UNIVERSIDADE FEDERAL DE GOIÁS
FACULDADE DE COMUNICAÇÃO E BIBLIOTECONOMIA
CURSO DE BIBLIOTECONOMIA

CARMINDA DE AGUIAR PEREIRA

AVALIAÇÃO DAS ARQUITETURAS DE SEGURANÇA DA INFORMAÇÃO NO TERCEIRO SETOR: APLICAÇÃO PILOTO NA COMISSÃO PASTORAL DA TERRA

GOIÂNIA
2012

CARMINDA DE AGUIAR PEREIRA

AVALIAÇÃO DAS ARQUITETURAS DE SEGURANÇA DA INFORMAÇÃO NO TERCEIRO SETOR: APLICAÇÃO PILOTO NA COMISSÃO PASTORAL DA TERRA

Monografia apresentada ao Curso de Biblioteconomia da Faculdade de Comunicação e Biblioteconomia da Universidade Federal de Goiás, como requisito parcial à obtenção do título de Bacharel em Biblioteconomia.

Orientador: Prof. Me. Arnaldo Alves Ferreira Júnior.

GOIÂNIA

2012

Dados Internacionais de Catalogação na Publicação (CIP)
GPT/BC/UFG

Pereira, Carminda de Aguiar
P436a Avaliação das arquiteturas de segurança da informação no terceiro setor [manuscrito] : aplicação piloto na Comissão Pastoral da Terra / Carminda de Aguiar Pereira. - 2012.
86 f.

Orientador: Prof. Me. Arnaldo Alves Ferreira Júnior.
Monografia (Graduação) – Universidade Federal de Goiás, Faculdade de Comunicação e Biblioteconomia, 2012.

1. Segurança da Informação – Normas. 2. Arquitetura da Informação. 3. Terceiro Setor. 4. Normas ABNT ISO/IEC. I.
Título

CDU: 004.056(083.74)

UNIVERSIDADE FEDERAL DE GOIÁS
FACULDADE DE COMUNICAÇÃO E BIBLIOTECONOMIA
CURSO DE BIBLIOTECONOMIA

CARMINDA DE AGUIAR PEREIRA

AVALIAÇÃO DAS ARQUITETURAS DE SEGURANÇA DA INFORMAÇÃO NO TERCEIRO SETOR: APLICAÇÃO PILOTO NA COMISSÃO PASTORAL DA TERRA

Monografia apresentada junto ao Curso de Biblioteconomia da Faculdade de Comunicação e Biblioteconomia da Universidade Federal de Goiás, como requisito parcial à obtenção do título de Bacharel em Biblioteconomia. Aprovada em ____/____/____ pela banca examinadora composta pelos profissionais:

_____
Professor Me. Arnaldo Alves Ferreira Júnior - FACOMB/UFG
Orientador

_____
Professora Dr.ª Eliany Alvarenga de Araújo - FACOMB/UFG
Examinadora

_____
Professora Dr.ª Maria de Fátima Garbelini - FACOMB/UFG
Examinadora

AGRADECIMENTOS

Agradeço primeiramente a Deus, por me dar paciência e sabedoria na elaboração deste trabalho.

Aos meus pais por todo amor e dedicação, à minha mãe em especial por não me deixar desistir do curso no segundo período.

A toda minha família, pelo apoio e carinho.

Ao meu orientador Prof. Me. Arnaldo Alves Ferreira Júnior, por ter me orientado durante este último ano de graduação, pelas dicas e por aceitar minha sugestão de tema.

Aos meus companheiros de graduação.

Aos professores que tive oportunidade de conviver.

Aos meus amigos de perto e aos de longe que sempre comemoram comigo minhas vitórias.

A equipe da Comissão Pastoral da Terra (CPT), por colaborar na aplicação desta pesquisa, principalmente a Cássia e a Jeane.

As professoras Eliany Alvarenga de Araújo e Maria de Fátima Garbelini, por aceitarem participar da minha banca avaliadora.

MUITO OBRIGADA A TODOS!

"O maior risco é crer que não há riscos"
Caruso & Steffen

"A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos"
John Naisbitt

RESUMO

Esta pesquisa tem como principal objetivo verificar o nível de eficiência e eficácia dos procedimentos de Gestão da Segurança da Informação, a partir dos requisitos apresentados pelas Normas de Gestão da Segurança da Informação ABNT NBR ISO/IEC em organizações do Terceiro Setor em Goiânia. Para verificar este nível de eficiência e eficácia, 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 modelo de Avaliação das Arquiteturas 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 do terceiro setor avaliada pelo modelo foi a Comissão Pastoral da Terra (CPT), entidade atuante no Terceiro Setor em Goiânia. Consiste em uma pesquisa exploratória de caráter descritivo e dimensão qualitativa. Os dados obtidos mediante aplicação de entrevista orientada a CPT foram apresentados em formato de relatório, que contem informações básicas da organização, assim como a época em que ocorreu a aplicação da pesquisa, contratempos ocorridos e avaliação crítica dos dados. Para alcançar o resultado final, que consiste em desvendar o atual nível de eficiência e eficácia das Arquiteturas de Segurança da Informação na organização, foi aplicado aos resultados fórmula de média aritmética simples. Foi elucidada a importância deste tipo de pesquisa no terceiro setor, assim como em outras áreas da economia no país, e a necessidade de futuras modificações e melhorias para validação do modelo de avaliação como instrumento de avaliação efetivo de procedimentos de Gestão da Segurança da Informação.

Palavras-Chave: Segurança da Informação. Arquitetura da Informação. Terceiro Setor. Modelo de Avaliação. Normas ABNT ISO/IEC.

ABSTRACT

This research has as its main purpose verifying the level of efficiency and effectiveness of the Management of Information Security procedures as from the requirements presented by the Guidelines for the Management of Information Security ABNT NBR ISO/IEC in Third Sector organizations in Goiânia. To verify this level of efficiency and effectiveness, it was produced a study about the standards of Management of Information Security formulated by ABNT NBR ISO/IEC 27001:2006; 27002:2005; 27003:2011 e 27005:2011 and elaborated from this study an Evaluation of Information Security Architectures model. It has been worked on theoretical issues as such Information Security; ABNT standards on Management of Information Security; Information Architecture and Third Sector. The Third Sector organization evalueted by the model was the Comissão Pastoral da Terra (CPT), entity of the Third Sector in Goiânia. Consists in exploratory research based on descriptive and qualitative aspects. The data obtained by applying the oriented interview with CPT were presented in a report format, which contains basic information about the organization, the period in what the research was applied, misadventures that has occured and critical evaluation of the data. To achive the main purpose, that consists in unviel the current level of efficiency and effectiveness of the Architectures of Information Security in the organization, it was applied on the results formula of simple arithmetic. It was elucidated the importance of this kind of research on the Third Sector as well as in others economy sectors of the nation, and the need to of future modifications and improvements to the validation of evaluation model as an instrument to effective evaluation of Security Management information procedures.

Keywords: Information Security; Information Architecture; Third Sector; Evaluation Model; Standards ISO/IEC.

LISTA DE ABREVIATURAS E SIGLAS

AI	Arquitetura da Informação
ABNT	Associação Brasileira de Normas Técnicas
CEDOC	Centro de Documentação
CERT.br	Centro de Estudos, Resposta e Tratamento de incidentes de Segurança no Brasil
CNBB	Conferência Nacional dos Bispos do Brasil
COBIT	*Control Objectives for Information and Related Technology*
CPT	Comissão Pastoral da Terra
IEC	*International Electrotechnical Commission*
IECLB	Igreja Evangélica da Confissão Luterana no Brasil
ISACF	*Information System Audit and Control Foundation*
ISO	*International Organization for standartization*
ITIL	*Information Technology Infrastructure Library*
OECD	*Organization for Economic Cooperation and Development*
OSC	Organização da Sociedade Civil
OSCIP	Organização da Sociedade Civil de Interesse Público
OSFL	Organização sem fins lucrativos
ONG	Organização não Governamental
ONU	Organização das Nações Unidas
PDCA	*Plan-Do-Check-Act*
SI	Segurança da Informação
SGSI	Sistema de Gestão da Segurança da Informação
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação

SUMÁRIO

1 INTRODUÇÃO

Garantir a recuperação da informação de forma eficaz e segura, independente do suporte em que esteja representada, depende de seu tratamento, organização e armazenamento. Atualmente, a maioria das organizações são dependentes das tecnologias de informação e comunicação (TIC). De acordo com Caruso e Steffen (1999, p. 22) esta dependência agrava-se muito em função da tecnologia de informática, que permite acumular e recuperar grandes quantidades de informações em espaços restritos (computadores). O meio de registro passa a ser ao mesmo tempo, meio de armazenamento, de acesso, de divulgação e recuperação destas informações.

Se o espaço físico é premissa básica para que haja efetivamente a segurança na guarda e recuperação de documentos gerados pela organização, e se esta por sua vez armazena cópias digitalizadas destes documentos em computadores e não delimita políticas/procedimentos que definem uma gestão da segurança da informação eficaz. Os danos causados por uma invasão a um servidor pode ser tal quais ou maiores do que se ter acesso a um arquivo da organização em papel, levando à perda de informações importantes, o que poderia trazer prejuízos à organização e aos seus colaboradores. O mesmo aconteceria se não houver a gestão da segurança das informações em meio físico, seria como guardar os documentos em um arquivo e deixar a janela aberta durante uma noite de temporal, de manhã estariam molhados e danificados documentos que poderiam não ter cópias armazenadas para recuperação em nenhum outro tipo de suporte (como por exemplo, cópias em computadores).

Segundo Zapater e Suzuki (2005) na medida em que as tecnologias avançam, as fronteiras da segurança se expandem continuamente. O universo das novas tecnologias evolui de forma rápida e imprevisível. Essa contínua evolução coloca as organizações em uma posição desconfortável no que diz respeito à Gestão da Segurança da Informação, levando-as a tentar estabelecer controle sobre um alvo que age e se modifica continuamente e de formas às vezes invisível (como é o caso de ataques aos sistemas da organização realizados por *hackers* e *crackers*[1], a fim de prejudicar os negócios da mesma). Muitas das novas TIC à disposição dos usuários, quando utilizadas com os controles de segurança apropriados, são benéficas como ferramenta de apoio aos negócios. Entretanto, quando funcionários incorporam essas tecnologias

[1] Hacker e cracker são pessoas que tentam acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. **Fonte:** ABNT NBR ISO/IEC 27002: 2005.

arbitrariamente (utilizando-as para outros fins, que não os instituídos pela organização) em seu ambiente de trabalho, podem trazer ameaças desconhecidas à organização, ameaças estas que devem ser evitadas, a fim de salvaguardar informações importantes e valiosas.

Em se tratando de segurança de informações em organizações do Terceiro Setor, organizações estas que emergem no Brasil nos anos 1990, de natureza privada e finalidade pública, portanto sem fins lucrativos, segundo Voltolini (2004, p. 07) "essas organizações não podem perder de vista a dimensão do humano e a dimensão sociocultural, mas tem que ser administradas com métodos atuais." Pensando na administração destas organizações por meio de métodos atuais é indispensável, que haja uma prática eficiente e eficaz de gestão da segurança da informação, focando na segurança tanto física, quanto lógica de informações produzidas por estas organizações, para que seja possível recuperá-las de forma efetiva no futuro.

Entende-se por eficiência a obtenção de resultados através da ênfase nos meios, da resolução dos problemas existentes e da salvaguarda dos recursos disponíveis com o cumprimento das tarefas e obrigações dentro da organização. Significa realizar de forma correta as tarefas diárias, administrar os custos, reduzir as perdas e os problemas na organização. Sendo que pode haver mais, ou menos eficiência nos processos da organização, dependendo de sua administração. Já a eficácia é a obtenção de resultados através da ênfase nos próprios resultados e nos objetivos a serem alcançados, com a exploração máxima do potencial dos processos. Significa a otimização das tarefas com a agilização de recursos para alcançar o resultado esperado. Sendo que pode haver ou não eficácia nos resultados alcançados pela organização. Segundo Chiavenato (2003, p. 155) "cada organização deve ser considerada sob o ponto de vista de eficiência e de eficácia, simultaneamente. Eficácia é uma medida do alcance de resultados, enquanto a eficiência é uma medida da utilização dos recursos nesse processo".

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[2] 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

[2] 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.

segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação".

Diante dos fatos elucidados acima, a presente pesquisa se pautará nos requisitos das Normas de Qualidade criadas em conjunto pela Associação Brasileira de Normas Técnicas (ABNT), *International Organization for Standardization* (ISO) e *International Electrotechnical Commission* (IEC) relativas à Gestão da Segurança da Informação, a fim de verificar o nível de eficiência e eficácia dos procedimentos de Segurança da Informação em Organizações do Terceiro Setor. Para proceder a tal avaliação, será elaborado a partir de um estudo das normas, um "Modelo de Avaliação das Arquiteturas de Segurança da Informação", que permitirá avaliar a atual situação da gestão da segurança da informação nas organizações do terceiro setor.

Para proceder à aplicação piloto do modelo elaborado de Avaliação das Arquiteturas de Segurança da Informação, foi selecionada uma organização atuante no terceiro setor, a Comissão Pastoral da Terra[3] (CPT) que possui sede nacional na capital Goiânia. O trabalho da CPT fundada em 1975, em plena ditadura militar, como resposta à grave situação dos trabalhadores rurais, posseiros e peões, sobretudo na Amazônia, abrange todo o território nacional e é realizado de forma autônoma, é uma pastoral com vínculos diretos a Conferência Nacional dos Bispos do Brasil (CNBB).

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

2 JUSTIFICATIVA

Relativo à segurança da informação em organizações do Terceiro Setor é importante ressaltar que muitas organizações não sobrevivem mais que poucos dias a um colapso do fluxo de informações. Não importando seu meio de armazenamento, este colapso deixaria os processos da organização vulneráveis. No que diz respeito à segurança da informação, haveria perdas significativas de informações, pois são necessárias para o funcionamento contínuo dos setores da organização, portanto medidas preventivas para evitar estes colapsos tornam-se necessárias. A atual dependência das organizações em relação à informática está se estendendo por toda a economia, tornando-as aos poucos altamente dependentes das TIC e dos computadores e, consequentemente, de acordo com Caruso e Steffen (1999, p. 23) casa vez mais "sensíveis aos riscos representados pelo eventual colapso do fluxo de informações de controle gerencial" causado por esta dependência.

Os segmentos que constituem o Terceiro Setor são as formas tradicionais de auxílio mútuo, os movimentos sociais e ações civis, a filantropia empresarial e as organizações não governamentais. Sendo todas organizações estruturadas, localizadas fora do aparato formal do Estado, não destinadas a distribuir lucros auferidos com suas atividades entre os seus diretores ou entre um conjunto de acionistas e autogovernadas, que envolvem indivíduos num significativo esforço voluntário. (MIRANDA, 2009, p. 05).

Estas organizações do Terceiro Setor, por serem voltadas a prestação de serviços sociais, devem 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 organização que as geram e utilizam. Essas informações podem ser tanto de caráter sigiloso ou relacionadas com atividades diárias da organização, que no caso das organizações do terceiro setor tornam-se indispensáveis. Sendo assim é necessário dar importância aos processos de gestão da segurança da informação, e que essa seja gerida de forma consistente e eficiente pelos gestores das organizações e que haja uma avaliação periódica destes processos, visando melhorias, modificações e reparos nesta gestão.

3 PROBLEMATIZAÇÃO

Qual a atual situação das 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?

4 OBJETIVOS

4.1 OBJETIVO GERAL

Verificar o nível de eficiência e eficácia dos procedimentos de Gestão da Segurança da Informação, a partir dos requisitos apresentados pelas Normas da ABNT NBR ISO/IEC na Comissão Pastoral da Terra.

