UNIVERSIDADE FEDERAL DO PARANÁ

LENÍSIA CRISTINA MENDES MONTEIRO

PROCESSO DE PREPARAÇÃO PARA CERTIFICAÇÃO DA QUALIDADE EM SEGURANÇA DA INFORMAÇÃO

CURITIBA

2010

LENÍSIA CRISTINA MENDES MONTEIRO

PROCESSO DE PREPARAÇÃO PARA CERTIFICAÇÃO DA QUALIDADE EM SEGURANÇA DA INFORMAÇÃO

Monografia apresentada à Disciplina de Pesquisa em Informação (SIN 119), como requisito parcial à conclusão do Curso de Bacharelado em Gestão da Informação, Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná.

Orientador: Prof. Mauro José Belli, Dr.

CURITIBA

2010

FOLHA DE APROVAÇÃO

LENÍSIA CRISTINA MENDES MONTEIRO

PROCESSO DE PREPARAÇÃO PARA CERTIFICAÇÃO DA QUALIDADE EM SEGURANÇA DA INFORMAÇÃO

Monografia aprovado como requisito parcial para obtenção do grau de bacharel no Curso de Gestão da Informação, Setor de Ciências Sociais e Aplicadas da Universidade Federal do Paraná, pela seguinte banca examinadora:

_____

Prof. Dr. Mauro José Belli - Orientador
Departamento de Ciência e Gestão da Informação, UFPR

_____

Prof. Dr. Edelvino Razzolini Filho - Membro
Departamento de Ciência e Gestão da Informação, UFPR

_____

Prof. Dr. Egon Walter Wildauer - Membro
Departamento de Ciência e Gestão da Informação, UFPR

Curitiba, 8 de Dezembro de 2010.

Dedico este trabalho,
Aos meus pais Maria e Manuel, aos meus irmãos e a minha sobrinha Jéssica.
Por todo o amor que nos une.

AGRADECIMENTOS

Primeiramente quero agradecer a Deus pela vida, por tudo de bom que ele me proporcionou ao longo do tempo.

Aos meus pais Maria e Manuel pela força, e por todo o apoio dado ao longo de toda a minha vida, pela oportunidade que eles me deram, sem vocês não estaria aqui.

Ao meu professor Mauro José Belli, pelo apoio, disponibilidade, confiança e atenção para que eu pudesse alcançar os objetivos do trabalho.

Aos meus irmãos pelo carinho e apoio dado, em especial à minha irmã Ivanilda que esteve presente apoiando, incentivando e amparando nos momentos de maior dificuldade.

Aos meus colegas e amigos que me auxiliaram e apoiaram em todos os momentos dessa caminhada.

Ao Senhor Roberto Melo representante da administração da DQS pelo apoio dado, na disponibilização do material técnico.

A todos que de forma direta ou indireta me apoiaram e incentivaram para que mais um objetivo da minha vida se concretizasse.

Muito Obrigada!

“È impossível avaliar a força que possuímos sem medir o tamanho do obstáculo que podemos vencer, nem o valor de uma ação sem sabermos o sacrifício que ela comporta.”

H. W. Belcher

RESUMO

A Segurança da Informação tem como objetivo principal garantir a confidencialidade, privacidade, disponibilidade, temporalidade e autenticidade dos dados, mitigando os riscos para garantia da competitividade da organização. Para qualquer organização é fundamental garantir que os seus ativos informacionais sejam protegidos, para isso deverão ser adotadas medidas de segurança. Neste intuito, o trabalho apresenta um processo de preparação para certificação da qualidade em Segurança da Informação. O trabalho está dividido em introdução, literatura pertinente, apresentação, análise dos resultados e conclusões. Na introdução apresenta-se a problemática em estudo, a justificativa, os objetivos, e a estrutura do trabalho. A literatura pertinente abrangeu assuntos relacionados à Segurança da Informação baseando-se em publicações técnicas e científicas da área. Para realização do trabalho, utilizou-se o método de pesquisa qualitativa, descritiva, documental e bibliográfica. Por meio dessas técnicas foram pesquisados dados, que posterior a análise, foram compilados de forma a apresentar um processo de preparação para certificação. Nos resultados, apresentou-se um processo composto das seguintes etapas: Auto-avaliação dos aspetos referente à Segurança da Informação, Política de Segurança da Informação, Sistema de Gerenciamento de Segurança da Informação, Modelos de Referência e Auditoria Interna. Por meio do processo apresentado, conclui-se que é importante ter conhecimento à cerca das normas de certificação, porém não é suficiente. É necessário também conhecer detalhadamente a organização.

Palavras – chave: Segurança da Informação. Normas técnicas de segurança da Informação. Certificação. Qualidade.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

BSI - British Standard Institute

COBIT - Control Objetives for Information and Related Technology

DQS - Manegement Systems Solutions

IEC - International Electrotechnical Commission.

ISACF - Information System Audit and Control Foundation

ISMS - Information Security Management System

ISO - International Organization for Standardization

ITIL - Information Technologie Infrastructure Library

NBR - Norma Brasileira

PDCA - Plan Do Check Act

PSI - Política de Segurança da Informação

SGSI - Sistema de Gestão de Segurança da informação

SWOT - Strenghts Weaknesses Opportunities Threats

TI - Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

O uso das tecnologias de informação e comunicação associado à disponibilidade da internet nas organizações tem gerado muitas vantagens para elas, porém o uso descontrolado das mesmas tem apresentado desvantagens. A internet é um meio para solução de inúmeros problemas organizacionais, garantindo principalmente a comunicação dentro e fora da organização, entretanto se usado de forma desordenada traz desvantagens principalmente no que diz respeito à salvaguarda dos ativos informacionais da organização. Com isto surge a necessidade de garantir a integridade desses ativos usados pela organização para que ela possa agregar valor e assim gerar vantagem competitiva. Para suprir essa necessidade surge a Segurança da Informação. Ela apresenta-se como um diferencial competitivo principalmente na área financeira, onde empresas centralizam grandes volumes de informações estratégicas, sendo assim a Segurança da Informação é de fundamental importância para a proteção do negócio.

A segurança da informação propõe um conjunto de técnicas e ferramentas para a gestão de risco e garantia de continuidade das atividades da organização.

A NBR ISO/IEC 17799 (2001, p. 2) afirma que a Segurança da Informação: “protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio”.

Segurança da Informação pode ser entendida como “o processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade.” (BEAL, 2005, p.1)

O trabalho apresentado tem como finalidade a descrição do processo de certificação da qualidade na área de segurança da informação.

Para a realização deste trabalho, primeiramente foi realizado um levantamento de dados da área, tais como, normas, empresas certificadoras e empresas que preparam para a certificação, os processos de auditoria entre outros. E em um segundo momento foi elaborado um documento apresentando as etapas que uma organização deverá seguir para obter certificação na área de qualidade da informação.

1.1. PROBLEMA

O problema a ser estudado é a **ausência de uma orientação estruturada para auxiliar as organizações que pretendem obter a certificação de qualidade na área de Segurança da Informação**. As organizações procuram adotar medidas de segurança a fim de proteger os seus ativos informacionais contra danos, perdas, acessos não autorizados ou extravios. Entretanto, grandes quantidades de dados a cerca da Segurança da Informação estão disponíveis na internet, porém elas estão de forma desorganizada, incompletas e repetitivas não oferecendo a necessária orientação de que a organização necessita.

1.2. OBJETIVOS

Os itens abaixo descrevem os objetivos do projeto de pesquisa. O trabalho é composto por seis objetivos sendo um geral e cinco específicos.

1.2.1. Objetivo geral

Apresentar um processo de preparação para certificação da qualidade na área de Segurança da Informação.

1.2.2. Objetivos Específicos

a) identificar as normas de certificação da qualidade em Segurança da Informação;
b) escolher as normas indicadas para a solução do problema proposto;

c) levantar os requisitos para possibilitar a certificação da organização na área de Segurança da Informação;

d) descrever o processo de preparação para certificação da qualidade em Segurança da Informação;

e) identificar algumas empresas certificadoras e que capacitam para certificação.

1.3. JUSTIFICATIVA

É muito importante que as organizações garantem a segurança dos seus ativos informacionais, pois estes constituem uma arma fundamental para o posicionamento estratégico e garantia da continuidade do negócio. A informação e os dados que a organização detém apresentam-se como um ativo extremamente importante. É utilizada na tomada de decisões importantes as quais colocam a “vida” da organização em risco, portanto essas informações deverão apresentar um determinado nível de confiabilidade para então serem utilizadas.

Na sociedade de informação atualmente vivida, a sobrevivência de diferentes tipos de organizações está exigindo cada vez mais o uso de informações certas no momento certo e sendo utilizadas por usuários autorizados. Para que isso aconteça é necessário que ela esteja capacitada no uso de técnicas e ferramentas relativas à salvaguarda das informações privativas.

A organização tem a necessidade de proteger as suas informações tanto de ameaças externas tais como concorrentes, e de ameaças internas oriundas de funcionários insatisfeitos, colaboradores entre outros. Para superar essas ameaças surge a necessidade de utilizar práticas e técnicas de Segurança da Informação. A Segurança da Informação dá apoio às organizações disponibilizando técnicas e ferramentas para:

a) controle de acesso;

b) segurança do ambiente lógico;

c) segurança do ambiente físico;

d) elaboração de políticas de segurança;

e) prevenção e tratamento de incidentes;

f) detecção de vulnerabilidades, gestão da continuidade de negócios entre outros.

A elaboração de um processo contendo as orientações para a certificação da qualidade na área de Segurança da Informação servirá como uma base de apoio às organizações que pretendem ser certificadas, minimizando desperdícios de tempo procurando por informações sobre o assunto na internet. Informações essas que se encontram de forma dispersa e desorganizada, dificultando o alcance do objetivo ao invés de ajudar.

O estudo sobre a certificação da qualidade em segurança da informação é viável por apresentar informações sólidas e estruturadas sobre o assunto oferecendo às organizações, que queiram obter a certificação, uma orientação efetiva.

1.4. ESTRUTURA DO TRABALHO

O trabalho encontra-se divido em cinco capítulos. No primeiro foi realizada uma introdução sobre o tema, nela foi exposto o problema a ser estudado, os objetivos do trabalho, a justificativa e também a estrutura do presente trabalho. No segundo capítulo foi feito a revisão da literatura, o assunto principal é a Segurança da Informação. Primeiramente foi definido o que é a Segurança da Informação, os tipos de segurança, as normas de segurança da informação. Em seguida foram abordados os seguintes temas: Políticas de Informação e Metodologias para representação de processos.

No terceiro capitulo foram descritos os procedimentos metodológicos utilizados, assim foi apresentado o tipo de pesquisa usado para elaboração do trabalho, os tipos de análise realizada quanto aos fins e quanto aos meios e por último foi apresentado a forma de análise e tratamento dos dados.

Feito isto, no quarto capítulo foram feitas a apresentação e análise dos resultados da pesquisa. Nele foi descrito o processo de preparação para certificação

da qualidade em Segurança da Informação, que engloba etapas como auto-avaliação dos aspetos de segurança das organizações por meio de análise de SWOT - Strenghts Weaknesses Opportunities Threats, elaboração de uma Política de Segurança da Informação (PSI), implementação do Sistema de Gestão de Segurança da informação (SGSI), auxilio á modelos externos e por última auditoria das etapas anteriormente apresentadas. Em seguida apresentou-se a análise dos resultados neste foram feitas comparações entre os processos identificando os principais pontos em comum entre as duas.

As considerações finais e recomendações para trabalhos futuros fazem parte do último capítulo, onde foi feito uma breve abordagem do que foi apresentado e recomendações para novos estudos em Segurança da Informação especificamente no que diz respeito ao processo de preparação para certificação.

2. REVISÃO DE LITERATURA

O capítulo que se segue apresenta conceitos relacionados à Segurança da Informação e em seguida são abordadas as normas, mais especificamente a ISO/IEC 27001, ISO/IEC 27002 e a ISO/IEC 27005 que são os objetos do estudo proposto. Por último foi feito uma abordagem sobre Políticas de Informação e metodologias para representação de processos com foco em qualidade.

2.1 SEGURANÇA DA INFORMAÇÃO

De acordo com a literatura revisada Segurança da Informação pode ser definida como o conjunto de ferramentas e técnicas utilizadas com o objetivo de proteger ativos informacionais contra danos e acesso não autorizado.

> Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada. (FONTES, 2006 p.11).

A segurança da informação poderá ser física ou lógica. A Segurança física tem como objetivo “prevenir acesso não autorizado, dano e interferência às informações e instalações físicas da organização” (NBR ISO/IEC 17799: 2001 p.13). A Segurança do ambiente lógico preocupa com a segurança das redes devendo abranger os problemas de autenticação de usuários e equipamentos e de restrição do acesso dos usuários aos serviços autorizados, contemplando o estabelecimento de interfaces seguras entre a rede interna e a rede pública ou de outra organização (LYRA, 2008, p.33). Para que haja a proteção dos ativos informacionais é necessário que exista uma combinação das medidas de segurança.

Segundo Imoniana (2005), medidas de segurança em ambiente físico visam proteger os escritórios, salas, instalações de processamento, proteção de documentos em papel, proteção de mídias de computadores; medidas de segurança

lógica preocupam com a proteção contra softwares maliciosos, segurança das comunicações eletrônicas, correio eletrônico e segurança do comércio eletrônico.

Para que seja garantida a segurança das informações da organização deverá haver um conjunto de normas que irão dar apoio ao desenvolvimento de processos para a segurança da organização. As seções que se seguem apresentam o processo de desenvolvimento das normas de certificação e em seguida alguns exemplos de normas para a segurança da informação.

2.2 PROCESSO DE DESENVOLVIMENTO DAS METODOLOGIAS DE CERTIFICAÇÃO

Inicialmente foi elaborada a norma BS7799 pela BSI (*British Standard Institute*), esta norma permite a implementação de sistemas de gestão de segurança baseados em controles definidos por normas e práticas de segurança.

A BS7799 foi concebida como sendo uma tecnologia “neutra” em termos de sistema de gestão, independente de fornecedor que corretamente aplicado, permitirá a gestão de uma organização assegurando que as medidas de segurança da informação são eficazes. A BS7799 objetiva proteger a disponibilidade, confidencialidade e integridade da informação da organização.

A norma BS7799 está dividida em três partes:

a) parte 1 que trata da tecnologia da informação;
b) parte 2 que diz respeito à especificação do ISMS (*Information Security Management System*); e
c) parte 3 que trata da gestão de riscos.

Segundo Beal (2005, p.33) a parte 1 da norma corresponde a um “código de boas práticas para gestão da segurança da informação”, tornou-se padrão internacional pela ISO sob o nome ISO/IEC 17799, no Brasil foi publicada pela ABNT com o código NBR ISO/IEC 17799. Com crescimento do número de

organizações que começaram a reconhecer a necessidade de garantir a Segurança da Informação e proteger os dados, surgiu a necessidade de se obter certificação e assim surgiu a segunda parte da BS7799 numerada como BS7799-2 (ou, parte 2).

A BS 7799-2 especifica uma série de processos voltados para garantir não só a avaliação e tratamento de riscos, mas também a revisão e melhorias dos processos para garantir que o ISMS seja atualizado frente às mudanças do ambiente de negócios e seus efeitos na organização. A BS 7799-2 oferece certificação. (BEAL, 2005 p.33)

Em outubro de 2005 a BS 7799 parte 2 foi adotado pela ISO e re-identificado, iniciando a nova série 27000 de padrões internacionais para segurança da informação lançada como norma ISO/IEC 27001:2005.

A parte 3 da BS7799 estabece diretrizes para gerenciamento de risco. Ela dá orientação para apoiar os requisitos indicados na ISO / IEC 27001:2005 em todos os aspectos de um Sistema de Gestão de Segurança da Informação (SGSI). Isso inclui a avaliação dos riscos, implementação de controles para tratar os riscos, monitoramento e análise dos riscos, e a manutenção e melhoria do sistema de controles de risco.

2.3 NORMAS E METODOLOGIAS PARA SEGURANÇA DA INFORMAÇÃO

As normas garantem que os processos sejam desenvolvidos em conformidade com o padrão de referência de qualidade aumentando assim a eficiência, eficácia e confiabilidade dos mesmos.

Algumas normas para a segurança da informação são exemplificadas a seguir:

a) BS 7799

b) ISO Guide 73 (*Risk Manegement – vocabulary – guidelines for use in Standards*)

c) ISO 13335 (*Guidelines Form the Manegement of IT Institute*)

d) NBR ISO/IEC 17799:2001

e) NBR ISO/IEC 27001:2006

f) NBR ISO/IEC 27002:2005

g) ISO/IEC 27005:2008

Como exemplos de metodologias de certificação têm:

a) ITIL (*Information Technologie Infrastructure Library*)

b) COBIT (*Control Objetives for Information and Related Technology*)

Para atender ao objetivo proposto foram abordadas as seguintes normas: NBR ISO/IEC 27001, NBR ISO/IEC 27002 e a ISO/IEC 27005.

As subseções que se seguem descrevem as normas especificando o objetivo de cada uma delas e descrevendo a sua aplicação.

