Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação (SGSI) baseado nas normas ABNT NBR ISO/IEC 27001 e 27002

Ricardo R. Mendes [1], Rômulo R. L. de Oliveira [2], Anderson F. B. F. da Costa [3], Reinaldo Gomes [4]

[1] rr2mendes, [2] romuloricardo@gmail.com ; IFPB – Campus Campina Grande. [3] anderson@ifpb.edu.br, IFPB – Campus Campina Grande. [4] reinaldo@dsc.ufcg.edu.br; Universidade Federal de Campina Grande.

RESUMO

A segurança da informação destaca-se como uma das principais preocupações em diversas organizações. Para garantir que as informações e os sistemas de informações estejam protegidos contra ameaças de todos os tipos é necessário definir processos gerenciados e assegurar a confidencialidade, integridade e disponibilidade delas. Com esta finalidade, as normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 provem um conjunto de técnicas para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Porém, ainda é preciso definir uma metodologia para aplicar os conceitos identificados nas normas. Este artigo traz uma metodologia para implantar um SGSI, tomando como base a ABNT NBR ISO/IEC 27001 e 27002 simplificando o processo de planejamento, implantação, análise crítica e modificação do sistema. Através do modelo sugerido, será possível classificar a informação, identificar os riscos relevantes que atingem as informações, selecionar controles das normas e construir um plano de ação para a implantação do SGSI em qualquer tipo de organização.

Palavras Chave: segurança da informação, Sistema de Gestão de Segurança da Informação, ABNT NBR ISO/IEC 27001 e 27002

ABSTRACT

Information security is highlighted as a major concern in many organizations. To ensure that information and information systems are protected against threats of all kinds should be defined and managed processes to ensure the confidentiality, integrity and availability of them. For this purpose, the standards ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 comes a set of techniques for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a Information Security Management System (ISMS). However, we still need to define a methodology for applying the concepts identified in the standards. This paper provides a methodology to implement an MSIS, based on the ABNT NBR ISO/IEC 27001 and 27002 and theorists studied during the literature search, simplifying the process of planning, implementation, review and modification of the system. Through the suggested model, you can sort the information, identify relevant risks affecting the information, select controls standards and build an action plan for implementation of ISMS in any type of organization.

Keywords: *Information security, Information Security Management System, ABNT NBR ISO/IEC 27001 e 27002*

1 Introdução

A tecnologia da informação e comunicação tem avançado rapidamente, o que tem possibilitado a transformação de ambientes coorporativos, resultando em novas estruturas organizacionais caracterizadas principalmente pela cooperação. A cooperação potencializa o compartilhamento da informação e as relações interpessoais e interorganizacionais (NAKAMURA e GEUS, 2007). Desta forma, em ambientes coorporativos, o ativo organizacional, que era basicamente composto por ativos físicos, passa a incorporar também a informação como um dos principais ativos.

A informação como um ativo pode definir o sucesso ou insucesso nos mais variados ambientes. Devido a sua importância, as organizações estão sendo cada vez mais expostas a um número crescente de ameaças. Nos ambientes coorporativos, falhas de segurança da informação logo afetam o desempenho de seu negócio, gerando prejuízos que podem acarretar até mesmo a sua falência. Sendo a informação um elemento essencial para o desenvolvimento de diversas atividades da empresa, mecanismos eficientes de gestão de segurança da informação são requeridos no intuito, principalmente, de minimizar o risco ao negócio (ABNT, 2005).

Assim como tantos outros processos e ações dentro de uma organização, a segurança da informação deve possuir uma estrutura de gestão adequada às necessidades do negócio. Além de estabelecer as ações de segurança, a organização precisa assegurar que os investimentos em segurança estão tendo o retorno pretendido e se os recursos estão sendo adequadamente utilizados.

É neste momento que a organização percebe a necessidade de uma estrutura para gerir adequadamente a segurança da informação. Desta forma, é cada vez maior o interesse das empresas em buscar um modelo de gestão de segurança da informação que melhor se adéque aos seus objetivos.

Na Pesquisa Global de Segurança da Informação 2012, o orçamento limitado se destaca como um das principais respostas que os CEOs (*Chief Executive Officer* – Presidente Executivo ou Diretor Geral da Empresa), CFOs (*Chief Financial Officer* – Diretor Financeiro), CIOs (*Chief Information Office* – Diretor de TI) e CISOs (*Chief Information Security Officer* – Diretor de Segurança de TI), apontaram no estudo como entrave para o aprimoramento geral da eficácia estratégica da prática de segurança da informação de suas empresas. Observando a Tabela 1, nota-se que para os CEOs, o orçamento insuficiente para os investimentos é o principal obstáculo para a aplicação da gestão de segurança da informação nas organizações, com 27% das respostas, ficando entre os quatro primeiros entraves para os CFOs, CIOs e CISOs respondentes. Dados estes que justificam a busca de uma metodologia de implantação de um SGSI eficiente e de livre acesso.