4.2 OJETIVOS ESPECÍFICOS

a) Realizar 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 do Modelo de Avaliação das Arquiteturas de Segurança da Informação;

b) Elaborar um Modelo de Avaliação das Arquiteturas de Segurança da Informação, a partir dos requisitos apresentados pelas normas ABNT NBR ISO/IEC 27001:2006; 27002:2005; 27003:2011 e 27005:2011.

5 FUNDAMENTAÇÃO TEÓRICA

5.1 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 a 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 informação 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, 1994, 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[4] 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.). Existem vários tipos de ativos, incluindo segundo ABNT (2005, p. 21):

- **Ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informação sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
- **Ativos de *software***: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

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

- **Ativos físicos**: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos tecnológicos;
- **Serviços**: serviços de computação e comunicações, utilidades gerais, como por exemplo, aquecimento, iluminação, eletricidade e refrigeração;
- **Pessoas** e suas qualificações, habilidades e experiências;
- **Intangíveis**, tais como a reputação e a imagem da organização.

Enquanto na área de informática os ativos de informação estão armazenados, em sua maior parte, em meios magnéticos, nas áreas fora desse ambiente eles estão representados ainda em grande parte no formato impresso (papel), sendo muito mais tangíveis e de entendimento mais fácil por parte dos seres humanos. (CARUSO; STEFFEN, 1999, p. 23). A informação existe de diversas formas, impressa, armazenada eletronicamente, transmitida por correio ou por meios eletrônicos, apresentada em filmes, imagens ou falada em conversas. Seja qual for a forma apresentada ou meio ao qual é armazenada e compartilhada é recomendado sua proteção de forma adequada.

Esse é o um dos motivos que, segundo Marciano e Lima-Marques (2006, p. 90) é importante propor-se uma análise da segurança da informação organizacional, pois a informação é "gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é eminentemente um processo grupal, seja ela interna ou externa às fronteiras da organização."

Para Caruso e Steffen (1999, p. 23) outro motivo importante para propor uma análise da SI é a atual dependência das organizações em relação à Tecnologia de informação e Comunicação (TIC), a internet e a informática. Esta dependência se estende cada vez mais por toda a economia, tornando aos poucos todas as organizações altamente dependentes dos computadores e, consequentemente, casa vez mais sensíveis aos riscos representados por esses equipamentos. Foi após a criação dos equipamentos de processamento de informações nos anos 1990, notadamente após os modernos computadores eletrônicos, que a concentração em um único lugar e o grande volume de informações passou a ser um problema considerado sério para a segurança. A recuperação deste grande volume de informações gera um caos dentro das organizações se não tratadas adequadamente, "os riscos agravaram-se após o aparecimento dos microcomputadores, redes e internet e a disseminação da cultura de informática em segmentos expressivos da sociedade." (CARUSO; STEFFEN, 1999, p. 35). Pemble (2004, tradução nossa) define três esferas aonde a segurança da informação deve ser compreendida:

- **A Esfera Operacional**, voltada ao impacto que os incidentes podem gerar à capacidade da organização de sustentar os processos do negócio;
- **A Esfera da Reputação**, voltada ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário;
- **A Esfera Financeira**, voltada aos custos em que se incorre na eventualidade de algum incidente.

Fontes (2006) alerta para o constante crescimento de incidentes de SI, principalmente no Brasil e no que tange aos acessos a *internet*. De forma crescente, as organizações estão potencialmente mais expostas a novas formas de ataques, independentemente do porte ou do tipo de negócio.

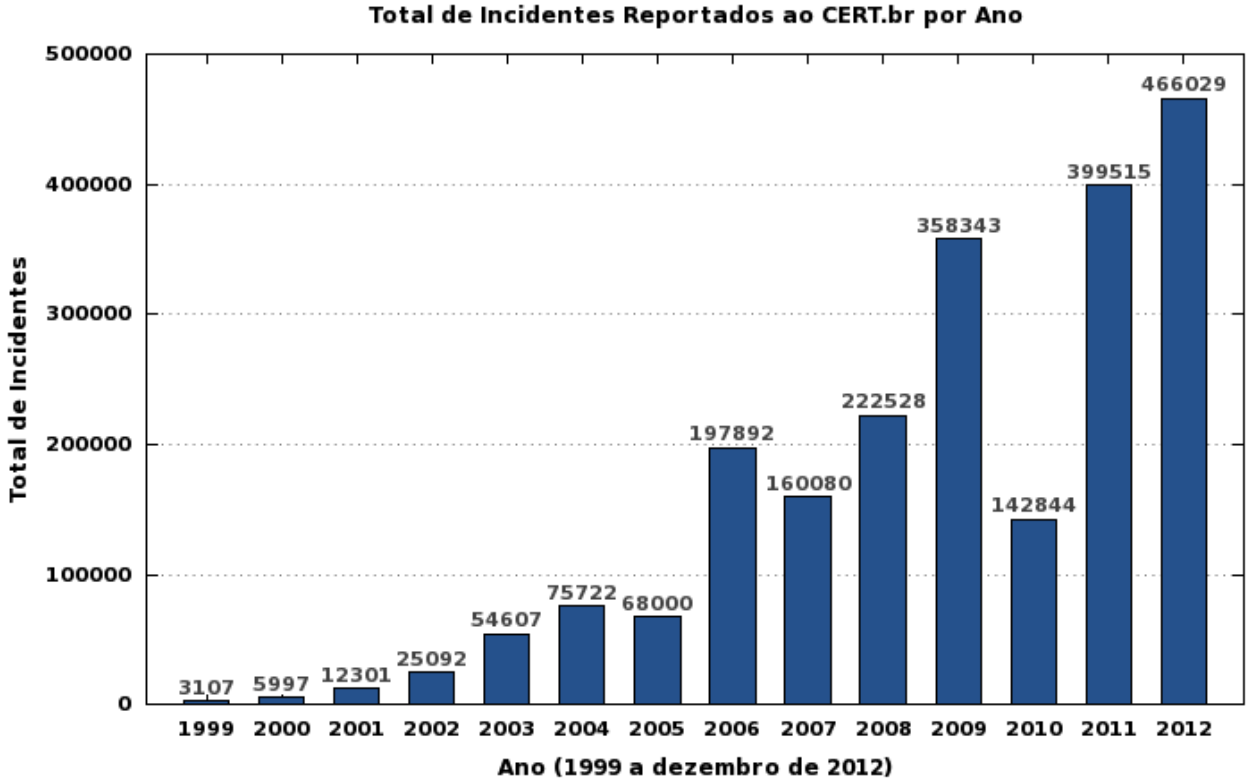
No artigo de 31 de janeiro de 2013 da revista digital *ComputerWorld*[5] diz que o ano de 2012 foi recorde em ameaças virtuais, afirma relatório da RSA[6], divisão de segurança da EMC[7]. O "Relatório de Fraudes" de dezembro de 2012 aponta crescimento de 59% no total de ataques de *phishing*[8] no mundo em comparação com o ano anterior. Segundo o levantamento, esses tipos de fraude eletrônica, caracterizada pela tentativa de adquirir informações sigilosas por meio da *web*, causou prejuízo de 1,5 bilhão de dólares para a economia mundial, expansão de 22%. O Brasil registrou 5% do volume total de ataques. O País está em 4º lugar entre os principais países hospedeiros de *phishers*, com 4% dos ataques hospedados, indica o estudo. Para 2013, a RSA prevê que os ataques vão continuar a crescer.

Na atualidade, ataques a informações confidenciais e privadas são cada vez mais comuns, em que, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação. Fraudes digitais; furtos de senhas; cavalos de Tróia (códigos de programas aparentemente inofensivos, mas que guardam instruções danosas ao usuário, ao *software* ou ao equipamento); vírus de diversas naturezas e outras formas de ameaças têm se multiplicado vertiginosamente. Para Marciano e Lima-Marques (2006, p. 93) em resposta a estas hostilidades, a "segurança da informação, em seu sentido mais abrangente, envolve requisitos voltados à

[5] ComputerWorld. Disponível em: <http://computerworld.uol.com.br/seguranca/2013/01/30/ataques-de-phishing-causam-prejuizo-de-us-1-5-bilhao-em-2012/>. Acesso em: 28 fev. 2013.
[6] RSA Data Security, Inc. Divisão de Segurança da EMC. Disponível em: <http://www.emc.com/domains/rsa/index.htm>. Acesso em: 28 fev. 2013.
[7] Empresa multinacional norte-americana que fornece sistemas para infraestrutura de informação, *software* e serviços. Disponível em: <http://brazil.emc.com/index.htm>. Acesso em: 28 fev. 2013.
[8] O conjunto de técnicas empregadas para roubar a Identidade Eletrônica de um indivíduo, permitindo o acesso a áreas ou serviços privados em benefício próprio constitui delito de fraude. Disponível em: <http://www.internetsegura.org/nsegura/phising.asp>. Acesso em: 28 fev. 2013.

garantia de origem, uso e trânsito da informação, buscando certificar todas as etapas do seu ciclo de vida".

O gráfico abaixo mostra o total de incidentes de Segurança da Informação em organizações, reportados entre os anos de 1999 a 2012. Pesquisa esta realizada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[9] (CERT.br).



Levando em consideração estes dados mostrados acima, 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, depende 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

[9] CERT.br. Disponível em: <http://www.cert.br/>. Acesso em: 28 fev. 2013.

> 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., torna-se necessário 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). Para Marciano e Lima-Marques (2006, p. 89) "as políticas de segurança da informação são, via de regra, apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem adequar-se integralmente".

Uma política de segurança deve contemplar os aspectos de classificação de ativos de informações quanto a 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 esses ativos. (BRASIL, 2007, p. 26).

A criação destas políticas de segurança da informação não deve ficar restrita aos profissionais da área de informática, mas sim ligada a outros setores dentro da organização. Segundo o documento do Tribunal de Contas da União (BRASIL, 2007, p. 27) alguns tópicos devem ser levados em consideração na hora da elaboração da Política de Segurança da Informação, são eles:

- Definição de Segurança de Informações e de sua importância como mecanismo que possibilita o compartilhamento de informações;
- Declaração do comprometimento da alta administração com a política de segurança da informação, apoiando suas metas e princípios; objetivos de segurança da organização;

- Definição de responsabilidades gerais na gestão de segurança de informações;
- Orientações sobre análise e gerência de riscos; princípios de conformidade dos sistemas computacionais com a política de segurança da informação;
- Padrões mínimos de qualidade que esses sistemas devem possuir;
- Políticas de controle de acesso a recursos e sistemas computacionais;
- Classificação das informações (de uso irrestrito, interno, confidencial, secretas, etc.);
- Procedimentos de prevenção e detecção de vírus;
- Princípios legais que devem ser observados quanto à tecnologia da informação (direitos de propriedade de produção intelectual, direitos sobre *software*, normas legais correlatas aos sistemas desenvolvidos, cláusulas contratuais);
- Princípios de supervisão constante das tentativas de violação da segurança de informações;
- Consequências de violações de normas estabelecidas na política de segurança;
- Princípios de gestão da continuidade do negócio;
- Plano de treinamento em segurança de informações.

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 à aplicação das seguintes etapas, **a) Desenvolvimento de políticas**, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas; **b) Papeis 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 a 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 um negócio se não for dada a devida atenção à segurança da informação na organização.

5.2 AS NORMAS

A Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização. As Normas Brasileiras, cujo conteúdo é de responsabilidade dos Comitês Brasileiros (ABNT/CB), dos Organismos de Normalização Setorial (ABNT/ONS) e das Comissões de Estudos Especiais Temporárias (ABNT/CEET), são elaboradas por Comissões de Estudo (CE), formadas por representantes dos setores envolvidos, deles fazendo parte: produtores, consumidores e neutros (universidades, laboratórios e outros).[10]

5.2.1 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** compreende a ABNT NBR ISO/IEC 17799:2005 (versão corrigida de 02.07.2007) e a Errata 2 de 10.09.2007. Seu conteúdo é idêntico ao da ABNT NBR ISO/IEC 17799:2005 (versão corrigida de 02.07.2007). A Errata 2:2007 altera o número de referência da norma de 17799 para 27002. [11]

Esta norma foi elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela comissão de Estudo de Segurança Física em Instalações de Informática, esta norma equivale à ISO/IEC 17799:2005 e faz parte da família de normas de Sistema de Gestão de Segurança da Informação (SGSI). Ela visa estabelecer um código de prática para a gestão da segurança da informação.

Seu objetivo é 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.

Esta norma compreende os seguintes tópicos que visam contribuir para uma melhor prática de gestão da segurança da informação:

---

[10] Prefácio Nacional da Associação Brasileira de Normas Técnicas (ABNT).
[11] Nota da ABNT NBR ISO/IEC 27002:2005.

- **Análise/avaliação e tratamento de riscos de segurança da informação:** convém que as análises/avaliações de riscos identifiquem, qualifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Convém que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos. O processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos. (ABNT, 2005, p. 06).
- **Política de segurança da informação:** seu objetivo é prover uma orientação e apoio a direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes. Convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização. (ABNT, 2005, p. 08).
- **Organizando a Segurança da Informação:** seu objetivo é gerenciar a segurança da informação dentro da organização. Convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização e que a direção aprove a política de segurança da informação, atribua as funções da segurança e coordene e analise criticamente a implementação da segurança da informação por toda a organização. (ABNT, 2005, p. 10).
- **Gestão de Ativos:** seu objetivo é alcançar e manter a proteção adequada dos ativos da organização. Convém que todos os ativos sejam inventariados e tenham um proprietário responsável e que esses proprietários dos ativos sejam identificados e a eles seja atribuída a responsabilidade pela manutenção apropriada dos controles. A implementação de controles específicos pode ser delegada pelo proprietário, conforme apropriado, porém o proprietário permanece responsável pela proteção adequada dos ativos. (ABNT, 2005, p. 21).
- **Segurança em Recursos Humanos:** seu objetivo é assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mau uso de recursos. Convém que as responsabilidades pela segurança da informação sejam atribuídas antes

da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação e que todos os candidatos ao emprego, fornecedores e terceiros sejam adequadamente analisados, especialmente em cargos com acesso a informações sensíveis, sendo necessário que todos os usuários dos recursos de processamento da informação, assinem acordos sobre seus papéis e responsabilidades pela segurança da informação. (ABNT, 2005, p. 25).

- **Segurança Física e do Ambiente:** seu objetivo é prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização. Convém que as instalações de processamento da informação críticas ou sensíveis sejam mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados e que sejam fisicamente protegidas contra o acesso não autorizado, danos e interferências. A proteção oferecida tem que ser compatível com os riscos identificados. (ABNT, 2005, p. 32).
- **Gerenciamento das Operações e Comunicações:** seu objetivo é garantir a operação segura e correta dos recursos de processamento da informação. Convém que os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações sejam definidos. Isto abrange o desenvolvimento de procedimentos operacionais apropriados. É necessário que seja utilizada a segregação de funções quando apropriado, para reduzir o risco de mau uso ou uso doloso dos sistemas. (ABNT, 2005, p. 40).
- **Controle de Acessos:** seu objetivo é controlar o acesso à informação. Convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação. É necessário que as regras de controle de acesso levem em consideração as políticas para autorização e disseminação da informação. (ABNT, 2005, p. 65).
- **Aquisição, desenvolvimento e manutenção de sistemas de informação:** seu objetivo é garantir que segurança é parte integrante de sistemas de informação. Sistemas de informação incluem sistemas operacionais, infraestrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário. O projeto e a implementação de sistemas de informação destinados a apoiar o processo de negócios podem ser cruciais para a segurança. Convém que os requisitos de segurança sejam identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação. Todos os requisitos de segurança tem que

ser identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios para um sistema de informações. (ABNT, 2005, p. 84).