2.3.1 Grupo de normas ISO/IEC 27000

A figura abaixo esquematiza a origem das normas da família 27000. Algumas delas tiveram a sua origem na BS7799, ou seja, esta norma serviu de modelo para criação de todas as outras normas complementares sobre Segurança da Informação, desde o desenvolvimento de uma medida ou política até a medição de sua eficácia.

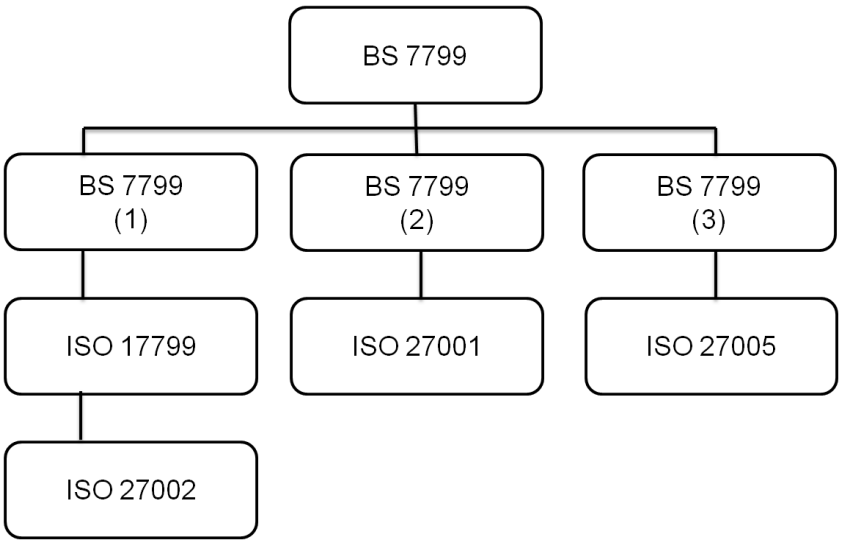

FIGURA 1 - REPRESENTAÇÃO ESQUEMÁTICA DAS NORMAS DE SEGURANÇA DA INFORMAÇÃO
FONTE: A AUTORA (2010)

a) **ISO/IEC 27000** Tecnologia da informação - técnicas da segurança - sistemas de gestão da segurança da informação – vocabulário

Esta norma objetiva apresentar o vocabulário e definições referentes à Segurança da Informação para serem utilizadas pelas outras normas, ela ainda apresenta um breve histórico sobre o Sistema de Gerenciamento de Segurança da Informação (SGSI) destacando a sua importância e como implementá-lo nas organizações. (ISO-IEC 27000, 2009)

b) **ISO/IEC 27001** Tecnologia da informação — técnicas de segurança — sistemas de gestão de segurança da informação — requisitos

Esta norma especifica as exigências para estabelecer, executar, operar, monitorar, rever, manter e melhorar um sistema de gestão de segurança (SGSI), para isso ela faz uso do modelo PDCA – "*Plan-Do-Check-Act".* (ISO-IEC 27000, 2009)

c) **ISO/IEC 27002** Tecnologia da informação - técnicas da segurança - código de prática para a gerência da segurança da informação

Atual ISO 17799 define boas práticas para a gestão da Segurança da Informação. Esta norma fornece orientação na execução de controles da Segurança da Informação. (ISO-IEC 27000, 2009)

d) **ISO/IEC 27003** Tecnologia da informação - técnicas da segurança - orientação para execução do sistema de gestão da segurança da informação

Guia para implementação de um SGSI, esta norma fornece orientação prática para executar, monitorar, rever, manter e melhorar o SGSI de acordo com a ISO/IEC 27001. (ISO-IEC 27000, 2009)

e) **ISO/IEC 27004** Tecnologia da informação - técnicas da segurança - gerência da segurança da informação – medida

Esta norma fornece orientação e o conselho no desenvolvimento e no uso das medidas a fim avaliar a eficácia do SGSI, dos objetivos de controle, e dos controles usados para executar e controlar a Segurança da Informação, como

especificado na ISO/IEC 27001. Define métricas e meios de medição para avaliar a eficácia de um SGSI. (ISO-IEC 27000, 2009)

f) **ISO/IEC 27005** Tecnologia da informação - técnicas da segurança - gestão de riscos da segurança da informação
Atual BS 7799-3 define linhas de orientação para a gestão do risco da segurança da informação. Esta norma fornece diretrizes para a gestão de riscos da segurança da informação, sendo que os aspectos descritos nela estão de acordo com os conceitos especificados na ISO/IEC 27001. (ISO-IEC 27000, 2009)

g) **ISO/IEC 27006** Tecnologia da informação - técnicas da segurança - exigências para as organizações que fornecem o exame e a certificação de sistemas de gestão da segurança da informação.
Esta norma apresenta os requisitos para a acreditação de organizações que oferecem serviços de certificação de sistemas de gestão da Segurança da Informação. (ISO-IEC 27000, 2009)

h) **ISO/IEC 27007** Tecnologia da informação - técnicas da segurança - diretrizes para o exame dos Sistemas de Gestão da Segurança da Informação
Fornece orientação em exames de condução do SGSI, assim como a orientação na competência de revisores de contas do Sistemas de Gestão da Segurança da Informação. (ISO-IEC 27000, 2009)

i) **ISO/IEC 27011** Tecnologia da informação - técnicas da segurança - diretrizes da gerência da segurança da informação para as organizações das telecomunicações baseadas em ISO/IEC 27002
Fornece as diretrizes que suportam a execução da SGSI em organizações das telecomunicações. (ISO-IEC 27000, 2009)

j) **ISO/IEC 27799** Informática da saúde - gerência da segurança da informação na saúde usando ISO/IEC 27002

Fornece as diretrizes que suportam a execução SGSI em organizações de saúde. (ISO-IEC 27000, 2009)

2.3.2 ABNT NBR ISO/IEC 27001

A norma ABNT NBR ISO/IEC 27001 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

Esta norma adota o modelo conhecido como PDCA "*Plan-Do-Check-Act*", que é aplicado para estruturar todos os processos do SGSI.

Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes (ABNT NBR ISO/IEC 27001). A ABNT NBR ISO/IEC 27001 é composta pelos seguintes itens:

a) termos e definições

b) sistema de gestão de segurança da informação

c) responsabilidades da direção

d) auditorias internas do SGSI

e) análise crítica do SGSI pela direção

f) melhoria do SGSI

A norma ABNT NBR ISO/IEC 27001 estabelece o ciclo PDCA como método para implementação do SGSI. A subseção que se segue objetiva a descrição do modelo PDCA e de como ele é utilizado na implementação do SGSI segundo a ABNT NBR ISO/IEC 27001.

2.3.2.1 Ciclo PDCA

O Ciclo PDCA é um método utilizado em processos de gestão da qualidade que se aplica aos mais diversos tipos e níveis de gestão, é útil para fornecer uma visualização global das etapas que devem compor a gestão da segurança da informação (BEAL, 2005 p. 37).

P – Planejar - estabelecer os objetivos e processos necessários para fornecer resultados de acordo com os requisitos e políticas pré-determinados.

D - Fazer - implementar as ações necessárias.

C – Checar - monitorar e medir os processos e produtos em relação às políticas, aos objetivos e aos requisitos estabelecidos e relatar os resultados.

A – Agir – executar ações para promover continuamente a melhoria dos processos.

A figura abaixo apresenta o processo de implementação de um SGSI de acordo com o modelo PDCA.

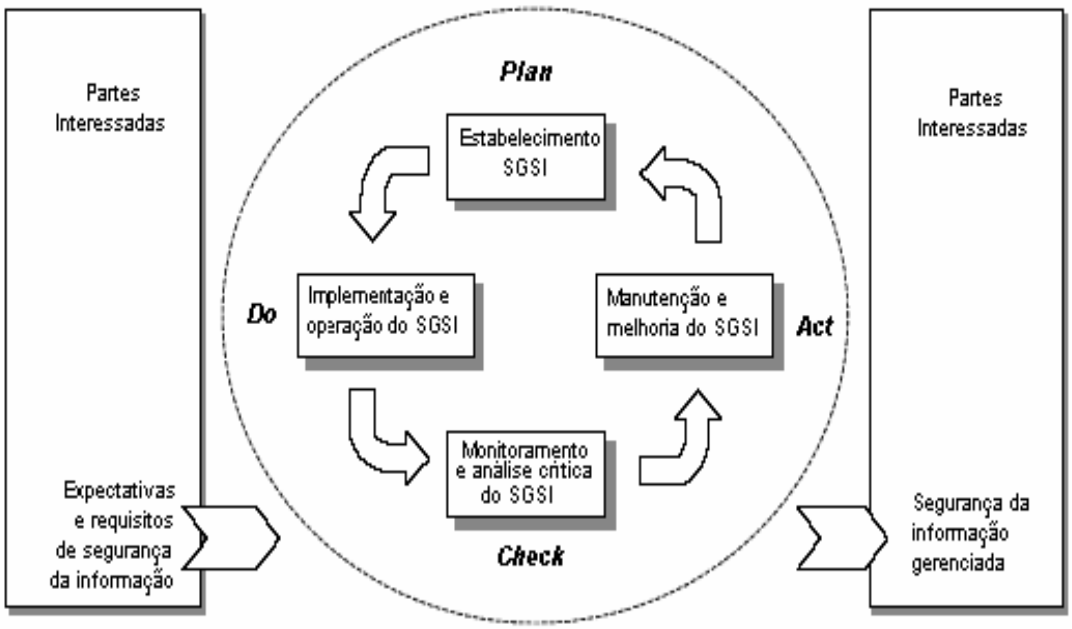

FIGURA 2 - MODELO PDCA APLICADO AOS PROCESSOS DO SGSI.
FONTE: ABNT NBR ISO/IEC 27001(2006, p. vi)

No estabelecimento de um SGSI o ciclo PDCA é utilizado com base no quadro abaixo:

PLAN (planejar) (estabelecer o SGSI)	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 o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
CHECK (checar) (monitorar e analisar criticamente o SGSI)	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) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

QUADRO 1 - MODELO PDCA APLICADO AOS PROCESSOS DE SGSI

FONTE: ABNT NBR ISO/IEC 27001(2006, p. vi)

Para atender aos objetivos propostos no trabalho a subseção que se segue abordou o SGSI.

2.3.2.2 Sistema de Gestão de Segurança da informação – SGSI

O Sistema de Gestão da Segurança da Informação - SGSI é definida pela ABNT NBR ISO/IEC 27001:2006 como sendo “a parte do sistema de gestão global, baseada na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a Segurança da Informação”(ABNT NBR ISO/IEC 27001:2006, p.11). O sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

A norma brasileira ABNT NBR ISO/IEC 27001:2006 item 4 referente ao Sistema de Gestão de Segurança da Informação apresenta um conjunto de critérios/requisitos para que se possa estabelecer, implementar, monitorar e manter um SGSI.

No que refere ao **estabelecimento** de um SGSI a ABNT NBR ISO/IEC 27001 seção 4.2.1 (2006, p.4) afirma que é necessário:

a) definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes e justificativas para quaisquer exclusões do escopo;

b) definir uma política do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia que:

   1) inclua uma estrutura para definir objetivos e estabeleça um direcionamento global e princípios para ações relacionadas com a Segurança da Informação;

   2) considere requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;

   3) esteja alinhada com o contexto estratégico de gestão de riscos da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer;

   4) estabeleça critérios em relação aos quais os riscos serão; e

   5) tenha sido aprovada pela direção.

c) definir a abordagem de análise/avaliação de riscos da organização;

   1) identificar uma metodologia de análise/avaliação de riscos que seja adequada ao SGSI e aos requisitos legais, regulamentares e de Segurança da Informação, identificados para o negócio;

   2) desenvolver critérios para a aceitação de riscos e identificar os níveis aceitáveis de risco;

d) Identificar os riscos;

   1) identificar os ativos dentro do escopo do SGSI e os proprietários destes ativos;

   2) identificar as ameaças a esses ativos;

   3) identificar as vulnerabilidades que podem ser exploradas pelas ameaças;

   4) identificar os impactos que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos.

e) analisar e avaliar os riscos;

1) avaliar os impactos para o negócio da organização que podem resultar de falhas de segurança, levando em consideração as conseqüências de uma perda de confidencialidade, integridade ou disponibilidade dos ativos;
2) avaliar a probabilidade real da ocorrência de falhas de segurança à luz de ameaças e vulnerabilidades prevalecentes, e impactos associados á estes ativos e os controles atualmente implementados;
3) estimar os níveis de riscos;
4) determinar se os riscos são aceitáveis ou se requerem tratamento utilizando os critérios para aceitação de riscos estabelecidos.

f) identificar e avaliar as opções para o tratamento de riscos;

Possíveis ações incluem:

1) aplicar os controles apropriados;
2) aceitar os riscos consciente e objetivamente, desde que satisfaçam claramente às políticas da organização e aos critérios de aceitação de riscos;
3) evitar riscos; e
4) transferir os riscos associados ao negócio a outras partes, por exemplo, seguradoras e fornecedores.

g) selecionar objetivos de controle e controles para o tratamento de riscos;

Objetivos de controle e controles devem ser selecionados e implementados para atender aos requisitos identificados pela análise/avaliação de riscos e pelo processo de tratamento de riscos. Esta seleção deve considerar os critérios para aceitação de riscos como também os requisitos legais, regulamentares e contratuais.

h) obter aprovação da direção dos riscos residuais propostos;

i) obter autorização da direção para implementar e operar o SGSI; e

j) preparar uma Declaração de Aplicabilidade.

Uma Declaração de Aplicabilidade deve ser preparada, incluindo o seguinte:

Os objetivos de controle e os controles selecionados e as razões para sua seleção.

A norma brasileira ABNT NBR ISO/IEC 27001 seção 4.2.2 (2006, p.6) referente à **implementação** de um SGSI afirma que é necessário:

a) formular um plano de tratamento de riscos que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para a gestão dos riscos de segurança;

b) implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que inclua considerações de financiamentos e atribuição de papéis e responsabilidades;

c) implementar os controles selecionados anteriormente para atender aos objetivos de controle;

d) definir como medir a eficácia dos controles ou grupos de controles selecionados, e especificar como estas medidas devem ser usadas para avaliar a eficácia dos controles de modo a produzir resultados comparáveis e reproduzíveis;

e) implementar programas de conscientização e treinamento;

f) gerenciar as operações do SGSI;

g) gerenciar os recursos para o SGSI; e

h) implementar procedimentos e outros controles capazes de permitir a pronta detecção de eventos de segurança da informação e resposta a incidentes de segurança da informação.

De acordo com a ABNT NBR ISO/IEC 27001 seção 4.2.3 (2006, p.7) em relação ao **monitoramento** de um SGSI é necessário que a organização:

a) execute procedimentos de monitoração e análise crítica e outros controles para:

   1) prontamente detectar erros nos resultados de processamento;

   2) prontamente identificar tentativas e violações de segurança bem-sucedidas, e incidentes de segurança da informação;

   3) permitir à direção determinar se as atividades de segurança da informação delegadas a pessoas ou implementadas por meio de tecnologias de informação são executadas conforme esperado;

4) ajudar a detectar eventos de segurança da informação e assim prevenir incidentes de segurança da informação pelo uso de indicadores; e
5) determinar se as ações tomadas para solucionar uma violação de segurança da informação foram eficazes.

b) realize análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica de controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultados da eficácia das medições, sugestões e realimentação de todas as partes interessadas;

c) meça a eficácia dos controles para verificar que os requisitos de segurança da informação foram atendidos;

d) analise criticamente as análises/avaliações de riscos a intervalos planejados e analise criticamente os riscos residuais e os níveis de riscos aceitáveis identificados, levando em consideração mudanças relativas a:
1) organização;
2) tecnologias;
3) objetivos e processos de negócio;
4) ameaças identificadas;
5) eficácia dos controles implementados;
6) eventos externos, tais como mudanças nos ambientes legais ou regulamentares, alterações das obrigações contratuais e mudanças na conjuntura social.

e) conduza auditorias internas do SGSI a intervalos planejados;

f) realizar uma análise crítica do SGSI pela direção em bases regulares para assegurar que o escopo permanece adequado e que são identificadas melhorias nos processos do SGSI;

g) atualize os planos de segurança da informação para levar em consideração os resultados das atividades de monitoramento e análise crítica; e

h) registre ações e eventos que possam ter um impacto na eficácia ou no desempenho do SGSI.

Por último a ABNT NBR ISO/IEC 27001 seção 4.2.4 (2006, p.8) referente à **manutenção e melhoramento** de um SGSI afirma que é necessário:

a) implementar as melhorias identificadas no SGSI;

b) executar as ações preventivas e corretivas apropriadas;

c) comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe apropriado às circunstâncias e, se relevante, obter a concordância sobre como proceder; e

d) assegurar-se de que as melhorias atinjam os objetivos pretendidos.

Segundo a ABNT NBR ISO/IEC 27001 (2006, p. 9-10) a direção da organização deve estar comprometida com o estabelecimento, implementação, operação, monitoramento, análise crítica, manutenção e melhoria do SGSI mediante:

a) o estabelecimento da política do SGSI;

b) a garantia de que são estabelecidos os planos e objetivos do SGSI;

c) o estabelecimento de papéis e responsabilidades pela segurança de informação;

d) a comunicação à organização da importância em atender aos objetivos de segurança da informação e a conformidade com a política de segurança de informação, suas responsabilidades perante a lei e a necessidade para melhoria contínua;

e) a provisão de recursos suficientes para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI;

f) a definição de critérios para aceitação de riscos e dos níveis de riscos aceitáveis;

g) a garantia de que as auditorias internas do SGSI sejam realizadas; e

h) a condução de análises críticas do SGSI pela direção.

