Arquitetura de segurança da informação no terceiro setor: avaliação na comissão pastoral da terra

Arnaldo Alves Ferreira Júnior (UFG) - arnaldo@facomb.ufg.br

Carminda de Aguiar Pereira (UFG) - carmindaaguiar1@gmail.com

Resumo:

Esta pesquisa teve como principal objetivo verificar o nível de eficiência de segurança da informação, a partir dos requisitos apresentados pelas Normas de Gestão da Segurança da Informação ABNT NBR ISO/IEC, no Terceiro Setor. Para verificar este nível de eficiência foi realizado um estudo das Normas relativas à Gestão da Segurança da Informação elaboradas pela ABNT NBR ISO/IEC 27001:2006; 27002:2005; 27003:2011 e 27005:2011 e elaborado a partir deste estudo um conjunto de critérios de avaliação que levasse em conta uma perspectiva de Arquitetura de Segurança da Informação. Foram trabalhados na fundamentação teórica temas como, Segurança da Informação; normas da ABNT relativas à Gestão da Segurança da Informação; Arquitetura da Informação e Terceiro Setor. A organização avaliada pelos critérios foi a Comissão Pastoral da Terra (CPT), entidade atuante no Terceiro Setor em Goiânia. Como resultado foi constatado a importância deste tipo de pesquisa no terceiro setor, assim como em outras áreas da economia no país. Além de destacar a necessidade de constantes atualizações nos processos e instrumentos de gestão, incluindo nestes a área relativa à segurança da informação, propor perspectivas de pesquisa baseado na inserção de metáfora de Arquitetura no setor de segurança de informação nas organizações.

Palavras-chave: *Segurança da informação. Arquitetura da informação. Terceiro setor. Avaliação. Normas ABNT ISO/IEC.*

Área temática: *Temática I: Tecnologias de informação e comunicação – um passo a frente*

Arquitetura de segurança da informação no terceiro setor: avaliação na comissão pastoral da terra

RESUMO
Esta pesquisa teve como principal objetivo verificar o nível de eficiência de segurança da informação, a partir dos requisitos apresentados pelas Normas de Gestão da Segurança da Informação ABNT NBR ISO/IEC, no Terceiro Setor. Para verificar este nível de eficiência foi realizado um estudo das Normas relativas à Gestão da Segurança da Informação elaboradas pela ABNT NBR ISO/IEC 27001:2006; 27002:2005; 27003:2011 e 27005:2011 e elaborado a partir deste estudo um conjunto de critérios de avaliação que levasse em conta uma perspectiva de Arquitetura de Segurança da Informação. Foram trabalhados na fundamentação teórica temas como, Segurança da Informação; normas da ABNT relativas à Gestão da Segurança da Informação; Arquitetura da Informação e Terceiro Setor. A organização avaliada pelos critérios foi a Comissão Pastoral da Terra (CPT), entidade atuante no Terceiro Setor em Goiânia. Como resultado foi constatado a importância deste tipo de pesquisa no terceiro setor, assim como em outras áreas da economia no país. Além de destacar a necessidade de constantes atualizações nos processos e instrumentos de gestão, incluindo nestes a área relativa à segurança da informação, propor perspectivas de pesquisa baseado na inserção de metáfora de Arquitetura no setor de segurança de informação nas organizações.

Palavras-Chave: Segurança da informação. Arquitetura da informação. Terceiro setor. Avaliação. Normas ABNT ISO/IEC.

1 INTRODUÇÃO

As ameaças à segurança da informação não estão relacionadas apenas com os sistemas e redes corporativas, em uma área tipicamente denotada por segurança lógica ou digital. O conceito de segurança da informação vai além; pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associados aos diversos ativos de informações[1] de uma organização, independente da forma representada, ou meio em que são compartilhados ou armazenados (digital ou impresso). De acordo com Zapater e Suzuki (2005, p. 06) “o objetivo da segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação”.