- **Gestão de incidentes de segurança da informação:** seu objetivo é assegurar que fragilidade e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil. Convém que sejam estabelecidos procedimentos formais de registro e escalonamento e que todos os funcionários, fornecedores e terceiros estejam conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança dos ativos da organização. Convém que seja requerido que os eventos de segurança da informação e fragilidades sejam notificados, tão logo quanto possível, ao ponto de contato designado. (ABNT, 2005, p. 98).
- **Gestão da continuidade do negócio:** seu objetivo é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso. Convém que o processo de gestão da continuidade do negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação. Convém que este processo identifique os processos críticos e integre a gestão de segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativos a tais aspectos como operações, funcionários, materiais, transporte e instalações. Ainda convém que a gestão da continuidade do negócio inclua controles para identificar e reduzir riscos, em complementação ao processo de análise/avaliação de riscos global, limite as consequências aos danos do incidente e garanta que as informações requeridas para os processos do negócio estejam prontamente disponíveis. (ABNT, 2005, p. 103).
- **Conformidade:** seu objetivo é evitar violações de quaisquer obrigações legais, estatuárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação. O projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatuários. (ABNT, 2005, p. 108).

Estes são os principais tópicos apresentados pela norma para que haja uma prática eficaz e eficiente de Gestão da Segurança da Informação nas organizações, todos estes tópicos seguidos de subtópicos explicativos compõem o código de prática para a gestão da segurança da informação.

5.2.2 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 elaborada no Comitê Brasileiro de Computadores e Processamento de Dados, pela Comissão de Estudo de Segurança Física em Instalações de Informática. Esta norma é uma tradução idêntica da ISO/IEC 27001:2005, que foi elaborada pelo *Join Technical Committee Information Technology, subcommittee IT Security Tecchniques*.

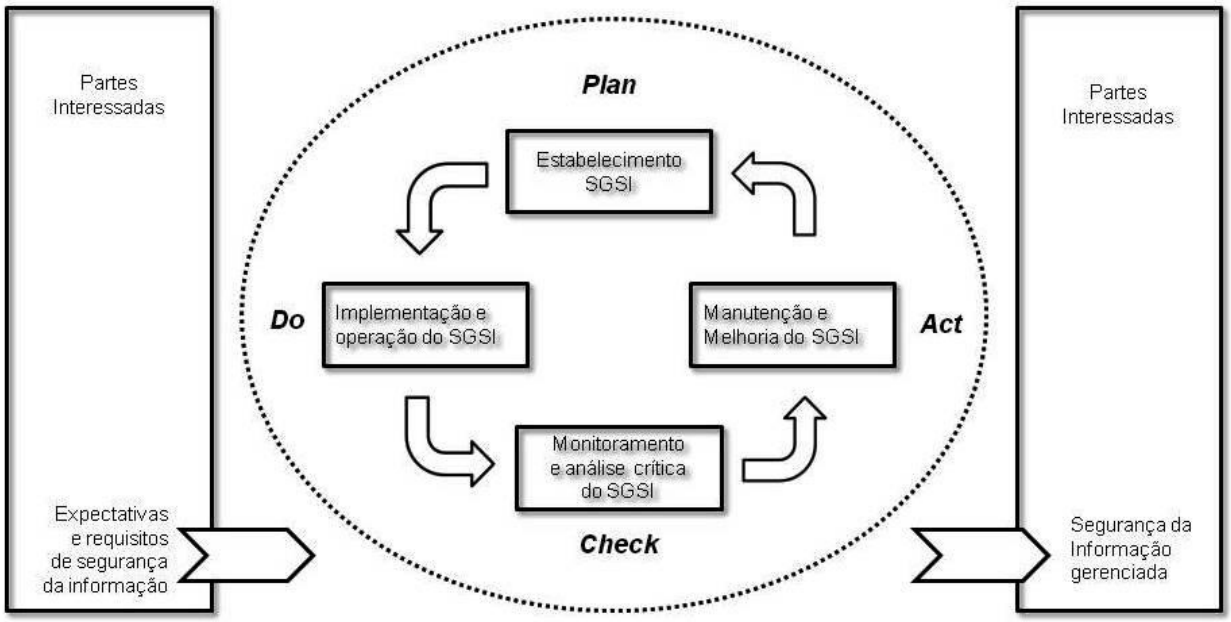
Esta norma foi preparada para prover um modelo de modo a estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão da Segurança da Informação (SGSI). Esta norma pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas. Ela adota o modelo conhecido como "*Plan-Do-Check-Act*" (PDCA), que é aplicado para estruturar todos os processos do SGSI.

***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 à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.

***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 continua do SGSI.



Fonte: Modelo PDCA aplicado aos processos do SGSI apresentado pela ABNT NBR ISO/IEC 27001:2006.

A adoção do modelo PDCA também refletirá os princípios como definidos nas diretrizes da *Organization for Economic Cooperation and Development* (OECD)[12] para governar a segurança de sistemas de informação e redes. Esta norma provê um modelo robusto para implementar os princípios nessas diretrizes para direcionar a análise/avaliação de riscos, especificações e implementação de segurança, gerenciamento de segurança e reavaliação.

O objetivo desta norma é cobrir todos os tipos de organizações (empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, etc.), ela especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização, especifica ainda requisitos para implementação de controles de segurança personalizados para as necessidades individuais de organizações e suas partes. (ABNT, 2006, p. 01).

Esta norma compreende os seguintes tópicos que visam estabelecer requisitos para os Sistemas de gestão da Segurança da Informação:

- **Sistema de gestão de segurança da informação**: Define que a organização deve estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto das atividades de negócio globais da

[12] Diretrizes da OECD para a Segurança de Sistemas de Informação e Redes – Para uma Cultura de Segurança. Paris: OECD, jul. 2002. Disponível em: <http://www.oecd.org.>.

organização e os riscos que ela enfrenta. Este processo está baseado no modelo PDCA. (ABNT, 2006, p. 04).

- **Responsabilidades da Direção**: compreende que a direção da organização deve fornecer evidência do seu comprometimento com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI mediante estabelecimento de políticas do SGSI de acordo com os objetivos do SGSI. (ABNT, 2006, p. 09).
- **Auditorias internas do SGSI**: compreende que a organização deve conduzir auditorias internas do SGSI a intervalos planeados para determinar se os objetivos de controle, controles, processos e procedimentos do seu SGSI atendem aos requisitos desta Norma e à legislação ou regulamentações pertinentes, se atende aos requisitos de segurança da informação identificados e se são mantidos e implementados de forma eficaz e são executados conforme o esperado. (ABNT, 2006, p. 11).
- **Análise crítica do SGSI pela direção**: compreende que a direção deve analisar criticamente o SGSI da organização a intervalos planejados para assegurar a sua contínua pertinência, adequação e eficácia. Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação e objetivos de segurança da informação. Os resultados dessas análises críticas devem ser claramente documentados e os registros devem ser mantidos. (ABNT, 2006, p. 11).
- **Melhorias no SGSI**: compreende que a organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção. (ABNT, 2006, p. 12).

Estes são os principais tópicos apresentados pela norma como sendo requisitos para implementação de um sistema de gestão da segurança da informação. Estes tópicos juntamente com seus subtópicos compõem um modelo para estabelecer, implementar, operar, monitorar, analisar, manter e melhorar um Sistema de Gestão da Segurança da Informação na organização.

5.2.3 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**, tem como propósito fornecer diretrizes práticas para a implantação de um Sistema de Gestão da Segurança da Informação em uma organização. Esta norma é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27003:2010, elaborada pela *Technical Committee Information Technology*.

Esta norma 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.

Esta norma compreende os seguintes tópicos que visam estabelecer diretrizes para implantação de um Sistema de Gestão da Segurança da Informação:

- **Obtendo aprovação da direção para iniciar o projeto do SGSI**: Compreende que para obter a aprovação da direção, convém que uma organização crie os motivos que justificam a implantação, os quais incluem os objetivos e as prioridades para implementar um SGSI, em contemplação à estrutura da organização para o SGSI. Convém que o plano do projeto inicial do SGSI também seja criado. (ABNT, 2011, p. 05).
- **Definindo o escopo do SGSI, limites e a política do SGSI**: seu objetivo é definir o escopo detalhado e os limites do SGSI, desenvolver a política do SGSI e obter aprovação da direção. (ABNT, 2011, p. 13).
- **Conduzindo a análise dos requisitos de segurança da informação**: seu objetivo é definir os requisitos relevantes a serem suportados pelo SGSI, identificar os ativos de informação e obter o atual status da segurança de informação dentro do escopo. (ABNT, 2011, p. 21).
- **Conduzindo a análise/avaliação de riscos e planejando o tratamento do risco**: Seu objetivo é definir a metodologia de análise/avaliação de riscos, identificar,

analisar e avaliar os riscos de segurança da informação para selecionar as opções de tratamento de riscos e seleção de objetivos de controle e controles. (ABNT, 2011, p. 27).

- **Definindo o SGSI**: seu objetivo é completar o plano final de implantação do SGSI através de: definição da segurança da organização com base nas opções de tratamento de risco selecionadas e nos requisitos de registros e documentação, definindo dos controles pela integração com as provisões de segurança para Tecnologia de Informação e Comunicação (TIC), infraestrutura e processos organizacionais, e definição dos requisitos específicos do SGSI. (ABNT, 2011, p. 32).

Estes são os principais tópicos apresentados pela norma para prover diretrizes para implantação de um sistema de gestão da segurança da informação. Estes tópicos juntamente com seus subtópicos fornecem explanações e recomendações para a implantação de um SGSI em quaisquer organizações.

5.2.4 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** é uma adoção idêntica, em conteúdo técnico, estrutura e redação, à ISO/IEC 27005:2011 que foi elaborada pelo *Technical Committee Information Technology*, *Subcommittee IT Security Techniques*, conforme ISO/IEC Guide 21-1: 2005. Esta segunda edição cancela e substitui a edição anterior (ABNT NBR ISO/IEC 27005:2008), a qual foi tecnicamente revisada.

Esta norma 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.

Esta norma apresenta os seguintes tópicos que visam fornecer diretrizes para o processo de gestão de ricos de segurança da informação:

- **Visão geral do processo de gestão de riscos de segurança da informação:** o processo de gestão de riscos de segurança da informação pode ser iterativo para o processo de avaliação de riscos e/ou para as atividades de tratamento de risco. Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. Permite também minimizar o tempo e o esforço despendidos na identificação de controles e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados. (ABNT, 2011, p. 09).
- **Definição do contexto:** convém que o contexto externo e interno para a gestão de riscos de segurança da informação seja estabelecido, o que envolva a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação, a definição do escopo e dos limites e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação. (ABNT, 2011, p.11).
- **Processo de avaliação de riscos de segurança da informação:** convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização. (ABNT, 2011, p. 15).
- **Tratamento do risco de segurança da informação:** é necessário que controles para modificar, reter, evitar ou compartilhar os riscos sejam selecionados e o plano de tratamento do risco seja definido. (ABNT, 2011, p. 25).
- **Aceitação do risco de segurança da informação:** é necessário que a decisão de aceitar os riscos de segurança da informação seja feita e formalmente registrada, juntamente com responsabilidade pela decisão. Convém que os planos de tratamento do risco descrevam como os riscos avaliados serão tratados para que os critérios de aceitação de riscos sejam entendidos. (ABNT, 2011, p. 30).
- **Comunicação e consulta do risco de segurança da informação:** as informações sobre riscos precisam ser trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas. A comunicação do risco é uma atividade que objetiva alcançar um consenso sobre como os riscos devem ser gerenciados, fazendo uso para tal da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e as outras partes interessadas. A informação inclui, entre outros possíveis fatores, a existência, natureza, forma, probabilidade, severidade, tratamento e aceitabilidade dos riscos. (ABNT, 2011, p. 30).

- **Monitoramento e análise crítica de riscos de segurança da informação:** é importante que os riscos e seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidades de ocorrência) sejam monitorados e analisados criticamente, a fim de identificar, o mai rapidamente possível , eventuais mudanças no contexto da organização e de manter uma visão geral dos riscos. (ABNT, 2011, p. 32).

Estes são os tópicos apresentados pela norma para gerir um processo de gestão de riscos dentro de qualquer tipo de organização, seus tópicos, subtópicos e anexos compreendem as formas adequadas de se fazer um planejamento da Gestão de Riscos de Segurança da Informação dentro da organização, a fim de evitar futuros danos a essas informações.

5.3 ARQUITETURA DA INFORMAÇÃO

A informação passou a ser de grande valia dentro das organizações, tem um valor agregado, onde ela é produto, serviço, lucro e informação estratégica para vencer a concorrência. “Numa economia de informação, a concorrência entre as organizações baseia-se em sua capacidade de adquirir, tratar, interpretar e utilizar a informação de forma eficaz.” (MACGEE; PRUSAK, 1994, p. 03).

Segundo Macgee e Prusak (1994, p. 04) a tecnologia vem em prol desta economia de informação, mas não é a tecnologia e sim o seu uso, que cria valor adicional, o valor da tecnologia da informação depende da informação e do papel desempenhado por ela nas organizações. A informação é capaz de criar valor significativo para as organizações, possibilitando a criação de novos produtos e serviços e aperfeiçoando a qualidade do processo decisório em toda a organização. Algumas informações existem de forma desorganizada e

> com os sistemas de informação, muitas vezes não há uma única resposta "certa" para uma determinada questão. Estamos preocupados com as informações de todas as formas e tamanhos: *sites*, documentos, aplicações de *software*, imagens, etc. Estamos também preocupados com metadados: os termos usados para descrever e representar objetos de conteúdo tais como documentos, pessoas, processos e organizações. (MORVILLE; ROSENFELD, 2006, p. 05, tradução nossa).

Para sanar estas necessidades informacionais, no que diz respeito aos sistemas de informação e na própria organização da informação, em auxílio a esta tecnologia, temos as arquiteturas da informação (AI), que permite o armazenamento, a organização e a recuperação

efetiva de informações em vários formatos. Segundo Macgee e Prusak (1994, p. 105-106) “a arquitetura é o estudo da forma pela qual diferentes espaços físicos contribuem para as atividades humanas que ocorrem dentro desses espaços”. Ela diz respeito aos processos que auxiliam os indivíduos a criarem espaços para atender às suas necessidades, que no caso da arquitetura da informação visa atender as necessidades informacionais de seus usuários.

> Os processos e a arquitetura da informação existem para promover determinados tipos de comportamento em relação à informação dentro das organizações. A informação não tem qualquer valor para uma organização até que seja colocada em prática. A maneira como os indivíduos se comportam em relação a informação – como eles a adquirem, filtram, analisam e comunicam – é tão importante para a organização quanto a própria informação. (MACGEE; PRUSAK, 1994, p. 106).

Segundo Macedo (2005) a AI se difere das arquiteturas de sistemas de informação. Por sistemas de informação entende-se que são “sinônimos de ambientes de informação, referindo-se a serviços de informação propriamente ditos, tais como bibliotecas ou centros de informação.” (MACEDO, 2005, p. 136). O objetivo da 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. Informação e conhecimento são, essencialmente, criações humanas, e nunca seremos capazes de administrá-los se não levarmos em consideração que as pessoas desempenham, nesse cenário, um papel fundamental, pois são elas as criadoras, mediadoras e disseminadoras destas informações dentro das organizações.

Morville e Rosenfeld (2006, p. 11-12, tradução nossa) tratam principalmente destes aspectos que dificultam os processos informacionais nas organizações como:

- o alto custo para encontrar informações;
- o de não encontrar esta informação;
- o de construir e manter informações pertinentes aos negócios, assim como;
- o alto custo no treinamento e manutenção de pessoal para lidar com essas informações e os ambientes em que elas estejam disponíveis.

