços e infraestruturas de TIC, através de sua proteção e mitigação de vulnerabilidades e ameaças.

REFERÊNCIAS

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO/IEC 27002:2013**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

2. BRASIL. Comando do Exército. **Portaria de aprovação da Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações**. Brasília, 2011. Disponível em: <www.sgex.eb.mil.br/sistemas/be/copiar.php?codarquivo=998& act=bre>. Acesso em: 12 jul. 2016, 16:33:12.

3. BRASIL. Departamento de Ciência e Tecnologia do Exército. **Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações**. Brasília, 2011. Disponível em: <www.2icfex.eb.mil.br/Portarias/cartilha_ seguranca.pdf>. Acesso em: 13 jul. 2016, 18:10:01.

4. BRASIL. Departamento de Ciência e Tecnologia do Exército. **Instruções Reguladoras sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro – IRASEG (IR13-09)**. Brasília, DF, 2007. Disponível em: <http:// stir.citex.eb.mil.br/Documentacao/IRASEG(IR%2013-09).pdf>. Acesso em: 13 jul. 2016, 11:20:21.

5. BRASIL. Estado Maior Conjunto das Forças Armadas. **MD-31-P-02: Política Cibernética de Defesa.** 1ª Ed. Brasília, DF, 2012. Disponível em <http://www.idcibereb.unb.br/images/documentos/doutrina /manual_pol_nac_def.pdf >. Acesso em: 13 jul. 2016, 10:10:32.

6. BRASIL, Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, 2012. Disponível em: <http://www.defesa.gov.br/ arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 13 jul. 2016, 14:09:10.

7. NEVES, E. B. e DOMINGUES, C. A. **Manual de Metodologia da Pesquisa Científica**. Rio de Janeiro: EB/CEP, 2007.