Tabela 1 – Principais dificuldades para o aprimoramento geral da eficácia estratégica da prática de segurança da informação nas empresas.

	CEO	CFO	CIO	CISO
Liderança – CEO, presidente, diretoria ou equivalente	25%	27%	25%	25%
Liderança – CIO ou equivalente	14%	23%	18%	21%
Liderança – CISO, CSO ou equivalente	12%	22%	16%	17%
Falta de estratégia eficaz de segurança da informação	18%	25%	25%	30%
Falta de visão e ou de entendimento	17%	25%	30%	37%
Orçamento insuficiente para os investimentos	27%	23%	29%	29%
Orçamento insuficiente para os gastos operacionais	23%	16%	23%	22%
Ausência ou escassez de especialistas na empresa	23%	19%	25%	23%
Sistemas de informação/TI mal integrados ou excessivamente complexos	13%	14%	19%	30%

Fonte: Andrea (2011).

A gestão da segurança da informação deve ser encarada, principalmente, como um processo de gestão (e não um processo tecnológico) que é obtido por meio da implantação de controles, políticas e procedimentos que, juntos, fortalecem os objetivos de negócio com a minimização dos seus riscos e a promoção da segurança da organização.

Nesse contexto, destacam-se duas normas: a norma ABNT NBR ISO/IEC 27001, que busca prover mecanismos para implantar, operar, monitorar, rever, manter e melhorar um sistema de gestão de segurança da informação (ABNT, 2006; FERNANDES e ABREU, 2008); e a norma ABNT NBR ISO/IEC 27002, que traz um conjunto de diretrizes e princípios gerais para iniciar, implantar, operar, analisar criticamente, e aperfeiçoar um sistema de gestão de segurança da informação (SGSI) (ABNT, 2005; FERNANDES e ABREU, 2008).

Os desafios que um estudo neste tema propõe são:

a) Estabelecer os requisitos de segurança da informação para uma organização que, para a norma ABNT NBR ISO/NBR 27002, podem ser obtidas através de três fontes principais:

- A partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócios da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes e é realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.

- A partir da legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.

- A partir de um conjunto particular de princípios, objetivos e dos requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações (ABNT, 2005).

b) Elaborar uma metodologia para implantar um SGSI que melhor se adéque à realidade da organização, observando suas particularidades, no intuito de prover um sistema eficiente de gestão de segurança da informação (foco principal deste trabalho).

Este trabalho está organizado da seguinte forma: na seção 2 serão abordados conceitos referentes a SGSI, na seção 3 será apresentada uma metodologia para implantação de SGSI e na última seção serão realizadas as considerações finais deste trabalho.

2 Sistema de Gestão de Segurança da Informação (SGSI) e as normas ABNT NBR ISO/IEC 27001 e 27002

Um Sistema de Gestão de Segurança da Informação é um conjunto de processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos. Tal sistema deve ser seguido por todos aqueles que se relacionam direta ou indiretamente com a infraestrutura de TI da organização, tais como: funcionários, prestadores de serviço, parceiros e terceirizados. O SGSI deve possuir obrigatoriamente o aval da direção e do departamento jurídico da organização para conferir sua legalidade.

A informação, conforme a ABNT NBR ISO/IEC 27002, é um ativo que, como outro ativo de grande importância, demonstra ser essencial para o negócio e necessita ser adequadamente protegido.

Ativos da informação são aqueles relevantes ao escopo do sistema de gestão de segurança da informação (ABNT, 2006). Normalmente é algo que uma organização atribui valor e que contém, transmite e armazena informação, também sendo necessário mantê-los para continuidade do negócio. Informações eletrônicas, documentos em papel, *software*, *hardware*, instalações, pessoas, imagem e reputação da companhia, serviços são todos considerados ativos da informação.

De acordo com Reis *et al.* (2007), a informação se localiza entre o que se pode chamar de dado puro e o conhecimento. Ela consiste em um dado com uma interpretação sobre ele.