A AI desempenha papel importante na diminuição destes custos, na melhoria e aumento de qualidade do nível estratégico, tático e operacional da organização, auxiliando assim na tomada de decisão, na identificação de falhas, na solução e aperfeiçoamento destas falhas, assim como na projeção de posicionamentos estratégicos e mudança cultural na organização. (CAMARGO; VIDOTTI, 2011, p. 34).

A ecologia da informação diferentemente da arquitetura da informação não se concentra na tecnologia, ela baseia-se na maneira como as pessoas criam, distribuem, compreendem e usam a informação dentro da organização. De acordo com Davenport (1998, p. 14) a abordagem ecológica acredita que:

> - a informação não é facilmente arquivada em computadores - e não é constituída apenas de dados;
> - quanto mais complexo o modelo de informação, menor será sua utilidade;
> - a informação pode ter muitos significados em uma organização;
> - a tecnologia é apenas um dos componentes do ambiente de informação e frequentemente não se apresenta como meio adequado para operar mudanças. (DAVENPORT, 1998, p. 14).

A tecnologia (incluindo computadores, redes de comunicação e *softwares*), tornou-se não apenas uma ferramenta para administrar a informação, mas também um setor vigoroso em si mesmo, mas a informação (ou ao menos o uso efetivo dela) não cresce na mesma proporção. O verdadeiro problema segundo Davenport (1998) é supor que a tecnologia, em si, possa resolver todas as dificuldades na gestão da informação, neste sentido o interessante é pensar no ser humano como principal responsável pela gestão destas informações, assim como agente na

organização, disseminação e recuperação destas informações pertinentes à organização, e a tecnologia um meio de apoio, ao qual podemos inserir, organizar, arquivar e recuperar essas informações. A tecnologia neste sentido torna-se um meio alternativo de armazenamento de informações aos arquivos, para salvaguardar essas informações, que estão apresentadas em variados formatos digitais, além de seus suportes físicos (planilhas, textos, manuais, relatórios, etc.).

Ainda segundo o autor "as abordagens informacionais predominantes enfatizam os atributos racionais, sequenciais e analíticos da informação e de seu gerenciamento." (DAVENPORT, 1998, p. 17). A ênfase primária não está na geração e na distribuição de enormes quantidades de informações desnecessárias à organização, mas no uso eficiente de uma quantia relativamente pequena, mas necessária e por pessoas certas dentro da organização. Este planejamento ecológico permite, no entanto, evolução e interpretação, elimina a rigidez de alguns controles centrais que nunca funcionam, e responsabiliza pelas informações específicas as pessoas que precisam delas e as utilizam dentro de cada setor da organização. "Em suma, a abordagem ecológica do gerenciamento da informação é mais modesta, mais comportamental e mais prática que os grandes projetos da arquitetura da informação e de máquina/engenharia." (DAVENPORT, 1998, p. 21).

Voltamos assim ao conceito de que AI permite elaborar uma estrutura que visa à organização das informações para que os usuários possam acessá-las mais facilmente e encontrar seus caminhos para a construção de conhecimentos, assim como a AI também auxilia no desenvolvimento de ambientes digitais capazes de facilitar este acesso aos usuários, sendo um esforço entre humano-tecnologia, já que o ser humano se torna o gestor destas informações, enquanto os sistemas de informação se tornam os ambientes facilitadores para a gestão destas informações.

Por fim, segundo Hagedorn (2000, p. 5, tradução nossa) "arquitetura da informação é a arte e a ciência da organização da informação para ajudar efetivamente pessoas a satisfazer suas necessidades informacionais". Envolve assim investigação, análise, desenho e implementação. Enquanto ecologia da informação é a rede dos relacionamentos que cria um espaço de informação. As partes de uma ecologia da informação são os conteúdos, as ferramentas criadas para veiculá-los, o contexto no qual se inserem e os usuários que o acessam.

Para Evernden e Evernden (2003, p. 98, tradução nossa) "a arquitetura da informação mudou drasticamente nos últimos 20 anos, tornando-se uma ferramenta sofisticada e multidimensional de gestão da informação." Em consequência desta mudança os autores afirmam que, "as organizações contemporâneas precisam de uma arquitetura da informação e de

uma tecnologia complementar que trabalhem em conjunto para poder oferecer supremacia comercial por meio da comunicação e uso de informação de forma produtiva e rentável." (EVERNDEN; EVERNDEN, 2003, p. 98, tradução nossa). A informação é mais que mero produto, ela é moeda de troca, é uma forma de crescimento significativo indispensável para as organizações contemporâneas, pois é através de sua gestão competente que se dará as tomadas de decisão; criação de capital intelectual para melhorias nos processos organizacionais, assim como sua consolidação no mercado em que esteja inserida.

5.4 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, porem, 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 a 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. Trataremos de definir um pouco algumas destas organizações.

A expressão ONG surgiu na Europa e tem sua origem na nomenclatura do sistema de representações das Nações Unidas. No início, foram designadas como “Organizações não Estatais” importantes a ponto de serem representadas na Organização das Nações Unidas (ONU). Já no Brasil, o termo ONG surge nos anos 1980 e é consolidado nos anos 1990, segundo Landim (1993, p. 33) “para identificar um conjunto de entidades que veio se formando a partir dos anos 1970, misturando cristianismo e marxismo, militância e profissionalismo.” Estas organizações estão presentes e atuantes no terceiro setor, assim como as fundações, associações, dentre outras.

De acordo com Bastos Júnior et. al (2001, p. 06) ONG é uma organização comprometida com a sociedade civil, com movimentos sociais e com a transformação social. Embora também estejam classificadas como associações no Código Civil, diferenciam-se das associações por estarem raramente voltadas para seus próprios membros e estarem, sobretudo orientadas para "terceiros" grupos, ou seja, para objetivos externos aos membros que compõem. Também se diferenciam das organizações filantrópicas, por não exercerem nenhum tipo de prática de caridade, o que seria contrário a sua ideia de construção de autonomia, de igualdade e de participação dos grupos populares.

Associação pode ser definida segundo (SZAZI, 2006, p. 27) “como um pessoa jurídica criada a partir da união de ideias e esforços de pessoas em torno de um propósito que não tenha finalidade lucrativa”. Tem-se uma associação quando não há fim lucrativo ou intenção de dividir o resultado, embora tenha patrimônio, formado por contribuição de seus membros para obtenção de fins culturais, educacionais, esportivos, religiosos, recreativos, morais, etc, não perdendo seu caráter de associação, caso realize negócios para manter ou aumentar seu patrimônio, sem, contudo, proporcionar ganho aos associados. Entretanto, o fato de criar-se uma associação, não implica necessariamente a criação de uma entidade de cunho social, já que diversos propósitos podem não visar lucro e mesmo assim não servir de proveito a todos.

Já os Institutos não correspondem a uma espécie de pessoa jurídica, podendo ser utilizado por uma entidade governamental ou privada, de fins lucrativos ou não, constituída sob a forma

de fundação ou de associação, eventualmente vemos o termo “instituto” associado a entidades dedicadas a educação, pesquisa ou produção científica. (SZAZI, 2006).

As fundações são vistas como um conjunto de bens, com um fim determinado, um patrimônio personalizado, destinado a um fim. Fundação é um patrimônio destinado a servir, sem intuito de lucro, a uma causa de interesse público determinada, que adquire personificação jurídica por iniciativa de seu instituidor. A fundação pode ainda, ser instituída após a morte de seu instituidor, em cumprimento à disposição testamentária. Fundações podem ser criadas pelo Estado, assumindo natureza de pessoa jurídica de direito público, ou por indivíduos ou empresas, quando assumem natureza de direito privado. (SZAZI, 2006).

Com a formação setorizada, fragmentada e focada apenas no social, no terceiro setor os aspectos administrativos e de gestão dessas instituições, foram desconsiderados pelos profissionais da área social, segundo Voltolini (2004, p. 18) “revelando a profunda dicotomia existente entre social e o administrativo”, esta fragilidade acarretou na herança histórica de instituições que não se sustentam, vivendo assim na dependência do Estado. No processo de constituição o terceiro setor, emerge no âmbito da área de administrativa, tendo como tema central e estruturante a “gestão social”.

Atualmente o Terceiro Setor, está relacionado ao âmbito das ciências da administração, seu ponto central agora é a gestão, operando segundo a lógica e a racionalidade do setor privado, que tem o lucro com objetivo.

> o termo terceiro setor é apropriado por uma série divergente de finalidades e aplicações que contribuem ainda mais para o escurecimento de sua compreensão e para o aumento das dificuldades em termos de definição conceitual. A superficialidade no trato do tema, a reprodução sem critérios de conceitos e definições frágeis e a multiplicidade de interesses que estão ao redor das organizações consideradas partes do terceiro setor são características, dentre outras, marcantes e fundamentais que contribuem para a manutenção da confusão conceitual. (FERREIRA; FERREIRA, 2006, p. 1).

De acordo com Ferreira e Ferreira (2006, p. 02-03) o terceiro setor está inserido em um inter-relacionamento indissociável com três esferas da sociedade:

- **Esfera privada** (composta principalmente por empresas com fins lucrativos) neste âmbito empresarial é possível perceber o interesse pelo tema, quer tanto por questões de imagem e marketing para as empresas, quer por preocupações realmente sérias de organizações para com o meio-ambiente que as cercam no tocante às diversas questões, como as sociais e ambientais;
- **Esfera pública** (governamental) neste âmbito público, o terceiro setor tem sido considerado um importante instrumento de apoio aos governos no estabelecimento de

políticas públicas para a área social e na execução e controle de projetos sociais através da liberação de verbas na forma de parcerias e convênios e de renúncias fiscais;

- **esfera da sociedade civil** (congrega parcelas de representantes institucionais da sociedade e da iniciativa privada e de indivíduos na qualidade de cidadãos conscientes de sua responsabilidade social) neste âmbito civil, observa-se a organização de grupos formalizados e legalizados com objetivos de defender interesses comuns ao grupo ou a uma parcela maior da sociedade ou ainda de prestar algum tipo de serviço para parcelas da população excluídas do acesso a tais serviços, como no fornecimento de alimentação, medicamentos, consultas e tratamentos médicos, assistência psicológica e espiritual, educação, cidadania, dentre outros.

Assim sendo, o Primeiro Setor-Estado; o Segundo Setor-Iniciativa Privada e o Terceiro Setor-Sociedade Civil. Entretanto, sob uma perspectiva geral passível de observação na literatura dominante sobre o tema, não há um corpo teórico que dê sustentação sólida para a abrangência do campo de estudos do terceiro setor, assim como não há consenso em relação às organizações que integram ou que podem integrar o setor generalizadamente, a escassez de materiais atuais sobre o tema dificulta um aprofundamento maior sobre o mesmo. (FERREIRA; FERREIRA, 2006).

Segundo Teodósio (2002, p. 14) apesar de nos últimos anos o Terceiro Setor ter se tornado objeto de estudo e linhas de investigação, tanto no Brasil quanto em outros países, grande parte da literatura destaca e/ou constata que o grau de informação e conhecimento sistematizado sobre o Terceiro Setor ainda é insuficiente, necessitando assim de um aprofundamento no tema pela comunidade acadêmica. No Brasil, a questão conceitual também se apresenta confusa devido ao fato de existirem inúmeras denominações para identificação das organizações inseridas no terceiro setor, como Organização não Governamental (ONG), Organização da Sociedade Civil (OSC), Organização da Sociedade Civil de Interesse Público (OSCIP) e Organização sem fim Lucrativo (OSFL) dentre outras, como organizações filantrópicas, organizações caridosas, organizações sociais, organizações associativas, etc.

Outro fator que permeia a dificuldade de estudar este tema, segundo Landim (1993) é que política, social e economicamente, o Terceiro Setor brasileiro é fragmentado e heterogêneo. O grande número de organizações é extremamente variado, notadamente com relação aos papeis desempenhados por elas na sociedade, tornando assim de difícil definição, qualquer tentativa de classificar as organizações do terceiro setor no Brasil encontra diversas dificuldades.

6 METODOLOGIA

Segundo Gressler (2004, p. 42) o objetivo da metodologia é o de descrever e analisar os métodos utilizados lançando luz sobre suas limitações, realçando sua utilidade, esclarecendo em que se baseiam e as consequências que acarretam, indicando suas potencialidades nas diversas áreas do conhecimento. Utilizando generalizações, baseadas no sucesso de técnicas particulares, sugerir novas aplicações para as técnicas, desvelar a importância que os princípios lógicos e metafísicos podem ter para as questões. Em suma, o objetivo da metodologia é o de ajudar-nos a compreender, nos mais amplos termos, não o produto da pesquisa, mas o próprio processo de pesquisa. A metodologia ainda trata das formas de se fazer ciência, ela determina os procedimentos a serem seguidos, as ferramentas a serem utilizadas e os caminhos a se seguir na produção científica.

Pretendeu-se nesta pesquisa, através da utilização de métodos qualitativos, elaborar um modelo de avaliação que permita avaliar a eficiência e eficácia das Arquiteturas de Segurança da Informação na Comissão Pastoral da Terra (CPT).

6.1 NATUREZA DA PESQUISA

A natureza da presente pesquisa é exploratória que “tem como principal finalidade, esclarecer e modificar conceitos e ideias, tendo em vista a formulação de problemas mais precisos ou hipóteses pesquisáveis para estudos posteriores.” (GIL, 2009, p. 27). Seu caráter é descritivo e segundo Gressler (2004, p. 54) a pesquisa descritiva é usada para descrever fenômenos existentes, situações presentes e eventos, identificar problemas e justificar condições, comparar e avaliar o que os outros estão desenvolvendo em situações e problemas similares, visando aclarar situações para futuros planos e decisões. E sua dimensão é qualitativa, esta abordagem é utilizada quando se pretende descrever a complexidade do problema de pesquisa, não envolve manipulação de variáveis e estudos experimentais, esta abordagem “busca levar em consideração todos os componentes de uma situação em suas interações e influências recíprocas, numa visão holística dos fenômenos.” (GRESSLER, 2004, p. 43).

6.2 CARACTERIZAÇÃO DO OBJETO DE PESQUISA

O objeto de estudo da seguinte pesquisa é a Comissão Pastoral da Terra (CPT), organização atuante no terceiro setor, com sede da Secretaria Nacional na capital Goiânia e diversas Secretarias Setoriais em vários Estados Brasileiros. A escolha desta organização aconteceu pela dificuldade em estabelecer contato com outras organizações atuantes no terceiro setor em Goiânia, sendo a CPT a única organização a demonstrar interesse em colaborar para realização desta pesquisa.

A CPT[13] 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. Inicialmente a CPT desenvolveu junto aos trabalhadores e trabalhadoras da terra um serviço pastoral. Em cada região, o trabalho da CPT adquiriu uma tonalidade diferente de acordo com os desafios que a realidade apresentava; sem, contudo, perder de vista o objetivo maior de sua existência: ser um serviço à causa dos trabalhadores rurais, sendo um suporte para a sua organização.

A CPT desde a sua criação se defrontou com os conflitos no campo e o grave problema da violência contra os trabalhadores e trabalhadoras da terra. Esta violência que saltava aos olhos começou a ser registrada sistematicamente já no final dos anos 1970. A partir de 1985 os dados começaram a ser publicados anualmente em forma de Cadernos. Durante este tempo, o Setor de Documentação trabalhou intensamente no levantamento de dados na luta e pela resistência na terra, pela defesa e conquista dos direitos. Em 2002 começou a registrar os conflitos pela água.