As organizações do Terceiro Setor, por serem voltadas à prestação de serviços sociais, devem também dar atenção a questões relativas à segurança da informação, já que independente do setor da economia em que a organização atue, as informações estão relacionadas com seus processos de produção e de negócios, políticas estratégicas, de *marketing*, cadastro de clientes/usuários e informações institucionais, dentre outros processos. Segundo Caruso e Steffen (1990, p. 22), independentemente do suporte em que as informações estejam armazenadas, elas possuem valor para a

[1] Ativos de informações são bases de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas. Fonte: ABNT NBR ISO/IEC 27002:2005.

organização que as geram e utilizam. Essas informações podem ser tanto de caráter sigiloso ou relacionadas com atividades diárias da organização.

Diante do contexto acima, a presente pesquisa se pautou nos requisitos das Normas de Qualidade criadas em conjunto pela Associação Brasileira de Normas Técnicas (ABNT), a *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC), relativas à Gestão da Segurança da Informação, a fim de verificar o nível de eficiência dos procedimentos de Segurança da Informação em Organizações do Terceiro Setor. Para proceder a tal avaliação, foi elaborada a partir de estudos detalhados destas normas, uma estrutura de critérios de avaliação que orientou a análise da atual situação de gestão da segurança da informação. Para proceder à pesquisa empírica, foi selecionada a Comissão Pastoral da Terra[2] (CPT) que possui sede nacional na cidade de Goiânia - Goiás.

Para cumprir os objetivos traçados de início, as seguintes etapas foram desenvolvidas: a) realizou-se um estudo das Normas relativas à Gestão da Segurança da Informação elaboradas pela ABNT NBR ISO/IEC - 27001:2006; 27002:2005; 27003:2011 e 27005:2011, para prover requisitos mínimos na construção dos critérios de avaliação da Segurança da Informação; b) elaborou-se uma estrutura de critérios de Arquitetura de Segurança da Informação, a partir dos requisitos apresentados pelas normas ABNT NBR ISO/IEC; e por fim, c) Avaliou-se o nível de eficiência e eficácia dos procedimentos de Gestão da Segurança da Informação na Comissão Pastoral da Terra, a partir dos critérios elaborados e baseados nas normas ABNT NBR ISO/IEC.

Os resultados desta pesquisa permitiram responder a questão problema que consistiu em saber: Qual a situação atual da Arquiteturas de Segurança da Informação no Terceiro Setor a partir dos requisitos apresentados pelas normas da ABNT NBR ISO/IEC relativas à Gestão da Segurança da Informação?

2 SEGURANÇA DA INFORMAÇÃO

O termo **segurança da informação** (SI) é geralmente vinculado aos sistemas informatizados e aos dados que estes manipulam. Segundo Almeida; Souza e Coelho (2010) diz respeito a aspectos relacionados à área de Tecnologia da Informação (TI), como por exemplo, controle de acesso a recursos computacionais; segurança em comunicação; gestão de riscos; políticas de informação; sistemas de segurança; diretrizes legais; segurança física; criptografia, etc. Entretanto a SI não se limita apenas

[2] Comissão Pastoral da Terra - CPT. Disponível em: <http://www.cptnacional.org.br>. Acesso em: 27 Jan., 2013.

à proteção de dados em computadores e em redes, uma vez que organizações não possuem apenas informações em formato digital, "segurança também pode envolver questões de natureza física, política e cultural". (ALMEIDA; SOUZA; COELHO, 2010, p. 155). Para Macgee e Prusak (1994) a informação não se limita a dados coletados,

> [...] na verdade [informações] são dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto. Informação deve informar, enquanto os dados absolutamente não tem essa missão. A informação deve ter limites, enquanto os dados podem ser ilimitados. (MACGEE; PRUSAK, p. 24).

Segurança da Informação é a proteção da informação de vários tipos de ameaças, a fim de garantir a continuidade; minimizar o risco e maximizar o retorno sobre os investimentos e as oportunidades do negócio. Segundo ABNT (2005) a informação é um ativo[3] que, como qualquer outro é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida (de ameaças, violações, fraudes, acesso não permitido, etc.).