A norma ABNT NBR ISO/IEC 27001 traz a ideia de que os ativos da informação não incluem necessariamente tudo o que uma empresa consta que tem um valor. Uma cadeira tem um valor, mas não é um ativo, pois não tem relação direta com informações. A organização deve determinar quais ativos podem materialmente afetar a entrega de um produto ou serviço pela sua ausência ou deteriorização, ou podem causar dano à organização

através de perda de disponibilidade, integridade ou confidencialidade.

A informação pode existir de diversas formas. Pode ser impressa ou escrita em papel, armazenada eletronicamente (através de *pendrive*, disco rígido, CD, DVD etc.), apresentada em filmes, ou até mesmo em conversa. Seja qual for o meio de transmissão, a forma de armazenamento ou apresentação, a informação deve ser sempre apropriadamente protegida.

Para cada forma que ela pode apresentar, é necessário tomar os procedimentos adequados e diferenciados para sua proteção, existindo assim a necessidade de classificá-la.

2.1 Classificação da informação

De forma simplificada, define-se que a Classificação da Informação é um processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo com a importância desta para as organizações, de modo a garantir a sua confidencialidade, integridade e disponibilidade.

Segundo Nakamura e Geus (2007), a inexistência de uma classificação das informações quanto ao seu valor e à sua confiabilidade, é um dos diversos aspectos que expõem as organizações a maiores riscos relacionados à segurança da informação.

A informação deve garantir os seguintes requisitos:

- *Confidencialidade*: A confidencialidade é entendida como a propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados (ABNT, 2006).
- *Integridade*: Significa proteger a exatidão e complexidade da informação e dos métodos de processamento. Também é definida como a garantia de que os dados recebidos estão exatamente como foram enviados por um emissor autorizado (STALLINGS, 2008).
- *Disponibilidade*: A disponibilidade é definida como sendo a propriedade de um sistema ou de um recurso do sistema ser acessível sob demanda por uma entidade autorizada, de acordo com especificações de desempenho (STALLINGS, 2008). Em outras palavras, é assegurar que os usuários autorizados tenham acesso à informação e ativos associados quando necessário.

A partir da análise de classificação da informação foi possível ampliar o conceito para classificar o ativo da informação, atribuindo níveis em uma escala numérica. Para efeito dessa classificação, a escala numérica varia de 1 a 3, seguindo o modelo abaixo:

a) Quanto à confidencialidade:

- *Público (1)*: ativos que contenham informações que não possuem restrições para divulgação e, portanto, podem ser de conhecimento público;
- *Interno (2)*: ativos que contenham informações que não exigem um nível de confidencialidade, mas que não é interessante permitir o acesso público a eles, sendo apenas utilizados internamente pela empresa;
- *Confidencial ou restrito (3)*: ativos que contenham informações que exigem um nível de confidencialidade e, caso sejam divulgados erroneamente, afetam gravemente a continuidade dos negócios da instituição.

b) Quanto à integridade:

- *Básica ou norma (1):* a perda de sua integridade decorrido um determinado prazo não implica impactos à empresa, sendo assim, não exige controles de auditoria e de acesso;
- *Relevante (2)*: sua perda gera transtornos de baixo impacto para a empresa, portanto, devem ser mantidos controles usuais para garantir sua integridade;
- *Vital (3)*: a empresa deve garantir que os ativos se preservaram intactos em seu estado original por todo o tempo de sua guarda, sob pena de impactar de forma grave o negócio.

c) Quanto à disponibilidade:

- *Baixa (1)*: a Perda da disponibilidade não afeta a continuidade do negócio;
- *Moderada (2)*: caso ocorra uma perda de disponibilidade que afete os ativos, é possível dar continuidade ao negócio com certa limitação;

• *Crítica (3)*: ativos nesse nível, caso sofra uma perda de disponibilidade, afetarão a continuidade do negócio.

2.2 Principais Aspectos e Estrutura da Norma ABNT NBR ISO/IEC 27001

Como escrito na norma ABNT NBR ISO/IEC 27001, ela foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (ABNT, 2006). A definição da utilização de um SGSI deve respeitar a estrutura da organização, o foco estratégico e suas reais necessidades, devendo ainda ser adaptável às situações encontradas (um problema de segurança da informação que não demonstre complexidade requer soluções igualmente simples de um SGSI).