A CPT tornou-se a única entidade a realizar tão ampla pesquisa sobre a questão agrária em âmbito nacional, assumiu a tarefa de registrar e denunciar os conflitos de terra, água e a violência contra os trabalhadores e seus direitos. Com este trabalho, a CPT formou uma das mais importantes bibliotecas com livros, cadernos, revistas, jornais e arquivos que tratam das lutas camponesas, criando assim na secretaria nacional o setor de Documentação, responsável por registrar, arquivar/salvaguardar e disponibilizar ao público documentos referentes aos conflitos.

Fundada em plena ditadura militar, como resposta à grave situação dos trabalhadores rurais, posseiros e peões, sobretudo na Amazônia, a CPT teve um importante papel. Ajudou a defender as pessoas da crueldade deste sistema de governo, que fazia o jogo dos interesses capitalistas nacionais e transnacionais, e abriu caminhos para que ele fosse superado. Ela nasceu

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

ligada à Igreja Católica porque a repressão estava atingindo muitos agentes pastorais e lideranças populares, e também, porque a igreja possuía certa influência política e cultural.

No período da ditadura, o reconhecimento do vínculo com a Conferência Nacional dos Bispos do Brasil (CNBB) ajudou a CPT a realizar o seu trabalho e se manter. Mas já nos primeiros anos, a entidade adquiriu um caráter ecumênico, tanto no sentido dos trabalhadores que eram apoiados, quanto na incorporação de agentes de outras igrejas cristãs, destacadamente da Igreja Evangélica de Confissão Luterana no Brasil (IECLB).

Os posseiros da Amazônia foram os primeiros a receber atenção da CPT. Rapidamente, porém, a entidade estendeu sua ação para todo o Brasil. Assim, a CPT se envolveu com os atingidos pelos grandes projetos de barragens e, mais tarde, com os sem-terra. Terra garantida ou conquistada, o desafio era o de nela sobreviver. Por isso, a Agricultura Familiar mereceu um destaque especial no trabalho da entidade, tanto na organização da produção, quanto da comercialização. A CPT junto com seus parceiros foi descobrindo que esta produção precisava ser saudável, que o meio ambiente tinha que ser respeitado, que a água é um bem finito. As atenções, então, se voltaram para a ecologia. A CPT também atua junto aos trabalhadores assalariados e os boias-frias, que conseguiram, por algum tempo, ganhar a cena, mas que enfrentam dificuldades de organização e articulação. Além destes, há ainda os "peões", submetidos, muitas vezes, a condições análogas às da escravidão.

Em cada região, o trabalho da CPT adquiriu uma tonalidade diferente de acordo com os desafios que a realidade apresentava; sem, contudo, perder de vista o objetivo maior de sua existência: ser um serviço à causa dos trabalhadores rurais, sendo um suporte para a sua organização. O homem do campo é que define os rumos que quer seguir, seus objetivos e metas. A CPT o acompanha, não cegamente, mas com espírito crítico. É por isso que a CPT conseguiu, desde seu início, manter a clareza de que os protagonistas desta história são os trabalhadores e trabalhadoras rurais.

Finalmente, os direitos humanos, defendidos pela CPT, permeiam todo o seu trabalho. Em sua ação, explícita ou implicitamente, o que sempre esteve em jogo foi o direito do trabalhador, em suas diferentes realidades. De tal forma que se poderia dizer que a CPT é também uma entidade de defesa dos Direitos Humanos ou uma Pastoral dos direitos dos trabalhadores e trabalhadoras da terra.

6.3 PROCEDIMENTOS METODOLÓGICOS

A presente pesquisa pautou-se nos requisitos das normas da ABNT ISO/IEC 27001:2006; 27002:2005; 27003:2011 e 27005:2011 relativas à Gestão da Segurança da Informação para a elaboração de um "Modelo de Avaliação das Arquiteturas de Segurança da Informação" a fim de avaliar o nível de eficiência e eficácia dos procedimentos de gestão da segurança da informação na Comissão Pastoral da Terra. O processo metodológico foi dividido em 3 passos, sendo:

1ª passo elaborar o Modelo de Avaliação das Arquiteturas de Segurança da Informação, 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", "Arquitetura da Informação";
2ª passo aplicar a pesquisa, através de um roteiro de entrevista orientada elaborado a partir do Modelo de Avaliação das Arquiteturas de Segurança da Informação, que consistirá em avaliar através de perguntas fechadas e de múltipla escolha, feitas diretamente ao responsável pelo Centro de Documentação (CEDOC) da CPT, a fim de avaliar a atual situação da Gestão da Segurança da informação na organização;
3ª passo analisar e apresentar os resultados obtidos através da realização da entrevista orientada com o responsável pelo CEDOC da CPT, a fim de apresentar o resultado final da pesquisa, que visa verificar a presente situação de Gestão da Segurança da Informação na organização atuante no Terceiro Setor.

6.4 MODELO DE AVALIAÇÃO DAS ARQUITETURAS DE SEGURANÇA DA INFORMAÇÃO

O Modelo de Avaliação das Arquiteturas de Segurança da Informação (ver Apêndice A, p. 65) foi elaborado, baseando-se em uma escala de intervalo que segundo Costa (2011, p. 28) toma "por base intervalos de intensidade entre dois extremos de verificação." Definimos aqui uma escala com a fixação de um ponto extremo para mínimo 1 e outro para máximo 5, fixação esta feita por convenção, podendo a variável ser medida em uma escala de 1 a 5 ou 1 a 100. A escala de intervalo em boa medida ordena percepções e tem o sentido de quantificação. De

acordo com Costa (2011, p. 30) com relação às operacionalizações possíveis, para o caso da escala de intervalo praticamente não há restrição quanto ao uso de ferramentas de análise, sendo possível a aplicação de praticamente todas as técnicas matemáticas e estatísticas (univariada e multivariada).

O modelo apresenta-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.".

MODELO DE AVALIAÇÃO DAS ARQUITETURAS 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: Elaboração própria.

Para este modelo 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.

6.4.1 Aplicação do modelo

A aplicação do modelo de avaliação consiste na busca de respostas à seguinte pergunta: Qual a atual situação das 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?.

Para cada um dos 3 indicadores dos 5 grupos será verificada a situação da gestão da segurança da informação na organização e em seguida, de acordo com a característica elencada em cada nível, indicar de acordo com a tabela de pontuação o nível em que se encontra a situação verificada. Ao final da verificação e pontuação das situações encontradas, será realizada a apuração da situação geral e do nível de eficiência e eficácia requerido pela questão colocada de início. Assim, deverá extrair, através de média aritmética simples, o índice que irá subsidiar a resposta para a questão sobre o nível de eficiência e eficácia das arquiteturas de segurança da informação da organização.

A média aritmética simples é uma das formas de obter um valor intermediário entre vários valores. Foi criada pelo filósofo, cientista, estratego, estadista, matemático e astrônomo grego Arquitas de Tarento[14] considerado um dos mais ilustres matemáticos pitagóricos que viveu entre 428 e 347 a.c., fundou a mecânica matemática e foi o primeiro a usar o cubo em geometria e a restringir as matemáticas às disciplinas técnicas como a geometria, aritmética, astronomia e acústica.

[14] **Fonte:** Wikipédia. Disponível em: <http://pt.wikipedia.org/wiki/Arquitas_de_Tarento>. Acesso em: 20 fev. 2013.

Em cada um dos Grupos de Indicadores, os índices encontrados (números dos níveis) deverão ser 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.

Ao final, após ter encontrado o índice para cada grupo indicador, será aplicado novamente a fórmula de média aritmética simples, somando os índices dos grupos de indicadores e dividindo pelo número de grupos de indicadores. Este índice encontrado revelará, de acordo com a tabela de níveis de eficiência, o nível de eficiência e eficácia das Arquiteturas de Segurança da Informação da organização escolhida previamente.

7 ANÁLISE E APRESENTAÇÃO DOS DADOS

A seguir, serão analisados e apresentados os dados obtidos mediante aplicação de entrevista orientada (ver apêndice B, p. 80) à Comissão Pastoral da Terra, estes resultados pretendem elucidar a atual situação de eficiência e eficácia das Arquiteturas de Segurança da Informação na organização. Os resultados serão apresentados em formato de relatório, onde constam principalmente, informações sobre a organização em que se realizou a avaliação, período em que ocorreu a avaliação, informações sobre contratempos ocorridos e uma análise crítica dos resultados encontrados.

Comissão Pastoral da Terra (CPT) – Secretaria Nacional, Rua 19, nº 35, Edifício Dom Abel, Centro - Goiânia, Goiás, foi a organização do terceiro setor escolhida para aplicação piloto do Modelo de Avaliação das Arquiteturas de Segurança da Informação, que pretende verificar o nível de eficiência e eficácia dos procedimentos de Gestão da Segurança da informação em organizações do terceiro setor. A avaliação ocorreu no mês de janeiro de 2013, o instrumento de coleta de dados utilizado, foi um roteiro de entrevista orientada, elaborado a partir dos Grupos de Indicadores do Modelo de Avaliação das Arquiteturas de Segurança da Informação, baseado nas normas da ABNT NBR ISO/IEC relativas à Gestão da Segurança da Informação. Os resultados serão descritos na ordem de cada grupo/indicador, sendo 5 grupos, com 3 indicadores cada, onde há a possibilidade das respostas serem: *sim, não e não aplicável.*

Abaixo está apresentado também o quadro com os resultados obtidos através da escala de valor, para a situação do nível de eficiência e eficácia de cada grupo indicador, sendo **5-ideal; 4-Satisfatório; 3-aceitável; 2-Insuficiente e 1-crítico** para cada um dos 3 indicadores dos 5 grupos do modelo de avaliação.

RESULTADOS DOS INDICADORES DE CADA GRUPO

GRUPOS	INDICADORES		
Gestão da Segurança da Informação	Análise/avaliação de riscos	Política de Segurança	Análise Crítica da Política de Segurança
	4	**2**	**2**
Gestão de Ativos	Inventário dos ativos	Uso de Ativos	Classificação da Informação
	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
	2	**1**	**1**
Infraestrutura Tecnológica	Hardware para Tecnologias de Informação e Comunicação	Softwares para Gestão	Serviços de Rede
	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
	2	**5**	**2**

Fonte: Elaboração própria.

Dos resultados obtidos no **GRUPO 1 - Gestão da Segurança da Informação:**

Indicador 1 - Análise/Avaliação de Riscos de Segurança da Informação, no que diz respeito ao levantamento periódico dos riscos presentes na organização, há um levantamento pensado nos desastres naturais, no acervo físico e no digital. Se Existem Parâmetros que envolvem o processo das rotinas de backup dos servidores, há uma empresa terceirizada responsável pela realização do backup dos servidores periodicamente, na sede em si não há um profissional da área de informática disponível. Não existe uma tabela que defina os níveis dos riscos de segurança da informação em aceitáveis, inaceitáveis e os que possam ser aceitáveis. É realizada análise e classificação dos riscos inerentes aos sistemas de informação, a fim de evitar ou minimizar danos e prejuízos. Também existem procedimentos contra ataques internos e

externos aos sistemas de informação, a fim de evitar perda ou dano em informações importantes à organização. Nos parâmetros de avaliação do modelo, para Análise/Avaliação de Riscos de Segurança da Informação o nível de eficiência e eficácia deste indicador é **4 (satisfatório),** atinge quase todos os requisitos do grupo.

Indicador 2 - Política de Segurança da Informação, no que diz respeito à existência do estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos, não há uma política/procedimento voltada propriamente para a gestão da segurança da informação. Não existe, portanto o estabelecimento de papeis e responsabilidades para a segurança da informação. Assim sendo, não há o comunicado à organização sobre a importância de atender aos objetivos de segurança da informação e da conformidade com a política de segurança da informação sobre suas responsabilidades perante as leis. Há a necessidade de melhorias contínuas nos sistemas de gestão da segurança da informação, na organização, assim como a aquisição de um sistema que permita essa gestão efetivamente. Não há recursos suficientes para desenvolver, implementar, operar, manter e melhorar o Sistema de Gestão da Segurança da Informação, há captação de recursos fora da instituição, mas o agravante é a falta de verba para investir nos sistemas e processos de documentação. O nível encontrado de eficiência e eficácia neste indicador é **2 (insuficiente)**, as situações encontram-se praticamente nulas, não havendo efetividade no que se refere ao estabelecimento de políticas de segurança da informação na organização.

Indicador 3 - Análise Crítica da Política de Segurança da Informação, no que diz respeito à existência de uma análise crítica das políticas, sendo elas revisadas e aprovadas pela alta direção da organização, como não há uma política de segurança da informação estabelecida, não há também a análise crítica destas políticas. Também não sendo publicado e comunicado a todos os funcionários e parte externa da instituição, quando das modificações nas políticas. Mas há o reconhecimento da validade da política de segurança da informação para a organização. Não sendo aplicáveis à organização se as políticas estão alinhadas com os objetivos de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação de segurança da informação e comunicação e se a política serve de base para o desenvolvimento das diretrizes de segurança. Não existe na organização um sistema próprio de Gestão da Segurança da Informação, mas existe um sistema para o processamento das informações (projetos estão sendo implementados para disponibilização *online* dos documentos da instituição, este processo está na etapa inicial de digitalização). Neste indicador o nível encontrado de eficiência e eficácia é **2 (insuficiente)**, percebendo que os requisitos para que haja uma análise crítica das políticas de

Segurança da informação são praticamente nulas, já que não existe na organização políticas de gestão da segurança da informação para serem analisadas criticamente.

Dos resultados obtidos no **GRUPO 2 – Gestão de Ativos**:

Indicador 1 - Inventário dos Ativos, na organização é feito um levantamento/atualização dos ativos tecnológicos (*Hardware* e *Software*, equipamentos de rede e mídias), só não há uma quantificação destes ativos. Existe uma planilha com as principais informações dos computadores. É realizado um levantamento/atualização pela alta administração dos ativos não tecnológicos (pessoas, ambientes e processos) da organização. É realizado um levantamento também pela alta administração de pessoal com suas respectivas funções dentro da organização e ainda há um proprietário designado responsável por cada ativo da organização, geralmente sendo um responsável por setor da organização. O nível de eficiência e eficácia no inventário dos ativos neste indicador é **5 (ideal),** as situações indicadas estão todas de acordo com os requisitos das normas.

Indicador 2 - Uso de Ativos, há uma política específica de gestão de ativos da organização (há um manual de procedimento que define os processos da documentação dentro da organização e este é seguido pelo setor de documentação). Os ativos são classificados quanto ao seu nível de segurança (sendo classificados em documentos de acesso livre e acesso restrito ao público). Há um controle de ativos a partir do inventário dos ativos da organização (todos os documentos da organização são inventariados pelo setor de documentação). São definidos escopos de acesso aos ativos quanto a seu grau de sigilo (informações sigilosas são arquivadas em locais específicos, não sendo divulgadas ao público). Há indicação de responsabilidades quanto ao acesso dos ativos e aos recursos de processamento da informação (acessando documentos e informações sigilosas à organização somente os responsáveis pelo centro de documentação). Neste indicador o nível de eficiência e eficácia no uso dos ativos é **5 (Ideal)**, as situações elencadas pelo indicador estão todas em conformidade com os requisitos das normas.

Indicador 3 - Classificação da Informação, há políticas/procedimentos para alcançar e manter a proteção adequada dos ativos da organização, assegurando que a informação seja classificada de acordo com seu nível adequado de proteção, as informações são classificadas em acesso restrito (sigilosas) e de acesso livre. Há uma classificação uniformizada para os níveis de segurança das informações que evite sua destruição e revelação indevida, assim como cópias digitalizadas (em processo) destas informações, além do documento arquivado. As informações são classificadas de acordo com seu grau de sigilo, permitindo restrições a acessos indesejados, sendo acessadas somente por pessoal autorizado. Há a implementação de critérios para classificação e marcação de informações e documentos sigilosos, assim como o arquivamento

dessas informações em locais diferentes dos demais documentos de acesso livre. As informações são armazenadas e acessadas de acordo com sua classificação, sendo as sigilosas acessadas somente por pessoal autorizado. O nível de eficiência e eficácia na classificação das informações neste indicador é **5 (ideal)**, pois as situações aqui elencadas correspondem a todos os requisitos das normas.