De acordo com Beal (2005) as organizações precisam adotar controles de segurança, medidas de proteção que abranjam uma grande diversidade de iniciativas, que sejam capazes de proteger adequadamente dados, informações e conhecimentos, levando-se em conta os riscos reais a que estão sujeitos esses ativos. Nenhuma organização pode escapar dos efeitos da revolução causada pela informação, deve-se ter consciência do fato de que, a informação é um requisito tão importante quanto os recursos humanos e tecnológicos, dela em parte dependem o sucesso ou fracasso das tomadas de decisões diárias. Segundo Almeida; Souza e Coelho (2010, p. 156), para muitas organizações a segurança da informação ainda é:

> [...] uma necessidade de negócio e ainda assim, nem sempre práticas dessa natureza são adotadas, visto que projetos e recursos necessários são caros, complexos, demandam tempo e não garantem efetividade. Problemas na implementação de estratégias de segurança da informação começam pela dificuldade em definir o que deve ser protegido, qual nível de proteção necessário e quais ferramentas devem ser utilizadas no ambiente corporativo. Cabe ainda à organização descobrir em que contexto se manifesta a informação relevante para seus objetivos de negócio, bem como as necessidades corporativas em relação à segurança. (ALMEIDA; SOUZA; COELHO, 2010, p. 156).

Essas necessidades são influenciadas por fatores humanos e por fatores inerentes ao próprio ciclo de vida da informação. Para evitar problemas de ataques a sistemas, vírus, acesso indesejado a informações sigilosas, fraudes eletrônicas, etc.,

[3] Qualquer bem que tenha valor para a organização. Fonte: ABNT NBR ISO/IEC 27002:2005.

deve-se proceder à elaboração, pela própria organização, de uma Política de Segurança da Informação, e esta política deve ser mais ampla e mais simples possível.

Por política de segurança, entende-se política elaborada, implantada e em contínuo processo de revisão, válida para toda a organização, com regras mais claras e simples e estrutura gerencial e material que dê suporte a esta política e que seja claramente sustentada pela alta hierarquia da organização (CARUSO; STEFFEN, 1999, p. 24). “As políticas de segurança da informação são, via de regra, apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adequar-se integralmente.” (MARCIANO; LIMA-MARQUES, 2006, p. 89).

Uma política de segurança deve contemplar os aspectos de classificação de ativos de informações quanto à sua proteção contra acessos não autorizados e sua preservação contra destruição e eliminação indevida. Além da proteção física e lógica, deve também contemplar o aspecto da recuperação da capacidade operacional, em casos de destruição parcial ou total da capacidade de processamento. (CARUSO; STEFFEN, 1999, p. 24).

As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações, privando o acesso a terceiros e delimitando entre os usuários que podem lidar com essas informações, sem alterá-las e os que de forma alguma podem ter acesso a estas informações. (BRASIL, 2007, p. 26). A criação destas políticas de segurança de informação não deve ficar restrita aos profissionais da área de tecnologias, mas sim ligada a outros setores dentro da organização.

De acordo com a *Information Systems Audit and Control Foundation* (ISACF, 2000, *tradução nossa*) para que ocorra a gestão e governança da segurança da informação é indispensável a aplicação das seguintes etapas, **a)** Desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas; **b)** Papéis e Autoridades, assegurando que cada responsabilidade seja claramente entendida por todos; **c)** Delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos; **d)** Implementação, em um tempo hábil e com capacidade de manutenção; **e)** Monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis; **f)** Vigilância,

treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

Informação adulterada, não disponível, sob o conhecimento de pessoas de má índole ou de concorrentes, pode comprometer significativamente não apenas a imagem da organização perante terceiros, como também o andamento dos próprios processos organizacionais. É possível inviabilizar a continuidade de uma organização se não for dada a devida atenção à segurança de suas informações.

3 NORMAS ABNT

3.1 ABNT NBR ISO/IEC 27002:2005

A norma técnica da **ABNT NBR ISO/IEC 27002: 2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação** tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Esta norma pode servir como um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança, e para ajudar a criar confiança nas atividades interorganizacionais.

3.2 ABNT NBR ISO/IEC 27001: 2006

A norma técnica da **ABNT NBR ISO/IEC 27001: 2006 – Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos** foi preparada para prover um modelo de modo a estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI). Esta norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas.