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 NBR ISO/IEC 27001 p.12)

2.3.3 ABNT NBR ISO/IEC 27002

A ABNT NBR ISO/IEC 27002 constitui-se de uma revisão da ABNT NBR ISO/IEC 17799, realizada em 2007, fazendo parte da família de normas 27000 referente ao Sistema de Gerenciamento de Segurança da Informação – SGSI.

Esta norma é composta por 11 sessões, sendo que cada seção é constituída por assuntos relativos à Segurança da Informação, são elas:

a) Política de Segurança da Informação;
b) Organizando a Segurança da Informação;
c) Gestão de ativos;
d) Segurança em Recursos Humanos;
e) Segurança física e do ambiente;
f) Gestão das Operações e Comunicações;
g) Controle de Acessos;
h) Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação;
i) Gestão de Incidentes de Segurança da Informação;
j) Gestão da Continuidade do Negócio; e
k) Conformidade.

A subseção que se segue descreve cada uma das 11 seções que compõem a ABNT NBR ISO/IEC 27002.

2.3.3.1 Controles que devem ser atendidos para garantir a Segurança da Informação

Os controles abaixo descritos servirão de referência para a organização, porém é necessário que eles sejam adaptados de acordo com as necessidades e o

ambiente em que a organização está inserida. Alguns desses controles não são aplicáveis em todos os sistemas de informação, ambientes ou organizações.

a) Política de Segurança da Informação

Tem como objetivo “prover uma orientação e apoio da direção para a Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes” (ABNT NBR ISO/IEC 27002: 2005, p. 20). A organização deverá estabelecer uma política clara, alinhada com os objetivos da organização e que demonstre apoio e comprometimento com a Segurança da Informação em todos os níveis da organização.

Sendo assim é necessário que exista um documento da política de segurança da informação aprovado pela direção e comunicado por todos os integrantes e partes interessadas inclusive a partes externas. A Política de Segurança da Informação deverá ser analisada criticamente em intervalos planejados ou quando mudanças significativas ocorrerem para assegurar a sua contínua pertinência, adequação e eficácia. Mais informações relativas à Política de Segurança da Informação são apresentadas na seção 2.5.

b) Organizando a Segurança da Informação

Segundo a ABNT (NBR ISO/IEC 27002:2005), a organização da segurança da informação é obtida através do estabelecimento de controles e procedimentos de gerência. É necessário que haja o comprometimento e o apoio da direção com a Segurança da Informação na organização e com a política direcionando-a e definindo atribuições de forma explícita e conhecendo as responsabilidades pela segurança da informação. As atividades de Segurança da Informação devem ser coordenadas por representantes de diferentes partes da organização, onde as responsabilidades pela Segurança da Informação estejam claramente definidas, para que haja o envolvimento da organização como um todo.

Ainda segundo a referida norma, para uma boa gestão da Segurança da Informação é necessário: definir e implementar um processo de gestão de autorização para novos recursos de processamento da informação; estabelecer requisitos de confidencialidade ou acordos de não divulgação para a proteção das informações; manter contatos com autoridades relevantes e com grupos de

interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais; analisar criticamente o enfoque da organização periodicamente independente da segurança da informação.

Deve ser mantida a segurança dos recursos de processamento da informação e da informação da organização, que são acessados, processados, comunicados ou gerenciados por partes externas. Para isso deverão ser identificados os riscos relacionados com as partes externas, identificar requisitos de segurança antes de conceder acesso aos ativos de informação á partes externas e respeitar todos os requisitos de Segurança da Informação relativos a acordos com terceiros envolvendo ativos informacionais.

c) Gestão de ativos

Objetiva “alcançar e manter a proteção adequada dos ativos da organização” (ABNT NBR ISO/IEC 27002: 2005, p.33). Para isto é necessário realizar um inventário dos ativos onde sejam claramente identificados e estruturados; designar proprietários responsáveis pelos ativos de informação e identificar, documentar e implementar regras para que seja permitido o uso de informações e de ativos associados aos recursos de processamento da informação. As informações deverão ser classificadas de acordo com o valor, requisitos legais, sensibilidade e criticidade para a organização, logo essas informações deverão ser rotuladas de acordo com o esquema de classificação.

d) Segurança em Recursos Humanos

Tem como finalidade “assegurar que funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, reduzindo o risco de roubo, fraude ou mau uso de recursos” (ABNT NBR ISO/IEC 27002:2005, p. 37). Para isso é necessário que sejam definidas as responsabilidades dos funcionários, fornecedores e terceiros de acordo com a politica de segurança estabelecida na organização, selecionar recursos humanos para a organização de acordo com as leis, regulamentações e ética.

Segundo a ABNT (NBR ISO/IEC 27002:2005) a direção deve solicitar aos funcionários, fornecedores e clientes que pratiquem a segurança da informação em conformidade com o estabelecido na política, assim sendo eles deverão ter o

treinamento/educação necessário relativa à segurança da informação e devidamente punidos caso não respeitem as regras estabelecidas na política. No momento em que um funcionário ou qualquer parte interessada deixa de exercer atividades na organização, ou ainda é trocado de cargo/setor a organização deverá assegurar que isso aconteça de forma ordenada, definindo responsabilidades para o desligamento ou mudança de atividade, os funcionários deverão devolver quaisquer ativos que estejam em sua posse e a organização deverá garantir que todos os direitos relativos a ativos informacionais sejam retirados assim que o funcionário encerrar o contrato com a organização.

e) Segurança física e do ambiente

Objetiva “prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização” (ABNT NBR ISO/IEC 27002: 2005, p.44). A organização deverá estabelecer perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação. As áreas deverão ser protegidas por meio de controles de acesso físico aplicando medidas de segurança física para escritórios e instalações.

De acordo com a ABNT (NBR ISO/IEC 27002:2005), a segurança física e do ambiente também preocupa com a proteção contra incêndios, terremotos, perturbações de ordem pública. Deverão ser impedidos perdas, danos, furtos ou comprometimento de ativos e interrupção das atividades da organização colocando os equipamentos em áreas seguras impedindo ou diminuindo o risco de ameaças do ambiente, equipamentos tanto internos como externos á organização devem ser protegidos contra a falta de energia e outras interrupções causadas por falhas das utilidades e impedir que sejam retirados do local sem autorização prévia. O cabeamento de energia e telecomunicações que transportam dados ou dá suporte aos serviços de informação devem ser protegidos contra interrupção e danos, os equipamentos devem ter uma manutenção correta para assegurar a sua disponibilidade e integridade permanente. Ao descartar mídias de armazenamento deverá ser assegurado que

todos os dados sensíveis e softwares foram removidos ou sobregravados com segurança.

f) Gestão das Operações e Comunicações

Objetiva “garantir a operação segura e correta dos recursos de processamento da informação” (ABNT NBR ISO/IEC 27002: 2005, p.52). Para isso a organização deverá documentar, manter e atualizar os procedimentos de operação; controlar modificações nos recursos de processamento da informação e sistemas; segregar funções e áreas de responsabilidade para reduzir oportunidades de modificação ou uso não autorizado ou intencional dos ativos de informação; separar os recursos de desenvolvimento, teste e produção para reduzir os riscos de acesso ou modificações não autorizadas.

Segundo a ABNT (NBR ISO/IEC 27002:2005), a organização deverá “implementar e manter o nível apropriado de Segurança da Informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados” (ABNT NBR ISO/IEC 27002:2005, p.54); monitorar e analisar criticamente os serviços prestados por terceiros; gerenciar mudanças para serviços terceirizados. Para uma boa Gestão das Operações e Comunicações deverá ser minimizado o risco de falhas nos sistemas monitorando e sincronizando os recursos e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido do sistema; estabelecer critérios de aceitações de sistemas; proteger a integridade do software e da informação contra códigos maliciosos e códigos móveis.

Para manter a disponibilidade e integridade das informações e dos recursos de processamento de informação deverão ser feitas cópias de segurança, garantindo a proteção das informações em redes e a proteção da infra-estrutura de suporte por meio de controles de rede. Deverá ser prevenida a divulgação não autorizada, modificação, remoção ou distruição dos ativos, e interrupções das atividades de negócio desenvolvendo medidas de gerenciamento de mídias removíveis, assegurando o descarte de forma segura dessas mídias, estabelecendo procedimentos para o tratamento e armazenamento das informações. A troca de informações entre sistemas internos e externos á empresa deve ser realizada de forma segura estabelecendo políticas e procedimentos de troca, acordos para

troca de informações e softwares e assegurar que as mensagens eletrônicas estejam sendo transmitidas de forma segura.

A proteção dos serviços do comércio eletrônico também faz parte da Gestão das Operações e Comunicações, garantindo assim a segurança das transações realizadas *on-line*, a integridade das informações disponibilizadas publicamente detetando atividades não autorizadas de processamento da informação, para isso deverá ser monitorado o uso dos sistemas registrando dados relativos às atividades dos usuários e falsificações desses dados.

g) Controle de Acessos

Objetiva controlar o acesso á informação por meio do estabelecimento de uma política de controle de acesso, gerenciamento do acesso dos usuários através de registro de usuários, gerenciamento de privilégios e de senhas de usuários (ABNT NBR ISO/IEC 27002: 2005). A organização deverá fazer a análise crítica do direito de acesso dos usuários, definir as responsabilidades dos usuários, solicitar o seguimento de boas práticas no uso de senhas. O usuário deverá garantir que os equipamentos não monitorados tenham proteção adequada adotando a política de mesa e tela limpa.

O controle de acesso também evita o acesso não autorizado aos serviços de rede por meio de políticas de uso dos serviços de rede; identificação de equipamentos em redes; autenticação para conexão externa do usuário; controle do acesso físico e lógico das portas de diagnóstico e configuração; controle de conexão de rede; controle de roteamentos de rede; controle de acesso ao sistema operacional e controle de acesso a informações e aplicações.

h) Aquisição, Desenvolvimento e Manutenção dos Sistemas de Informação

Tem como “finalidade garantir que a segurança é parte integrante dos sistemas de informação” (ABNT NBR ISO/IEC 27002: 2005, p.96), especificando os requisitos de segurança; garantindo o correto processamento das aplicações através da validação dos dados de entrada e saída; controle do processamento interno e integridade das mensagens.

De acordo com a ABNT (NBR ISO/IEC 27002:2005), os controles criptográficos auxiliam na Aquisição, Desenvolvimento e Manutenção dos Sistemas de

Informação protegendo a confidencialidade, a autenticidade ou a integridade das informações por meios criptográficos, sendo assim deverão ser estabelecidas políticas para o uso de controles criptográficos e gerenciamento de chaves. Deve ser mantida a segurança dos arquivos dos sistemas por meio de controle de software operacional, proteção dos dados para teste de sistema e restringindo o acesso ao código-fonte. A segurança em processos de desenvolvimento e de suporte deve ser garantida por meio do estabelecimento de procedimentos de controle para mudanças, análise crítica e técnica das aplicações após mudanças no sistema operacional e restrições sobre mudanças em pacotes de *software.*

i) Gestão de Incidentes de Segurança da Informação

Objetiva “assegurar que fragilidades e eventos de Segurança da Informação associados aos sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil” (ABNT NBR ISO/IEC 27002: 2005, p.110), para isso deverão ser notificados os eventos e as fragilidades de segurança da informação.

Para gerenciamento de incidentes de Segurança da Informação deverá ser estabelecida as responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação. È necessário que sejam estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados.

j) Gestão da Continuidade do Negócio

Tem como finalidade evitar 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 (ABNT NBR ISO/IEC 27002: 2005). È necessário que o processo de gestão da continuidade do negócio seja implementado para minimizar o impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação.

k) Conformidade

Objetiva “evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação” (ABNT NBR ISO/IEC 27002:2005, p.120). Para isso deverá ser definida a legislação, os direitos de propriedade intelectual e garantida a proteção dos registros organizacionais, proteção de dados e privacidade de informações pessoais, prevenindo o mau uso de recursos de processamento da informação e a regulamentação de controles de criptografia.

A ABNT (NBR ISO/IEC 27002:2005) afirma que deverá ser garantida a conformidade com normas e políticas de segurança da informação e conformidade técnica. Para a auditoria de sistemas de informação convém que requisitos e atividades de auditoria envolvendo verificação nos sistemas operacionais sejam cuidadosamente planejados e acordados para minimizar os riscos de interrupção dos processos do negócio e garantir que o acesso às ferramentas de auditoria de sistema de informação seja protegido, para prevenir qualquer possibilidade de uso impróprio ou comprometimento.

2.3.3.2 Normas e metodologias complementares a ABNT NBR ISO/IEC 27002

A ABNT NBR ISO/IEC 27002 define medidas de controle para qualquer tipo de organização, sendo assim tem-se a necessidade de normas que sugerem controles específicos para a área de Tecnologia da Informação. Segundo Janssen (2008, p. 34) algumas normas complementares a ABNT NBR ISO/IEC 17799 atual NBR ISO/IEC 27002 é a ISO/IEC 13335 que é um conjunto de diretrizes de gestão de segurança voltadas especificamente para a tecnologia da informação e a ISO/ IEC 15408 que aborda de maneira mais profunda os critérios de avaliação dos produtos e sistemas de TI, definindo os níveis de defesa necessários através de medidas de segurança. Outras normas complementares são as abaixo descritas:

a) ISO/IEC TR 19791:2010 fornece a orientação e os critérios para a avaliação de segurança de sistemas operacionais.

b) ISO/IEC 9798-1:2010 especifica um modelo da autenticação, exigências gerais para os mecanismos de autenticação da entidade que usa técnicas da segurança, define uma série de requisitos para que possa acreditar que uma organização é o que ela afirma ser.

c) ITIL (*Information Technologie Infrastructure Library*) é um conjunto de documentos desenvolvidos pelo governo do Reino Unido para registrar as melhores práticas na área de gestão de serviços de TI colaborando para a padronização e a melhoria da qualidade do serviço ofertado pela área de TI. (BEAL, 2005 p.31)

d) COBIT *(Control Objetives for Information and Related Technology*) é um conjunto de diretrizes para a gestão e auditoria de processos, práticas e controles de TI. Foi desenvolvido pela ISACF *(Information System Audit and Control Foundation)*, seu foco é a redução de riscos voltada para a governança. O COBIT oferece um modelo de maturidade para o controle dos processos de TI e abrange práticas em quatro domínios: planejamento e organização, aquisição e implementação, entrega e suporte e monitoração. (BEAL, 2005, p.32)

2.4 GERENCIAMENTO DE RISCO

A seção que se segue apresenta a gestão de risco e a gestão da continuidade de negócios. Primeiro foi feita uma abordagem desses dois assuntos e por último uma descrição da norma ISO/IEC 27005 que define orientações para o gerenciamento de riscos.

2.4.1 Gestão e Análise de Riscos

A análise de riscos diz respeito a projeções futuras, facilitando a tomada de decisões a curto, médio e longo prazo. Ela deve ser realizada sempre que a organização pretende fazer um investimento, iniciar um novo projeto ou um novo

negócio. Segundo Imoniana (2005, p. 52) “a análise de riscos é uma metodologia adotada pelos auditores de TI para saber, com antecedência, quais as ameaças prováveis em um ambiente de TI em uma organização”. A análise de risco tem por objetivo quantificar o impacto dos riscos existentes no ambiente sobre os resultados da organização. O processo de gestão de riscos inicia-se com a identificação dos riscos e de seus elementos: alvos, ameaças, vulnerabilidades e impactos. As ameaças pelas quais a informação está sujeita podem ser classificadas em:

a) ambientais – naturais (fogo, incêndio, chuva, raios) ou decorrentes das condições do ambiente (interferência eletrônica, contaminação por produtos químicos, falhas no fornecimento de energia);
b) técnicas - configuração incorreta de componentes de TI, falhas de hardware e software;
c) lógicas – vírus e invasão de sistemas; e
d) humanas – erro de operação, fraude, sabotagem. (BEAL, 2005, p.18)

Beal (2005, p.27) afirma que para tratamento de riscos são utilizadas as seguintes medidas:

a) medidas preventivas – controles que reduzem a probabilidade de uma ameaça se concretizar ou diminuem o grau de vulnerabilidade do ambiente/ativo/sistema, reduzindo assim a probabilidade de ataque;
b) medidas corretivas ou reativas – reduzem o impacto de um ataque/incidente. São tomadas durante ou após a ocorrência de um evento; e
c) métodos detetivos – expõem ataques/incidentes e disparam medidas reativas, tentando evitar a concretização do dano, reduzi-lo ou impedir que se repita.