Dos resultados obtidos no **GRUPO 3 - Sistema de Gestão da Segurança da Informação:**

Indicador 1 - Implementação de Sistema de Gestão da Segurança da Informação, não se aplica à organização a existência de um modelo de gestão da segurança da informação com uma sistemática abrangente, integrada e contínua, para minimizar os riscos associados ao tratamento da informação em qualquer área da organização. Há uma gestão estratégica na adoção de um sistema de gestão da segurança da informação, no entanto ainda não há um sistema propriamente dito. Não há o atendimento dos requisitos básicos: entender os requisitos de segurança da organização, implementar e operar controles, monitorar e revisar o desempenho do sistema e melhorar continuamente o Sistema de Gestão da Segurança da Informação. Não havendo assim uma avaliação contínua do sistema de gestão da segurança da informação (há uma prática periódica dos processos de informação, quanto aos equipamentos, não visando especificamente à segurança). Há uma avaliação dos riscos envolvendo o Sistema de Gestão da Segurança da Informação, aqui se avalia os riscos envolvendo o sistema utilizado para armazenamento e recuperação das informações da organização (percebem que o risco existe, mas não há um responsável a disposição da organização, tendo consultorias de profissionais da informática terceirizados). O nível de eficiência e eficácia no que diz respeito à implementação de sistemas de gestão de segurança da informação é **2 (insuficiente)**, já que as situações encontradas no indicador estão praticamente nulas, não contribuindo assim para uma gestão efetiva da Segurança da informação.

Indicador 2 - Monitoramento e Análise do Sistema de Gestão da Segurança da Informação, não há políticas/procedimentos de monitoramento e análise crítica do Sistema de Gestão da Segurança da Informação (SGSI). Não há procedimentos que permitem a identificação e detenção de erros nos acessos dos usuários. Não existe monitoramento de acesso e tentativas de violação física e virtual. Não existem recursos para recuperação de informações danificadas ou perdidas (pretende-se utilizar um *software* capaz deste processo de recuperação de informações perdidas ou danificadas, a fim de recuperá-las com a máxima precisão). Não existem responsabilidades referentes ao Sistema de Gestão da Segurança da Informação, já que não existe também um SGSI na organização. O nível de eficiência e eficácia no monitoramento e

análise do SGSI é **1 (crítico)**, pois as situações verificadas neste indicador estão completamente nulas.

Indicador 3 - Melhorias no Sistema de Gestão da Segurança da Informação, na organização não há uma avaliação crítica do Sistema de Gestão da Segurança da Informação. Não há identificação de falhas no Sistema de Gestão da Segurança da Informação. Não há implementação e execução de ações preventivas e corretivas no Sistema de Gestão da Segurança da Informação. Não existem políticas e procedimentos que visam realizar melhorias no Sistema de Gestão da Segurança da Informação. Como também não existem melhorias do Sistema de Gestão da Segurança da Informação a fim de assegurar o fluxo de informações, sem que essas sejam danificadas ou prejudicadas por danos internos e externos à organização. Neste indicador o nível de eficiência e eficácia das melhorias no SGSI é **1 (crítico)**, pois as situações verificadas estão completamente nulas, já que não existe na organização um Sistema de Gestão da Segurança da Informação.

Dos resultados obtidos no **GRUPO 4 - Infraestrutura Tecnológica:**

Indicador 1 - Hardware para Tecnologias de Informação e Comunicação, existe uma infraestrutura de tecnologia de informação e comunicação (TIC) que permite a gestão da segurança da informação, mas necessita de melhorias que visam à segurança da informação. Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação. Há um plano estratégico relacionado às tecnologias de informação e comunicação. O *hardware* dos computadores garante a segurança dos sistemas. Existe uma gestão de infraestrutura tecnológica, que fica a cargo de uma empresa terceirizada e é responsabilidade da alta administração da organização. O nível de eficiência e eficácia do Hardware para TIC é **5 (ideal)**, a situação encontrada no indicador corresponde a todos os requisitos apresentados pelas normas.

Indicador 2 - Softwares para Gestão da Segurança da Informação, não existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização (problemas monetários impedem esta aquisição). Existe um *software* instalado que permite o armazenamento, organização e processamento das informações com segurança, portanto não visa à segurança da informação em si (pretende-se utilizar um *software* livre para armazenar, recuperar e disponibilizar *online* todo o acervo da organização, o *software* em análise pela equipe de documentação é o ICA-AtoM[15]). O *software* instalado não está livre de falhas ou

[15] ICA-AtoM é um *software* livre destinado a apoiar as atividades de Descrição Arquivística em conformidade com os padrões do Conselho Internacional de Arquivos (CIA). Disponível em: <http://213.63.25.16:8800/icaatom-1.1/index.php/?sf_culture=pt>. Acesso em: 04 fev. 2013.

bugs que possam gerar vulnerabilidades ao sistema de gestão da segurança da informação como um todo. A arquitetura da informação é amigável ao usuário. Não há uma gestão de falhas e erros relacionados ao processamento de informações, evitando perda ou modificações de informações importantes. O nível de eficiência e eficácia do *software* para gestão da segurança da informação é **2 (insuficiente)**, pois as situações verificadas neste indicador apresentam-se praticamente nulas, o que não permite uma gestão completa da Segurança da Informação.

Indicador 3 - Serviços de Rede, há na organização o fornecimento seguro de uma rede de conexão com a internet que permita a transferência de arquivos e informações, sem que essas sejam desviadas ou atacadas por *hacker* ou *cracker*. Não existem serviços de rede privados que permitem um maior monitoramento da segurança da informação, assim como um servidor específico para o Sistema de Gestão da Segurança da Informação. Não existem antivírus e *firewalls* para detenção de ameaças de *softwares* maliciosos com a intenção de danificar informações. Há um sistema e serviços de rede baseado em senhas, certificados e autenticação de usuário, sendo acessados somente através de *login* e senha por usuários cadastrados. Não há políticas/procedimentos que definam os controles de acesso e indicação de responsabilidade a estes acessos à rede. O nível de eficiência e eficácia dos serviços de rede da organização é **2 (insuficiente)**, pois as situações verificadas estão praticamente nulas, o que impede a gestão digital das informações da organização de forma efetiva, visando assim sua segurança em rede.

Dos resultados obtidos no **GRUPO 5 - Controle de Acessos:**

Indicador 1 - Política de Controle de Acesso, não existe uma política/procedimento, regras de controle de acesso que inclua direito dos usuários, recursos, operações, autoridade e domínio de acesso. Não existem diretrizes de controle de acesso físico e lógico aos ativos da organização. Não há procedimentos que impeça o acesso ilegal e não autorizado aos sistemas de gestão da segurança da informação. Há indicação de responsabilidade de um controlador de acessos aos ativos para a realização de análise crítica periódica. Há autorização do acesso por meio de senhas, autenticações e certificações de usuário, tanto em meio físico quanto lógico. O nível de eficiência e eficácia das políticas de controle de acesso, é **2 (insuficiente)**, as situações aqui verificadas estão praticamente nulas, pois não existem políticas/procedimentos definindo os controles de acesso na organização.

Indicador 2 - Gerenciamento de Acesso de Usuários, há uma gestão e monitoramento de acessos de usuários. Existe uma inscrição de usuários autorizados e identificação dos ativos que este pode acessar. Existe bloqueio de acesso a usuários não autorizados. Existe a criação de senhas, *login*, autenticação e certificação de usuários aos sistemas de gestão da segurança da informação e restrição de acesso a documentos armazenados em espaços físicos como arquivos,

etc. Há exclusão de dados de usuários assim como bloqueio de senha, após este não possuir mais acesso livre a determinados ativos. O nível de eficiência e eficácia no gerenciamento de acesso de usuários, é **5 (ideal)**, as situações verificadas neste indicador estão de acordo com os requisitos das normas.

Indicador 3 - Controle de Acesso à Rede e a Sistemas Operacionais, existem sistemas operacionais e conexões de redes acessadas mediante identificação do usuário. Não existem listas de acesso contemplando usuários que possuem privilégios de uso de ativos e os que não podem acessar os sistemas e redes da organização. Não há políticas/procedimentos que definam os direitos de acesso aos usuários de sistemas e redes. Há indicação de responsabilidade para controlar os acessos aos sistemas operacionais e as redes de conexão da organização. Não há uma avaliação e monitoramento aos acessos diariamente, a fim de evitar danos aos ativos da organização. Os níveis de eficiência e eficácia nos controles de acesso à rede e a sistemas operacionais é **2 (insuficiente)**, as situações verificadas neste indicador estão praticamente nulas, o que não permite uma gestão efetiva nos controles de acesso à redes e aos sistemas operacionais da organização.

7.1 RESULTADOS

Após realizada a verificação e pontuação das situações encontradas em cada indicador, será 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 (3 indicadores para cada grupo). É um quociente geralmente representado pelo símbolo $\bar{x}$. Se tivermos uma série de *n* valores de uma variável *x*, a média aritmética simples será determinada pela expressão[16]:

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

[16] Fonte. Disponível em: <http://pt.wikipedia.org/wiki/M%C3%A9dia_aritm%C3%A9tica>. Acesso em: 20 fev. 2013.

Para proceder à apresentação dos resultados, em cada um dos Grupos de Indicadores, os índices encontrados (números dos níveis) deverão ser 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.

$$\textbf{Grupos} = \frac{\text{Soma dos Resultados dos Indicadores}}{\text{Nº de Indicadores}} = \textbf{Resultado Final de cada grupo}$$

RESULTADOS DOS GRUPOS

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: Elaboração própria.

Após encontrado o índice para cada grupo indicador, aplicaremos novamente a fórmula de média aritmética simples, somando assim os índices dos grupos de indicadores e dividindo pelo número de grupos de indicadores. Este índice encontrado revelará, de acordo com a tabela

de níveis de eficiência, o nível de eficiência e eficácia das Arquiteturas de Segurança da Informação na Comissão Pastoral da Terra.

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

RESULTADO FINAL

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: Elaboração própria.

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 modelo de avaliação. 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 solução a problemas reais das organizações.

8 CONSIDERAÇÕES FINAIS

Esta pesquisa almejou criar um modelo que permitisse avaliar as arquiteturas de segurança da informação em organizações do terceiro setor em Goiâna. Para proceder a elaboração deste, fez-se necessário um estudo das normas relativas à gestão da segurança da informação. Para aplicação do modelo de avaliação, escolheu-se uma organização do terceiro setor, a Comissão Pastoral da Terra (CPT).

A elaboração desse tipo de instrumento de análise é importante, pois permite avaliar situações que podem existir de forma regular e satisfatória, não tão satisfatória ou identificar até mesmo situações nulas de procedimentos de segurança da informação na organização. 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 a 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 uma forma de implementar políticas, procedimentos e padrões para contribuir de forma efetiva para 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 pesquisa, melhorar estes processos de segurança na CPT.

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 não é muito estudado e na maioria das vezes é de difícil acesso.

Uma das dificuldades encontradas na aplicação desta pesquisa foi conseguir uma organização atuante no terceiro setor em Goiânia que possibilitasse que a pesquisa fosse realizada em seu ambiente, fornecendo informações sobre seus processos documentais e informacionais e os possíveis processos de gestão da segurança da informação, caso este fosse parte dos processos da mesma. Mesmo com alguns empecilhos, a coleta de dados na instituição selecionada foi satisfatória para atingir os objetivos desta pesquisa. O modelo construído mostrou-se capaz de avaliar a situação das arquiteturas de segurança da informação, assim como se mostrou eficiente para propor melhorias nos pontos fracos apontados na coleta dos dados.

É importante ressaltar que este tipo de pesquisa pode vir a contribuir significativamente, tanto no terceiro setor, como em outras organizações inseridas em áreas de atuação nos diversos setores econômicos do país. Para futuras pesquisas, sugere-se que seja melhorado e aperfeiçoado o modelo de avaliação, que contempla apenas requisitos apresentados pelas normas da ABNT NBR ISO/IEC relativas à Gestão da Segurança da Informação.

Nas futuras melhorias, interessante seria pensar em contemplar outros recursos que proveem a Gestão da Segurança da Informação e não se limitar apenas as normas da ABNT 27001:2006; 27002:2005; 27003:2011 e 27005:2011 utilizadas nesta pesquisa como requisitos para criação do modelo de avaliação. Interessante seria a utilização também de outras normas de qualidade ISO/IEC que estão inseridas na família de normas sobre segurança da informação da ABNT, como as normas ABNT NBR ISO/IEC 27011:2009 - Tecnologia da informação - Técnicas de segurança - Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseadas na ABNT NBR ISO/IEC 27002; 27004:2010 - Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição e 27007:2012 - Diretrizes para auditoria de sistemas de gestão da segurança da informação.

Assim como as diretrizes definidas pela OECD; os princípios de segurança e tratamento de incidentes para sistemas e internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e guias de boas práticas em Tecnologia da Informação, como o *Information Technology Infrastructure Library* (ITIL) e o *Control Objectives for Information and related Technology* (COBIT).

O Modelo de Avaliação das Arquiteturas de Segurança da Informação, posteriormente poderá ser estudado, revisado, modificado, melhorado e aplicado em outras organizações para sua efetiva validação como instrumento de Avaliação das Arquiteturas de Segurança da Informação.

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.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007. 70 p.

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.

CERT.br. Disponível em: <http://www.cert.br/>. Acesso em: 28 fev. 2013.

CHIAVENATO, Adalberto. **Introdução à teoria geral da administração**: uma visão abrangente da moderna administração das organizações. 7 ed. ver. e atual. Rio de Janeiro: Elsevier, 2003.

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

COMPUTERWORLD. Disponível em: <http://computerworld.uol.com.br/seguranca/2013/01/30/ataques-de-phishing-causam-prejuizo-de-us-1-5-bilhao-em-2012/>. Acesso em: 28 fev. 2013.

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

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.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. 2. Reimpr. São Paulo: Atlas, 2009.

GRESSLER, Lori Alice. **Introdução à pesquisa; projetos e relatórios**. 2. ed. rev. Atual. São Paulo: Loyola, 2004, 295 p.

HAGEDORN, A. C. **The information architecture glossary**. USA, 2000. Disponível em: <http://argus-acia.com/white_papers/iaglossary.html>. Acesso em: 28 fev. 2013.

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.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION (ISACF). **Control objectives for information and related technology (COBIT).** 2000. Disponível em: <http://www.isaca.org/>. Acesso em: 28 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.

MIRANDA, Kátia Juraci de. A inteligência competitiva e seu impacto em organizações do terceiro setor. **Revista Terceiro Setor**, v. 3, n.1, 2009. Disponível em: <http://revistas.ung.br/index.php/3setor/article/viewFile/508/602>. Acesso em: 01 maio 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.

PEMBLE, M. What do we mean by “information security”. **Computer fraud & security**, v. 2004, n. 5, p. 17–19, May 2004.

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.

WIKIPÉDIA. Enciclopédia Livre. Disponível em: <http://pt.wikipedia.org/wiki>. Acesso em: 20 fev. 2013.

ZAPATER, Marcio; SUZUKI, Rodrigo. Segurança da informação um diferencial determinante na competitividade das corporações. **Promon Business & Technology Review**, Rio de Janeiro: Promon, 2005.