3.3 ABNT NBR ISO/IEC 27003: 2011

A norma técnica da **ABNT NBR ISO/IEC 27003:2011 – Tecnologia da informação – Técnicas de segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação** foca os aspectos críticos necessários para e implantação e projeto bem sucedidos de um SGSI, de acordo com a ABNT NBR ISO/IEC 27001:2005. A norma descreve o processo de especificação e projeto do SGSI desde a concepção até a elaboração dos planos de implantação. Ela descreve o

processo de obter aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI e fornece diretrizes sobre como planejar o projeto do SGSI, resultando em um plano final para implantação do projeto de SGSI. A intenção desta Norma é que ela seja usada pelas organizações que desejam implementar um SGSI.

3.4 ANBT NBR ISO/IEC 27005:2011

A norma técnica da **ABNT NBR ISO/IEC 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação** fornece diretrizes para o processo de gestão de riscos de segurança da informação. Está de acordo com os conceitos especificados na ANBT NBR ISO/IEC 27001 e foi elaborada para facilitar a implementação satisfatória da segurança da informação tendo como base uma abordagem de gestão de riscos. Esta norma se aplica a todos os tipos de organização que pretendem gerir os riscos que poderiam comprometer a segurança da informação da organização.

4 ARQUITETURA DA INFORMAÇÃO

O objetivo da Arquitetura da Informação (AI) visa agregar de forma eficiente e eficaz informações necessárias à organização, a fim de organizá-la de forma lógica e recuperá-la de forma efetiva, “a arquitetura da informação fornece suporte às ações de gestão do conhecimento, à medida que visa promover a acessibilidade à informação armazenada para garantir a eficácia do processo decisório nas organizações.” (LIMA-MARQUES; MACEDO, 2006, p. 250).

O termo arquitetura da informação foi cunhado por Richard Saul Wurman em meados da década de 1960, sendo seu principal objeto de estudo. Para Wurman a arquitetura da informação tinha a finalidade de organizar informações de forma que seus usuários pudessem acessá-las com facilidade. Em 1950 estudos começaram a enfocar os sistemas de informação. A arquitetura da informação valorizou-se ainda mais após o surgimento dos sistemas de informação automatizados, nesta época a arquitetura da informação preocupava-se principalmente em tratar a informação para a recuperação da mesma, abordando desde os catálogos das bibliotecas até os sistemas automatizados e de banco de dados. (CAMARGO, VIDOTTI, 2011).

Segundo Siqueira (2008, p. 30) “a visão de Wurman é derivada de sua formação como arquiteto, e seu principal propósito é estender os conceitos chave de organização de espaços informacionais”. Para Davenport (1998) nosso fascínio pela tecnologia nos

fez esquecer o objetivo principal da informação, o de informar. Todos os computadores do mundo de nada servem se seus usuários não estão interessados nas informações que esses computadores podem gerar, ou se essas informações forem imprecisas e incertas. O crescimento de equipamentos de telecomunicações e compartilhamento de informações será inútil se os funcionários de uma organização não compartilharem as informações que possuem. Sistemas de especialistas não irão proporcionar informações úteis se as mudanças nessa área de conhecimento forem muito rápidas, ou se os criadores destes sistemas não puderem encontrar especialistas dispostos a ensinar o que sabem.

5 TERCEIRO SETOR

As entidades criadas durante os três primeiros séculos do Brasil, pertencentes atualmente ao chamado terceiro setor, em sua origem existiram basicamente no espaço da igreja católica e permeada, portanto, pelos valores da caridade cristã. Foi a partir das características do catolicismo e de suas relações com o Estado que se implantou no país. No período pós-colonial, rompe-se a simbiose entre Igreja e Estado, consolidando-se com a proclamação da República e a promulgação da Constituição Liberal de 1891, que estabelece a liberdade de cultura, proíbe subvenções governamentais aos templos e a educação religiosa. Somente em 1930, pode-se dizer que o Estado assume para si a responsabilidade por uma ação mais efetiva na área social (direitos, seguridade, etc.). (VOLTOLINI, 2004).