Ela utiliza a abordagem de processo na intenção de estabelecer, implantar, operar, realizar a análise crítica, manter e melhor o SGSI de uma organização (ABNT, 2006; FERNANDES e ABREU, 2008). Conforme apresentam a ABNT (2006) e Fernandes e Abreu (2008), essa abordagem estimula os usuários a enfatizar a importância de:

Entender os requisitos de segurança da informação de uma organização e a necessidade de estabelecer um conjunto de diretrizes e objetivos para a segurança da informação;

Com base na compreensão dos riscos de negócios globais da organização, implantar e operar controles para gerenciar os riscos de segurança da informação;

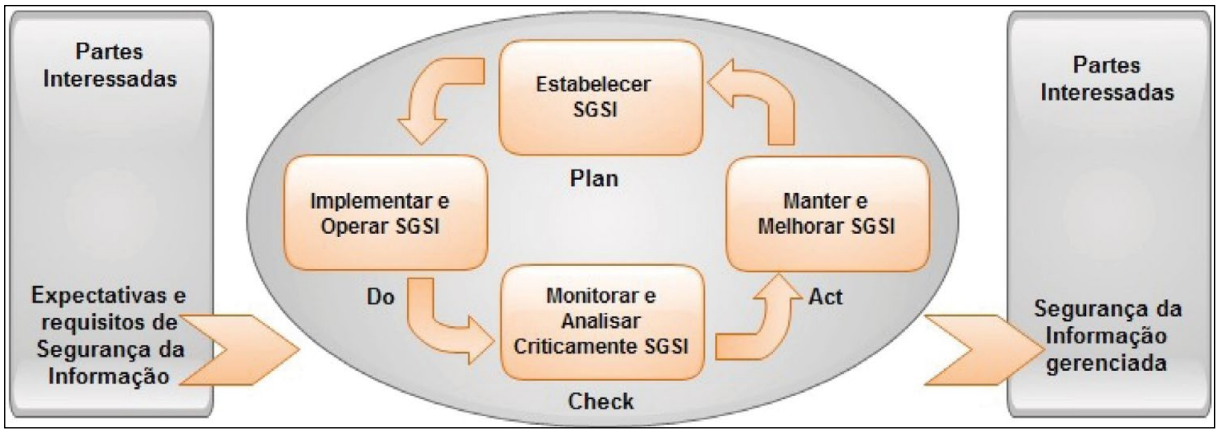
Monitorar e analisar criticamente o próprio SGSI;

Melhorar continuamente seguindo métricas objetivas.

Segundo a ABNT (2006) e Fernandes e Abreu (2008), essa norma utiliza o modelo *Plan-Do-Check-Act* (PDCA), também chamado de ciclo de Deming, sendo aplicado na estrutura de todos os processos do SGSI. A Figura 1 ilustra como o SGSI se relaciona com o modelo PDCA.

Em Faria (2008) o PDCA é definido como *"um método amplamente aplicado para o controle eficaz e confiável das atividades de uma organização, principalmente àquelas relacionadas às melhorias, possibilitando a padronização nas informações do controle de qualidade e a menor probabilidade de erros nas análises ao tornar as informações mais entendíveis"*.

Figura 1 – modelo Plan-Do-Check-Act (PDCA).



Fonte: ABNT (2006)

A mesma autora define as etapas do PDCA da seguinte forma:

PLAN - É o primeiro passo para a aplicação do PDCA, constitui em um planejamento estabelecido com base nos objetivos do negócio das organizações e considera três fases importantes: o estabelecimento dos objetivos, o estabelecimento do caminho para alcançar os objetivos e a definição do método para alcançá-los.

DO – Representa o segundo passo do PDCA e se constitui na definição do plano de ação e na execução propriamente dita.

CHECK – É o terceiro passo do PDCA, nesta fase podem ser detectados erros ou falhas, de acordo com

a análise ou verificação dos resultados alcançados e dados coletados.

ACT – Representa a última fase do PDCA, nela serão realizadas ações corretivas de acordo com falhas encontradas no terceiro passo.

A norma ISO/IEC 27001 é uma norma certificadora, sendo utilizada por institutos credenciados nos mais diversos países, no Brasil o IMETRO (Instituto Nacional de Metrologia, Normalização e Qualidade Industrial), para certificar organizações quanto à implantação de um SGSI. Com essa certificação, a empresa garante ao mercado que em todos os seus processos as informações são resguardadas, dando credibilidade e uma melhor projeção para ela. Por este motivo, é crescente o número de empresas que se certificam na ISO/IEC 27001 conforme é possível verificar em http://www.iso27001certificates.com/.

2.3 Principais aspectos e estrutura da norma ABNT NBR ISO/IEC 27002

O objetivo principal dessa norma é estabelecer diretrizes e princípios gerais que vão auxiliar a iniciar, implementar, manter e melhorar a governança de segurança da informação em uma organização (ABNT, 2005; FERNANDES e ABREU, 2008). Tais objetivos provêem diretrizes gerais sobre as metas para a gestão de segurança da informação (ABNT, 2005). Ela contém objetivos de controle e controles que têm como finalidade ser implantados para atender aos requisitos que foram identificados por meio da análise/avaliação de riscos. Além disso, tem como outro objetivo servir como um guia prático no desenvolvimento de procedimentos de segurança da informação na organização, como forma de ajudar a estreitar laços nas atividades interorganizacionais (ABNT, 2005; FERNANDES e ABREU, 2008; MATOS, 2010).

Segundo apresentado na própria norma, ela contém 11 seções de controles de segurança da informação, que juntas totalizam 39 categorias principais de segurança e uma seção introdutória que aborda a análise/avaliação e o tratamento de riscos. Cada seção cobre um tópico ou área diferente e são organizadas da seguinte forma:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;
- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gestão das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Gestão de incidentes de Segurança da Informação;
- Gestão da Continuidade do Negócio;
- Conformidade.

2.4 Áreas de atuação da norma ABNT NBR ISO/IEC 27001 e 27002

A norma ABNT NBR ISO/IEC 27001 apresenta requisitos genéricos, por isso é possível que seja aplicada em todas as organizações, independente da sua razão social e área de atuação (ABNT, 2006). De forma semelhante, a norma ABNT NBR ISO/IEC 27002, de acordo com Matos (2010), cobre todos os tipos de organizações seja, por exemplo, empreendimentos comerciais, agências governamentais ou mesmo organizações sem fins lucrativos. Ela especifica requisitos para implementação de controles de segurança adaptados as particularidades de cada organização.

3 Metodologia para Implantação do SGSI

A metodologia para implantação do SGSI é baseada no ciclo de Deming, sendo representada através dos módulos Planejar, Fazer, Checar e Monitorar (PDCA) (SERRANO, 2012) e seguindo as diretrizes referentes nas normas ABNT NBR ISO/IEC 27001 e 27002.

As seções seguintes exploram todos os módulos do ciclo de Demming, de tal modo que define cada etapa da metodologia de implantação de um SGSI.

3.1 Planejar

3.1.1 Definir o escopo

O primeiro passo na implantação do SGSI, segundo a norma ISO/IEC 27001, é definir o escopo e os limites do SGSI, que devem observar as "características do negócio, a organização, sua localização, ativos e tecnologia, incluindo detalhes

e justificativas para quaisquer exclusões do escopo" (ABNT, 2006).

3.1.2 Definir uma política de segurança da informação

A política de segurança da informação é uma declaração formal da empresa acerca do compromisso com a proteção do ativo da informação e deve se fundamentar no escopo do SGSI (ABNT, 2006). Destaca-se na ISO/IEC 27001 que ela:

a) inclua uma estrutura para definir objetivos e estabeleça uma orientação global e princípios para ações que envolvam a segurança da informação;

b) observe as obrigações contratuais de segurança, regulamentações e os requisitos de negócio;

d) estabeleça limites e critérios para definir quais riscos serão avaliados; e

e) seja aprovada pela direção

Ferreira e Araújo (2008) ressaltam, entre outros pontos, que a política deve ser simples, compreensiva (escrita de maneira clara e concisa), estruturada de forma a permitir a sua implantação por fases, alinhada à estratégia de negócio da empresa, padrões e procedimentos e orientadas aos riscos.

Portanto, a especificação da política deve:

- Ser breve, utilizar palavras simples e formalizar o que é esperado dos funcionários da organização;
- Fornecer aos leitores informações suficientes para saber se os procedimentos descritos na política são aplicáveis a eles ou não;
- Descrever sua finalidade específica.

3.1.3 Definir o escopo

a) Identificar os ativos dentro do escopo do SGSI e os proprietários destes ativos, listando-os no Quadro 1;

b) Outro ponto consiste em classificar os ativos com base na perda de sua integridade, disponibilidade e integridade, seguindo uma escala de 1 a 3 e representá-los conforme o Quadro 2. O número 1 representa o menor impacto para a organização e o 3 representa um dano crítico. Nesse quadro, o campo Valor será composto por uma média aritmética entre os 3 campos, arredondado para um número inteiro.

Quadro 1 – Inventário dos ativos da informação.

Natureza do Ativo	Ativos
Informação	
Documentos em papel	
Software	
Físico	
Recursos Humanos	
Serviços ou atividades	

Quadro 2 – Classificação dos ativos da informação.

Ativos	Confidencialidade	Integridade	Disponibilidade	Valor
...	...	...	...	...

3.1.4 Avaliar os riscos

Para isto, é preciso criar um terceiro quadro (Quadro 3) representando as vulnerabilidades, ameaças e a probabilidade de ocorrência destas ameaças. Por vulnerabilidade entende-se como as fraquezas associadas ao ativo da informação (ponto fraco), já as ameaças são as ocorrências que podem atingir as vulnerabilidades.

Haja vista que um sistema, por mais eficiente que seja, não consiga eliminar a totalidade dos riscos devido a fatores como a ocorrência de ameaças não previstas e do alto custo/benefício, é necessário aceitar riscos residuais, que pela ABNT NBR ISO/IEC 27001 pode ser definido como o risco remanescente após o tratamento de risco (ABNT, 2006).

Quadro 3 – Avaliação de risco

Ativos	Vulnerabilidade	Ameaça	Probabilidade
...	...	...	...

3.1.5 Selecionar os objetivos de controle

Para atender aos requisitos de análise/avaliação de riscos identificados, é preciso selecionar e implementar os objetivos de controle e controles. Esta seleção deve considerar os requisitos legais, regulamentares e contratuais, bem como os critérios para aceitação de riscos (ABNT, 2006).

Os objetivos de controle e controles listados no Anexo A da norma ABNT NBR ISO/IEC 27001 devem ser selecionados para cobrir os requisitos identificados, mas eles não são exaustivos, portanto, objetivos de controles e controles adicionais podem também ser selecionados (ABNT, 2006).

3.1.6 Preparar uma declaração de aplicabilidade

A declaração de aplicabilidade, nada mais é do que um resumo das decisões relativas ao tratamento de riscos, ela deve incluir no mínimo três aspectos, são eles:

a) Os objetivos de controle e os controles selecionados para o tratamento de riscos e a justificativa para sua seleção;

b) Os objetivos de controles que já se encontram implementados na organização

c) A relação dos objetivos de controles excluídos do SGSI e a justificativa para tal exclusão.

O Quadro 4 apresenta o modelo de Declaração de aplicabilidade.

Quadro 4 – Declaração de Aplicabilidade

Declaração de Aplicabilidade			
Versão			
Responsável pela Declaração			
Responsável pela Aprovação			
Última Revisão	__/__/__	Responsável:	
	__/__/__	Responsável:	
Controles	Controles já implantados	Controles em implantação	Controles não implantados/ Justificativa

3.2 Fazer

O módulo Fazer constitui a segunda fase do PDCA. Portanto, ele deverá ser desenvolvido logo após o planejamento do Sistema de Gestão de Segurança da Informação, através da elaboração de um plano de ação para implementação do SGSI e da própria execução deste plano na prática.

De acordo com o exposto anteriormente, o módulo Fazer segue as seguintes etapas:

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.

Para a criação do plano de tratamento de riscos, será utilizado o modelo 5W1H, que pode ser definida como uma ferramenta estratégica de qualidade nas empresas que tem como propriedade estabelecer um plano de ação tático, onde ações deverão ser executadas em geral em um período curto de tempo, por volta de um ano (HASS, 2010). A sigla 5W1H é originada do inglês e representa os seis pilares do plano de ação.

Seguindo a técnica do 5W1H, o plano de tratamento de riscos deverá ser preenchido de acordo com o Quadro 5 apresentado a seguir:

Quadro 5 – Plano de tratamento de risco

PLANO DE TRATAMENTO DE RISCO						
Responsável:						
Data: ____/____/____						
Versão:						
Nº	O quê	Porque	Como	Quando	Quem	Onde
1 -						

b) Implementar o plano de tratamento de riscos para alcançar os objetivos de controle identificados, que incluam considerações de financiamentos e atribuição de papéis e responsabilidades. Para isto, deverão ser implementados os controles selecionados anteriormente durante a análise/avaliação de riscos.

Após isso, é preciso mensurar o desempenho do plano de tratamento de risco, e para isso é necessário definir como medir a eficácia dos controles selecionados. Esse procedimento irá permitir que os gestores determinem o quanto os controles alcançaram com eficácia os objetivos de controles planejados (ABNT, 2006).

c) Implementar programas de capacitação, gerenciar as operações do SGSI e gerenciar os recursos para o SGSI (ABNT, 2006).

3.3 Verificar

A terceira fase do PDCA, módulo Verificar, define ações para serem realizadas com o objetivo de identificar não conformidades do SGSI. A partir da análise crítica do sistema e da identificação destas não conformidades, será possível selecionar novos controles e aplicar melhorias pontuais no sistema.

Este módulo deverá seguir os seguintes passos:

a) Realizar 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.

Para este fim, será utilizada a ferramenta criada pelo economista Vilfredo Pareto em 1897, denominada Diagrama de Pareto. O economista tinha a intenção de provar que a distribuição de renda era feita de forma desigual e posteriormente utilizou esta técnica para classificar problemas relacionados à qualidade em triviais e vitais. Elaina (2011) define o Diagrama de Pareto como *"uma ferramenta administrativa usada para destacar os elementos de um grupo de acordo com a sua importância"*.

Sua representação é realizada através de um gráfico, permitindo que as prioridades do problema sejam melhor visualizadas e auxilia a estabelecer metas (ELAINA, 2011).

Segundo Elaina (2011), o diagrama de Pareto serve para tornar mais clara a relação entre a ação tomada e o benefício que esta ação proporciona e, a partir da análise do gráfico, priorizar a ação que dará um melhor resultado para a organização.

Para a construção do diagrama, deverão ser realizados os seguintes passos:

1) Elaborar um quadro com todos os aspectos que serão analisados conforme o modelo a seguir (Quadro 6):

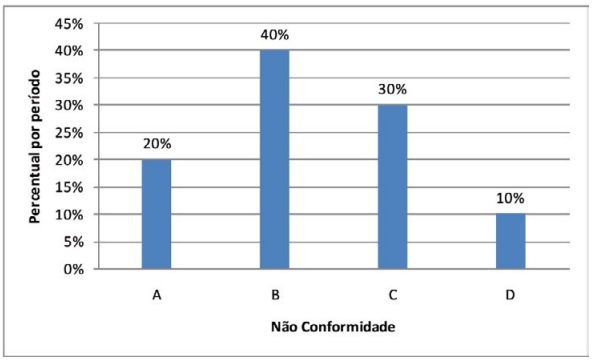
Quadro 6 – Identificação de não conformidade/período

	A	B	C	D
Não conformidade/ Período				
Janeiro				
...	...	...	...	...
N° total de não conformidade				
Porcentagem				

As colunas representam as não conformidades a serem analisadas, as linhas representam os números de eventos detectados no período definido. Logo abaixo existe uma representação da quantidade total de não conformidades e sua porcentagem em relação ao total.

2) Logo após a listagem de todos os eventos acontecidos no período deve ser construído um gráfico em barras seguindo o modelo exemplificado na Figura 2.

Figura 2 – Diagrama de Pareto.



A análise do Diagrama de Pareto possibilitará detectar erros nos resultados de processamento, identificar tentativas e violações de segurança bem-sucedidas e incidentes de segurança da informação e determinar se as ações tomadas para prevenir incidentes de segurança da informação foram eficazes, cumprindo assim os requisito estabelecidos no subitem 4.2.3 (Monitorar e analisar criticamente o SGSI) da norma ABNT NBR ISO/IEC 27001.

3.4 Agir

A última etapa da metodologia do SGSI consiste no módulo Agir, do PDCA. Nessa etapa o objetivo é implantar as melhorias identificadas, tomar ações preventivas e corretivas apropriadas, levar ao conhecimento da direção os resultados e ações e garantir que as melhorias alcancem os objetivos definidos (ABNT, 2006).

3.5 Documentação

Para atender aos requisitos de documentação do SGSI, é preciso que a documentação inclua registros de decisões da direção, assegure que seja possível rastrear as ações de acordo com as políticas e decisões da direção (ABNT, 2006).

A documentação do SGSI deve incluir:

1) A política do SGSI;

2) O escopo do SGSI;

3) Uma descrição da metodologia de análise/ avaliação de riscos junto com um relatório;

4) O plano de tratamento de riscos;

5) Toda e qualquer alteração e registros posteriores, bem como os registros requeridos pela norma ABNT NBR ISO/IEC 27001;

4 Considerações Finais

A segurança da informação vem se destacando como um elemento fundamental para que processos e serviços que dependam da informação continuem a se desenvolver nas diversas organizações.

Neste sentido, manter a segurança da informação com um gerenciamento eficaz implica garantir a continuidade do negócio da organização. Por isso, se torna necessário um sistema que envolva planejamento, documentação, definições de responsabilidades e provisões de recursos.

As normas ISO/IEC 27001 e 27002, traduzidas pela ABNT, abordam o tema segurança da informação e revelam boas práticas para que os gestores de TI implantem um sistema gerenciado de segurança da informação. Porém, ainda era preciso definir uma metodologia, para que qualquer profissional que desejasse implantar esse sistema em uma organização encontrasse nela um modelo que relacionasse todos os requisitos da norma de forma simples e eficaz, servindo como um guia para real implantação do SGSI.

O forte do modelo sugerido é que ele é genérico e, portanto, pode ser aplicado desde uma instituição de ensino, até em instituições financeiras, por exemplo.

Além disso, a implantação do SGSI em sua totalidade e para seguir os requisitos de uma certificação deve ir além do planejamento e implementação do plano de ação. Auditorias devem ser realizadas periodicamente com a finalidade identificar não conformidades e é preciso realizar uma análise crítica do SGSI para que seja possível melhorar e corrigir falhas pontuais.

Estes dois fatores são abordados pela norma e podem ser utilizados em um estudo posterior.

As auditorias internas devem ser realizadas pela organização em intervalos de tempos planejados para determinar se os objetivos do SGSI estão sendo alcançados (ABNT, 2006). Para as auditorias, é preciso um programa planejado que leve em consideração os objetivos de controle das normas ISO 27001 e ISO 27002.

Para auxiliar no processo de auditoria pode ser utilizado a norma ABNT NBR ISO 19011:2002 – Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental – constituindo assim, mais uma norma para estudo.

No mesmo estudo, também pode ser observado a análise crítica do SGSI, pois de acordo com a norma ISO/IEC 27001, a organização deve de forma periódica analisar criticamente o sistema. Com essa medida ela visa a melhoria contínua do sistema aplicando ações preventivas e corretivas (ABNT, 2006).

Para a análise crítica deve ser levado em consideração aspectos como os resultados de auditorias internas, não conformidades não contemplados na análise/avaliação de riscos e quaisquer mudanças que possam afetar o SGSI (ABNT, 2006).

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da segurança da Informação**. Rio de Janeiro: ABNT, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos**. Rio de Janeiro: ABNT, 2006

ANDREA, E. **O centro do furacão**: muitos veem a luz do sol, apesar da nebulosidade causada pela estagnação da economia global e pelo aumento do crime cibernético e das ameaças de segurança da informação. São Paulo: PwC, 2011

ELAINA, J; **Diagrama de Pareto**. 2011. Disponível em: http://www.empresasedinheiro.com/diagrama-de-pareto/. Acesso em: 10 jun. 2012.

FARIA, C. **PDCA (Plan, Do, Check, Action)**. 2008. Disponível em: http://www.infoescola.com/administracao/pdca-plan-do-check-action/. Acesso em: 28 jun. 2012.

FERNANDES, A.; ABREU, V. **Implantando a governança de TI***:* da estratégia à gestão dos processos e serviços. 2. ed. Rio de Janeiro: Brasport, 2008.

FERREIRA, F. N. F; ARAUJO, M. T.; **Política de sgurança da informação:** guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

HAAS, V. **Sistema de qualidade:** 5W1H(5W2H). 2010. Disponível em: http://www.ebah.com.br/content/ABAAABYqYAK/5w1h-5w2h#. Acesso em: 05 jun. 2012.

MATOS, F.; **Proposta de um checklist para verificação da segurança física de uma empresa baseada na norma ABNT NBR ISO/IEC 27002:2005**. Monografia apresentada ao curso de Ciências da Computação. Fortaleza: Faculdade Lourenço Filho, 2010.

NAKAMURA, E.; GEUS, P. **Segurança de redes em ambientes cooperativos.** 2 ed. Rio de Janeiro: Novatec, 2007.

REIS, B; MOTA J. C.; OLIVEIRA, P. P. **Classificação da informação**. 2007. Disponível em: <www.lyfreitas.com/artigos_mba/artclassinfo.pdf>. *Acesso em: 20 jan. 2012.*

STALLINGS, W.; **Criptografia e segurança de redes***:* princípios e práticas. 4. ed. Rio de Janeiro: Pearson., 2008.

SERRANO, D. P. **Ciclo PDCA.** 2012. Disponível em: <http://www.portaldomarketing.com.br/Artigos3/Ciclo_PDCA.htm>. Acesso em: 01 nov, 2012.