APÊNDICES

APÊNDICE A - MODELO DE AVALIAÇÃO DAS ARQUITETURAS DE SEGURANÇA DA INFORMAÇÃO

Grupo 1 – Gestão da Segurança da Informação

Objetivo: Verificar a existência de um código de prática para Gestão da Segurança da Informação.

Indicador: Análise/avaliação de riscos de segurança da Informação

	Situação	Nível
Refere-se à análise/avaliação de riscos periodicamente, para contemplar mudanças nos requisitos de segurança da informação e na situação de risco.	• Há um levantamento periódico dos riscos presentes na organização; • Existem Parâmetros que envolvem o processo das rotinas de backup dos servidores; • Existe uma tabela que defina os níveis dos riscos de segurança da informação em aceitáveis, inaceitáveis e os que possam ser aceitáveis; • É feita a análise e classificação dos riscos inerentes aos sistemas de informação, a fim de evitar ou minimizar danos e prejuízos; • Existem procedimentos contra ataques internos e externos aos sistemas de informação, a fim de evitar perda ou dano em informações importantes à organização.	**5**
	• Há um levantamento periódico dos riscos presentes na organização; • Existem Parâmetros que envolvem o processo das rotinas de backup dos servidores; • Existe uma tabela que defina os níveis dos riscos de segurança da informação em aceitáveis, inaceitáveis e os que possam ser aceitáveis; • Existem procedimentos contra ataques internos e externos aos sistemas de informação, a fim de evitar perda ou dano em informações importantes à organização.	**4**
	• Há um levantamento periódico dos riscos presentes na organização; • Existem procedimentos contra ataques internos e externos aos sistemas de informação, a fim de evitar perda ou dano em informações importantes à organização.	**3**
	• Há um levantamento periódico dos riscos presentes na organização;	**2**
	• Não há nenhum tipo de análise/avaliação de riscos pra a segurança da informação na organização.	**1**

Indicador: Política de Segurança da Informação

	Situação	Nível
Refere-se à existência de políticas de segurança da informação alinhadas com os objetivos do negócio e que demonstre apoio e comprometimento com a segurança da informação.	• Estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos; • Estabelecimento de papeis e responsabilidades para a segurança da informação; • Comunicado à organização sobre a importância de atender aos objetivos de segurança da informação e da conformidade com a política de segurança da informação sobre suas responsabilidades perante as leis; • Necessidade de melhorias contínuas nos sistemas de gestão da segurança da informação; • Prover recursos suficientes para desenvolver, implementar, operar, manter e melhorar o SGSI.	**5**
	• Estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos; • Estabelecimento de papeis e responsabilidades para a segurança da informação; • Comunicado à organização sobre a importância de atender aos objetivos de segurança da informação e da conformidade com a política de segurança da informação sobre suas responsabilidades perante as leis;	**4**
	• Estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos; • Prover recursos suficientes para desenvolver, implementar, operar, manter e melhorar o SGSI.	**3**
	• Estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos;	**2**
	• Não há políticas de segurança da informação alinhadas com os objetivos da organização.	**1**

Indicador: Análise Crítica da Política de Segurança da Informação

	Situação	Nível
Refere-se à existência de uma análise crítica da política de segurança da informação a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar sua contínua pertinência, adequação e eficácia.	• Existe uma análise crítica das políticas, sendo elas revisadas e aprovadas pela alta direção da organização; • É publicado e comunicado a todos os funcionários e parte externa da instituição, quando das modificações nas políticas; • O reconhecimento da validade da política de segurança da informação para a organização; • Verificar se as políticas estão alinhadas com os objetivos de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação de segurança da informação e comunicação. • Verificar se a política serve de base para o desenvolvimento das diretrizes de segurança.	**5**
	• Existe uma análise crítica das políticas, sendo elas revisadas e aprovadas pela alta direção da organização; • É publicado e comunicado a todos os funcionários e parte externa da instituição, quando das modificações nas políticas; • O reconhecimento da validade da política de segurança da informação para a organização;	**4**
	• Existe uma análise crítica das políticas, sendo elas revisadas e aprovadas pela alta direção da organização; • O reconhecimento da validade da política de segurança da informação para a organização;	**3**
	• O reconhecimento da validade da política de segurança da informação para a organização;	**2**
	• Não há uma análise crítica da situação das políticas de segurança da informação.	**1**

Grupo 2 - Gestão de Ativos

Objetivo: Verificar a existência de uma gestão de ativos, visando alcançar e manter a proteção das informações da organização.

Indicador: Inventário dos ativos

	Situação	**Nível**
Refere-se à identificação de todos os ativos tecnológicos e não tecnológicos e a importância destes ativos para a organização.	• É feito um levantamento/atualização dos ativos tecnológicos (*Hardware* e *Software*, equipamentos de rede e mídias); • Existe uma planilha com as principais informações dos computadores; • É feito um levantamento/atualização dos ativos não tecnológicos (pessoas, ambientes e processos); • É feito um levantamento de pessoal com suas respectivas funções dentro da organização. • Há um proprietário designado responsável por cada ativo da organização.	**5**
	• É feito um levantamento/atualização dos ativos tecnológicos (*Hardware* e *Software*, equipamentos de rede e mídias); • Existe uma planilha com as principais informações dos computadores; • É feito um levantamento de pessoal com suas respectivas funções dentro da organização. • Há um proprietário designado responsável por cada ativo da organização.	**4**
	• É feito um levantamento/atualização dos ativos tecnológicos (*Hardware* e *Software*, equipamentos de rede e mídias); • Existe uma planilha com as principais informações dos computadores; • É feito um levantamento de pessoal com suas respectivas funções dentro da organização.	**3**
	• Existe uma planilha com as principais informações dos computadores; • É feito um levantamento de pessoal.	**2**
	• Não é realizado nenhum tipo de levantamento/atualização dos ativos tecnológicos e não tecnológicos.	**1**

Indicador: Uso de Ativos

	Situação	**Nível**
Refere-se à identificação, documentação e implementação de regras que permitem o uso de informações e de ativos associados aos recursos de processamento da informação.	• Há uma política específica de gestão de ativos da organização; • Os ativos são classificados quanto ao seu nível de segurança; • Há um controle de ativos a partir do inventário dos ativos da organização; • São definidos escopos de acesso aos ativos quanto a seu grau de sigilo; • Indicação de responsabilidades quanto ao acesso dos ativos e aos recursos de processamento da informação.	**5**
	• Os ativos são classificados quanto ao seu nível de segurança; • Há um controle de ativos a partir do inventário dos ativos da organização; • São definidos escopos de acesso aos ativos quanto a seu grau de sigilo;	**4**
	• Os ativos são classificados quanto ao seu nível de segurança; • Há um controle de ativos a partir do inventário dos ativos da organização;	**3**
	• Há uma política específica de gestão de ativos da organização;	**2**
	• Não há políticas, regras ou procedimentos que definam o controle ao acesso de ativos na organização implementados.	**1**

Indicador: Classificação da Informação

	Situação	Nível
Refere-se à classificação da informação quanto a sua necessidade, prioridade e nível esperado de proteção quando do tratamento da informação.	• Há políticas para alcançar e manter a proteção adequada os ativos da organização, assegurando que a informação seja classificada de acordo com seu nível adequado de proteção; • Há uma classificação uniformizada para os níveis de segurança das informações que evite sua destruição e revelação indevida; • As informações são classificadas de acordo com seu grau de sigilo, permitindo restrições a acessos indesejados; • Há a implementação de critérios para classificação e marcação de informações e documentos sigilosos; • As informações são armazenadas e acessadas de acordo com sua classificação.	**5**
	• Há uma classificação uniformizada para os níveis de segurança das informações que evite sua destruição e revelação indevida; • As informações são classificadas de acordo com seu grau de sigilo, permitindo restrições a acessos indesejados; • Há a implementação de critérios para classificação e marcação de informações e documentos sigilosos;	**4**
	• Há uma classificação uniformizada para os níveis de segurança das informações que evite sua destruição e revelação indevida; • As informações são classificadas de acordo com seu grau de sigilo, permitindo restrições a acessos indesejados;	**3**
	• As informações são armazenadas e acessadas de acordo com sua classificação.	**2**
	• Não é realizada a classificação dos ativos da organização.	**1**

Grupo 3 – Sistema de Gestão da Segurança da Informação

Objetivo: Verificar a existência de Sistema de Gestão da Segurança da Informação na organização.

Indicador: Implementação de Sistema de Gestão da Segurança da Informação

	Situação	**Nível**
Refere-se à existência do estabelecimento e implementação de um sistema de gestão da segurança da informação, a fim de proteger os ativos da organização.	• Existe um modelo de gestão da segurança da informação com uma sistemática abrangente, integrada e contínua, para minimizar os riscos associados ao tratamento da informação em qualquer área da organização; • Há uma gestão estratégica na adoção de um sistema de gestão da segurança da informação; • O atendimento dos requisitos básicos: entender os requisitos de segurança da organização, implementar e operar controles, monitorar e revisar o desempenho do sistema e melhorar continuamente o SGSI; • Avaliação contínua do sistema de gestão da segurança da informação; • Avaliação dos riscos envolvendo a SGSI.	**5**
	• Existe um modelo de gestão da segurança da informação com uma sistemática abrangente, integrada e contínua, para minimizar os riscos associados ao tratamento da informação em qualquer área da organização; • O atendimento dos requisitos básicos: entender os requisitos de segurança da organização, implementar e operar controles, monitorar e revisar o desempenho do sistema e melhorar continuamente o SGSI; • Avaliação contínua do sistema de gestão da segurança da informação;	**4**
	• O atendimento dos requisitos básicos: entender os requisitos de segurança da organização, implementar e operar controles, monitorar e revisar o desempenho do sistema e melhorar continuamente o SGSI;	**3**
	• Há uma gestão estratégica na adoção de um sistema de gestão da segurança da informação;	**2**
	• Não há implementado e estabelecido nenhum sistema de gestão da segurança da informação.	**1**

Indicador: Monitoramento e análise do Sistema de Gestão da Segurança da Informação

	Situação	**Nível**
Refere-se aos procedimentos de monitoramento e análise crítica do sistema de gestão da segurança da informação, para detectar erros nos resultados de processamento; identificar tentativas de violação de segurança e incidentes de segurança da informação.	• Políticas de monitoramento e análise crítica do SGSI; • Procedimentos que permitem a identificação e detenção de erros nos acessos dos usuários; • Monitoramento de acesso e tentativas de violação física e virtual; • Recursos para recuperação de informações danificadas ou perdidas; • Responsabilidades referentes ao SGSI.	**5**
	• Políticas de monitoramento e análise crítica do SGSI; • Procedimentos que permitem a identificação e detenção de erros nos acessos dos usuários; • Monitoramento de acesso e tentativas de violação física e virtual;	**4**
	• Procedimentos que permitem a identificação e detenção de erros nos acessos dos usuários; • Monitoramento de acesso e tentativas de violação física e virtual;	**3**
	• Políticas de monitoramento e análise crítica do SGSI;	**2**
	• Não há um monitoramento efetivo dos procedimentos executados pelo SGSI.	**1**

Indicador: Melhorias no Sistema de Gestão da Segurança da Informação

	Situação	**Nível**
Refere-se à implementação de melhorias identificadas no sistema de gestão da segurança da informação, assim como executar ações preventivas e corretivas apropriadas e assegurar que as melhorias atinjam os objetivos pretendidos.	• Avaliação crítica do SGSI; • Identificação de falhas no SGSI; • Implementação e execução de ações preventivas e corretivas no SGSI; • Políticas e procedimentos que visam realizar melhorias no SGSI; • Melhoria do SGSI a fim de assegurar o fluxo de informações, sem que essas sejam danificadas ou prejudicadas por danos internos e externos à organização.	**5**
	• Avaliação crítica do SGSI; • Identificação de falhas no SGSI; • Melhoria do SGSI a fim de assegurar o fluxo de informações, sem que essas sejam danificadas ou prejudicadas por danos internos e externos à organização.	**4**
	• Avaliação crítica do SGSI; • Melhoria do SGSI a fim de assegurar o fluxo de informações, sem que essas sejam danificadas ou prejudicadas por danos internos e externos à organização.	**3**
	• Avaliação crítica do SGSI;	**2**
	• Não há análise crítica do SGSI a fim de realizar modificações visando sua melhoria efetiva.	**1**

Grupo 4 - Infraestrutura Tecnológica

Objetivo: Verificar a implantação de infraestrutura de tecnologia de informação e comunicação que atenda as demandas de segurança da informação.

Indicador: *Hardware* para Tecnologias de Informação e Comunicação

	Situação	**Nível**
Refere-se à existência de equipamentos e *Hardware* capaz de suportar a implantação de TIC que auxilie o Sistema de Gestão da informação.	• Existe uma infraestrutura de tecnologia de informação e comunicação que permite a gestão da segurança da informação; • Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação; • Há um plano estratégico relacionado às tecnologias de informação e comunicação; • O *hardware* dos computadores garante a segurança dos sistemas; • Existe uma gestão de infraestrutura tecnológica.	**5**
	• Existe uma infraestrutura de tecnologia de informação e comunicação que permite a gestão da segurança da informação; • Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação; • O *hardware* dos computadores garante a segurança dos sistemas;	**4**
	• Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação; • O *hardware* dos computadores garante a segurança dos sistemas;	**3**
	• Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação;	**2**
	• Não há infraestrutura tecnológica que atenda a demanda de segurança da informação.	**1**

Indicador: *Softwares* para Gestão da Segurança da Informação

	Situação	**Nível**
Refere-se à existência de sistemas computacionais e *softwares* autorizados que permitem a armazenagem, processamento, avaliação de riscos e recuperação de informações de forma que não comprometa a segurança da informação e garanta sua total integridade.	• Existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização; • O *software* instalado/criado permite o armazenamento, organização e processamento das informações com segurança; • O *software* instalado/criado está livre de falhas ou *bugs* que possam gerar vulnerabilidades ao sistema de gestão da segurança da informação como um todo; • Arquitetura da informação amigável ao usuário; • Gestão de falhas e erros relacionados ao processamento de informações, evitando perda ou modificações de informações importantes.	**5**
	• Existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização; • O *software* instalado/criado permite o armazenamento, organização e processamento das informações com segurança; • O *software* instalado/criado está livre de falhas ou *bugs* que possam gerar vulnerabilidades ao sistema de gestão da segurança da informação como um todo;	**4**
	• Existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização; • O *software* instalado/criado permite o armazenamento, organização e processamento das informações com segurança; • Arquitetura da informação amigável ao usuário;	**3**
	• Existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização;	**2**
	• Não há a implantação de um *software* que permita a gestão da segurança da informação na organização.	**1**

Indicador: Serviços de Rede

	Situação	Nível
Refere-se à existência de um provedor de rede para gerenciar serviços de forma segura, isto inclui fornecimento de conexões, serviços de rede privados, redes de valor agregado e soluções de segurança de rede como *firewalls* e sistemas de detecção de intrusos.	• Fornecimento seguro de uma rede de conexão com a internet que permita a transferência de arquivos e informações, sem que essas sejam desviadas ou atacadas por *hacker* ou *cracker*; • Existência de serviços de rede privados que permitem um maior monitoramento da segurança da informação, assim como um servidor especifico para a SGSI; • Antivírus e *firewalls* para detenção de ameaças de *softwares* maliciosos com a intenção de danificar informações; • Sistema e serviços de rede baseado em senhas, certificados e autenticação de usuário; • Políticas que definam os controles de acesso à rede; • Indicação de responsabilidade aos acessos em rede.	**5**
	• Fornecimento seguro de uma rede de conexão com a internet que permita a transferência de arquivos e informações, sem que essas sejam desviadas ou atacadas por *hacker* ou *cracker*; • Antivírus e *firewalls* para detenção de ameaças de *softwares* maliciosos com a intenção de danificar informações; • Sistema e serviços de rede baseado em senhas, certificados e autenticação de usuário;	**4**
	• Fornecimento seguro de uma rede de conexão com a internet que permita a transferência de arquivos e informações, sem que essas sejam desviadas ou atacadas por *hacker* ou *cracker*; • Antivírus e *firewalls* para detenção de ameaças de *softwares* maliciosos com a intenção de danificar informações;	**3**
	• Políticas que definam os controles de acesso à rede;	**2**
	• Não há um sistema de conexão em rede que garanta a segurança dos ativos.	**1**

Grupo 5 - Controle de Acessos

Objetivo: Controlar o acesso às informações, recursos de processamento das informações e processos de negócios.