2.4.2 Gestão da Continuidade do Negócio

As organizações têm como uma das suas finalidades desenvolverem as suas atividades durante muitos anos, investindo recursos e tempo para que isso

aconteça. A gestão da continuidade do negócio tem por objetivo “não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos” (ISO 17799: 2001 item 11.1 p.45). Para que isso aconteça é realizado um Plano da Continuidade de Negócios (PCN). O PCN tem por objetivo preparar a organização para a recuperação de seus processos críticos em caso de desastres, seu resultado é um plano/projeto que contem as seguintes etapas: concepção do projeto (abrangendo estimativas de custo e prazo, definição do escopo, seleção da equipe, etc.), identificação dos processos críticos, análise e classificação dos impactos, análise das alternativas de recuperação (viabilidade e custo/benefício das opções de recuperação), escolha das medidas de recuperação a serem adotadas, desenvolvimento e documentação do plano, treinamento e conscientização dos responsáveis pela implementação do plano e teste. (BEAL, 2005, p. 138)

A elaboração do plano de continuidade do negócio envolve todas as atividades necessárias para garantir que todos os processos de negócios críticos dos clientes sejam contemplados numa solução de continuidade, que busca o menor custo operacional possível. Para tanto, é levantada toda a infra-estrutura de TI e são mapeadas todas as ameaças que podem determinar uma interrupção de atividades.

A adoção de metodologia de continuidade de negócios padrão internacional garante a implantação de um plano eficaz.

Para auxiliar na gestão de riscos e na continuidade do negócio surgiu à norma ISO/IEC 27005 que é descrita abaixo.

2.4.3 ISO/IEC 27005:2008

Esta subseção abordou a norma apontando os principais termos relacionados à ISO/IEC 27005, assim como as fases que constituem o processo de gerenciamento de risco e as atividades que deverão ser realizadas em cada fase.

Para melhor entendimento de o que é o risco e de cada uma das fases do processo de gerenciamento de risco primeiramente serão expostas algumas

definições relacionadas. Estas definições foram retiradas da norma ABNT NBR ISO/IEC 17799 e da ISO/IEC 27005 traduzida pela autora são elas:

a) impacto: mudança adversa no nível de negócios;

b) risco: é uma combinação da conseqüência que seguiria da ocorrência de um evento não desejado e da probabilidade da ocorrência do evento;

c) risco de segurança da informação: potencial que uma ameaça dada explorará as vulnerabilidades de um recurso ou de recursos de um grupo e causará desse modo danos á organização;

d) gestão do risco: coordena atividades para direcionar e controlar uma organização com relação ao risco. A gestão do risco normalmente inclui avaliação do risco, tratamento do risco, aceitação do risco e comunicação do risco;

e) avaliação de risco: avaliação das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência;

f) aceitação do risco: decisão de aceitar um risco;

g) gerenciamento de risco: processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável;

h) prevenção do risco: decisão de não se envolver, ou ignorar uma situação de risco, são os riscos que a organização sabe da sua existência, porém por questões econômicas não o considera para fins de gerenciamento;

i) comunicação de risco: troca ou partilha da informação sobre o risco entre o responsável pelas decisões e outras partes interessadas;

j) identificação de risco: é o processo de encontrar, listar e caracterizar elementos de risco;

k) redução do risco: ações tomadas que diminuem a probabilidade, as conseqüências negativas ou ambas associadas a um risco;

l) tratamento do risco: processo de seleção e implementação de medidas para modificar um risco;

m) retenção de risco: aceitação do encargo de perda ou benefício de determinado risco; e

n) transferência do risco: compartilhamento com outras pessoas a perda ou o beneficio resultante de um risco.

2.4.3.1 Métodos de avaliação de risco

Para que a organização tenha um entendimento da dimensão do risco a qual ela está sujeita há que haver métricas para que se estime ou calcule a dimensão do risco. Para isso existem alguns métodos usados para determinar o risco. Segundo a ISO/IEC 27005:2008 estes métodos podem ser quantitativos, qualitativos ou uma mistura dos dois. A norma revela que a avaliação qualitativa geralmente é mais usada para ter uma idéia geral do risco e depois se necessário uma análise mais especifica usa-se a análise quantitativa. Isto acontece porque a análise qualitativa é menos complexa e menos cara que a quantitativa.

a) Análise Qualitativa

Usa uma escala de atributos qualificativos para descrever o valor das conseqüências (por exemplo: baixo, médio e alto) e a probabilidade daquela conseqüência ocorrer. Tem como vantagem a facilidade de compreensão por todas as pessoas e como desvantagem a subjetividade na escolha da escala (ISO IEC 27005:2008, p.20, tradução da autora). A escala pode ser adaptada ou ajustada para diferentes circunstâncias e pode ser usada para riscos diferentes.

- Uso de cenários
- Classificação subjetiva de impactos e probabilidades

Os métodos qualitativos utilizam questionários e matrizes de risco. O quadro abaixo exemplifica um modelo de matriz de risco.

Gravidade do impacto	**Probabilidade de ocorrência do incidente**					
	F impossível	E improvável	D remota	C ocasional	B provável	A freqüente
I Catástrofe			///////	XXXXXX	XXXXXX	XXXXXX
II Alta				///////	XXXXXX	
III Média					///////	///////
IV Baixa						
Legenda: ///////: Imperativo reduzir o impacto. XXXXXX: Medidas de proteção adicionais requeridas. Em branco: As medidas básicas de proteção adotadas pela organização são consideradas suficientes para manter os riscos em níveis aceitáveis.						

QUADRO 2 - EXEMPLO DE MATRIZ DE RISCO
FONTE: BEAL (2005, p.23)

b) Análise Quantitativa

Usa-se uma escala com valores numéricos para as conseqüências e probabilidades usando dados de uma variedade de fontes. A qualidade da análise depende da integridade e exatidão dos valores numéricos e da validez dos modelos usados (ISO IEC 27005:2008, p.20).

- Baseado em números
- Todos os valores são mensurados objetivamente

Segundo Beal (2005, p.22) um exemplo de método quantitativo é o cálculo da Expectativa de Perda Anual (ALE – *Annual Loss Expectation*). Ela é calculada pela multiplicação da perda prevista para um incidente pela freqüência esperada de ocorrência desse incidente.

Beal (2005, p.25) afirma que independentemente da abordagem escolhida, a avaliação do risco deve ser efetuada por pessoa ou pessoas que detenham:

a) entendimento aprofundado do papel e da importância dos ativos de informação sob análise para a organização;
b) formação técnica nas áreas que estão sendo avaliadas;
c) experiência de aplicação dos princípios, procedimentos e práticas de segurança da informação; e
d) experiência na metodologia de análise e avaliação de risco a ser empregada, e conhecimento das suas limitações.

Segundo a ISO/IEC 27005 (2008, p.20, tradução da autora) a maneira como as conseqüências e a probabilidade são expressas e combinadas para fornecer o nível de risco varia de acordo com o tipo de risco e a finalidade que vai ser dada ao resultado da avaliação de risco.

2.4.3.2 Finalidade do gerenciamento de riscos da Segurança da Informação

A norma ISO/IEC 27005 define medidas para a gestão de risco em consonância com os padrões estabelecidos pelas normas ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27002. De acordo com a literatura revisada ela tem como objetivo fornecer diretrizes para a gestão de riscos da Segurança da Informação. A ISO/IEC 27005 (2008, p.10, tradução da autora) estabelece que a gestão de risco da segurança da informação deverá contribuir nos seguintes aspectos:

a) identificação de riscos;
b) identificação dos riscos e avaliação das suas conseqüências nos negócios e a sua probabilidade de ocorrência;
c) as conseqüências dos riscos devem ser comunicadas e compreendidas;
d) ordem de prioridade para o tratamento dos riscos estabelecidos;
e) ordem de prioridade de estabelecimento de ações que reduzam a ocorrência dos riscos;
f) as partes interessadas (*stakeholders*) devem ser mantidas informadas sobre o andamento do processo de gestão de risco;
g) eficácia na monitoração do tratamento de riscos;
h) os riscos e o processo de gestão de risco devem ser monitorados e revisto regularmente;
i) toda a informação deve estar subordinada a um gerenciamento de risco;
j) treinamento dos gerentes e equipe de funcionários sobre os riscos e as ações que devem ser realizadas para minimizá-los.

2.4.3.3 Processo de gerenciamento de risco da segurança da informação

O processo da gestão de riscos da segurança da informação consiste nas seguintes fases ilustradas na figura abaixo.

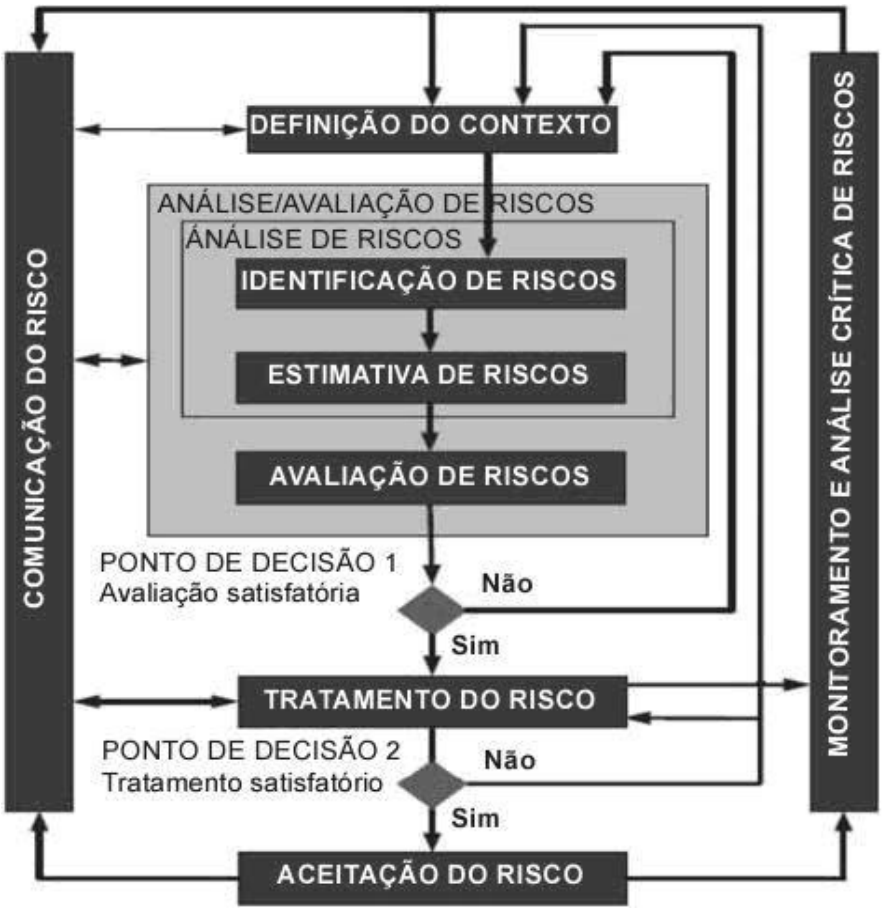

FIGURA 3 - PROCESSO DE GESTÃO DE RISCO DA SEGURANÇA DA INFORMAÇÃO
FONTE: ISO/IEC 27005 (2008, p.5)

Cada uma dessas fases possui uma entrada (*input*), uma ação (*action*), uma orientação para execução (*implementation guidance*) e uma saída (output) como ilustrada no quadro que se segue.

Fase	**Entrada *(input)***	**Ação *(action)***	**Orientação para execução (*implementation guidance*)**	**Saída *(output)***
Estabelecimento do contexto	Toda a informação da organização relevante para a gestão do risco de SI	Ajustar os critérios básicos necessários para a gerência do risco de SI, definir o espaço e os limites de abrangência e estabelecer uma organização apropriada para a gestão de risco de SI	Determinar a finalidade do gerenciamento de risco da segurança da informação. A finalidade poderá ser: suportar o SGSI, conformidade com o plano de continuidade de negócios, preparação de um plano de continuidade de negócio, preparação de um plano de resposta a incidentes, descrição das exigências de segurança da informação ou ainda elementos necessários para suportar o SGSI.	Especificação dos critérios básicos, definição do espaço e dos limites e a organização para o processo da gestão de riscos de SI
Avaliação de risco	Lista de riscos com valores atribuídos aos critérios de avaliação	Nível de riscos deve ser comparado com os critérios da avaliação e aceitação de risco	Determina ou descreve de forma qualitativa ou quantitativamente o risco e permite aos gerentes dar prioridade a riscos de acordo com a seriedade percebida ou outros critérios estabelecidos.	Lista de riscos estabelecidos de acordo com critérios de avaliação do risco com relação ás encenações de incidentes que conduzem a riscos
Tratamento de risco	Lista de riscos com as respectivas encenações de cenários que poderão conduzir a aqueles riscos	Controles para reduzir, reter, evitar ou transferir os possíveis riscos e um plano de tratamento de riscos definido	Há quatro opções disponíveis para o tratamento do risco: redução do risco, retenção de risco, vacância do risco e transferência do risco	Plano de tratamento de riscos e aceitação dos riscos pelos gerentes da organização (alta administração)
Aceitação do risco	Plano de tratamento de riscos e aceitação dos riscos pelos gerentes da organização (alta administração)	Formalização da aceitação dos riscos e das responsabilidades	Descrever como os riscos avaliados devem ser tratados para encontrar critérios de aceitação do risco. È importante para os gerentes rever e aprovar riscos residuais e planos de tratamento de risco	Lista de riscos com a justificação para aqueles que não encontraram os critérios de aceitação normais dos riscos da organização
Comunicação do risco	Toda a informação obtida nas atividades de gestão de risco	A informação obtida nas atividades de gestão de risco deve ser trocada e/ou compartilhada entre o responsável pelas decisões e outras partes interessadas	Atividade para conseguir o acordo em como controlar risco trocando e/ou compartilhando a informação sobre o risco entre os responsáveis pelas decisões e outros interessados (*stakeholders*)	Compreensão dos resultados do processo de gestão de riscos pela organização
Monitoração e análise critica de riscos	Toda a informação obtida nas atividades de gestão de risco	O risco e as suas causas devem ser monitoradas e revistas para identificar as mudanças no contexto da organização em fase inicial e para manter uma vista geral do retrato completo do risco	Os riscos, ameaças, vulnerabilidades não são estáticos, consequentemente é necessário a monitoração constante para que sejam detectadas essas mudanças	Alinhamento contínuo da gestão de risco com os objetivos do negocio da organização e com os critérios de aceitação de risco

QUADRO 3 - FASES DO PROCESSO DE GESTÃO DE RISCO, ENTRADAS, AÇÃO, ORIENTAÇÃO PARA EXECUÇÃO E SAÍDA
FONTE: A AUTORA (2010) BASEADA NA TRADUÇÃO DA ISO/IEC 27005 (2008)

Ao longo do processo de tratamento e gestão de riscos de Segurança da Informação é importante que se comunique aos responsáveis pela informação dos riscos que tal informação está exposta e qual o devido cuidado que ele deve ter para evitar que a informação seja exposta a esses riscos.

2.4.3.4 Gerenciamento de riscos e o modelo PDCA

A aplicação de um processo de gestão de riscos da Segurança da Informação satisfaz os requisitos de controles especificados no SGSI, sendo que os gestores deverão utilizar os termos que melhor se adaptam a realidade vivida pela organização (ISO/IEC 27005: 2008, p.6, tradução da autora). A tabela que se segue sumariza as atividades da gestão de risco da Segurança da Informação relevantes as quatro fases do processo de SGSI (ciclo PDCA).

Processo SGSI	**Processo de gestão de riscos de segurança da informação**
Planejar	Definição do contexto Análise/avaliação de riscos Plano de tratamento de risco Aceitação de risco
Executar	Implementação do plano de tratamento de risco
Verificar	Monitoramento contínuo e análise crítica dos riscos
Agir	Manter e melhorar o processo de gestão de riscos de segurança da informação

QUADRO 4 - ALINHAMENTO DO SGSI COM O PROCESSO DE GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

FONTE: ISO/IEC 27005 (2008, p.6, tradução da autora)

Segundo a ISO/IEC 27005 (2008, p.7, tradução da autora) os propósitos da gestão de risco da segurança da informação são:

a) suporte ao SGSI;

b) conformidade e evidencias;

c) preparação de um plano de continuidade de negócio;

d) preparação de um plano de resposta a incidentes; e

e) descrição das exigências da segurança da informação para um produto, serviço ou mecanismo.

2.5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO - PSI

As políticas de segurança da informação facilitam o alcance dos objetivos da organização em relação aos seus ativos informacionais. Um dos principais passos para estabelecer um Sistema de Gestão de Segurança da Informação (SGSI) é a elaboração de uma política de segurança de informação. Nela são registradas as principais diretrizes adotadas pela organização, a serem seguidos por todos os colaboradores e aplicados a todos os sistemas de informação e processos corporativos (BEAL, 2005, p.43). A aprovação de uma política de segurança da informação deve ser feita no mais alto nível hierárquico para que haja o comprometimento da direção com as metas e princípios de segurança da informação adotada.

A Política de Segurança da Informação deve identificar as responsabilidades que cada colaborador terá em relação á segurança da informação delineando responsabilidades em relação á implementação, verificação de conformidade, auditoria e avaliação da segurança e estabelecer as orientações necessárias em relação a todas as medidas de proteção a serem implementadas (BEAL, 2005, p.44).

Imoniana (2005, p.78) aponta dois tipos de Política de Segurança da Informação:

a) Política de responsabilidades – que tem como objetivo definir as responsabilidades da organização e de todos a respeito de manipulação e salvaguarda dos ativos da organização no processo de geração de riquezas;

b) Política de continuidade de negócios - objetiva assegurar que haja planos para minimizar impactos de desastres que resultam na interrupção das operações normais da organização devido à falta de segurança da informação.

A ISO 17799 item 3.1.1 (2001, p.4) afirma que na Política de Segurança da Informação deverão ser incluídas as seguintes orientações:

a) definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação;

b) declaração do comprometimento da alta direção, apoiando as metas e princípios da segurança da informação;

c) breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização, por exemplo:

   1) conformidade com a legislação e cláusulas contratuais;

   2) requisitos na educação de segurança;

   3) prevenção e detecção de vírus e *software* maliciosos;

   4) gestão da continuidade do negócio;

   5) conseqüências das violações na política de segurança da informação;

   6) definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro dos incidentes de segurança; e

d) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que convém que os usuários sigam.

A política de informação deverá ser elaborada antes ou depois da ocorrência de incidentes para evitar reinicidências. Para elaboração de uma Politica de Segurança da Informação deverá ser primeiramente estabelecida o escopo e abrangência da mesma. Segundo Ferreira e Araújo (2006, p.11-12) as normas, procedimentos e políticas de informação devem ser:

a) simples;

b) compreensíveis (escritas de maneira clara e concisa);

c) homologadas e assinadas pela alta administração;

d) estruturadas de forma a permitir a sua implementação por fases;

e) alinhadas com as estratégias de negócio da empresa, padrões e procedimentos já existentes;

f) orientadas aos riscos (qualquer medida de proteção das informações deve direcionar para os riscos da empresa);

g) flexíveis (moldáveis aos novos requerimentos de tecnologia e negócio, dentre outros);

h) protetores dos ativos de informações, priorizando os de maior valor e de maior importância; e

i) positivas e não apenas concentradas em ações proibitivas ou penutivas.

2.5.1 Etapas para desenvolvimento de uma PSI

Para o desenvolvimento de uma Política de Segurança da Informação Ferreira e Araújo (2006, p.12-14) sugerem quatro fases são elas:

a) Levantamento de informações – para o levantamento dessas informações recomenda-se o uso de questionários;

b) Desenvolvimento do conteúdo das políticas e normas de segurança;

c) Elaboração dos procedimentos de segurança da informação; e

d) Revisão, aprovação e implementação das políticas, normas e procedimentos de segurança. O quadro que se segue diz respeito às atividades que deverão ser realizadas em cada uma das fases da elaboração da política de segurança.

Fases	**Descrição**
Fase I	**Levantamento de informações**
1.1	Obtenção dos padrões, normas e procedimentos já existentes para análise.
1.2	Entendimento das necessidades e uso dos recursos da tecnologia da informação (sistemas, equipamentos e dados) nos processos de negócio
1.3	Obtenção de informações sobre os ambientes de negócios: • Processos de negócios; • Tendências de mercado; • Controles e áreas de risco.
1.4	Obtenção de informações sobre o ambiente tecnológico: • Workflow entre ambientes; • Redes de aplicações; • Plataformas computacionais.

(Continua)

(Continuação)

Fase II	**Desenvolvimento do conteúdo das políticas e normas de segurança**
2.1	Gerenciamento da política de segurança: • Definição da segurança da informação; • Objetivo do gerenciamento; • Fatores críticos de sucesso; • Gerenciamento da versão e manutenção da política; • Referência para outras políticas, padrões e procedimentos.
2.2	Atribuição de regras e responsabilidades: • Comitê de segurança da informação; • Proprietário das informações; • Área de segurança da informação; • Usuários de informações; • Recursos humanos; • Auditoria interna.
2.3	Critérios para classificação das informações: • Introdução; • Classificando a informação; • Níveis de classificação; • Reclassificação; • Armazenamento e descarte; • Armazenamento e saídas.
2.4	Procedimentos de segurança de informações: • Classificação e tratamento da informação; • Notificação e gerenciamento de incidentes de segurança da informação; • Processo disciplinar; • Aquisição e uso de hardware e software; • Proteção contra software malicioso; • Segurança e tratamento de mídias; • Uso de internet; • Uso de correio electrônico; • Utilização de recusos de TI; • Backup; • Manutenção de teste e equipamentos; • Coleta e registro de falhas; • Gerenciamento e controle de rede; • Monitoração do uso e acesso aos sistemas; • Uso de controles de criptografia e gerenciamento de chaves; • Controle de mudanças operacionais; • Inventário de ativos de informação; • Controle de acesso físico às áreas sensíveis; • Segurança física; • Supervisão de visitantes e prestadores de serviços.
Fase III	**Elaboração dos procedimentos de segurança da informação**
3.1	Pesquisas sobre as melhores práticas em segurança da informação utilizadas no mercado.
3.2	Desenvolvimento de procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização.

(Continua)

(Conclusão)

Fases	Descrição
3.3	Formalização dos procedimentos para integrá-los ás políticas corporativas.
Fase IV	**Revisão, aprovação e implementação das políticas, normas e procedimentos de segurança**
4.1	Revisão e aprovação das políticas, normas e procedimentos de segurança da informação.
4.2	Efetiva implantação das políticas, normas e procedimentos de segurança da informação por meio das seguintes iniciativas: • Atuação junto à área responsável pela comunicação, ou área correspondente, na orientação para a preparação do material promocional de divulgação e de consulta; • Divulgação das responsabilidades dos colaboradores, bem como da importância das políticas, normas e procedimentos de segurança da informação; • Realização de palestras executivas referentes ás políticas, normas e procedimentos de segurança da informação desenvolvidas, tendo por público-alvo a Presidência, Diretorias e Gerências; • Realização de palestras referentes ás políticas, normas e procedimentos de segurança, tendo por público-alvo outros colaboradores da organização.

QUADRO 5 - ETAPAS PARA O DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
FONTE: FERREIRA; ARAÚJO (2006, p. 12-14)

Para a realização das atividades de cada uma das fases acima descritas Ferreira e Araújo (2006) sugerem o seguinte cronograma:

Atividades	Quinzenas							
	1	2	3	4	5	6	7	8
Fase 1 – Levantamento de informações	■	■						
Fase 2 – Desenvolvimento do conteúdo das políticas e normas de segurança		■	■	■				
Fase 3 – Elaboração dos procedimentos de segurança da informação			■	■	■	■	■	
Fase 4 – Revisão, aprovação e implementação das políticas de segurança da informação e palestras							■	■

QUADRO 6 - CRONOGRAMA PARA O DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
FONTE: FERREIRA; ARAÚJO (2006, p.14)

Segundo o item 3.1.2 da ABNT NBR ISO/IEC 17799 (2001, p. 1) “convém que a política de informação tenha um gestor responsável pela manutenção e análise crítica, de acordo com um processo de análise crítica definido”. Sendo assim a análise e manutenção da política deverá ocorrer como decorrência de qualquer mudança que venha a afetar a avaliação do risco, tais como um incidente de segurança significativo, novas vulnerabilidades ou mudanças organizacionais ou na

infra-estrutura técnica. Convém que também sejam agendadas as seguintes análises críticas periódicas:

a) efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados;

b) custo e impacto dos controles na eficiência do negócio; e

c) efeitos das mudanças na tecnologia (ABNT NBR ISO/IEC 17799:2001 item 3.1.2 p. 5).

2.5.2 Benefícios da PSI

A Política de Segurança da Informação constitui-se de um elemento que irá auxiliar as organizações no desenvolvimento de medidas de segurança da informação. Sendo assim, ela deverá ser um documento formalmente reconhecido, aprovado e respeitado por todos os membros da organização principalmente a Alta Administração. A sua implementação retorna benefícios á organização a curto, médio e longo prazo.

Ferreira e Araújo (2006, p. 19-20) apontam benefícios da Política á:

Curto prazo

a) formalização e documentação dos procedimentos de segurança adotados pela empresa;

b) implementação de novos procedimentos e controles;

c) prevenção de acessos não autorizados, danos ou interferência no andamento dos negócios, mesmo nos casos de falhas ou desastres; e

d) maior segurança nos processos do negócio.

Médio prazo:

a) padronização dos procedimentos de segurança incorporados na rotina da empresa;

b) adaptação segura de novos processos de negócio;

c) qualificação e quantificação dos sistemas de resposta a incidentes; e

d) conformidade com padrões de segurança, como a ABNT NBR ISO/IEC 17799.

Longo prazo:

a) retorno sobre o investimento realizado, por meio da redução da incidência de problemas relacionados à segurança; e

b) consolidação da imagem associada á Segurança da Informação.

2.6 REPRESENTAÇÃO DE PROCESSOS COM FOCO NA QUALIDADE

A construção de um processo de preparação para certificação tem como objetivo a representação esquemática do processo proposto que será descrito no capitulo 4. O processo de certificação constitui-se de uma tarefa complexa que exige a execução de inúmeras atividades. A omissão de determinadas etapas do processo poderá comprometer o resultado final.

Para que se possa definir o melhor modelo que se adeqúe ao processo proposto é necessário primeiramente entender o que vem a ser um processo e também o que é a qualidade e posteriormente conhecer metodologias para se estabelecer o processo com foco na qualidade.

A subseção que se segue inicia com a apresentação de definições para processo e qualidade e posteriormente são apresentadas algumas metodologias utilizadas para construir processos e assim ter base teórica para desenhar um processo para certificação da qualidade em segurança da informação.

2.6.1 Definições

Processo**:**

> “combinação dos elementos e equipamentos, insumos, métodos ou procedimentos, condições ambientais, pessoas e informações do processo ou medidas, tendo como objetivo a fabricação de um bem ou fornecimento de um serviço.” (Werkema, 1995, p.6)

Qualidade:

> “Conjunto das características de uma entidade que lhe conferem a aptidão para satisfazer necessidades exprimidas e implícitas.” (ISO 8402-94)

> “grau de satisfação de requisitos dado por um conjunto de características intrínsecas.” (ISO 9000:2000)

2.6.2 Ferramentas para representação de processos com foco na qualidade

Todo o processo para atingir os objetivos desejados e para que ele possa ser de qualidade deverá ser gerenciado. Para isso existem algumas ferramentas que auxiliam na garantia da qualidade. Alguns exemplos de ferramentas para gestão de processos com foco na qualidade são: Diagrama causa e efeito, Fluxogramas e Folha de Verificação (*checklist*). Essas ferramentas são descritas nas subseções que se seguem.

2.6.2.1 Diagrama de causa e efeito

O Diagrama de causa e efeito é também conhecido como Espinha de Peixe ou de Ishikawa tem como objetivo mostrar a relação entre as caraterísticas e os fatores de causa (Ishikawa, 1993, p.65).

O número de causas pode ser infinito, logo deverá ser distinguidas aquelas causas verdadeiramente importantes, aqueles que influenciarão agudamente os efeitos daqueles que influenciam, mas de forma indireta (Ishikawa, 1993, p.65).

É um instrumento muito usado para estudar:

a) os fatores que determinam resultados que desejamos obter (processo, desempenho, oportunidade);
b) as causas de problemas que precisamos evitar (defeitos, falhas, variabilidade).

Graficamente podemos representar o processo como mostra a figura abaixo.

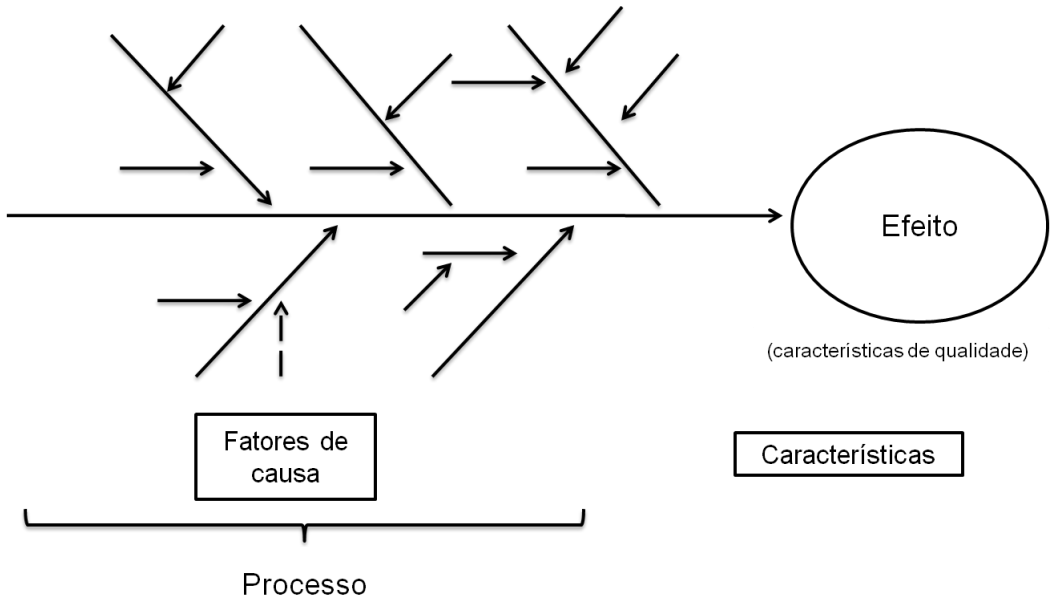

FIGURA 4 - DIAGRAMA DE CAUSA E EFEITO
FONTE: ISHIKAWA (1993, p.64)

2.6.2.2 Fluxogramas

O fluxograma é a representação gráfica que apresenta a sequência de um trabalho de forma análitica, caracterizando as operações, os responsáveis e/ou unidades organizadoras (OLIVEIRA, 2009, p.260). Ele representa de forma esquemática um processo, sendo bastante utilizada na documentação das atividades ou tarefas relativas a cada processo. Ele apresenta apenas o que tem

que ser feito em determinada ordem sequencial e quem deve fazer, porém não determinada como deve ser feito.

Segundo Oliveira (2009, p.262) algumas vantagens do fluxograma são:

a) propiciar a utilização e manutenção do método administrativo;
b) possibilidade de identificação mais fácil e rápida dos pontos fortes e fracos do método administrativo;
c) propiciar o uso de conveções de simbologias;
d) propiciar o adequado levantamento e análise de qualquer método administrativo.

Existem 3 tipos de fluxograma: fluxograma vertical, fluxograma parcial ou descritivo e fluxograma global ou de coluna. (OLIVEIRA, 2009, p.265)

2.6.2.3 Folha de Verificação (*checklist*)

"Formulário no qual os itens a serem verificados para a observação do problema já estão impressos, com o objetivo de facilitar a coleta e o registro dos dados. O tipo de folha de verificação a ser utilizado depende do objetivo da coleta de dados. Normalmente é construída após a definição das categorias para a estratificação dos dados." (WERKEMA, 1995, p.42)

2.7 CONSIDERAÇÕES SOBRE A REVISÃO DE LITERATURA

Ao longo da revisão da literatura foi descrito todo o processo de desenvolvimento das normas, com o objetivo de se compreender a necessidade de cada uma delas para depois entrar nas normas que são objeto do estudo.

Para isso o ideal foi à abordagem iniciada pelo processo de desenvolvimento das normas onde começou pela descrição da BS7799, pois ela é o inicio do desenvolvimento de todas as outras principalmente do grupo de normas 27000, pode-se dizer que ela é a "mãe" das normas para segurança da informação.

Estão sendo desenvolvidas normas de segurança da informação que atendam ás necessidades dos mais diferentes tipos de organização, isto é percebido através do grupo de normas 27000, nela estão contidas normas relativas às mais diversas áreas entre elas a saúde e as telecomunicações que já estão prontas. Esse processo de desenvolvimento tem-se levado ao longo de anos com o objetivo de melhor se adequar ás necessidades dos seus usuários, sendo que, as normas criadas estão voltadas ao SGSI, ou seja, atendem aos critérios estabelecidos pelo SGSI.

Ao longo da seção 2.4.3 objetivou-se descrever a norma ABNT NBR ISO/IEC 27002, porém ela é a norma ABNT NBR ISO/IEC 17799 com revisões. A bibliografia analisada é referente à ABNT NBR ISO/IEC 17799, entretanto por serem idênticas salvo algumas alterações foi utilizada para se referenciar a ABNT NBR ISO/IEC 27002.

A abordagem sobre Politica de Segurança da Informação - PSI foi realizada depois do conhecimento das normas, pois segundo a literatura é necessário conhecer bem as normas e suas aplicações para depois se elaborar uma PSI. Sendo assim, ela traz aspetos gerais sobre o processo de elaboração da PSI e os beneficios causados por ela á curto, médio e longo prazo.

Por último na seção 2.6 foi feita uma abordagem sobre processos com foco na qualidade, pois o objetivo do estudo é a apresentação de um processo e necessariamente deverão ser conhecidas as melhores ferramentas para representação.

3. PROCEDIMENTOS METODOLÓGICOS

A escolha de uma metodologia de levantamento de dados é uma etapa importante para elaboração do trabalho, pois por meio dela definem-se procedimentos para alcançar os objetivos propostos. O presente trabalho foi realizado durante o segundo semestre do ano de 2010.

Para realização de uma pesquisa podem ser utilizadas duas abordagens: qualitativa ou quantitativa. A pesquisa quantitativa é um método de pesquisa social que utiliza técnicas estatísticas, normalmente implica a construção de inquéritos por questionário. Os dados da pesquisa qualitativa objetivam uma compreensão profunda de certos fenômenos sociais apoiados no pressuposto de maior relevância do aspecto subjetivo da ação social.

> Na pesquisa qualitativa a quantidade é substituída pela intensidade, pela imersão profunda através da observação participante, das entrevistas em profundidade, da análise de diferentes fontes que podem ser cruzadas e que atingem diferentes níveis de compreensão que não podem ser alcançadas através de uma pesquisa quantitativa. (GOLDENBERG, 1998, p.50).

A pesquisa qualitativa tem caráter exploratório, sendo que ela estimula o entrevistado a pensar e falar livremente sobre o tema, fazendo emergir aspectos subjetivos de forma espontânea.

“Enquanto que o método quantitativo supõe uma população de objetos comparáveis, o método qualitativo enfatiza as particularidades de um fenômeno em termos de seu significado para o grupo pesquisado”. (GOLDENBERG, 1998, p.49-50)

Para realização do trabalho foi feita a abordagem **qualitativa**, pois esta apresenta um conjunto de características que se adequam ao projeto.

3.1 CLASSIFICAÇÃO DA PESQUISA REALIZADA

Para definição de uma metodologia há que se considerarem os tipos de pesquisa que melhor se adequam ao projeto a ser realizado.

Vergara (2006) propõe dois critérios para classificação das pesquisas: quanto aos fins e quanto aos meios.

A presente pesquisa é classificada quanto aos fins como **descritiva**, pois foi realizado um levantamento das características que compõem um fenômeno/fato/processo. Segundo Santos (2004, p.26) a pesquisa descritiva "é normalmente feita na forma de levantamentos ou observações sistemáticas". A pesquisa descritiva visa descrever as características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis. Foi feito uma aproximação do tema Segurança da Informação, de forma a explorar o assunto por meio da apresentação de conceitos e da apresentação das normas de Segurança da Informação em seguida a apresentação de um processo com bases nos requisitos previamente apontadas.

Quanto aos meios é classificada como pesquisa **documental**, pois faz uso de documentos diversos como normas e do modelo utilizado pela DQS e também como pesquisa **bibliográfica**, uma vez que é realizada extensa revisão da literatura pertinente para a construção do referencial teórico.

De acordo com Gil (2009) enquanto a pesquisa bibliográfica utiliza fundamentalmente contribuições dos diversos autores sobre determinado assunto, a pesquisa documental vale-se de materiais que não receberam ainda um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetivos da pesquisa.

As informações que foram utilizadas na pesquisa foram obtidas por meio da análise e interpretação das normas e dos documentos disponibilizados pela DQS, também foram obtidas informações em sites e livros da área.

3.2 ANÁLISE E TRATAMENTO DOS DADOS

Os dados obtidos foram analisados e interpretados de forma a comprovar a sua veracidade, e posteriormente foram explicitados por meio de figuras ou quadros explicativos.

Com os dados organizados e com o apoio da literatura apresentou-se um processo para certificação da qualidade na área de Segurança da Informação.

4. APRESENTAÇÃO E ANÁLISE DOS RESULTADOS DA PESQUISA

O capítulo que se segue objetiva a apresentação e análise dos resultados obtidos na pesquisa, sendo assim foi descrito um processo de preparação para certificação da qualidade em Segurança da Informação, objetivo do estudo. Em seguida foram analisados o processo apresentado e o modelo utilizado pela DQS a fim de realizar comparações entre as duas.

4.1 RESULTADOS DA PESQUISA

Nessa seção é apresentada a proposta de um processo de preparação para certificação da qualidade em Segurança da Informação.

Para representar o processo proposto foi utilizado o diagrama de causa e efeito. O processo de certificação em Segurança da Informação proposto apresenta um conjunto de causas que são as etapas pela qual é formada e da realização de todas as etapas surgirá um efeito que é a certificação da qualidade em Segurança da Informação.

A organização só obterá o certificado de qualidade em Segurança da Informação se ela adotar todos os procedimentos descritos no processo, sendo assim o objetivo final do processo apresentado é a qualidade em Segurança da Informação. A figura 6 apresenta o processo de preparação para certificação da qualidade em Segurança da Informação proposto.

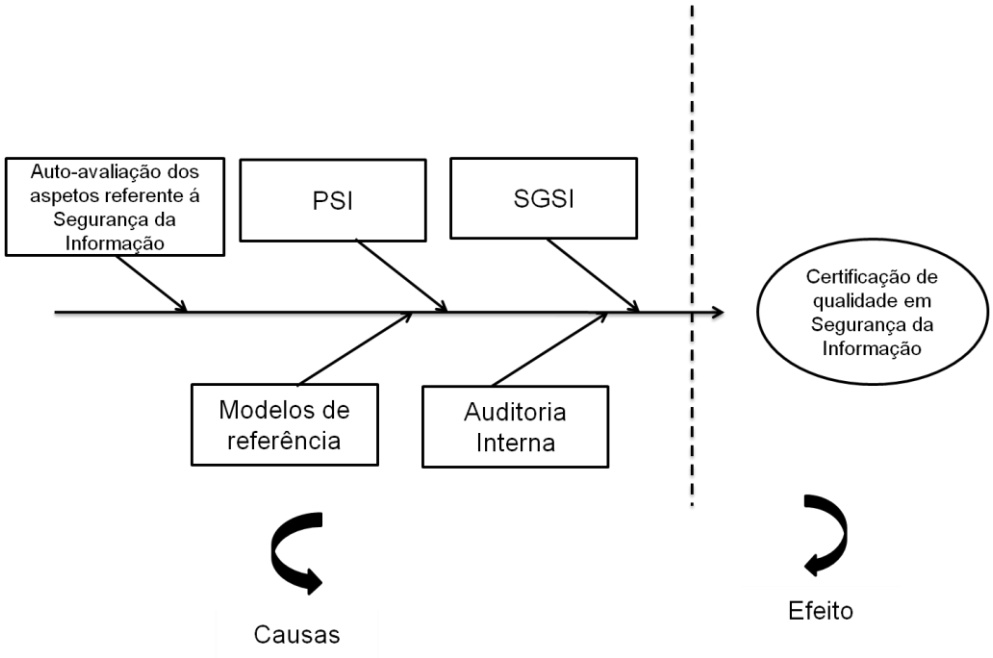

FIGURA 5 – PROCESSO DE PREPARAÇÃO PARA CERTIFICAÇÃO DA QUALIDADE EM SEGURANÇA DA INFORMAÇÃO
FONTE: AUTORA (2010) ADAPTADO DO DIAGRAMA DE CAUSA E EFEITO

O processo proposto é constituído de cinco etapas são elas:

Etapa1: Auto-avaliação dos aspetos referente à Segurança da Informação

Etapa2: Política de Segurança da Informação (PSI) – aqui foram sugeridas orientações que a organização deverá seguir para elaborar a PSI.

Etapa3: Sistema de Gerenciamento de Segurança da Informação (SGSI) – nesta fase foi descrita como a organização deverá implementar o SGSI e os controles utilizados para monitorar a sua eficácia.

Etapa4: Modelos de Referência – aqui foi apresentado um processo de preparação para certificação utilizado por uma empresa experiente no mercado.

Etapa5: Auditoria interna – toda a organização que deseja obter uma certificação deve passar por uma auditoria interna, sendo assim nessa etapa foram descritos os principais aspetos da Segurança da Informação que deverão passar por um processo de auditoria.

As subseções que se seguem objetivam a descrição de cada uma dessas etapas.

4.1.1 Etapa1 - Auto-avaliação dos aspetos referente á Segurança da Informação

Para preparação para a certificação inicialmente tem que ser realizada uma análise organizacional referente á Segurança da Informação.

Necessariamente para o desenvolvimento de qualquer processo dentro de uma organização há que se conhecer bem o ambiente interno e externo em que ela está inserida. Para realizar a análise tanto interna como externa do ambiente organizacional relativo á medidas de segurança recomenda-se o uso da ferramenta SWOT.

A análise de SWOT consiste da avaliação global das forças, fraquezas, oportunidades e ameaças, ela envolve o monitoramento dos ambientes interno e externo da organização (Kotler e Keller, 2007). A organização deverá realizar a análise de SWOT com o objetivo de conhecer os riscos originados pelo ambiente (interno e externo), assim como conhecer os benefícios que a segurança das informações traz ou poderá trazer para ela.

A figura 6 retrata alguns aspetos que deverão ser avaliados na organização tendo em conta os requisitos de segurança de que ela dispõe.

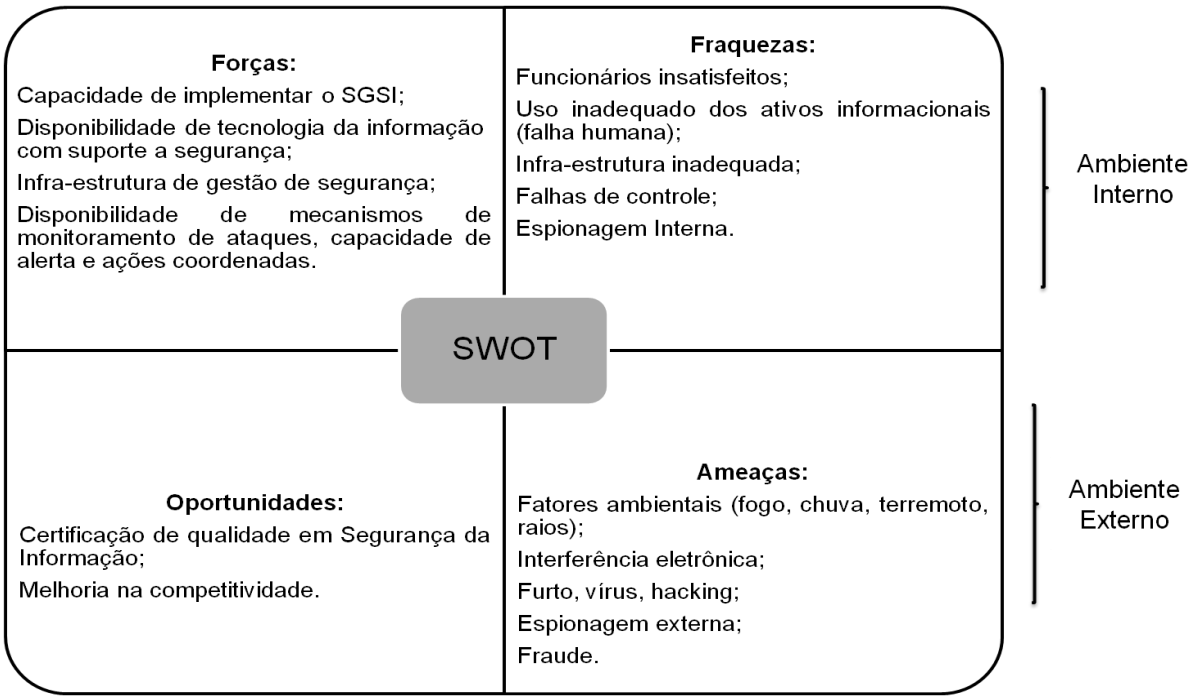

FIGURA 6 - ANÁLISE DE SWOT RELATIVA Á SEGURANÇA DA INFORMAÇÃO NA ORGANIZAÇÃO
FONTE: A AUTORA (2010)

4.1.2 Etapa2 - Política de Segurança da Informação (PSI)

Nessa etapa foram apresentadas as orientações que a organização deverá seguir no momento de elaboração de uma PSI. Esta etapa aborda os seguintes assuntos: fases para elaboração da PSI, a estrutura da PSI e por último algumas considerações que a organização deverá levar em conta no momento da elaboração da PSI.

A norma ABNT NBR ISO/IEC 27002 estabelece que a PSI deva ser clara e alinhada com os objetivos da organização. A norma acrescenta ainda que a direção da organização deve demonstrar total apoio e comprometimento com a PSI por meio de apoio e revisão contínua da norma.

Outro aspecto que deverá ser mencionado a cerca das diretivas estabelecidas na ABNT NBR ISO/IEC 27002 e em outras bibliografias consultadas (FERREIRA; ARAÚJO, 2006) é a necessidade da existência de um gestor de segurança da informação e de um Comitê de Segurança da Informação que se responsabilize pelo desenvolvimento, análise crítica e avaliação da política de segurança da informação. Ferreira e Araújo (2006, p. 11) acrescentam que esse "Comitê deve catalogar todas as informações da organização e agrupá-las por categorias", cada uma dessas categorias deverá ter um proprietário responsável para controle, acesso, manuseio e segurança geral.

Descrita as orientações apontadas pela norma ABNT NBR ISO/IEC 27002 e por Ferreira e Araújo (2006), a seção que se segue apresenta as fases para elaboração da PSI de acordo com as orientações acima apresentadas.

4.1.2.1 Fases para elaboração da PSI

Para a elaboração de uma PSI há que se ter uma determinada ordem a seguir para que não seja ignorada nehuma das fases. Recomenda-se que antes de

iniciar a descrição da política seja elaborado um *checklist* contendo todas as fases demonstradas na figura abaixo.

De acordo com Ferreira e Araújo (2006) e a ABNT NBR ISO/IEC 27002 (2005) foram apontadas as seguintes fases de elaboração da PSI:

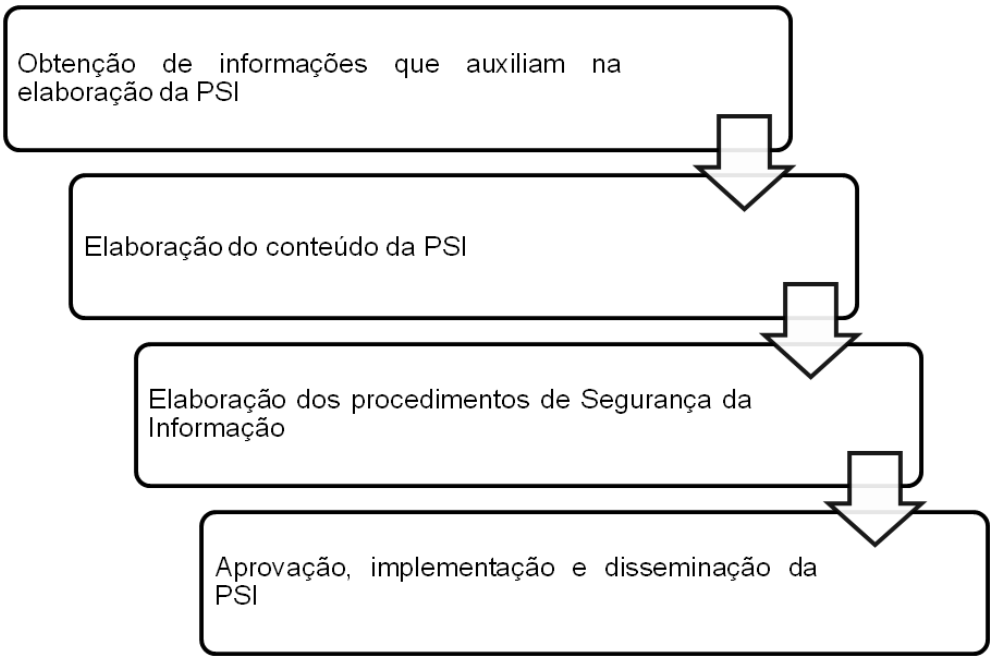

FIGURA 7 - ETAPAS PARA ELABORAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
FONTE: A AUTORA (2010) BASEADO EM FERREIRA; ARAÚJO (2006, p.12)

a) Obtenção de informações que auxiliam na elaboração da PSI

De acordo com Ferreira e Araújo (2006), para obtenção dessas informações o autor da política deverá conhecer os objetivos, a missão e a visão da organização, assim como os processos de negócio, as tendências de mercado no ramo de atividade da organização, os fluxos de informação entre os ambientes da organização. Para elaboração da PSI o autor deverá levantar informações a cerca da estrutura da organização.

Para atender os objetivos da primeira etapa, poderá ser realizado um levantamento de dados, por meio de:

- entrevistas com a alta administração nível estratégico - para coleta de informações com a alta administração é recomendado entrevista, pois esta técnica pode ser aplicada a um número menor de indivíduos que é o caso da alta administração normalmente formado por um grupo de poucas pessoas.

- questionários para os funcionários de nível tático e operacional – essa técnica é recomendada quando se tem um maior número de indivíduos a serem estudados, e o tempo para realização do estudo ser relativamente pouco.

b) Elaboração do conteúdo da PSI

Ferreira e Araújo (2006) afirmam que na elaboração ou desenvolvimento do conteúdo da PSI deverão estar contidas os seguintes requisitos:

1. Gerenciamento da política de segurança - nela deverá conter:
   - definição de segurança da informação;
   - conjunto de termos relacionados à PSI e a Segurança da Informação relativa á organização;
   - objetivos da política;
   - gestão de versões, manutenção e revisão da PSI;
   - referências.

2. Definição das regras e responsabilidades

A responsabilidade pela preservação da segurança da informação e dos recursos que as produzem é da organização (FERREIRA; ARAÚJO, 2006, p.41), para garantir a segurança da informação na organização, deverão ser estabelecidas as regras e responsabilidades para cada área da organização. Ferreira e Araújo (2006, p. 41) apontam as seguintes áreas:

- Comitê de Segurança da Informação – responsável pela divulgação e estabelecimento dos procedimentos de segurança. O comitê deverá conter representantes das áreas de Tecnologia, Jurídica, Comercial, Financeira, Negócio, entre outros. Dentre as responsabilidades do comitê destacam aprovação da PSI, aprovação dos controles de segurança, apoio para implementação e minimização de riscos, suporte ás iniciativas de segurança. No final do semestre deverá ser elaborado um documento denominado Relatório do Comitê de Segurança contendo a descrição de todas as atividades realizadas, a avaliação da efetividade do sistema de controle de segurança, análise parcial das ações realizadas e descrição das deficiências detectadas.
- Proprietário das Informações – responsável pela autorização do acesso ás informações de acordo com a PSI estabelecida na organização. O proprietário

das informações tem total domínio sobre as informações geradas, ele é responsável por classificar as informações conforme os critérios estabelecidos pela PSI, pela revisão das informações classificadas, autorização do acesso e revisão das informações e pela garantia de que os usuários compreendam e sigam os procedimentos de segurança.

- Área de Segurança da Informação - responsável pela proteção dos ativos informacionais, minimizando os riscos. De entre as suas responsabilidades destacam-se fazer com que se cumpre a PSI.

- Usuário das Informações – indivíduos com acesso á informação. São responsáveis pelo entendimento e seguimento da política, cumprimento das regras, uso das informações apenas para propósitos de negócio e informar qualquer violação/incidente de segurança.

- Recursos Humanos - responsável pelo estabelecimento de sanções e penalidades a serem aplicadas nas situações em que a política foi desrespeitada.

3. Classificação das Informações

Após o estudo da organização é necessário realizar uma classificação dos ativos informacionais de que a organização dispõe. Segundo Ferreira e Araújo (2006) a organização poderá fazer um inventário dos ativos de informação que ela dispõe de acordo com a natureza do ativo – ver quadro 8.

Natureza do ativo	**Ativos de Informação**
Informação	Banco de dados e serviços magnéticos Documentação de sistema e manual do usuário Material de treinamento Procedimentos operacionais de recuperação Planos de continuidade
Documentos em papel	Contratos Documentos da empresa Relatórios confidenciais
Software	Aplicativos Sistemas Operacionais Ferramentas de desenvolvimento Utilitários do sistema

(Continua)

(Conclusão)

Natureza do ativo	Ativos de Informação
Físico	Equipamentos computacionais Equipamentos de comunicação (roteadores, PABXs, fax, secretárias eletrônicas) Mídia magnética (fitas e discos) Gerador, no-break e ar-condicionado Móveis e acomodações
Pessoa	Empregados, estagiários, terceiros e fornecedores
Serviço ou atividade	Computação (aplicação de patches, backup) Comunicação (ligações telefônicas, videoconferências) Utilidades gerais

QUADRO 7 - INVENTÁRIO DOS ATIVOS DE INFORMAÇÃO
FONTE: FERREIRA; ARAÚJO (2006, p.50)

As informações podem ser classificadas segundo Ferreira e Araújo (2006, p.52-53) em 3 níveis, são eles:

- informação pública: aquela que não necessita de sigilo e de livre acesso para todos os membros da organização. Essas informações não precisam ser protegidas e se divulgadas não trarão impactos á organização. Ex.: demonstrações financeiras, testes de sistemas.
- informação interna: aquela em que o acesso deve ser evitado, porém se tornarem públicas não trará impactos críticos á organização. Ex.: agendas de telefone e ramais.
- informação confidencial: aquela que deve ser protegida o acesso por indivíduos de dentro da organização e externos. O acesso não autorizado á essas informações compremeterão as operações da organização causando perdas financeiras e de competitividade.

A PSI deverá conter orientações relativas ao armazenamento e descarte das informações, sendo que as orientações devem obedecer aos requisitos de confidencialidade (FERREIRA; ARAÚJO, 2006).

4. Descrição dos procedimentos de segurança

Os procedimentos de segurança são todas as ações realizadas para garantir a Segurança da Informação. Alguns exemplos apontados por Ferreira e Araújo (2006) são:

- orientações para classificação e tratamento das informações;
- controles (acesso, criptografia) e monitoramento;
- uso da internet;
- aquisição e uso de hardware e software entre outros.

c) Elaboração dos procedimentos de Segurança da Informação

A Política de Segurança da Informação é de fundamental importância na garantia da Segurança da Informação da organização. Ela abrange toda a organização, sendo que ela pode ser dividida em 3 blocos segundo Ferreira e Araújo (2006, p.59-60):

- diretrizes: direcionadas ao nível estratégico;
- normas: direcionadas ao nível tático;
- procedimentos e instruções: direcionadas ao nível operacional.

Ferreira e Araújo (2006) afirmam que a PSI deverá ser elaborada tendo em conta os seguintes aspectos:

- utilização dos recursos de TI: referente á disponibilidade dos recursos de tecnologia, titularidade e segurança das informações, sigilo da informação, autorização para uso dos recursos de TI, estações de trabalho e servidores, estações móveis de trabalho e termo de confidencialidade.
- proteção contra software malicioso: referente aos vírus de computador e aos softwares não autorizados.
- procedimentos para acesso à internet: relativo aos procedimentos de uso da internet nas organizações.

d) Aprovação, Implementação e disseminação da PSI

A ABNT NBR ISO/IEC 27002 estabelece que a PSI deverá ser aprovada pela alta administração e cumprida por todos. Ela acrescenta ainda que a PSI deverá ser seguida por todos inclusive a alta administração para que seja respeitada e tenha resultados efectivos.

Para a implementação a norma brasileira ABNT NBR ISO/IEC 27002 estabelece que primeiramente deva ser definido o que é a Segurança da Informação, quais os seus objetivos e a sua importância para a organização. A direção da organização deverá demonstrar:

- apoio e compremetimento da organização com a PSI que deverá estar alinhada com os objetivos e estratégias do negócio;
- definição dos objetivos de controle, ou seja, o que se deseja controlar com a implementação da PSI e gerenciamento de risco;
- descrição das políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização.

A disseminação da PSI na organização e pelas partes externas poderá ser feita por meio de:

- distribuição de cópias impressas ou eletrônicas;
- palestras;
- teatros.

4.1.2.2 A estrutura da PSI

O documento correspondente a Política de Segurança da Informação deverá conter os seguintes elementos:

a) cabeçalho do documento: onde deverá constar o título do documento, a data de criação, data de aprovação e de modificação.

b) corpo do documento: onde deverá constar uma introdução explicando á necessidade da criação da política, objetivos da política, a estrutura normativa do

documento (normas, procedimentos), descrição de todos os ativos de informação, apresentação do comitê gestor de segurança da informação e as suas respetivas responsabilidades, área de abrangência da política de segurança, normas e procedimentos relativos às diversas áreas de abrangência e as sanções relativas ao não cumprimento da política.

c) final do documento: glossário contendo o conjunto de termos relativos à segurança e política de segurança da informação vale lembrar que para elaboração do glossário e da política deverá ser evitado o uso de termos técnicos, também deverá constar uma ata de aprovação da política.

4.1.2.3 Considerações relativas à PSI

A elaboração da PSI é importante para a garantia da segurança das informações da organização, entretanto durante o seu desenvolvimento deverão ser consideradas as seguintes constatações:

a) o autor da política deverá considerar que a Política de Segurança da Informação não é só relativa aos equipamentos (hardware e software), mas sim principalmente as pessoas, sendo assim deverão despendiar algum tempo treinando e educando as pessoas no que diz respeito á segurança da informação;

b) è necessário conhecer bem a organização e as normas de Segurança da Informação para poder elaborar uma PSI;

c) não existe um modelo pronto de política para se adotar à organização, o que se pode encontrar são sugestões para elaboração que deverão ser adaptados ás necessidades da organização;

d) deverá haver a renovação da política sempre que houver mudanças na organização tanto a nível de negócios como da segurança da informação;

e) a Segurança da Informação depende exclusivamente dos usuários, logo deverá ser implementada na organização uma “cultura de segurança da informação”;

f) sugere-se a elaboração de um *checklist* para verificar se a política atende a todos os requisitos de Segurança da Informação da organização;

g) analisar a relação custo benefício da adoção da Política de Segurança da Informação.

4.1.3 Etapa3: Sistema de Gerenciamento de Segurança da Informação (SGSI)

Para que haja segurança da informação nas organizações deverá existir um meio de controlar o quê e como estão sendo realizadas ações relativas á Segurança da Informação. A necessidade de gerenciamento da Segurança da Informação na organização deverá ser suprida por meio da criação de um sistema que controla todas as ações realizadas para satisfazer os requisitos de segurança.

A norma brasileira ABNT NBR ISO/IEC 27001(2006, p.3) define Sistema de Gerenciamento da Segurança da Informação como sendo “a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação”. Ainda acrescenta que o sistema de gestão inclui estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

Pela definição apresentada pode-se afirmar que o SGSI é composto pelas fases apresentadas na figura 9:

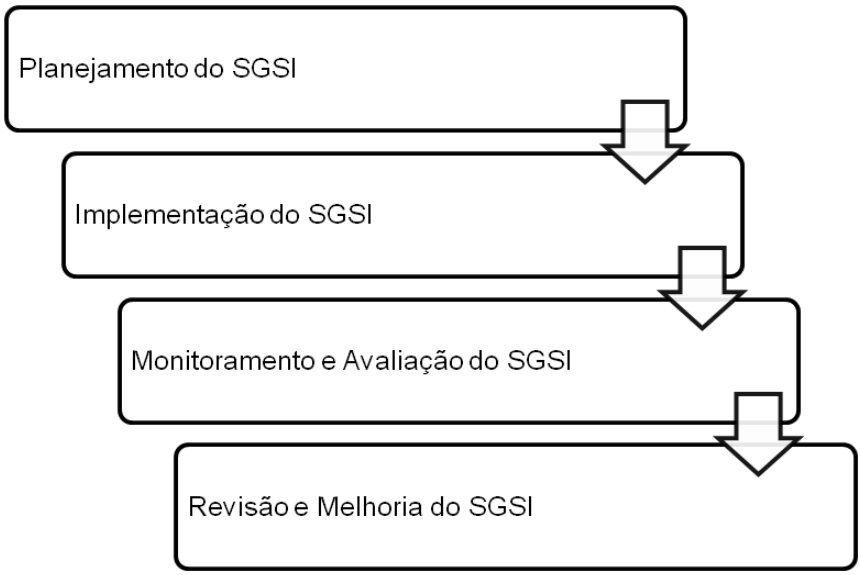

FIGURA 8 - ETAPAS DO SISTEMA DE GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO
FONTE: A AUTORA (2010) BASEADO NA ABNT NBR ISO/IEC 27001 (2006)

A seguir são descritas cada uma das fases acima apresentadas de acordo com o estabelecido na ABNT NBR ISO/IEC 27001 a cerca do SGSI.

Fases para elaboração do SGSI

a) Planejamento do SGSI

O planejamento do SGSI é a etapa mais importante do sistema, pois nela se define todos os objetivos que deverão ser alcançados com o uso do sistema e as respetivas ações a serem realizadas para alcance desses objetivos. O planejamento deverá ser feito visando atingir objetivos a curto, médio e longo prazo relativo á Segurança da Informação.

O planejamento do sistema deverá ser feito em dois níveis:

No nível da organização deverá ser feito um planejamento definindo:

- quais os objetivos que a organização pretende alcançar com o SGSI;
- que meios ela dispõe que podem auxiliar no desenvolvimento do SGSI;
- quais os processos críticos de negócio que deverão ser assegurados pelo SGSI.

No nível da Segurança da Informação o planejamento deverá definir:

- quais os fluxos informacionais que existem na organização;

- quais os ativos informacionais de que a organização dispõe;
- qual o nível de segurança que esses ativos informacionais necessitam.

As respostas á essas perguntas devem ser obtidas por meio de aplicação de questionário ou entrevista á alta administração.

No planejamento do sistema a organização deverá definir:

- os limites do SGSI, ou seja, quais os ativos que necessitam ser gerenciados;
- uma política de segurança da informação que atenda aos requisitos do SGSI;
- determinar a aplicabilidade do SGSI, ou seja, para que ele está sendo projetada, quais os objetivos que se pretende atingir;
- apontar os problemas que levam ao desenvolvimento do SGSI e as soluções para esses problemas – análise e gestão de riscos;
- apontar de onde surgem as falhas na segurança dos sistemas (provocadas por falta de soluções técnicas ou devido ao mau uso pelos usuários e demais) e apontar possíveis soluções á essas falhas;
- os objetivos do SGSI, o que a organização pretende com o desenvolvimento do sistema, assim como quais os problemas que deverão ser solucionados por meio do SGSI;
- documentar o SGSI.

O documento da definição do SGSI deverá ser apresentado à alta administração para que possa ser aprovado antes de passar para a etapa seguinte.

b) Implementação do SGSI

A implementação de um Sistema de Gerenciamento da Segurança da Informação na organização requer a colaboração e a disponibilidade de todos os funcionários, pois essa é a etapa em que as atividades planejadas serão colocadas na prática. Para implementar o SGSI deverão ser realizadas as seguintes tarefas:

- desenvolvimento e implementação de um plano de análise e gestão de riscos;
- realizar uma análise de como a organização está hoje em relação á requisitos de segurança, essa análise deverá ser documentada para posterior comparação em relação á como a organização estará depois da implementação do SGSI;

- descrever os procedimentos para a solução dos problemas de segurança da Informação;
- definir medidas para deteção de problemas de segurança;
- definir meios para controlar a eficácia das soluções apresentadas para os problemas expostos anteriormente.

c) Monitoramento e Avaliação do SGSI

O monitoramento e avaliação é a etapa em que a organização verifica a eficácia do Sistema de Gerenciamento de Segurança da Informação para a organização.

Para o monitoramento deverão ser realizadas as seguintes atividades:

- estabelecer medidas de controle (indicadores);
- identificar os principais pontos onde deverão ser colocados meios para monitoramento a fim de apontar erros, identificar tentativas de violação á segurança, determinar medidas para mitigar essas tentativas, etc;
- estabelecer um período especifico para realização do monitoramento e de auditorias internas para verificar a eficácia do SGSI;
- apresentar um relatório do monitoramento, que deverá ser disseminado por toda a organização.

Para avaliação do SGSI deverão ser realizadas as seguintes atividades:

- comparar a análise realizada anterior à aplicação do SGSI com o relatório resultante do monitoramento do SGSI (após a implementação do SGSI);
- identificar as melhorias alcançadas e os pontos em que não houve melhorias consideráveis;
- identificar o porquê de não haver melhorias em determinados aspectos da organização após a implementação do SGSI (identificar as falhas).

d) Revisão e melhoria do SGSI

Após o monitoramento do SGSI e sua avaliação deverá se pensar em medidas corretivas a serem estabelecidas a fim de corrigir as falhas apresentadas. Para isso deverão ser realizadas as seguintes atividades:

- rever o SGSI que foi proposto e que está sendo implementado;
- apresentar medidas corretivas correspondentes as falhas apresentadas no SGSI;
- aplicar essas medidas;
- verificar se essas medidas aplicadas estão auxiliando no alcance dos objetivos do SGSI.

4.1.4 Etapa4 - Modelos de Referência

Nesta etapa deverão ser consultadas modelos de referência que corresponde aos processos de preparação para certificação utilizada por outras empresas. Esses modelos servirão como base de apoio proporcionando a organização o contato com experiências benéficas evitando que ela caia em algum erro já conhecido. Sendo assim foi apresentada uma organização de renome em Segurança da Informação, tanto na preparação como na certificação das organizações.

A empresa escolhida para ser apresentada é a DQS – *Manegement Systems Solutions.* As causas que levaram a escolha do processo de preparação para certificação utilizada pela DQS é primeiramente pelo fato de ela ser uma empresa mundialmente conhecida na área de Segurança da Informação e também devido ao fato de ela prestar serviços sem fins lucrativos.

A DQS está preocupada com a divulgação e conscientização das organizações da importância da proteção dos ativos informacionais. Sendo assim ela se disponibilizou em auxiliar no desenvolvimento do trabalho sem que por isso houvesse a necessidade de dispêndios com a realização de um curso ou certificação para conhecer o processo por ela utilizado.

4.1.4.1 DQS – Manegement Systems Solutions

A DQS é uma Associação Alemã para Certificação de Sistemas de Gestão, constituída em 1985, para certificar Sistemas da Qualidade em conformidade com os requisitos das normas ISO série 9000 ou outras de igual relevância.

Fundada no Brasil em agosto de 1994 é responsável pela coordenação das certificações no Brasil e nos países vizinhos. Ela mantém acordos operacionais com várias certificadoras de outros países latino-americanos a fim de atender empresas que solicitem uma “auditoria conjunta”. A DQS não objetiva lucros e desempenha sua atividade com o propósito e objetivo dos seus fundadores e de fazer agregar real valor a empresa por ela certificada, resultando em satisfação de todas as partes envolvidas, clientes, sócios, colaboradores e fornecedores.

Com 45 mil localidades certificadas em mais de 100 países a DQS contém mais de 60 escritórios em quase 50 países assegura um vasto leque de serviços de avaliação que garante a proximidade com o cliente e valor agregado duradouro.

No Brasil a DQS fica localizada em São Paulo na Avenida Adolfo Pinheiro, 1001 - 3º andar. Para obtenção das informações sobre o processo utilizado pela DQS foi feito contacto via telefone e email com o senhor Roberto Melo que é o Representante da Administração da empresa.

4.1.4.2 Processo de preparação para certificação utilizado pela DQS com base na ISO 27001

A DQS desenvolveu um conceito de avaliação que pode ser personalizado a fim de atender as necessidades de segurança de cada cliente. Ela apóia os seus clientes em todas as etapas do processo, desde a mais simples que é a auto avaliação até o mais complexo. A figura 9 descreve o processo de preparação para certificação utilizada pela DQS.

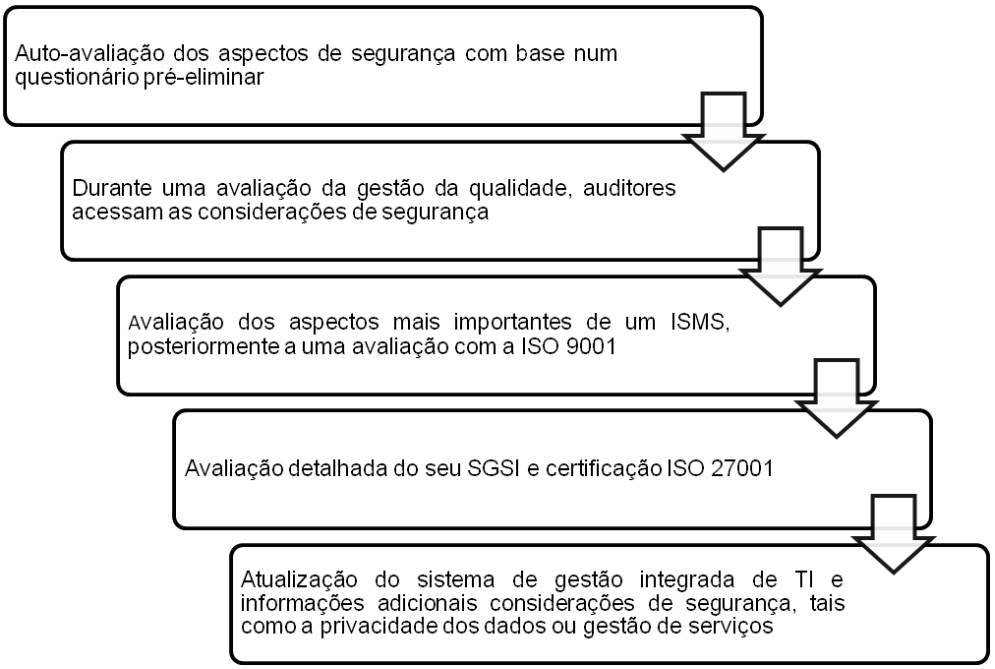

FIGURA 9 – PROCESSO DE PREPARAÇÃO PARA CERTIFICAÇÃO UTILIZADO PELA DQS
FONTE: A AUTORA (2010) BASEADA NO MATERIAL TÉCNICO DA DQS (04/2010)

Segundo informações fornecidas pela DQS (04/2010), o processo de certificação garante o sucesso empresarial sustentável através da segurança da informação por meio da:

- manutenção da continuidade de negócios;
- transparência para os clientes com requisitos de segurança rigorosos;
- consciência maior segurança dentro da organização;
- melhoria da proteção dos dados/informações;
- maior confiança entre as partes interessadas;
- redução do risco de responsabilidade;
- proteção de áreas de segurança física.

4.1.5 Etapa5 - Auditoria interna

Para verificar se o Sistema de Gerenciamento de Segurança da Informação SGSI está em conformidade com os padrões estabelecidos pelas normas de referência e que a Política de Segurança da Informação tem todos os controles

estabelecidos pelo SGSI recomenda-se a realização de uma auditoria interna. Essa auditoria realizará uma análise de todos os documentos do SGSI e do PSI, com o objetivo de identificar possíveis inconsistências. Segundo Ferreira (2003, p.137) a auditoria consiste em um serviço de apoio da organização, cuja natureza é examinar, avaliar, a adequação e eficiência dos controles de segurança.

A organização deverá aplicar a auditoria interna a fim de identificar se o SGSI estabelecido:

- atende aos requisitos estabelecidos pela norma de referência (ANBT NBR ISO/IEC 27001);
- resolve os problemas identificados no momento do planejamento que justificaram a sua implementação (atende aos objetivos propostos);
- está de acordo com o que foi estabelecido no planejamento.

A auditoria interna deverá ser realizada no sentido de acompanhamento das atividades da organização em relação ao processo de certificação da qualidade em Segurança da Informação, analisando o efetivo desempenho das funções que o SGSI deverá desempenhar, bem como verificar se estão sendo adotados os procedimentos sugeridos na PSI para correção de eventuais falhas cometidas durante planejamento e que tenham sido detetadas no momento do monitoramento e avaliação.

Segundo Imoniana (2005, p.41), os principais objetivos de um sistema de controle interno são:

- salvaguardar o ativo de uma organização;
- manter a integridade;
- correção e confiabilidade dos registros;
- promover a eficiência operacional e encorajar o cumprimento dos procedimentos e políticas da gerência.

Ferreira (2003, p.139) afirma que o objetivo da auditoria é avaliar se a organização está operando dentro dos padrões desejados pela política de segurança da informação.

Os principais objetivos do desenvolvimento da auditoria interna como parte do processo de certificação são:

- controle da Segurança da Informação na Organização;
- análise financeira (custo/benefício) - verificar se os custos financeiros realizados para manter a segurança da informação estão sendo bem aproveitados;
- garantia dos ativos informacionais da organização - verificar se estão sendo salvaguardados os ativos informacionais de que a organização dispõe.

4.1.5.1 Controles de segurança e privacidade

Esses controles são referentes á proteção da informação, evitando-se atos de destruição intencionais, ou não intencionais, acidentes e outros atos de sabotagem. Os ativos informacionais da organização deverão ser protegidos de furtos, manipulação fraudulenta ou divulgação de informações sigilosas para competidores a fim de obter vantagens próprias e também deverão prevenir a ocorrência de incidentes fatais que podem causar estragos irreversíveis á organização (IMONIANA, 2005, p.45-46). Os controles internos em segurança são dinâmicos, pois mudam de acordo com as mudanças na evolução tecnológica. No momento de estabelecimento de um processo de auditoria deverá ser definidos períodos de tempo em que a auditoria deverá ser realizada para que ela não deixe de identificar possíveis problemas.

Para implementação de controles de segurança numa organização Imoniana (2005) sugere o mapeamento do ambiente de segurança – aquele onde os recursos de segurança são instalados. A figura 10 apresenta o modelo sugerido por Imoniana.

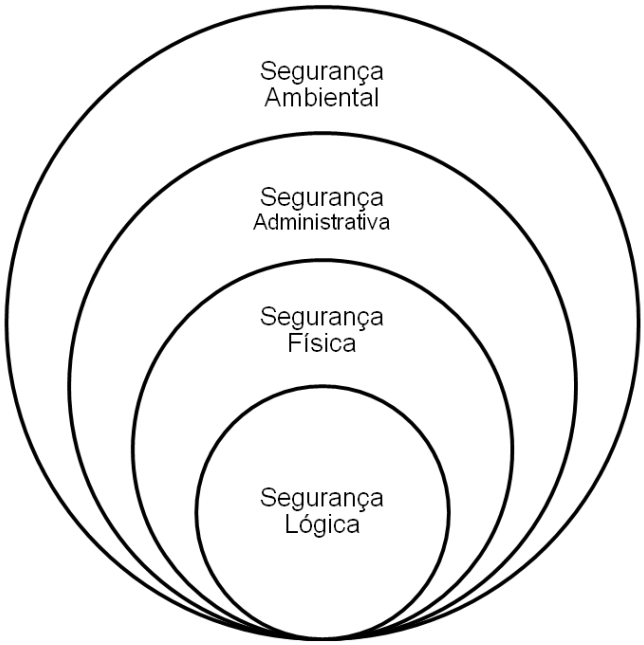

FIGURA 10 - ORGANIZAÇÃO E AMBIENTE DE SEGURANÇA
FONTE: IMONIANA (2005, p.47)

4.1.5.2 Fases para estabelecimento de uma auditoria

No processo de preparação para a certificação da qualidade em Segurança da Informação proposto apresentou-se como modelo de auditoria interna o estabelecido pelo IMONIANA (2005, p.23). Esse processo de auditoria é composto pelas seguintes fases:

a) Planejamento

Objetiva evitar quaisquer surpresas que possam acontecer tanto nas atividades empresariais, como também em relação ás responsabilidades do auditor. Nesta etapa deverá ser desenhada uma “Matriz de Risco” que deverá ser atualizada a partir dos resultados obtidos nos testes e nas avaliações dos auditores, assim como do impacto das mudanças ocorridas no negócio.

b) Escolher a equipe

A partir do planejamento é possível definir o perfil da equipe de auditoria que deverá contemplar:

- perfil histórico e profissional;

- experiência acumulada por ramos de atividade;
- conhecimentos específicos;
- formação acadêmica;
- apoio do grupo de especializações;
- línguas estrangeiras;
- disponibilidade para viagens; etc.

c) Programar equipe

A equipe deve ser programada a fim de executar os trabalhos;

d) Execução dos trabalhos e supervisão

As tarefas deverão ser realizadas por auditores que tenham formação, experiência e treinamento adequados no ramo de especialização. Os trabalhos serão desenvolvidos conforme a experiência que cada auditor detém, ou seja, o auditor mais experiente realizará tarefas mais complexas e de maior risco e os menos experientes realizarão tarefas menos complexas e com menor risco.

e) Revisão dos papéis de trabalhos

Toda a prática de auditoria objetiva atingir a qualidade, para isso os papéis de trabalhos deverão ser revisados por supervisores que tem como função verificar se cada passo da auditoria foi cumprida.

f) Atualização do conhecimento permanente

A manutenção, revisão e atualização de todas as atividades e documentos que fazem parte da auditoria contribuirão para a melhoria do processo e assim para a redução das horas de auditoria do período seguinte.

g) Avaliação da equipe

Para que haja aprimoramento da equipe de auditoria deverá ser feita a avaliação do desempenho da equipe, elogiando os pontos fortes, auxiliar no reconhecimento das fraquezas e na elaboração de um plano para superá-las.

4.2 ANÁLISE DOS RESULTADOS

Após a apresentação dos resultados da pesquisa, faz-se necessário a análise dos mesmos. Os dois processos apresentados (a proposta e o da DQS) proporcionaram um meio de reflexão de modo a questionar sobre a completeza e abrangência de um processo de certificação. A comparação permite concluir que primeiramente deve-se auto-avaliar a organização, pois nos dois processos essa é a primeira etapa.

Enquanto que o processo apresentado pela DQS embasou apenas na norma 27001 (elaboração do SGSI) deixando aspetos como a política de segurança como dados secundários, o processo proposto apresentou além do SGSI, a PSI como os principais aspetos para que haja a Segurança da Informação e assim alcançar a certificação da qualidade.

O processo apresentado pela DQS enfatiza a necessidade de integrar o SGSI com os outros sistemas de gestão da organização proporcionando assim maior vantagem competitiva à organização.

Ambos os processos enfatizam a necessidade de conhecer a organização para que possam ser desenvolvidas produtos/serviços de Segurança da Informação que se adequam as suas necessidades. Para isso ressalta-se o que foi dito no primeiro parágrafo que todos os processos começam com a auto-avaliação da organização.

O SGSI como sistema de gestão da segurança da informação é enfatizado nos dois processos destacando principalmente a necessidade de um bom planejamento do mesmo.

Outro aspecto em comum entre os processos é a auditoria como recurso para revisão das etapas que já foram realizadas.

Por fim destaca-se a necessidade *apriori* de recorrer às normas de referência internacional, ou seja, tanto o processo apresentado como o processo da DQS adotam as normas internacionais como referencial a ser seguida.

5. CONCLUSÃO E SUGESTÕES PARA TRABALHOS FUTUROS

Neste capítulo são apresentadas as considerações finais do estudo, em seguida são apresentadas sugestões para estudos posteriores que poderão complementar e/ou melhorar o trabalho realizado.

Com relação à proposta colocada para este trabalho, procurou-se apresentar um processo que as organizações poderão tomar como referência para se preparem para certificação em consonância com as normas em vigência.

Com a análise da bibliografia, concluiu-se que de nada adianta preparar uma organização para certificação, se não houver o devido apoio nas normas, pois não se pode “fugir” ou dizer algo diferente do que é tomado como referência internacional. Isto é demostrado inclusive nos livros de referência que são basicamente baseados nos conteúdos apresentados pelas normas.

O objetivo geral do trabalho foi alcançado. Em relação aos objetivos específicos todos foram atingidos por meio das seguintes atividades, a revisão bibliográfica sobre segurança da informação enfatizando normas, possibilitou o alcance dos objetivos a) e b). Por meio da análise e interpretação das normas e demais documentos analisados atingiu-se o objetivo c) e com a revisão sobre ferramentas de representação de processos atingiu-se o objetivo d). Finalmente para atingir o objetivo e) realizou-se pesquisa na internet. Pelos dados analisados pode-se concluir que, ter conhecimento a cerca das normas é bastante útil para se proceder a preparação de uma organização para certificação. Porém não é suficiente, é necessário que se conheça bem a organização para que se tenha conhecimento dos pontos fracos, possiveis ameaças a que ela está sujeita, é necessário também conhecer quem é a organização, em que estágio ela se encontra neste momento e onde ela pretende estar futuramente. Para isso recomenda-se que o processo para preparação para certificação seja aplicado pelos próprios integrantes da organização, pois estes já têm o conhecimento a cerca da organização que se faz necessário.

Trabalhos Futuros

Como sugestão de trabalhos futuros relacionado ao processo de preparação para certificação da qualidade em Segurança da Informação, sugere-se a realização de um estudo semelhante para uma organização específica (banco, hospital etc.), isto porque o processo apresentado é referente a qualquer tipo de organização, surge então à necessidade de adequar esse processo a uma organização que já possui normas de Segurança da Informação especificas para ela. Ressalta-se a necessidade de conhecer as particularidades de cada tipo de organização.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:** Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

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 27002:** Information technology — Security techniques — Code of practice for information security management. Rio de Janeiro, 2005.

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

BSI - British Standard Institute. Disponível em <http://www.bsibrasil.com.br/busca/index.asp>. Acesso em 25/06/2010.

DQS – Manegement Systems Solutions. Disponível em https://br.dqs-ul.com/home.html . Acesso em 30/10/2010.

_____. **DQS – IT – Safety_Brochure**. DQS GmbH 04/2010.

_____. **DQS – ISO 27001 _ ProductSheet.** DQS GmbH 04/2010.

GIL, A.C. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo. Atlas, 2008.

FERREIRA, F.N.F.; ARAÚJO, M.T. **Política de segurança da informação**: guia prático para embalagem e implementação. Rio de Janeiro: Editora Ciência Moderna Ltda. 2006.

FERREIRA, F.N.F. **Segurança da informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2003.

FONTES, E. **Segurança da informação**: o usuário faz a diferença. 1. ed. Editora Saraiva, 2005.

GOLDENBERG, M. **A arte de pesquisar:** como fazer uma pesquisa qualitativa em ciências sociais. 2. ed. Rio de Janeiro: Record, 1998.

IMONIANA, J. O. **Auditoria em sistemas de informação.** _ São Paulo: Atlas, 2005.

ISHIKAWA, K. **Controle de qualidade total**: à maneira japonesa. Rio de Janeiro: Campus, 1993.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO-IEC 27000**: Information Technology – Security techniques – Information security management systems – Overview and vocabulary. Switzerland, 2009.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO-IEC 27005**: Information Technology – Security techniques – Information security risk management. Switzerland, 2008.

IT GOVERNANCE. Disponível em < http://www.itgovernance.co.uk/files/download/Infosec_101v1.3.pdf>. Acesso em 19/09/2010.

_____. Disponível em < http://www.itgovernance.co.uk/products/162>. Acesso em 19/09/2010.

JANSSEN, L. A. **Instrumento de avaliação de maturidade em processos de segurança da informação:** estudo de caso em instituições hospitalares. 166 f. Dissertação (Mestrado em Administração e Negócios) - Faculdade de Administração, Contabilidade e Economia, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Janeiro de 2008. Disponível em: < http://tede.pucrs.br/tde_arquivos/2/TDE-2008-04-22T140541Z-1200/Publico/400421.pdf >. Acesso em: 13/09/2010.

KOTLER, P.; KELLER, K.L.. **Administração de marketing**: a bíblia do marketing. Prentice Hall Brasil, 12. Ed., 2006.

LYRA, M.R., **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

OLIVEIRA, D. de P. R. de. **Sistema, organização e métodos**: uma abordagem gerencial. São Paulo, Editora Atlas S.A 18. Ed., 2009.

SANTOS, A.R.dos. **Metodologia cientifica**: a construção de conhecimento. 6. ed. Rio de Janeiro: DP&A, 2004.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 7.ed. São Paulo: Atlas, 2006.

WERKEMA, M. C. C. **As ferramentas da qualidade no gerenciamento de processos**. 2. ed. Belo Horizonte: Ed. da UFMG: Fundação Christiano Ottoni, 1995.