Nos anos 1990 começa a expandir-se no Brasil, segundo Voltolini (2004, p. 07), “mudando o conceito antes dominante do serviço social com base em organizações dedicadas à caridade e à filantropia.” O termo Terceiro Setor tem procedência norte-americana, foi cunhado por John D. Rockefeller III e introduzido no Brasil através da Fundação Roberto Marinho. (MONTAÑO, 2002). De acordo com Falconer e Vilela (2001) a expressão surgiu há pouco mais de duas décadas e seu uso mais generalizado se deu há menos de cinco anos. Entretanto, ressaltam os autores, o termo é relativamente inédito no Brasil, “mas o fato a que se referem não o é em absoluto. Não se trata de um setor novo, mas de algo que tem raízes tão antigas quanto à presença portuguesa na América.” (FALCONER; VILELA, 2001, p. 27).

> A legislação que regula o terceiro setor brasileiro – incluindo as organizações doadoras – pode ser descrita como uma colcha de retalhos de leis de distintas épocas, instituídas por motivações diferentes, regidas por lógicas diversas, em constante processo de alteração [...]. Essa realidade, porém, é compatível com a ausência, até um passado recente, de compreensão de que as organizações

> sem fins lucrativos comporiam um setor regido por princípios comuns. (FALCONER; VILELA, 2001, p. 35).

Exemplo do êxito no Terceiro Setor no Brasil está na multiplicação de Organizações não Governamentais (ONG), que prestam serviços sociais aos variados públicos de diversas áreas como educação, saúde, cultura e lazer, direitos civis, moradia, meio ambiente, desenvolvimento de pessoas, conflitos por terras, dentre outras áreas. Existem no terceiro setor várias nomenclaturas para definir as organizações inseridas neste âmbito social, como Organizações não Governamentais, Associações, Fundações, Institutos, etc.

6 METODOLOGIA

Na presente pesquisa pretende-se através da utilização de métodos qualitativos, avaliar a eficiência e eficácia de Arquitetura de Segurança da Informação em organizações do Terceiro Setor. A instituição na qual se desenvolveu esta pesquisa foi a Comissão Pastoral da Terra (CPT), organização atuante no terceiro setor, com sede da Secretaria Nacional na cidade de Goiânia e diversas Secretarias Setoriais em vários Estados Brasileiros.

A CPT é uma entidade do terceiro setor, nasceu em 1975, durante o Encontro de Pastoral da Amazônia, convocado pela Conferência Nacional dos Bispos do Brasil (CNBB), e realizado em Goiânia, Goiás (CANUTO, 2012).

O processo metodológico foi dividido em 3 passos, sendo:

1ª passo: elaborar conjunto de critérios, baseado nos requisitos apresentados pelas normas da ABNT ISO/IEC referentes à gestão da segurança da informação e na ampla revisão de literatura acerca dos assuntos “Segurança da informação” e “Arquitetura da Informação”;

2ª passo: aplicar a pesquisa, através de um roteiro de entrevista orientada, elaborada a partir do critérios definidos na etapa anterior, que consistiu em verificar através de perguntas fechadas e de múltipla escolha, feitas diretamente ao responsável pelo Centro de Documentação (CEDOC) da CPT;

3ª passo: analisar e apresentar os resultados obtidos através da realização da entrevista orientada, a fim de apresentar o resultado final da pesquisa.

Os critérios apresentam-se na forma de Grupos de Indicadores – **Gestão da Segurança da Informação; Gestão de Ativos; Sistema de Gestão da Segurança da Informação; Infraestrutura Tecnológica e Controle de Acessos** – onde cada um desses grupos consiste em uma dimensão de análise para verificação do nível de

eficiência e eficácia deste conjunto, visto como um sistema complexo de gestão da segurança da informação. Cada um destes 5 (cinco) Grupos de Indicadores subdivide-se em 3 (três) Indicadores, que são responsáveis por medir a situação específica de cada grupo, indicando o nível em que se encontra. Segundo Costa (2011, p. 03) “medir, ou mensurar, concerne antes de tudo a um esforço de compreensão sobre um objeto qualquer, desde que este objeto possua condições bem definidas de aplicação do procedimento de medição”.

Quadro 1 - Conjunto de Critérios para Avaliação de Arquitetura de Segurança da Informação.

GRUPOS	INDICADORES		
Gestão da Segurança da Informação	Análise/avaliação de riscos	Política de Segurança	Análise Crítica da Política de Segurança
Gestão de Ativos	Inventário dos ativos	Uso de Ativos	Classificação da Informação
Sistema de Gestão da Segurança da Informação	Implementação de Sistema de Gestão	Monitoramento e análise do Sistema de Gestão	Melhorias no Sistema de Gestão
Infraestrutura Tecnológica	Hardware para Tecnologias de Informação e Comunicação	Softwares para Gestão	Serviços de Rede
Controle de Acessos	Política de Controle de Acesso	Gerenciamento de acesso de usuários	Controle de Acesso à rede e a sistemas operacionais

Fonte: Os autores.

Para este conjunto de critérios de avaliação, foi construída uma escala de eficiência e eficácia com 5 (cinco) níveis de avaliação, sendo eles: **5-ideal; 4-Satisfatório; 3-aceitável; 2-Insuficiente e 1-crítico**. É importante frisar neste ponto o que de acordo com Costa (2011, p. 13) em uma escala de mensuração nós (1) não mensuramos o objeto, mas uma característica bem definida deste; para tanto (2) a característica deve ser claramente diferençável de outras características do objeto; e (3) deve possuir uma variação que indique o sentido da regra de atribuição definida.

7 RESULTADOS

Depois de realizada a verificação e pontuação das situações encontradas, foi realizada a apuração da situação geral e do nível de eficiência e eficácia requerido pela questão colocada de início – Qual o nível de eficiência e eficácia das Arquiteturas de Segurança da Informação na Comissão Pastoral da Terra? – através de média aritmética simples.

A média aritmética simples é obtida dividindo-se a soma dos valores encontrados em cada indicador dividido pelo número deles, no caso 3 indicadores para cada grupo. É um quociente, na maioria das vezes, representado pelo símbolo $\bar{x}$. Nesse caso, a média aritmética simples será determinada pela expressão:

Equação 1- Fórmula matemática da média aritmética simples.

$$\bar{x} = \frac{x_1 + x_2 + ... + x_n}{n} = \frac{1}{n}\sum_{i=1}^{n} x_i$$

Fonte: Crespo, 2009.

Para proceder à apresentação dos resultados, em cada um dos Grupos de Indicadores, os índices encontrados (números dos níveis) foram somados e divididos pelo número de indicadores do grupo, para esses casos será encontrado o nível de eficiência e eficácia daquele grupo de indicador especificamente.

Grupos = Soma dos Resultados dos Indicadores = **Resultado Final de cada grupo**
Nº de Indicadores

Tabela 1: Resultados por Indicadores.

GRUPOS	INDICADORES			TOTAL
Gestão da Segurança da Informação	Análise/avaliação de riscos	Política de Segurança	Análise Crítica da Política de Segurança	**2,67**
	4	2	2	
Gestão de Ativos;	Inventário dos ativos	Uso de Ativos	Classificação da Informação	**5**
	5	5	5	

Sistema de Gestão da Segurança da Informação	Implementação de Sistema de Gestão	Monitoramento e análise do Sistema de Gestão	Melhorias no Sistema de Gestão	**1,33**
	2	1	1	
Infraestrutura Tecnológica	Hardware para Tecnologias de Informação e Comunicação	Softwares para Gestão	Serviços de Rede	**3**
	5	2	2	
Controle de Acessos	Política de Controle de Acesso	Gerenciamento de acesso de usuários	Controle de Acesso à rede e a sistemas operacionais	**3**
	2	5	2	

Fonte: Os autores.

Após encontrado o nível para cada grupo indicador, aplicamos novamente a fórmula de média aritmética simples, somando assim os níveis dos grupos de indicadores e dividindo pelo número de grupos de indicadores. Este nível encontrado revelou, de acordo com a tabela de níveis, o nível de eficiência e eficácia das Arquiteturas de Segurança da Informação na Organização escolhida.

$$\mathbf{X} = \frac{\text{Soma dos resultados dos grupos}}{\text{N º de Grupos}} = \textbf{RESULTADO FINAL}$$

Tabela 1 - Resultados do Nível de Eficiência de Acordo com Cada Grupo Indicador.

GRUPOS	TOTAL
Gestão da Segurança da Informação	2,67
Gestão de Ativos;	5

Sistema de Gestão da Segurança da Informação	1,33
Infraestrutura Tecnológica	3
Controle de Acessos	3
RESULTADO FINAL	**3**

Fonte: Os autores.

Com a aplicação da fórmula de média aritmética simples, obtemos o resultado final para o nível de eficiência e eficácia das Arquiteturas de Segurança da Informação na Comissão pastoral da Terra, **3 (aceitável)** de acordo com a escala de nível do conjunto de critérios. Para Costa (2011, p. 07) a mensuração não precisa ser perfeita (o que seria um intento inalcançável), mas pode ser adequada para se alcançar resultados consistentes e dar soluções a problemas reais das organizações.

8 CONSIDERAÇÕES FINAIS

A segurança da informação é um procedimento, uma gestão necessária em todos os tipos de organização da economia mundial, afinal essa gestão efetiva é que permite eliminar ataques a sistemas computadorizados, evitando assim modificações e até perdas de informações relevantes à instituição geradora tanto em meio físico, quanto digital. Com o acelerado avanço da internet, ataques ficam cada vez mais sofisticados e isso se torna cada vez mais um risco à segurança de informações. Organizações não suportam o chamado colapso no fluxo de informações, pois este atrasaria os processos da mesma e, em caso de grandes perdas levar a organização até mesmo a falência. Informação na atualidade é moeda de troca, tem valor monetário tanto para as empresas geradoras, quanto para seus concorrentes. É um ativo de destaque na chamada corrida pela melhor posição no mercado, para garantir vantagens sobre os possíveis concorrentes e melhorias contínuas dos negócios.

Em se tratando de organizações do terceiro setor, a necessidade de gestão da segurança da informação torna-se clara ao observar-se que estas instituições lidam diariamente com informações importantes para seus usuários e para seus próprios processos financeiros, administrativos, de pessoal, etc. A fim de sanar este tipo de problema, indispensável seria pensar em formas sistematizadas de implementar políticas e procedimentos para contribuir efetivamente futuras melhorias no Sistema de Gestão da Segurança da Informação e pensar uma avaliação contínua dessa gestão nessas organizações e no que tange os objetivos desta análise.

Esta pesquisa possibilitou conhecer e entender melhor como são realizados os processos de segurança da informação, assim como perceber a importância deste processo dentro de instituições e empresas e, principalmente a importância de se aplicar estes métodos em organizações do terceiro setor, já que este setor não é muito estudado e na maioria das vezes é de difícil acesso.

REFERÊNCIAS

ALMEIDA, Maurício Barcellos; SOUZA, Renato Rocha; COELHO, Kátia Cardoso. Uma proposta de ontologia de domínio para segurança da informação em organizações: descrição do estágio terminológico. **Inf. & Soc.**: Est., João Pessoa, v.20, n.1, p. 155-168, jan./abr. 2010. Disponível em: <http://www.ies.ufpb.br/ojs2/index.php/ies/article/view/3753/3427>. Acesso em: 15 abr. 2012.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001**: 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 27003**: Tecnologia da informação: técnicas de segurança: diretrizes para implantação de um sistema de gestão da segurança da informação. Rio de Janeiro, 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005**: Tecnologia da informação: técnicas de segurança: gestão de riscos de segurança da informação. Rio de Janeiro, 2011.

BASTOS JUNIOR, Paulo Alberto; *et. al*. **Sistemas de inteligência empresarial aplicado às organizações do terceiro setor:** uma tentativa de modelagem. Out./2001. Disponível em: **<**http://www.abraic.org.br/V2/artigos_detalhe.asp?c=368>. Acesso em: 2 Maio 2012.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CAMARGO, Liriane Soares de Araújo de; VIDOTTI, Silvana Aparecida. Borseti Gregório. **Arquitetura da informação**: uma abordagem prática para o tratamento de conteúdo e interface em ambientes informacionais digitais. Rio de Janeiro: LTC, 2011. 231 p.

CANUTO, Antônio; LUZ, Cássia Regina da Silva; WICHINIESKI, Isolete (Org.). **Conflitos no campo Brasil 2011**. Goiâna: CPT Nacional Brasil, 2012. 182p.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações**. 2ª Ed. rev. e ampl. São Paulo: Editora SENAC São Paulo, 1999.

COMISSÃO PASTORAL DA TERRA. Disponível em: <http://www.cptnacional.org.br>. Acesso em: 27 Jan., 2013.

COSTA, Francisco José da. **Mensuração e desenvolvimento de escalas**: aplicações em administração. Rio de Janeiro: Editora Ciência Moderna Ltda., 2011. 386 p.

CRESPO, Antônio Arnot. **Estatística Fácil**. São Paulo: Saraiva, 2009.

DAVENPORT, T. H. **Ecologia da informação**: por que só a tecnologia não basta para o sucesso na era da informação. São Paulo: Futura, 1998.

EVERNDEN, R.; EVERNDEN, E. Third-generation information architecture. 2003. **Communications of the ACM**, v. 46, n. 3, p. 95-98. Disponível em: <http://portal.acm.org/ft_gateway.cfm?id=636777&type=pdf&coll=Portal&dl=GUIDE&CFID=70269974&CFTOKEN=97204999>. Acesso em: 28 fev. 2013.

FALCONER, A. P.; VILELA, R.. **Recursos privados para fins públicos**: as grantmakers brasileiras. São Paulo: Peirópolis, 2001.

FERREIRA, Marcelo Marchine; FERREIRA, Cristina Hillen Marchine. Terceiro setor: um conceito em construção, uma realidade em movimento. In: SEMANA DO CONTADOR DE MARINGÁ, 18, 2006, Maringá. **Anais**... Maringá: UEM, 2006.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva, 2006.

ICA-AtoM: **Open source archival description software**. Disponível em: <http://213.63.25.16:8800/icaatom-1.1/index.php/?sf_culture=pt>. Acesso em: 04 fev. 2013.

LANDIM, L. **Para além do mercado e do Estado?** Filantropia e cidadania no Brasil. Rio de Janeiro: ISER, 1993.

LIMA-MARQUES, Mamede; MACEDO, F. L. O. Arquitetura da informação: base para a gestão do conhecimento. In: TARAPANOFF, K. (Org.). **Inteligência, informação e conhecimento em corporações**. Brasília: IBICT, UNESCO, 2006.

MACEDO, F. L. O. **Arquitetura da informação**: aspectos epistemológicos, científicos e práticos. Brasília, 2005. 186 p. Dissertação (Mestrado em Ciência da Informação). Universidade de Brasília.

MACGEE, James; PRUSAK, Laurence. **Gerenciamento estratégico da informação:** aumente a competitividade e eficiência de sua empresa utilizando a informação como uma ferramenta estratégica. Rio de Janeiro: Elsevier, 1994.

MARCIANO, João Luiz ; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. **Ci. Inf.**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. Disponível em: <http://revista.ibict.br/cienciadainformacao/index.php/ciinf/article/view/805/647>. Acesso em: 13 abr. 2012.

MONTAÑO, Carlos. **Terceiro setor e questão social**: crítica ao padrão emergente de intervenção social. São Paulo: Cortez, 2002.

MORVILLE, Peter; ROSENFELD, Louis. **Information architecture for the world wide web**. 3ed. Sebastopol: O'Reilly, 2006.

SIQUEIRA, A. **A lógica e a linguagem como fundamentos da arquitetura da informação**. Brasília, 2008. 143 p. Dissertação (Mestrado em Ciência da Informação e Documentação). Universidade de Brasília. Disponível em: <http://bdtd.bce.br/tedesimplificado/tde_busca/arquivo.php?codArquivo=3180>. Acesso em: 13 jan. 2013.

SZAZI, Eduardo. **Terceiro setor**: regulação no Brasil. 4. ed, rev. e ampl. São Paulo: Peirópolis, 2006.

TEODÓSIO, Armindo. dos S. de S. **O Terceiro setor como utopia modernizadora da provisão de serviços sociais**: dilemas, armadilhas e perspectivas no cenário brasileiro. 2002. 120 f. Dissertação (mestrado) – Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2002.

VOLTOLINI, Ricardo (Org.). **Terceiro setor**: planejamento e gestão. 2. ed. São Paulo: Editora Senac São Paulo, 2004.

ZAPATER, Marcio; SUZUKI, Rodrigo. Segurança da informação um diferencial determinante na competitividade das corporações. **Promon Business & Technology Review**, 2009.