Indicador: Política de Controle de Acesso

	Situação	**Nível**
Refere-se à existência de políticas de controle de acesso lógico e físico bem como sua análise crítica, tendo como base os requisitos de acesso dos negócios e segurança da informação.	• Existe uma política, regras de controle de acesso que inclua direito dos usuários, recursos, operações, autoridade e domínio de acesso; • Existem diretrizes de controle de acesso físico e lógico aos ativos da organização; • Procedimentos que impeça o acesso ilegal e não autorizado aos sistemas de gestão da segurança da informação; • Indicação de responsabilidade de um controlador de acessos aos ativos para a realização de análise crítica periódica; • Autorização do acesso por meio de senhas, autenticações e certificações de usuário, tanto em meio físico quanto lógico.	**5**
	• Existem diretrizes de controle de acesso físico e lógico aos ativos da organização; • Procedimentos que impeça o acesso ilegal e não autorizado aos sistemas de gestão da segurança da informação; • Indicação de responsabilidade de um controlador de acessos aos ativos para a realização de análise crítica periódica;	**4**
	• Procedimentos que impeça o acesso ilegal e não autorizado aos sistemas de gestão da segurança da informação; • Indicação de responsabilidade de um controlador de acessos aos ativos para a realização de análise crítica periódica;	**3**
	• Existe uma política, regras de controle de acesso que inclua direito dos usuários, recursos, operações, autoridade e domínio de acesso;	**2**
	• Não existem políticas, procedimentos, diretrizes, regras e análise crítica envolvendo controles de acesso a ativos da organização.	**1**

Indicador: Gerenciamento de acesso de usuários

	Situação	Nível
Refere-se ao acesso aos sistemas de segurança da informação por usuários autorizados, a fim de prevenir acessos não autorizados e evitar violação de informações importantes à organização, tal como verificar procedimentos que cubram todas as fases do ciclo de vida de acesso do usuário, da inscrição inicial como novos usuários até o cancelamento final do registro de usuários que já não requerem acesso a sistemas de informação e serviços.	• Gestão e monitoramento de acessos de usuários; • Inscrição de usuários autorizados e identificação dos ativos que este pode acessar; • Bloqueio de acesso a usuários não autorizados; • Criação de senhas, login, autenticação e certificação de usuários aos sistemas de gestão da segurança da informação e restrição de acesso a documentos armazenados em espaços físicos como arquivos, etc.; • Exclusão de dados de usuários assim como bloqueio de senha, após este não possuir mais acesso livre a determinados ativos.	**5**
	• Gestão e monitoramento de acessos de usuários; • Bloqueio de acesso a usuários não autorizados; • Criação de senhas, login, autenticação e certificação de usuários aos sistemas de gestão da segurança da informação e restrição de acesso a documentos armazenados em espaços físicos como arquivos, etc.; • Exclusão de dados de usuários assim como bloqueio de senha, após este não possuir mais acesso livre a determinados ativos.	**4**
	• Gestão e monitoramento de acessos de usuários; • Inscrição de usuários autorizados e identificação dos ativos que este pode acessar; • Bloqueio de acesso a usuários não autorizados;	**3**
	• Inscrição de usuários autorizados e identificação dos ativos que este pode acessar;	**2**
	• Não há controle e monitoramento de acesso de usuários autorizados aos ativos da organização.	**1**

Indicador: Controle de Acesso à rede e a sistemas operacionais

	Situação	**Nível**
Refere-se à prevenção de acessos não autorizados aos serviços de redes, sendo necessário o controle interno e externo de acesso a serviços de rede, assim como a prevenção de acesso não autorizado aos sistemas operacionais, convém que recursos de segurança da informação sejam usados para restringir o acesso aos sistemas operacionais para usuários não autorizados.	• Sistemas operacionais e conexões de redes acessadas mediante identificação do usuário; • Listas de acesso contemplando usuários que possuem privilégios de uso de ativos e os que não podem acessar os sistemas e redes da organização; • Políticas que definam os direitos de acesso aos usuários de sistemas e redes; • Indicação de responsabilidade para controlar os acessos aos sistemas operacionais e as redes de conexão da organização; • Avaliar e monitorar os acessos diariamente, a fim de evitar danos aos ativos da organização.	**5**
	• Sistemas operacionais e conexões de redes acessadas mediante identificação do usuário; • Políticas que definam os direitos de acesso aos usuários de sistemas e redes; • Indicação de responsabilidade para controlar os acessos aos sistemas operacionais e as redes de conexão da organização; • Avaliar e monitorar os acessos diariamente, a fim de evitar danos aos ativos da organização.	**4**
	• Sistemas operacionais e conexões de redes acessadas mediante identificação do usuário; • Avaliar e monitorar os acessos diariamente, a fim de evitar danos aos ativos da organização.	**3**
	• Sistemas operacionais e conexões de redes acessadas mediante identificação do usuário;	**2**
	• Não há controle de acesso aos sistemas operacionais e a rede de conexão com a internet na organização.	**1**

APÊNDICE B – ROTEIRO DE ENTREVISTA ORIENTADA

INSTITUIÇÃO:
ENDEREÇO:
COORDENADOR:
ÁREA DE ATUAÇÃO:
CONTATO:

GRUPO 1 - Gestão da Segurança da Informação			
INDICADOR 1 - Análise/Avaliação de Riscos de Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há um levantamento periódico dos riscos presentes na organização?			
2. Existem Parâmetros que envolvem o processo das rotinas de backup dos servidores?			
3. Existe uma tabela que defina os níveis dos riscos de segurança da informação em aceitáveis, inaceitáveis e os que possam ser aceitáveis?			
4. É feita a análise e classificação dos riscos inerentes aos sistemas de informação, a fim de evitar ou minimizar danos e prejuízos?			
5. Existem procedimentos contra ataques internos e externos aos sistemas de informação, a fim de evitar perda ou dano em informações importantes à organização?			

NOTAS:

GRUPO 1 - Gestão da Segurança da Informação			
INDICADOR 2 - Política de Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe o estabelecimento de uma política de segurança da informação garantindo que os planos e objetivos de segurança da informação sejam estabelecidos?			
2. Existe o estabelecimento de papeis e responsabilidades para a segurança da informação?			
3. Há o comunicado à organização sobre a importância de atender aos objetivos de segurança da informação e da conformidade com a política de segurança da informação sobre suas responsabilidades perante as leis?			
4. Há a necessidade de melhorias contínuas nos sistemas de gestão da segurança da informação?			
5. Há recursos suficientes para desenvolver, implementar, operar, manter e melhorar o Sistema de Gestão da Segurança da Informação?			

NOTAS:

GRUPO 1 - Gestão da Segurança da Informação			
INDICADOR 3 - Análise Crítica da Política de Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe uma análise crítica das políticas, sendo elas revisadas e aprovadas pela alta direção da organização?			
2. É publicado e comunicado a todos os funcionários e parte externa da instituição, quando das modificações nas políticas?			
3. Há o reconhecimento da validade da política de segurança da informação para a organização?			
4. As políticas estão alinhadas com os objetivos de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação de segurança da informação e comunicação?			
5. A política serve de base para o desenvolvimento das diretrizes de segurança?			

NOTAS:

GRUPO 2 - Gestão de Ativos			
INDICADOR 1 - Inventário dos Ativos			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. É feito um levantamento/atualização dos ativos tecnológicos (*Hardware* e *Software*, equipamentos de rede e mídias)?			
2. Existe uma planilha com as principais informações dos computadores?			
3. É feito um levantamento/atualização dos ativos não tecnológicos (pessoas, ambientes e processos)?			
4. É feito um levantamento de pessoal com suas respectivas funções dentro da organização?			
5. Há um proprietário designado responsável por cada ativo da organização?			

NOTAS:

GRUPO 2 - Gestão de Ativos			
INDICADOR 2 - Uso de Ativos			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há uma política específica de gestão de ativos da organização?			
2. Os ativos são classificados quanto ao seu nível de segurança?			
3. Há um controle de ativos a partir do inventário dos ativos da organização?			
4. São definidos escopos de acesso aos ativos quanto a seu grau de sigilo?			
5. Há indicação de responsabilidades quanto ao acesso dos ativos e aos recursos de processamento da informação?			

NOTAS:

GRUPO 2 - Gestão de Ativos			
INDICADOR 3 - Classificação da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há políticas para alcançar e manter a proteção adequada dos ativos da organização, assegurando que a informação seja classificada de acordo com seu nível adequado de proteção?			
2. Há uma classificação uniformizada para os níveis de segurança das informações que evite sua destruição e revelação indevida?			
3. As informações são classificadas de acordo com seu grau de sigilo, permitindo restrições a acessos indesejados?			
4. Há a implementação de critérios para classificação e marcação de informações e documentos sigilosos?			
5. As informações são armazenadas e acessadas de acordo com sua classificação?			

NOTAS:

GRUPO 3 - Sistema de Gestão da Segurança da Informação			
INDICADOR 1 - Implementação de Sistema de Gestão da Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe um modelo de gestão da segurança da informação com uma sistemática abrangente, integrada e contínua, para minimizar os riscos associados ao tratamento da informação em qualquer área da organização?			
2. Há uma gestão estratégica na adoção de um sistema de gestão da segurança da informação?			
3. Há o atendimento dos requisitos básicos: entender os requisitos de segurança da organização, implementar e operar controles, monitorar e revisar o desempenho do sistema e melhorar continuamente o Sistema de Gestão da Segurança da Informação?			
4. Há uma avaliação contínua do sistema de gestão da segurança da informação?			
5. Há uma avaliação dos riscos envolvendo o Sistema de Gestão da Segurança da Informação?			

NOTAS:

GRUPO 3 - Sistema de Gestão da Segurança da Informação			
INDICADOR 2 - Monitoramento e Análise do Sistema de Gestão da Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há políticas de monitoramento e análise crítica do Sistema de Gestão da Segurança da Informação?			
2. Há procedimentos que permitem a identificação e detenção de erros nos acessos dos usuários?			
3. Há monitoramento de acesso e tentativas de violação física e virtual?			
4. Existem recursos para recuperação de informações danificadas ou perdidas?			
5. Existem responsabilidades referentes ao Sistema de Gestão da Segurança da Informação?			

NOTAS:

GRUPO 3 - Sistema de Gestão da Segurança da Informação			
INDICADOR 3 - Melhorias no Sistema de Gestão da Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há uma avaliação crítica do Sistema de Gestão da Segurança da Informação?			
2. Há identificação de falhas no Sistema de Gestão da Segurança da Informação?			
3. Há implementação e execução de ações preventivas e corretivas no Sistema de Gestão da Segurança da Informação?			
4. Existem políticas e procedimentos que visam realizar melhorias no Sistema de Gestão da Segurança da Informação?			
5. Existe melhoria do Sistema de Gestão da Segurança da Informação a fim de assegurar o fluxo de informações, sem que essas sejam danificadas ou prejudicadas por danos internos e externos à organização?			

NOTAS:

GRUPO 4 - Infraestrutura Tecnológica			
INDICADOR 1 - *Hardware* para Tecnologias de Informação e Comunicação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe uma infraestrutura de tecnologia de informação e comunicação que permite a gestão da segurança da informação?			
2. Os computadores da organização são compatíveis com os requisitos mínimos para implantação do *software* de gestão da segurança da informação?			
3. Há um plano estratégico relacionado às tecnologias de informação e comunicação?			
4. O *hardware* dos computadores garante a segurança dos sistemas?			
5. Existe uma gestão de infraestrutura tecnológica?			

NOTAS:

GRUPO 4 - Infraestrutura Tecnológica			
INDICADOR 2 - *Softwares* para Gestão da Segurança da Informação			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe um *software* instalado/criado para a gestão da segurança da informação que atenda as necessidades da organização?			
2. O *software* instalado/criado permite o armazenamento, organização e processamento das informações com segurança?			
3. O *software* instalado/criado está livre de falhas ou *bugs* que possam gerar vulnerabilidades ao sistema de gestão da segurança da informação como um todo?			
4. A arquitetura da informação é amigável ao usuário?			
5. Há uma gestão de falhas e erros relacionados ao processamento de informações, evitando perda ou modificações de informações importantes?			

NOTAS:

GRUPO 4 - Infraestrutura Tecnológica			
INDICADOR 3 - Serviços de Rede			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há fornecimento seguro de uma rede de conexão com a internet que permita a transferência de arquivos e informações, sem que essas sejam desviadas ou atacadas por *hacker* ou *cracker?*			
2. Existem serviços de rede privados que permitem um maior monitoramento da segurança da informação, assim como um servidor específico para o Sistema de Gestão da Segurança da Informação?			
3. Existem antivírus e *firewalls* para detenção de ameaças de *softwares* maliciosos com a intenção de danificar informações?			
4. Há sistema e serviços de rede baseado em senhas, certificados e autenticação de usuário?			
5. Há políticas que definam os controles de acesso e indicação de responsabilidade a estes acessos à rede?			

NOTAS:

GRUPO 5 - Controle de Acessos			
INDICADOR 1 - Política de Controle de Acesso			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existe uma política, regras de controle de acesso que inclua direito dos usuários, recursos, operações, autoridade e domínio de acesso?			
2. Existem diretrizes de controle de acesso físico e lógico aos ativos da organização?			
3. Há procedimentos que impeça o acesso ilegal e não autorizado aos sistemas de gestão da segurança da informação?			
4. Há indicação de responsabilidade de um controlador de acessos aos ativos para a realização de análise crítica periódica?			
5. Há autorização do acesso por meio de senhas, autenticações e certificações de usuário, tanto em meio físico quanto lógico?			

NOTAS:

GRUPO 5 - Controle de Acessos			
INDICADOR 2 - Gerenciamento de Acesso de Usuários			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Há uma gestão e monitoramento de acessos de usuários?			
2. Existe uma inscrição de usuários autorizados e identificação dos ativos que este pode acessar?			
3. Existe bloqueio de acesso a usuários não autorizados?			
4. Existe a criação de senhas, login, autenticação e certificação de usuários aos sistemas de gestão da segurança da informação e restrição de acesso a documentos armazenados em espaços físicos como arquivos, etc.?			
5. Há exclusão de dados de usuários assim como bloqueio de senha, após este não possuir mais acesso livre a determinados ativos?			

NOTAS:

GRUPO 5 - Controle de Acessos			
INDICADOR 3 - Controle de Acesso à Rede e a Sistemas Operacionais			
PERGUNTAS	**SIM**	**NÃO**	**NÃO APLICÁVEL**
1. Existem sistemas operacionais e conexões de redes acessadas mediante identificação do usuário?			
2. Existem listas de acesso contemplando usuários que possuem privilégios de uso de ativos e os que não podem acessar os sistemas e redes da organização?			
3. Há políticas que definam os direitos de acesso aos usuários de sistemas e redes?			
4. Há indicação de responsabilidade para controlar os acessos aos sistemas operacionais e as redes de conexão da organização?			
5. Há uma avaliação e monitoramento aos acessos diariamente, a fim de evitar danos aos ativos da organização?			

NOTAS: