CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
MESTRADO EM TECNOLOGIA

EDISON LUIZ GONÇALVES FONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:
UMA CONTRIBUIÇÂO PARA O ESTABELECIMENTO DE UM PADRÃO MÍNIMO

SÃO PAULO
AGOSTO/2011

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
MESTRADO EM TECNOLOGIA

EDISON LUIZ GONÇALVES FONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO:
UMA CONTRIBUIÇÂO PARA O ESTABELECIMENTO DE UM PADRÃO MÍNIMO

Dissertação apresentada como exigência parcial para a obtenção do Título de Mestre em Tecnologia no Centro Paula Souza de Educação Tecnológica no Programa de Mestrado em Tecnologia: Gestão do Desenvolvimento de Tecnologias da Informação Aplicadas, sob a orientação do Prof. Dr. Napoleão Verardi Galegale.

SÃO PAULO
AGOSTO/2011

Fontes, Edison Luiz Gonçalves

F683p Política de segurança da informação: uma contribuição para os estabelecimento de um padrão mínimo / Edison Luiz Gonçalves Fontes. – São Paulo: CEETEPS, 2011.
157 f. : il.

Orientador: Prof. Dr. Napoleão Verardi Galegale.
Dissertação (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, 2011.

1. Política de segurança. 2. Segurança da informação. 3. NBR ISO/IEC 27002. 4. NBR ISO/IEC 27001. I. Galegale, Napoleão Verardi. II. Centro Estadual de Educação Tecnológica Paula Souza. III. Título.

EDISON LUIZ GONÇALVES FONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA CONTRIBUIÇÃO PARA O ESTABELECIMENTO DE UM PADRÃO MÍNINO

PROF. DR. NAPOLEÃO VERARDI GALEGALE

PROF. DR. PEDRO LUIZ CORTEZ

PROFA. DRA. MARILIA MACORIN DE AZEVEDO

São Paulo, 04 de agosto de 2011

Dedico este trabalho a minha esposa e namorada,

Fatima Fontes.

Nestes trinta anos de caminhada juntos, a cada

dia descobrimos a beleza de viver a vida,

e de criar a vida através dos nossos filhos

Edison e Vinícius.

UM PADRÃO MÍNIMO

- Mestre qual o mais importante de todos os mandamentos da Lei?

Jesus respondeu: “Ame o Senhor teu Deus com todo o coração,

com toda a alma e com toda a mente.”

Este é o maior mandamento e o mais importante.

E o segundo mais importante é parecido com o primeiro:

“Ame os outros como você ama a você mesmo.”

Evangelho segundo Mateus, Capítulo 22, Versículos 36-39. Versão Bíblia de Estudo Conselheira, Sociedade Bíblica do Brasil, Nova tradução na Linguagem de Hoje, 2000.

AGRADECIMENTOS

Em primeiro lugar ao nosso Deus, que permite o milagre da vida e que sem ele nada disso aconteceria.

Ao Prof. Dr. Napoleão Verardi Galegale, meu orientador, pelo seu apoio, seu conselhos para o amadurecimento do tema, sua revisão de material, seus questionamentos que me permitiram escrever um texto mais consistente, sua paciência e sua sabedoria tão bem compartilhada.

À Profa. Dra. Marília Macorin de Azevedo e ao Prof. Dr. Pedro Luiz Cortez, componentes da banca examinadora, pelas orientações desde o exame de qualificação, buscando garantir que esta pesquisa alcançasse o seu objetivo.

Aos demais professores do Mestrado em Tecnologia do Centro de Educação Tecnológica Paula Souza, em especial aqueles com quem realizei disciplinas: Profa. Dra. Marcia Ito, Prof. Dr. Aristides Novelli Filho, Prof. Dr. Alfredo Colenci Junior, Prof. Dr. Marcelo Duduchi Feitosa e a Profa. Dra. Senira Anie Ferraz Fernandez. Serei sempre agradecido a todos vocês.

A todo o pessoal da Secretaria do Curso de Mestrado em Tecnologia, representado pela amável e generosa Cleonice Viana Lima da Silva.

A todos os colegas do curso, em especial aqueles que a vida permitiu um maior compartilhamento de tempo em trabalhos de equipe e conversas no dia a dia: César Fernandes, Carlos Palhares, Cristina Ito, Danúbio Borba, Francisco Felinto, Nilton Barioto, Thiago Ferauche, Emerson Borges e José Abranches. Aprendi muito com todos vocês.

A todos os bons professores que tive e terei na minha vida.

A todas as organizações pelas quais já contribui profissionalmente. A experiência adquirida em cada trabalho realizado como funcionário ou consultor, me permitiu

construir o conhecimento que me motivou realizar uma pesquisa com a contribuição de um produto final proveitoso para o ambiente acadêmico e também para o ambiente organizacional.

Aos meus alunos que tanto me ensinam.

Ao jardim de uma ilha chamada de Itamaracá (Pedra que canta), que me ensinou sobre o tempo, crescimento e colheita.

À minha esposa Fatima e ao meu filho Vinícius pelas revisões realizadas em cada etapa do sonho e da construção desta pesquisa.

Aos meus pais, Thomas Edison Camerino Fontes e Marta Jônitas Fontes que sempre me incentivaram pelos estudos. (Em memória).

Esta pesquisa não poderia ser feita sem a colaboração e generosidade das organizações e dos profissionais de segurança da informação que tão gentilmente forneceram as suas políticas de segurança e responderam ao questionário. Infelizmente pelo sigilo acertado não posso indicar seus nomes e das organizações que vocês trabalham. Mas, cada um de vocês sabe de quem estou falando e eu gostaria de agradecer a colaboração de vocês. Muito obrigado pela generosa colaboração e pela confiança em me repassar informações das suas organizações.

RESUMO

FONTES, Edison Luiz Gonçalves**. Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo. 2011**. 157 f. Dissertação (Mestrado) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2011.

Este trabalho tem como objetivo identificar os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização. Busca responder a seguinte pergunta de pesquisa: “Quais são os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização?” O processo estruturado de segurança da informação é cada vez mais exigido para as organizações e a política é um elemento mandatório deste processo. As organizações que já implantaram política de segurança da informação utilizaram um subconjunto dos requisitos da NBR ISO/IEC 27002:2005. A grande quantidade de requisitos da Norma gera dificuldades para as organizações que estão no estágio inicial do processo de segurança da informação e precisam elaborar suas políticas. A existência de um padrão mínimo ajudará estas organizações. A metodologia utilizada neste estudo compreende o levantamento da literatura sobre o assunto política de segurança da informação considerando fontes acadêmicas e empresariais, o estudo teórico deste tema e o desenvolvimento de um estudo de caso múltiplo de modo a analisar políticas de segurança da informação já implantadas em organizações e identificar elementos comuns que possam estabelecer um padrão mínimo de política de segurança da informação.

Palavras-chave: Política de segurança. Segurança da informação. NBR ISO/IEC 27002. NBR ISO/IEC 27001.

ABSTRACT

FONTES, Edison Luiz Gonçalves**. Information security policy: a contribution to the establishment of a minimum standard. 2011**. 157 f. Dissertation (Masters) – Centro Estadual de Educação Tecnológica Paula Souza, São Paulo, 2011.

This work aims to identify the elements that should comprise a minimum standard for information security policy of an organization. Seeks to answer the following research question: "What are the elements that should comprise a minimum standard for information security policy of an organization?" The structured process of information security is increasingly required for organizations and politics is a mandatory element of this process. Organizations that have deployed security policy information using a subset of the requirements of ISO / IEC 27002:2005. The large number of requirements of the standard creates difficulties for organizations that are in the initial stage of information security and must develop their policies. The existence of a minimum standard will help these organizations. The methodology used in this study reviews the literature on the subject of information security policy considering academic and business sources, the theoretical study of this issue and the development of a multiple case study in order to analyze information security polices already implemented in organizations and identify common elements that could establish a minimum standard of information security policy.

Keywords: Security policy. Information security. NBR ISO/IEC 27002. NBR ISO/IEC 27001

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
BSI	British Standard International
BS	British Standard
COBIT	*Control Objectives for Information and related Technology*
IBGC	Instituto Brasileiro de Governança Corporativa
IEC	*International Electro technical Commission*
ISACA	*Information Systems Audit and Control Foundation*
ISO	*International Organization for Standardization*
IT	*Information Technology*
ITGI	*Information Technology Governance Institute*
ITIL	*Information Technology Infrastructure Library*
NACD	*National Association of Corporate Directors*
NBR	Norma Brasileira
OECD	Organization for Economic Co-operation and Development
OGC	*Office of Government Commerce*
PDCA	*Plan, Do, Check, Act*
SGSI	Sistema de Gestão de Segurança da Informação
TI	Tecnologia da Informação

LISTA DE FIGURAS

SUMÁRIO

1- INTRODUÇÃO

Desde o início da vida a informação é um elemento fundamental para a sobrevivência dos seres de todas as espécies e mais especialmente para a raça humana. A informação permitiu descobertas como o fogo, a roda e tantas outras que são consideradas comuns nos dias de hoje. A informação continua parte da vida das pessoas.

Considerando o ambiente corporativo, a informação é um recurso essencial para toda organização, independente do seu porte e do seu segmento de atuação. É utilizando a informação que processos organizacionais funcionam, as pessoas podem realizar as suas atividades profissionais, a geração de conhecimento acontece e o compartilhamento desse conhecimento é realizado. Enfim, a informação possibilita que a organização atinja os seus objetivos. Silva e Tomaél (2007) consideram a importância da informação para organizações e pessoas quando declaram:

> *É evidente, na atualidade, que nada poderia funcionar sem uma quantidade significativa de informação como um elemento que impulsiona os fenômenos sociais e que é por eles impulsionada. Pessoas e organizações – públicas e privadas – dependem da informação em seus processos decisórios. (Silva e Tomaél, 2007, p.1)*

Silva e Tomaél (2007) complementam que a informação é um importante ativo para o compartilhamento do conhecimento nas organizações. Albertin e Pinochet (2010, p.45) exprimem pensamento semelhante quando indicam que “a competição entre as empresas não se dá mais de acordo com o uso racional dos fatores de produção; o que torna uma empresa competitiva no mundo contemporâneo é o conhecimento principalmente àquele associado à tecnologia”.

Brito, Antonialli e Santos (1997) em sua pesquisa sobre a influencia da tecnologia da informação em uma organização constatam que:

> *A informação passa a ser um recurso estratégico para as organizações. Ela pode gerar as condições necessárias ao alcance dos objetivos, o cumprimento da missão corporativa e subsidiar elementos básicos para melhoria da competitividade. (Brito, Antonialli e Santo, 1997, p.78)*

A informação também é importante para a sociedade. A Unesco considera o acesso à informação como um direito da sociedade e desenvolve ações para que este direito seja disponibilizado. Werthein (2000) descreve como este processo acontece.

> *Na Unesco, o Programa Geral de Informação (PGI) e o Programa Intergovernamental de Informática (IIP), hoje fundidos no Programa Informação para Todos, enfeixavam as ações desse organismo internacional em duas áreas principais, conteúdo para a sociedade da informação e "infoestrutura" para esta sociedade em evolução, por meio da cooperação para treinamento, apoio ao estabelecimento de políticas de informação e promoção de conexões em rede.*
>
> *No espírito da Declaração Universal dos Direitos do Homem que constitui a base dos direitos à informação na sociedade da informação, e levando em consideração os valores e a visão delineados anteriormente, o novo Programa Informação para Todos deverá prover uma plataforma para a discussão global sobre acesso à informação, participação de todos na sociedade da informação global e as conseqüências éticas, legais e societárias do uso das tecnologias de informação e comunicação. Deverá prover também a estrutura para colaboração internacional e parcerias nessas áreas e apoiar o desenvolvimento de ferramentas comuns, métodos e estratégias para a construção de uma sociedade de informação global e justa. (Werthein, 2000, p.77)*

Retornando ao ambiente das organizações, Freitas e Kladis (1995) entendem que a informação como um recurso fundamental acontece em todos os níveis organizacionais: operacional, estratégico e tático.

> *A importância da informação dentro das organizações aumenta com o crescimento da sociedade e das organizações. Em todos os níveis organizacionais (operacional, tático e estratégico) a informação é um recurso fundamental. (Freitas e Kladis, 1995, p.73)*

A necessidade da proteção do recurso informação também acontece para as pequenas e médias empresas. Neto e Silveira (2007) registram esta questão.

> *Os riscos aumentaram com o uso dos microcomputadores, a utilização de redes locais e remotas, a abertura comercial da Internet e a disseminação da informática para diversos setores da sociedade.*
>
> *As pequenas e médias empresas também são atingidas por estes problemas, porém dispõem de menos recursos para investir na gestão da segurança da informação. (Neto e Silveira, 2007, p.376)*

Domeneghetti e Meir (2009) consideram que o conhecimento é a base para a geração de valor nas corporações e que a informação é a matéria prima para o conhecimento estruturado nas organizações. Eles acrescentam:

> *A globalização da economia, impulsionada pela Tecnologia da Informação e pela malha intermitente, multiformato e multicanal das comunicações, é uma realidade da qual não se pode escapar. A informação tornou-se a fonte de aproximadamente três quartos do valor agregado nas indústrias. É neste contexto que o Conhecimento, ou melhor, que a Gestão do Conhecimento e a Inteligência Competitiva se transformam em valiosos recursos estratégicos para a vida das pessoas e das empresas. (Domeneghetti e Meir, 2009, p.176).*

Maximiniano (2010) considera a informação como um dos recursos que compõem a organização e que possibilita que esta organização realize seus objetivos através dos produtos ou serviços.

Assis (2006) considera a informação como um dos insumos importantes para o desenvolvimento empresarial quando disponibilizada com rapidez e precisão, refletindo o contexto atual do mercado e da economia mundial. Para Laureano e Moraes (2005) a informação é substrato da inteligência competitiva e deve ser administrada em seus particulares, diferenciada e salvaguardada. Freitas e Kladis (1995) defendem que a informação na sociedade moderna é um bem de extrema importância, sendo um dos fatores responsáveis pela sobrevivência das organizações, e quando bem gerenciado, um forte fator de vantagem competitiva. E considerando a informação e a tecnologia da informação Ikenaga (2008, p.2) afirma que “As empresas estão cada vez mais dependentes de seus sistemas de informação e dos recursos de tecnologia da informação.”

Sales e Almeida (2007) declaram que a informação é a fonte do conhecimento.

> *O conhecimento não existe se não houver uma fonte, uma origem, de informação que fornece subsídios para sua construção. Tem-se que durante todo o processo histórico do desenvolvimento do conhecimento o homem dependeu das fontes de informação, que se transformaram e continuam se transformando até hoje.(Sales e Almeida, 2007, p.68)*

A informação transformada em conhecimento é reconhecida como um elemento crítico para o desenvolvimento e crescimento da organização, como bem demonstra a resposta de um gerente em uma pesquisa sobre a proteção do conhecimento.

> *O conhecimento foi um dos fatores críticos que mais contribuiu para que a empresa chegasse aonde chegou e com as perspectivas futuras que possui. (Lobo e Jamil, 2008, p.104)*

Em alguns casos a informação é a essência do objetivo da organização (serviço ou produto). James Téboul (1999) considera que qualquer atividade que trate da informação ou da gestão de conhecimento pode ser considerada serviço, que é um dos objetivos da organização segundo Maximiniano (2010).

Sendo a informação um recurso essencial para a realização dos negócios da organização, a ABNT (2005) normatiza que esta informação precisa ser protegida adequadamente de maneira a garantir a sua confidencialidade, integridade e disponibilidade.

O não atendimento a estes requisitos (confidencialidade, integridade e disponibilidade) ou a um deles, acarreta impactos para a organização. Uma pesquisa realizada pela Universidade do Texas indicou que 93% das organizações que tiveram indisponibilidade de informação por mais de dez dias em função de desastre nos recursos de TI, chegaram à falência um ano depois (Brotby, 2009). Em termos de impactos financeiros e perda de clientes, Brotby (2009) complementa:

> *Uma análise detalhada realizada pela PGP Corporation em conjunto com a Vontu Company, identificou que 31 companhias que sofreram violações de informação em 2006 tiveram uma perda média de US$ 4,8 milhões, além do que 19% dos clientes deixaram de se relacionar com a companhia e outros 40% dos clientes consideravam a possibilidade de deixar de serem clientes. (Brotby, 2009, p.14).*

Brotby (2009) continua exemplificando o impacto direto da segurança da informação quando cita um estudo da *Aberdeen Group* que considerou empresas de vários tamanhos, porém todas elas com faturamento anual maior que US$ 500 milhões:

> *Firmas que operaram com excelência (Best-in-class) em segurança possuem nível de perdas financeiras a menos de um por cento, enquanto as demais organizações têm experimentado perdas que superam cinco por cento. (Brotby, 2009, p.9).*

Segundo Pereira e Nascimento (2005) erros e ações de má fé em relação à informação acarretam mais do que prejuízos às organizações e afetam à sociedade.

> *Os erros e fraudes cometidos contra as empresas têm impactos diretos na sociedade, pois com a globalização da economia os mercados financeiros deixaram de ser regionais e passaram a ser mundiais. (Pereira e Nascimento, 2005, p. 46)*

As organizações precisam implantar um processo de segurança da informação, e este processo deve ser considerado um ativo da organização, como tantos outros. Domeneghetti e Meir (2009) consideram a segurança da informação como um dos ativos intangíveis de proteção de valor. Na opinião destes autores os bens ou ativos de uma organização podem ser classificados como bens tangíveis e bens intangíveis.

Os bens tangíveis são os bens físicos ou bens financeiros. Os bens intangíveis podem ser divididos em intangíveis que geram valor e intangíveis que protegem valor. Como intangíveis que geram valor eles citam as Marcas, a Inovação e o Capital Intelectual. Como ativos intangíveis de proteção de valor são considerados a Segurança da Informação, Gestão de Riscos e Governança Corporativa. Estes ativos intangíveis de proteção de valor devem proteger os ativos intangíveis de geração de valor e os ativos tangíveis.

Para exemplificar que os bens intangíveis possuem valor, Domeneghetti e Meir (2009) citam casos práticos:

> *Em 1996, especialmente emblemático, a IBM possuía US$ 19 bilhões de bens móveis, fábricas e equipamentos. A Microsoft somava US$ 30 milhões, mas seu valor de venda, traduzido pelos papéis negociados na Bolsa, superava em muito a oponente. Havia algo muito mais valioso do que ativos físicos ou financeiros. (Domeneghetti e Meir, 2009, p.2).*
>
> *Quando a Philip Morris incorporou a Kraft por US$ 10 bilhões, esta última tinha um patrimônio contabilizado de pouco mais de US$ 1 bilhão. A diferença entre os valores contábeis e os valores de aquisição da empresa pode ser atribuída a ativos intangíveis. (Domeneghetti e Meir, 2009, p.2).*
>
> *Segundo a Economática, a Nike vale quase quatro vezes o seu balanço contábil. A diferença são os bens intangíveis. (Domeneghetti e Meir, 2009, p.14).*

A informação é um bem para organização e necessita ser adequadamente protegida pela utilização de um processo de segurança da informação. Para implantar e manter um processo de segurança da informação a Norma NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Código de prática para a gestão da segurança da informação, orienta:

> *Convém que a direção estabeleça uma clara orientação da política, alinhada com os objetivos de negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma*

> *política de segurança da informação para toda a organização. (ABNT, 2005, p.8)*

É estrutural que a organização tenha uma política de segurança da informação para que o processo de segurança da informação possa ser elaborado, implantado e mantido. Esta política definirá as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na sua proteção da informação. (ABNT, 2005; Vianez, Segobia e Camargo, 2008)

Por força da legislação, as organizações do segmento financeiro e as grandes corporações que possuem ações em Bolsas de Valores em alguns países, como nos Estados Unidos por causa da Lei Sarbane-Oxley, já foram obrigadas a elaborar suas políticas de segurança da informação. Outras organizações por decidirem seguir a estrutura da Governança Corporativa, inclusive no Brasil, também se viram obrigadas a desenvolver e implantar políticas de segurança da informação. Muitas dessas organizações já possuem políticas de segurança há alguns anos e já fizeram revisões e ajustes práticos para estes regulamentos.

No entanto existem outras organizações que não se enquadram nestes casos e que começam a ser pressionadas para protegerem a sua informação de uma maneira mais formal e estruturada. Este fato acontece porque estas organizações prestam serviços para organizações maiores que estão obrigadas a possuírem uma estrutura de segurança da informação. Estas organizações maiores entendem que seus fornecedores, que são elementos da sua cadeia de realização do negócio, devem ter o mesmo grau e estrutura de segurança da informação que elas possuem.

Em outros casos, a conscientização do empresário e a atitude madura dos acionistas, desejando a sustentabilidade do negócio, têm exigido que a organização funcione de maneira bem estruturada, utilize as melhores práticas e possua os controles organizacionais adequados para a segurança da informação.

Em relação às organizações que utilizam dados de saúde, existe um projeto em andamento na ABNT - Associação Brasileira de Normas Técnicas denominado Projeto 78:000.00-19 – Informática em Saúde – Gestão de segurança da informação em saúde usando a ABNT NBR ISO/IEC 27002. Esta futura Norma define regras

complementares para as organizações de saúde ou demais organizações que tratam com informações pessoais de saúde:

> *Esta Norma fornece orientação às Organizações de saúde e aos outros custodiantes de informações pessoais de saúde sobre a melhor maneira de proteger a confidencialidade, a integridade e a disponibilidade de tais informações pessoais de saúde através da implementação da ABNT NBR ISO/IEC 27002. (ABNT, 2009, p.5)*

Nesta Norma, as orientações para as organizações de saúde ou demais organizações que tratam com informações pessoais de saúde são mais rígidas do que as orientações para as organizações em geral. Diferentemente da Norma ISO/IEC 27002:2005 – Tecnologia da Informação – Código de prática para a gestão da segurança da informação, que declara (ABNT, 2005, p.8) que "convém que a direção estabeleça uma clara orientação da política..." o Projeto 78:000.00-19 indica:

> *Organizações processando informações de saúde, incluindo informação pessoal de saúde, **devem** possuir uma política de segurança da informação escrita que seja aprovada pela gerência, publicada, e comunicada para todos os funcionários e partes externas relevantes (ABNT, 2009, p.29)*

Muitas organizações que tratam de dados de saúde ainda não possuem suas políticas de segurança da informação apesar de seus executivos entenderem a importância de regulamentos de segurança da informação. Em sua pesquisa "Ciclo contínuo de acompanhamento para desenvolvimento de uma política de segurança da informação em organizações hospitalares", Albertin e Pinochet (2010) descrevem o levantamento em cinco unidades hospitalares no Estado de São Paulo, onde em todas elas, de uma maneira direta ou indireta, os gestores declaram a importância da segurança da informação, porém nenhuma delas possui uma política adequada para a segurança da informação. Quando muito, possuem algumas regras de controle de acesso ao ambiente computacional. Algumas das proposições geradas a partir de depoimentos dos gestores desses hospitais demonstram a dificuldade que estas organizações têm para gerar uma política de segurança da informação:

> *O hospital possui deficiência em desenvolver uma política de segurança da informação. (Albertin e Pinochet, 2010, p.275).*
>
> *Os gestores na sua maioria consideram que falta conhecimento de como mapear as necessidades para se desenvolver uma política de segurança da informação formal. (Albertin e Pinochet, 2010, p.275).*
>
> *O hospital possui claras deficiências em desenvolver uma política de segurança da informação devido à falta de orientação da Secretaria (de Estado) e do conselho de saúde. (Albertin e Pinochet, 2010, p.275).*

Ao buscar elaborar uma política de segurança da informação a organização vai se deparar com uma grande quantidade de requisitos descritos na NBR ISO/IEC 2007:2005. Estes requisitos são tratados por esta Norma de maneira igualitária, indicando que uma política deveria conter todos eles. Este fato gera dificuldades como as citadas na pesquisa acima e impede que a organização comece o amadurecimento no seu processo de segurança da informação utilizando um padrão mínimo de política de segurança da informação.

A literatura existente se concentra em definir como desenvolver e implantar os controles, principalmente os controles técnicos. São raras as orientações em termos de elaboração, conteúdo e estrutura de políticas ou outros regulamentos. O material publicado quando recomenda os elementos que uma política deve conter, repete sem priorização, todos os elementos que estão descritos na Norma ISO/IEC 27002:2005 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação.

Uma grande quantidade das organizações que atuam no Brasil precisa ou precisará definir seu conjunto de regulamentos de segurança da informação pelo fato de serem fornecedoras, ou desejarem ser fornecedoras de organizações que estão submetidas a regulamentos que exigem um processo de segurança estruturado e que agora estão exigindo esta mesma proteção das organizações que fazem parte da sua cadeia de valor. Outras organizações estão implantando Governança Corporativa que por sua vez exigirá a existência da Governança de Segurança da Informação e conseqüentemente será necessária a existência da política de segurança da informação nesta organização e nas outras organizações que participam da sua cadeia de valor. Estes fatos acrescem relevância a este estudo.

A segurança da informação abrange mais que o ambiente da tecnologia da informação, porém este ambiente de tecnologia, cada vez mais, processa e armazena informações da organização. Desta maneira as atividades operacionais e o atendimento aos objetivos estratégicos da organização dependem totalmente do ambiente de tecnologia da informação e da própria informação. Conseqüentemente é necessário proteger a informação e definir diretrizes (políticas) para esta proteção.

Os gestores estão cientes dessa criticidade. Albertin e Pinochet (2010) comentam sobre a 12ª. Edição da Pesquisa da FGV-EAESP de Comércio Eletrônico:

> *A Pesquisa da FGV-EAESP de Comercio Eletrônico, em sua 12ª edição, de março de 2010, apresentou uma mostra significativa formada por 434 empresas, de vários setores e portes, que atuam no ambiente tradicional e também estão atuando no ambiente de comércio eletrônico, em maior ou menor nível, e aquelas constituídas apenas por este ambiente. ...*
>
> *... Esta pesquisa evidenciou que as empresas estão atribuindo maior importância aos aspectos de relacionamento com clientes, privacidade e segurança, adoção de clientes e alinhamento estratégico, entre outros. Sendo que o aspecto de privacidade e segurança é considerado um dos itens mais críticos. Embora a Pesquisa da FGV-EAESP de Comércio Eletrônico, em sua 12ª edição de março de 2010, indique que o item privacidade e segurança esteja posicionado em segundo lugar, a oitava edição da mesma pesquisa, de março de 2006, apresentou o item privacidade e segurança em primeiro lugar. Portanto tem-se obtido certa estabilidade na priorização pelas empresas quanto à necessidade na utilização de tecnologia da informação em relação ao tema da privacidade e segurança. (Albertin e Pinochet, 2010, p.10).*

Outro fato que reforça que a segurança da informação e a existência de políticas são preocupações contínuas e prioritárias nas organizações, é o conjunto de respostas do estudo conduzido pela Consultoria PricewaterhouseCopers, CIO Magazine e CSO Magazine. Este é o maior estudo do gênero do mundo, o qual representa a análise consolidada dos dados fornecidos por mais de 12.800 executivos, entre CEOs, CFOs, CIOs e CSOs, vice presidentes e diretores de TI e segurança da informação de empresas médias, grandes e gigantes de 135 países e de todos os setores. No Brasil houve a participação de 500 executivos. Apesar de toda a crise mundial em relação à segurança da informação descrita no estudo, destaca-se no documento PWC (2010):

* A conformidade com políticas internas é um dos cinco fatores direcionadores mais importantes para o gasto com a segurança da informação. Isto significa a pré existência de políticas de segurança. Os outros fatores foram: condições econômicas, continuidade do negócio/recuperação de desastres, reputação da empresa e conformidade regulatória.

* 56% responderam que o ambiente regulatório se tornou mais complexo e oneroso.

* 55% responderam que o ambiente de risco crescente aumentou o papel e a importância da função de segurança da informação.

* 43% responderam que ameaças à segurança dos ativos aumentaram.

* 53% responderam que não reduziu o orçamento para iniciativas de segurança e nem adiaram estas iniciativas.

* 52% responderam que vão aumentar os gastos com segurança da informação nos próximos 12 meses.

Todas estas respostas demonstram que as organizações consideram a segurança da informação um fator importante para o alcance dos seus objetivos de negócio. Isto significa que as organizações precisam ter as suas políticas de segurança, pois conforme afirmam Albertin e Pinochet (2010) “No âmbito das organizações, a manutenção da segurança depende da adequada formulação e implantação de políticas corporativas.” (Albertin e Pinochet, 2010, p.10).

Para este trabalho de pesquisa, utilizaremos o termo política como sendo a diretriz, a orientação básica para o assunto segurança da informação. Define Maximiniano (2010, p.86):

> *Política é sinônimo de diretriz. Uma política ou diretriz é uma orientação genérica que define em linhas gerais o curso de ação a ser seguido quando determinado tipo de problema se apresenta. A política orienta o processo de tomada de decisões através da definição de critérios que devem ser seguidos.*

Peltier (2004) considera a Política como o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. A política é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades.

Outros autores colaboram nesta linha de definição:

> *Uma política é um guia genérico para a ação. Ela delimita uma ação, mas não especifica o tempo. É uma definição de propósitos de uma empresa e estabelece linhas de orientação e limites para a ação dos indivíduos responsáveis pela implantação. As políticas são princípios que estabelecem*

> *regras para a ação e contribuem para o alcance bem sucedido dos objetivos. (Chiavenatto, 2010, p.173).*
>
> *Política de segurança é um conjunto de diretrizes gerais destinadas a governar a proteção que será dada aos ativos de informação. (Caruso e Steffen, 1999, p.49)*
>
> *Política de segurança é um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações recebam a proteção conveniente que possibilite garantir a sua confidencialidade, integridade e disponibilidade. (Barman, 2002, p.4).*
>
> *As políticas são as linhas mestras que indicam os limites ou restrições sobre aquilo que se quer conseguir. (Albertin e Pinochet, 2010, p.34)*

A própria NBR ISO/IEC 27002:2005 tem a sua definição do termo política:

> *2. Termos e definições*
> *2.8 Política*
> *Intenções e diretrizes globais formalmente expressas pela direção. (ABNT, 2005, p.2).*

É neste ambiente que o presente trabalho busca contribuir para a elaboração de um padrão mínimo de política de segurança da informação de maneira a ajudar principalmente as organizações que estão começando o seu processo de segurança da informação.

1.1. Questão Problema

Com o objetivo de facilitar os primeiros passos da organização no processo de segurança da informação, surge a indagação: seria possível elaborar e formalizar uma política de segurança da informação para um primeiro estágio de maturidade da organização considerando apenas alguns desses requisitos?

Pensar a implementação por etapas é referendada pela NBR ISO/IEC 27001:2006 quando ela orienta sobre a maneira de implantação de um Sistema de Gestão de Segurança da Informação:

> *É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (ABNT, 2006, p.v)*

Considerando este cenário indagativo, o presente estudo considera a seguinte questão-problema:

- Quais são os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização?

Uma vez estabelecida a questão-problema, foram estabelecidas as seguintes delimitações:

* o foco do trabalho diz respeito aos documentos de políticas e não considera os documentos de procedimentos ou de regras detalhadas que indicam como executar o que as políticas definem;

* o trabalho foi baseado no conjunto de controles definidos na NBR ISO/IEC 2002:2005.

1.2. Objetivos da Pesquisa

Este estudo tem como objetivo principal:

- Identificar os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização tomando por base elementos comuns existentes em políticas de organizações distintas.

Contempla, ainda, os seguintes objetivos específicos:

- realizar um levantamento da literatura sobre o assunto política de segurança da informação;
- desenvolver um estudo teórico sobre o assunto política de segurança da informação;
- realizar um estudo de caso múltiplo a partir de uma pesquisa exploratória em organizações que possuem políticas de segurança da informação;
- analisar estas políticas de segurança;

- identificar a existência de elementos comuns nestas políticas;
- estabelecer os elementos que comporão o padrão mínimo para a política de segurança da informação.

1.3. Justificativas e Contribuições da Pesquisa

Apesar da NBR ISO/IEC 27001:2006 (ABNT, 2006, p.v) indicar que "É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização", atualmente não existe um padrão mínimo para as políticas de segurança da informação que cada organização precisa implantar. Este fato evidencia a necessidade de um estudo exploratório desta temática.

Um aspecto relevante para este estudo é o fato de que os controles de segurança definidos pela NBR ISO/IEC 27002:2005 são necessários e pertinentes para as organizações, porém, a norma não indica quais desses controles deveriam ser considerados em um conjunto mínimo de maneira a permitir que as organizações construam sua proteção de informação por etapas começando por este conjunto mínimo. A NBR ISO/IEC 27001:2006 contempla uma implementação modular do SGSI – Sistema de Gestão da Segurança da Informação:

> *É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (ABNT, 2006, p.v)*

As organizações que já implantaram as políticas de segurança da informação não consideraram todos os requisitos da Norma ISO/IEC 27002:2005. Essas organizações elaboraram políticas que utilizaram um subconjunto desses requisitos.

Esta pesquisa vem, pois suprir a lacuna na orientação de como as organizações no seu estado inicial de maturidade em segurança da informação devem considerar os requisitos quando do desenvolvimento e implantação de sua política de segurança da informação.

Ao ser identificado um padrão mínimo para a política de segurança da informação, o esforço das empresas que necessitam elaborar sua política de segurança da informação será minimizado e o processo de construção será facilitado. Esta forma permitirá uma implantação modular e um amadurecimento crescente da política de segurança da informação.

Este trabalho pretende contribuir com os estudos relacionados às políticas de segurança da informação e busca instrumentalizar as organizações que estão no estágio inicial da construção das suas políticas de segurança da informação.

1.4. Metodologia

A metodologia utilizada neste estudo considera o estudo de caso integrado (unidades múltiplas de análise) utilizando a pesquisa exploratória.

Será utilizado o estudo de caso para esta pesquisa exploratória por ser a estratégia que melhor atende às características da mesma. Segundo Yin (2010) o estudo de caso é utilizado para examinar acontecimentos contemporâneos e também para contribuir ao nosso conhecimento os fenômenos individuais, grupais, organizacionais, sociais, políticos e relacionados. Complementa que as aplicações de estudo de caso podem ser feitas para explorar situações em que a intervenção que está sendo avaliada não apresenta um conjunto simples e claro de resultados.

Yin (2010) explicita:

> *O estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto na vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente evidentes. Yin (2010, p.39).*

Neste estudo a metodologia considerará as seguintes etapas:

a) Levantamento da literatura sobre o assunto política de segurança da informação, considerando fontes acadêmicas e empresariais.

b) Estudo teórico do tema política de segurança da informação.

c) Desenvolvimento de um estudo de caso múltiplo de modo a analisar políticas de segurança da informação já implantadas em organizações e identificar elementos comuns que possam estabelecer um padrão mínimo de política de segurança da informação.

1.5. Estrutura da Dissertação

A estrutura deste estudo descreve o problema de pesquisa, a fundamentação teórica, o estudo de caso e a conclusão, contendo as considerações finais e as sugestões de estudos futuros.

O primeiro capítulo consta da Introdução e o seu conteúdo apresenta a questão problema, o objetivo da pesquisa, a justificativa e contribuições do estudo, a metodologia da dissertação e este item de estrutura da dissertação.

O segundo capítulo contempla a fundamentação teórica. Este capítulo aborda o requisito política de segurança da informação em diversos elementos (processos, estruturas conceituais, normas):

- Processo de segurança da informação e gestão de riscos.
- NBR ISO/IEC 27002:2005
- NBR ISO/IEC 27001:2006
- NBR ISO/IEC 27005:2008
- Futura NBR ISO/IEC 27799
- COBIT
- ITIL
- Governança Corporativa e Governança de Segurança da Informação

O terceiro capítulo apresenta uma revisão do estado da arte da temática em questão, levando-se em consideração teses, dissertações e artigos científicos que foram examinados nesta pesquisa.

O quarto capítulo descreve o estudo de caso realizado, a metodologia utilizada e a análise da aplicação do estudo de caso.

O quinto capítulo relata os resultados do estudo de caso.

Por fim têm-se as conclusões, considerações finais, sugestão de estudos futuros, referências utilizadas para a elaboração deste trabalho e material complementar apresentado como apêndice.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a política de segurança da informação relacionada com diversos elementos que normatizam, estruturam, realizam, controlam ou gerenciam o uso da informação no ambiente corporativo.

2.1. Política de segurança da informação - Processo de Segurança da informação e Gestão de risco

O processo de segurança da informação existe para possibilitar que a organização utilize de maneira confiável os recursos que suportam as informações necessárias para as suas atividades estratégicas, táticas e operacionais.

Thomas Peltier define a segurança da informação dando ênfase na proteção dos recursos:

> *Segurança da informação direciona e suporta a organização para a proteção de seus recursos de informação contra intencional ou não intencional divulgação indevida, modificação não autorizada, destruição não desejada, ou negação de serviço através da implantação de controles de segurança definidos em políticas e procedimentos. (Peltier, 2004, p. 9).*

Peltier continua indicando que a segurança da informação está ligada fortemente aos objetivos de negócio. Para Peltier a segurança da informação não deve existir

para ela mesma; a segurança da informação deve existir para atender à organização e aos seus objetivos de negócio:

> *Para garantir que os objetivos de negócio são alcançados no tempo previsto e de uma maneira eficiente, padrões e políticas eficazes devem existir na organização. (Peltier, 2004, p. 14).*
>
> *Segurança pela própria segurança, não possui valor. A criação de políticas, padrões, e procedimentos deve ser benéfica para a organização. Nenhuma política deve ser criada para garantir que a organização está em conformidade com os requerimentos de auditoria. Políticas, padrões e procedimentos são criados para garantir que a organização atende aos requisitos legais e obrigações contratuais para seus clientes, acionistas e funcionários. (Peltier, 2004, p. 14).*
>
> *Boas regras de segurança da informação não são definidas para satisfazer a própria segurança, elas são implantadas para proteger recursos de informação utilizados no funcionamento da organização e conseqüentemente protegem os objetivos da organização. (Peltier, 2005, p. XV).*

A NBR ISO/IEC 27002:2005 reforça estas orientações acima descritas quando ela explica que a segurança da informação é importante para o setor público e para o setor privado:

> *A segurança da informação é importante para os negócios, tanto do setor público como do setor privado, e para proteger as infra-estruturas críticas. Em ambos os setores, a função da segurança da informação é viabilizar os negócios como o governo eletrônico (e-gov) ou o comércio eletrônico (e-business), e evitar ou reduzir os riscos relevantes. (ABNT, 2005, p.x).*

Para que a proteção da informação aconteça de maneira eficaz, eficiente e contínua a NBR ISO/IEC 27002:2005 indica a necessidade da existência de políticas, entre outros controles:

> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.*
>
> *Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p.x).*

Por sua vez a NBR ISO/IEC 27001:2006 orienta sobre a maneira de implantação de um Sistema de Gestão de Segurança da Informação declarando:

> *É esperado que a implementação de um SGSI seja escalada conforme as necessidades da organização, por exemplo, uma situação simples requer uma solução de um SGSI simples (ABNT, 2006, p.v)*

Em relação ao processo de gestão da segurança da informação a NBR ISO/IEC 27001:2006 provê um modelo para estabelecer, implantar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI) conforme as necessidades da organização.

A NBR ISO/IEC 27001:2006 especifica:

> *A abordagem de processo para a gestão da segurança da informação apresentada nesta Norma encoraja que os seus usuários enfatizem a importância de:*
>
> > *a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança da informação;*
> >
> > *b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;*
> >
> > *c) monitoração e análise crítica do desempenho e eficácia do SGSI;*
> >
> > *d) melhoria continua baseada em medições objetivas.*
> > *(ABNT, 2006, p.v)*

Para a implantação desta gestão a norma adota uma abordagem de processo utilizando o modelo conhecido como PDCA *(Plan-Do-Check-Act).*

A primeira etapa é de Planejamento *(P-Plan*), e acontece no início do ciclo PDCA,. Nesta etapa deve-se:

> *Estabelecer a política, os objetivos, os processos e os 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. (ABNT, 2006, p. vi).*

Nesta etapa de planejamento são enfatizados dois elementos para gestão da segurança da informação: a política e a gestão de riscos. A orientação para o desenvolvimento da política encontra-se na ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação e a orientação para a gestão de risco em segurança da informação encontra-se na ABNT NBR ISO/IEC 27005:2008 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos.

A NBR ISO/IEC 27002:2005 declara em relação à política de segurança da informação:

> *5.1 Política de segurança da informação*
> *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 regulamentos pertinentes.*
>
> *Convém que a direção estabeleça uma clara orientação de política, alinhada com os objetivos de negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização. (ABNT, 2005, p. 8).*

A NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação indica que para que a gestão de risco seja realizada é necessário que ela seja parte da gestão da segurança da informação e que seja definida a sua contextualização indicando onde a gestão de risco será aplicada: na organização como um todo, em uma área, em um sistema ou a controles específicos.

> *Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI. (ABNT, 2008, p. 3).*
>
> *Em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase "planejar". (ABNT, 2008, p. 6).*
>
> *O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo: um departamento, uma localidade, um serviço), a um sistema de informações, a controles já existentes, planejados ou apenas aspectos particulares de um controle (Por exemplo: o plano de continuidade de negócio). (ABNT, 2008, p. 4).*

A ABNT NBR ISO/IEC 27002:2005, ao tratar da análise, avaliação e tratamento de risco, orienta:

> *Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz. (ABNT, 2005, p.6)*

Ao se definir o escopo e os limites para a gestão de riscos a ABNT NBR ISO/IEC 27005:2008 declara que:

> *O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI conforme requerido na ABNT ISO/IEC 27001 4.2.1.a. (ABNT, 2008, p. 9).*

A ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistema de gestão de segurança da informação – Requisitos, item 4.2.1, indica os primeiros elementos para que a organização estabeleça um SGSI e cita a política de segurança da informação:

> *4.2.1 Estabelecer o SGSI*
> *a) Definir o escopo e os limites do SGSI (Sistema de gestão de Segurança da Informação) nos termos das características do negócio, a organização, sua localização, ativos de tecnologia, incluindo detalhes 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 as ações relacionadas com a segurança da informação;*
>
> *2. considere os requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;*
>
> *3. esteja alinhada com o contexto estratégico de gestão de risco da organização no qual o estabelecimento e manutenção do SGSI irá ocorrer;*
>
> *4. estabeleça critérios em relação aos quais os riscos serão avaliados*
>
> *c) Definir a abordagem de análise e avaliação de riscos da organização*
> *(ABNT, 2006, p. 4)*

Desta forma a Política do Sistema de Gestão da Segurança da Informação deverá considerar e contextualizar a gestão de riscos, conforme a própria ABNT NBR ISO/IEC 27005:2008 – Tecnologia de segurança – Técnicas de segurança – Gestão de riscos em segurança da informação e a ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação indicam:

> *Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com análises/avaliações de riscos de outras áreas, se necessário. (ABNT, 2005, p.6)*
>
> *Convém que a organização defina o escopo e os limites da gestão de riscos de segurança da informação. (ABNT, 2008, p. 8)*
>
> *O escopo do processo de gestão de riscos de segurança da informação precisa ser definido para assegurar que todos os ativos relevantes sejam considerados na análise/avaliação de riscos. Além disso, os limites precisam ser identificados para permitir o reconhecimento dos riscos que possam transpor esses limites. (ABNT, 2008, p.8).*

> *Convém que a organização e as responsabilidades para o processo de gestão de riscos de segurança da informação sejam estabelecidas e mantidas. (ABNT, 2008, p. 9)*
>
> *O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI (ABNT, 2008, p. 9).*

A gestão de riscos por sua vez será parte do Sistema de Gestão de Segurança da Informação e fará com que este SGSI se mantenha contínuo:

> *Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação cotidiana de um SGSI. (ABNT, 2008, p. 3)*
>
> *Convém que a gestão de riscos de segurança da informação seja um processo contínuo. (ABNT, 2008, p. 3)*
>
> *Convém que as análises/avaliações de riscos também sejam realizadas periodicamente para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação de risco e quando uma mudança significativa ocorrer. Essas análises/avaliações devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.*

Peltier (2001, 2004, 2005) orienta sobre a questão da política e da gestão de riscos, no que diz respeito à segurança da informação:

> *A política é uma diretiva da direção executiva para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades. (Peltier, 2004, p. 47)*
>
> *Ao implantar a sua política, a organização toma controle do seu destino. (Peltier, 2004, p. 47).*
>
> *O primeiro e mais importante aspecto da segurança da informação é a política de segurança. Se a segurança da informação fosse uma pessoa a política de segurança seria o sistema nervoso. Política é a base da segurança da informação, providencia a estrutura e define os objetivos dos demais aspectos da segurança da informação. (Peltier, 2005, p. 17).*
>
> *Um importante fator para o sucesso na implantação de um processo de segurança da informação é implantar uma completa arquitetura de gerenciamento de risco. Esta arquitetura deve estar conectada as políticas e padrões de segurança da informação e deve direcionar o risco para o negócio em um ambiente automático e continuo. (Peltier, 2001, p. 17).*
>
> *A análise de risco permite a organização colocar foco nos seus objetivos de segurança da informação. (Peltier, 2001, p. 17).*

As políticas e diretrizes definem o escopo para o qual serão considerados os controles de segurança da informação que serão desenvolvidos e implantados. A Gestão de Risco, considerando o contexto definido pela política de segurança,

identificará os ativos, selecionará os controles apropriados e definirá as prioridades de implantação destes controles.

A não implantação da política impede o desenvolvimento adequado da segurança da informação na organização, uma vez que faltarão referenciais para implantação dos controles.

Existe um risco básico para o SGSI: não existência de políticas. Ele deve ser minimizado e até eliminado. Para que isto aconteça é necessário implantar o conjunto de regulamentos iniciando pela política principal (diretriz) que definirá o escopo e os limites da própria gestão de risco.

Page (2002) confirma este risco, não existência de regulamentos, ao declarar:

> *A priorização para o desenvolvimento e implantação dos elementos de segurança da informação deve ser obtida da análise e avaliação de riscos. Entendemos que a ameaça e o risco da não existência de um conjunto de regulamentos para que os controles tomem por base e sejam implantados é uma questão estrutural para o processo de segurança da informação, que deve ser tratado adequadamente, pois a sua ausência pode inclusive inviabilizar o processo de segurança. (Page, 2002, p. 18)*

Por fim, a ABNT NBR 27002:2005 orienta o uso de controles como ponto de partida e a utilização da gestão de riscos para a identificação da relevância da implantação e existência desses controles:

> *0.6 - Ponto de partida para a segurança da informação.*
> *Um certo número de controles pode ser considerado um bom ponto de partida para a implementação da segurança da informação. Estes controles são baseados tanto em requisitos legais como nas melhores práticas de segurança da informação normalmente usadas.*
>
> *Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem dependendo da legislação aplicável:*
> *a) proteção de dados e privacidade de informações pessoais;*
> *b) proteção de registros organizacionais;*
> *c) direitos de propriedade intelectual.*
>
> *Os controles considerados práticas para a segurança da informação incluem:*
> *a) documento da política de segurança da informação;*
> *b) atribuição de responsabilidades para a segurança da informação;*
> *c) conscientização, educação e treinamento em segurança da informação;*
> *d) processamento correto nas aplicações;*
> *e) gestão de vulnerabilidades técnicas;*
> *f) gestão de continuidade de negócio;*
> *g) gestão de incidentes de segurança da informação.*

> *Esses controles se aplicam para a maioria das organizações e na maioria dos ambientes.*
>
> *Convém observar que, embora todos os controles nesta Norma sejam importantes e devam ser considerados, a relevância de qualquer controle deve ser determinado segundo os riscos específicos a que uma organização está exposta. Por isso, embora o enfoque acima seja considerado um bom ponto de partida, ele não substitui a seleção de controles, baseado na análise/avaliação de riscos.*
> *(ABNT, 2005, p. xii)*

Desta maneira as organizações devem primeiramente considerar para o seu processo de segurança da informação, os controles definidos/descritos na NBR ISO/IEC 27002:2005 e tomá-los como controles básicos. Depois deve considerar a análise/avaliação de riscos específicos a que a organização está exposta, um instrumento para graduar a relevância da aplicação de cada um destes controles na organização.

2.2 – Política de segurança da informação – Norma NBR ISO/IEC 27002:2005

Título da Norma: NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação, ABNT, 2005.

A NBR ISO/IEC 27002:2005 é a norma estrutural da gestão da segurança da informação. Ela define um código de prática para a gestão da segurança da informação e orienta quais os elementos que devem ser considerados para uma adequada proteção da informação.

A própria norma considera que “controles adicionais e recomendações não incluídas nesta norma podem ser necessários” (ABNT, 2005, p. xiii). Porém, independente da existência destes controles adicionais, a norma recomenda a integração destes controles:

> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessários, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p.x)*

Esta norma é base desta pesquisa e algumas das categorias principais de segurança da informação que ela considera, tiveram normas específicas detalhando esta categoria, como é o caso dos riscos em segurança da informação que são considerados e tratados com mais detalhe na NBR ISO/IEC 27005 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

As Normas ISO/IEC 27002 e ISO/IEC 27001 têm origem no Padrão Britânico que em 1993 criou a Norma BS 7799. Oliveira Jr (2010), Sêmola (2003) e Martins e Santos (2005) descrevem que em 1995 em função do avanço das empresas e do crescimento da tecnologia este código de prática foi republicado em 1995 pelo BSI (British Standart International). No final da década de 1990 o BSI criou um programa de certificação de empresas certificadoras capazes de atestarem organizações na Norma BS 7799. Neste momento a Norma BS 7799 tinha duas partes. A parte 1 continha o código de conduta ou o guia de execução para a gestão da segurança da informação. A parte 2 continha os requisitos de auditoria para a certificação de um sistema de gestão de segurança da informação. Em função da importância do assunto segurança da informação, era fundamental que estas normas fossem publicadas por um órgão de reconhecimento internacional. No ano de 2000, foi publicadas pela ISO (International Organization for Standardization) a norma ISO 17799, baseada na Norma BS 7799-1. Em 2005 esta norma passou por uma nova revisão que culminou na nova versão ISO/IEC 17799:2005. Neste mesmo ano de 2005, a BS 7799-2 foi adotada pela ISO e foi a primeira norma da família 27000, dedicada à segurança da informação. A BS 7799-2 tornou-se a ISO/IEC 27001:2005. Em 2007 a ISO/IEC 17799:2005 passou para o novo padrão e tornou-se a Norma ISO/IEC 27002:2005.

No Brasil estas normas foram consideradas pela Associação Brasileira de Normas Técnicas – ABNT, que é o Foro Nacional de Normatização. Na ABNT elas foram submetidas ao Comitê Brasileiro de Computadores e Processamento de Dados – ABNT/CB-2 e foram publicadas como: NBR ISO/IEC 27001 - Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos, ABNT, 2006; e NBR ISO/IEC 27002 Tecnologia da

informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação, ABNT, 2005. (ABNT, 2005).

O objetivo da NBR ISO/IEC 27002:2005 é declarado da seguinte forma:

> *Esta Norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão da segurança da informação. (ABNT, 2005, p. 1).*

A NBR ISO/IEC 27002:2005 é composta por 16 (dezesseis) capítulos, numerados de 0 (zero) à 15 (quinze) e são consideradas 11 (onze) seções de controles de segurança da informação. Cada seção é composta por um número variado de categorias principais de segurança da informação e cada categoria possui certo número de controles. Estes controles são os elementos que definem o que a norma considera importante para um processo de segurança da informação na organização e devem ser os elementos considerados para as políticas de segurança da informação das organizações.

Existem 133 (cento e trinta e três) controles explícitos nesta norma. Estes controles, de maneira isolada ou agrupada, ou considerando outros controles não descritos nesta norma, são os elementos considerados nesta pesquisa para a identificação do padrão mínimo para a política de segurança da informação de uma organização tomando por base elementos comuns existentes em políticas de organizações distintas.

Segue abaixo a descrição de cada capítulo e a relação dos 133 (cento e trinta e três) controles explicitados nesta norma.

a) Capítulo 0 – Introdução

Este capítulo inicia o assunto segurança da informação descrevendo o que á a segurança da informação, porque a segurança da informação é necessária, como se deve estabelecer requisitos de segurança da informação, a análise e avaliação dos riscos de segurança da informação, como começar o processo segurança da informação, fatores críticos de sucesso e desenvolvimento de diretrizes.

b) Capítulo 1 – Objetivo

Este capítulo descreve o objetivo da norma.

c) Capítulo 2 – Termos e definições

Neste capítulo estão definidos os termos utilizados na norma. O Anexo 3 contem os termos descritos na norma e que são utilizados nesta pesquisa.

d) Capítulo 3 – Estrutura

A divisão das seções e das categorias de segurança da informação são explicadas neste capítulo.

e) Capítulo 4 – Análise/avaliação e tratamento de riscos

Neste ponto a Norma descreve o processo de risco em duas fases: análise/avaliação do risco e tratamento do risco. Apesar deste capítulo definir alguns controles, eles não são considerados controles oficiais da norma, ficando apenas como orientações, como por exemplo (ABNT, 2005, p.6):

> *Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para a aceitação dos riscos e dos objetivos relevantes para a organização.*
>
> *Convém que as análises/avaliação de riscos também sejam realizadas periodicamente, para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco, ou seja, nos ativos, ameaças, vulnerabilidades, impactos, avaliação do risco e quando mudança significativa ocorrer.*

Em relação à política de segurança, este capítulo não cita diretamente política, mas pode-se fazer uma referencia indireta, quando ele declara:

> *Convém que a análise/avaliação de riscos de segurança da informação tenha um escopo claramente definido para ser eficaz e inclua os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário. (ABNT, 2005, p.6).*

Isto porque mais adiante na cronologia das normas, a NBR ISO/IEC 27005:2008 ao considerar o escopo e os limites para a gestão de riscos declara que:

> *O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI conforme requerido na ABNT ISO/IEC 27001 4.2.1.a. (ABNT, 2008, p. 9).*

Por sua vez a NBR ISO/IEC 27001:2008 descreve em relação ao SGSI:

> *4.2.1 Estabelecer o SGSI*
> *A organização deve;*
> *a) Definir o escopo e os limites do SGSI nos termos das características do negócio, a organização, sua localização, ativos e tecnologia.*
>
> *b) Definir uma política do SGSI nos termos das características do negócio: a organização, sua localização, ativos e tecnologia que:*
>
> *....*
> *3) esteja alinhada com o contexto estratégico de gestão de risco da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer;*
>
> *4) estabeleça critérios em relação aos quais os riscos serão avaliados. (ABNT, 2006, p.4)*

f) Capítulo 5 – Política de segurança da informação

Neste capítulo a norma recomenda que o documento de política de segurança da informação que deve definir como a organização vai se posicionar e exigir em relação aos controles das demais categorias de segurança.

A partir deste capítulo começam a ser definidos os controles de segurança. Para esta pesquisa, estes controles, de maneira independente ou agrupados, são a referência para a identificação dos elementos mínimos que devem compor um padrão mínimo para a política de segurança da informação de uma organização.

g) Controles

Descrevemos abaixo o título (assunto tratado) de cada controle. O Anexo 2 contem a descrição detalhada de cada um deles.

Controles do Capítulo 5 – Política de segurança da informação

(1) Documento da política de segurança da informação.

(2) Análise crítica da política de segurança da informação.

Controles do Capítulo 6 – Organizando a segurança da informação

(3) Comprometimento da direção com a segurança da informação

(4) Coordenação da segurança da informação.

(5) Atribuição de responsabilidades para a segurança da informação.

(6) Processo de autorização para os recursos de processamento da informação.

(7) Acordos de confidencialidade.

(8) Contato com autoridades.

(9) Contato com grupos especiais.

(10) Análise crítica independente de segurança da informação.

(11) Identificação dos riscos relacionados às partes externas.

(12) Identificando a segurança da informação, quando tratando com os clientes.

(13) Identificando a segurança da informação nos acordos com terceiros.

Controles do Capítulo 7 – Gestão de ativos

(14) Inventário dos ativos.

(15) Proprietário dos ativos.

(16) Uso aceitável dos ativos.

(17) Classificação da informação – Recomendações para classificação.

(18) Classificação da informação – Rótulos e tratamento da informação.

Controles do Capítulo 8 – Segurança em recursos humanos

(19) Papéis e responsabilidades.

(20) Seleção.

(21) Termos e condições de contratação.

(22) Responsabilidades da direção.

(23) Conscientização, educação e treinamento em segurança da informação.

(24) Processo disciplinar.

(25) Encerramento das atividades.

(26) Devolução de ativos.

(27) Retirada de direitos de acesso.

Controles do Capítulo 9 – Segurança física e do ambiente

(28) Perímetro de segurança física.

(29) Controles de entrada física.

(30) Segurança em escritórios, salas e instalações.

(31) Proteção contra ameaças externas e do meio ambiente.

(32) Trabalhando em áreas seguras.

(33) Acesso do público, áreas de entrega e de carregamento

(34) Instalação e proteção de equipamento.

(35) Utilidades.

(36) Segurança do cabeamento

(37) Manutenção dos equipamentos

(38) Segurança de equipamentos fora das dependência da organização.

(39) Reutilização e alienação segura de equipamentos.

(40) Remoção de propriedade

Controles do Capítulo 10 – Gerenciamento das operações e comunicações

(41) Documentação dos procedimentos.

(42) Gestão de mudanças.

(43) Segregação de funções.

(44) Separação dos recursos de desenvolvimento, teste e de produção.

(45) Entrega de serviço.

(46) Monitoramento e análise crítica de serviços terceirizados.

(47) Gerenciamento de mudanças para serviços terceirizados.

(48) Gestão de capacidade.

(49) Aceitação de sistemas.

(50) Proteção contra códigos maliciosos e códigos móveis.

(51) Controles contra códigos móveis.

(52) Cópias de segurança da informação.

(53) Controles de redes.

(54) Segregação dos serviços de rede.

(55) Gerenciamento de mídias removíveis.

(56) Descarte de mídias.

(57) Procedimentos para tratamento de informação.

(58) Segurança da documentação dos sistemas.

(59) Políticas e procedimentos para troca de informações.

(60) Acordos para trocas de informações.

(61) Mídias em trânsito.

(62) Mensagens eletrônicas.

(63) Sistemas de informações de negócio.

(64) Serviços de comércio eletrônico.

(65) Transações on-line.

(66) Informações publicamente disponíveis.

(67) Registros de auditoria.

(68) Monitoramento do uso do sistema.

(69) Proteção das informações dos registros (log).

(70) Registro (log) de administrador e operador.

(71) Registro (log) de falhas.

(72) Sincronização dos relógios.

Controles do Capítulo 11 – Acessos à informação

(73) Política de controle de acesso.

(74) Registro de usuário.

(75) Uso de privilégio.

(76) Gerenciamento de senha do usuário.

(77) Análise crítica dos direitos de acesso de usuário.

(78) Uso de senhas.

(79) Equipamento de usuário sem monitoração.

(80) Política de mesa limpa e tela limpa.

(81) Política de uso de serviços de rede

(82) Autenticação para conexão externa do usuário

(83) Identificação de equipamentos em redes

(84) Proteção de portas de configuração e diagnóstico remotos

(85) Segregação de redes

(86) Controle de conexão de redes

(87) Controle de roteamento de redes

(88) Procedimentos seguros de entrada nos sistema (log on).

(89) Identificação e autenticação do usuár

(90) Sistema de gerenciamento de senha

(91) Uso de utilitários de sistema

(92) Limite de tempo de sessão

(93) Limitação de horário de conexão

(94) Restrição de acesso à informação

(95) Isolamento de sistemas sensíveis

(96) Computação e comunicação móvel

(97) Trabalho remoto

Controles do Capítulo 12 – Aquisição, desenvolvimento e manutenção de sistemas de informação.

(98) Análise e especificação dos requisitos de segurança

(99) Validação dos dados de entrada.

(100) Controle do processamento interno

(101) Integridade de mensagens

(102) Validação dos dados de saída

(103) Política para uso de controles criptográficos

(104) Gerenciamento de chaves.

(105) Controle de software operacional

(106) Proteção dos dados para teste de sistema

(107) Acesso ao código fonte de programa

(108) Procedimentos para controle de mudanças.

(109) Análise crítica técnica das aplicações após mudanças no sistema operacional.

(110) Restrições sobre mudanças em pacotes de software

(111) Vazamento de informações

(112) Desenvolvimento terceirizado de software

(113) Controle de vulnerabilidades técnicas

Controles do Capítulo 13 – Gestão de incidentes de segurança da informação.

(114) Notificação de eventos de segurança da informação.

(115) Notificando fragilidades de segurança da informação.

(116) Responsabilidades e procedimentos

(117) Aprendendo com os incidentes de segurança da informação.

(118) Coletas de evidência

Controles do Capítulo 14 – Gestão da continuidade do negócio.

(119) Incluindo a segurança da informação no processo de gestão de continuidade de negócio.

(120) Continuidade de negócios e análise/avaliação de riscos

(121) Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
(122) Estrutura do plano de continuidade do negócio
(123) Testes, manutenção e reavaliação dos planos de continuidade do negócio

Controles do Capítulo 15 – Conformidade.
(124) Identificação da legislação aplicável
(125) Direitos de propriedade intelectual.
(126) Proteção de registros organizacionais
(127) Proteção de dados e privacidade de informações pessoais
(128) Prevenção de mau uso de recursos de processamento de informação
(129) Regulamentação de controles de criptografia
(130) Conformidade com as políticas e normas de segurança da informação.
(131) Verificação com a conformidade técnica.
(132) Auditoria de sistemas de informação
(133) Proteção de ferramentas de auditoria de sistemas de informação

2.3 – Política de segurança da informação - Norma NBR ISO/IEC 27001:2006

Norma NBR ISO/IEC 27001 - Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos, ABNT, 2006.

Esta norma tem como objetivo principal “prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação – SGSI”. ABNT (2006, p.v)

Como objetivo complementar esta norma “pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas”, (ABNT, 2006, p.v).

Isto significa que quando de uma certificação por uma organização em segurança da informação, esta é a norma tomada por base. Os controles aqui descritos, e que

serão considerados para a certificação, são os controles definidos na NBR ISO/IEC 27002:2005.

Esta norma descreve uma orientação para a existência de um Sistema de Gestão da Segurança da informação – SGSI, considerando o Modelo PDCA *(Plan, Do, Check, Act).* O relacionamento desta norma com esta pesquisa se deve ao fato de que a política de segurança da informação está contemplada na etapa de Planejamento *(Plan)* de Modelo PDCA do SGSI – Sistema de Gestão da Segurança da Informação.

Esta norma possui 9 (nove) capítulos, numerados do 0 (zero) ao 8 (oito). Possui também três anexos informativos.

a) Capítulo 0 – Introdução

Neste capítulo são definidos:

- a motivação da norma,
- a abordagem de processo para o SGSI,
- a compatibilidade com outros sistemas de gestão.

Na abordagem para o processo do SGSI são definidas as principais ações para cada uma das etapas do PDCA:

A Figura 1 abaixo apresenta em conjunto as quatro etapas do PDCA e as definições de cada uma destas etapas.

***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.

Figura 1 – Atividades do PDCA. Fonte: NBR ISO/IEC 27001:2006

A política de segurança da informação encontra-se na etapa de Planejamento *(Plan)* quando da sua elaboração e na etapa de Fazer *(Do)*, quando da sua implantação e operação. Desta maneira a política de segurança da informação é um dos primeiros elementos que devem ser definidos, seguindo o Modelo PDCA.

Ainda neste capítulo é estruturado o Modelo de PDCA aplicado ao SGSI.

A Figura 2, abaixo, apresenta o relacionamento do Modelo de PDCA com as etapas do SGSI – Sistema de Gestão de Segurança da Informação. Este relacionamento indica que o Estabelecimento do SGSI encontra-se na etapa de Planejamento *(Plan);* a manutenção e melhoria do SGSI encontram-se na etapa de Elaboração *(Act);* o Monitoramento e Análise Crítica se apresenta na etapa de Verificação *(Check)* e Implementação e Operação do SGSI encontra-se na etapa do Fazer *(Do).*

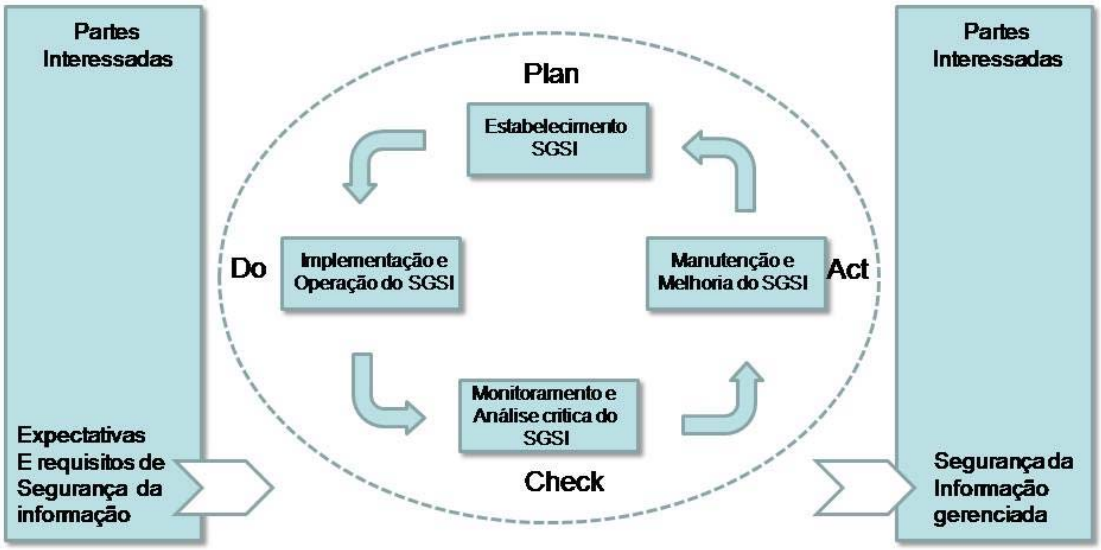


Figura 2 – Modelo do PDCA aplicado aos processos do SGSI
Fonte: NBR ISO/IEC 27001:2006

b) Capítulo 1 – Objetivo

Neste capítulo são descritos o objetivo geral da norma e a sua aplicação.

O conjunto de requisitos ou controles considerados define a maneira como a organização deseja tratar o escopo da segurança da informação.

> *Esta Norma especifica os requisitos para estabelecer, implantar, operar, monitorar, analisar criticamente manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócio globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes. (ABNT, 2006, p.1)*
>
> *O SGSI é projetado para assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas. (ABNT, 2006, p.1)*
>
> *Qualquer exclusão de controles considerados necessários para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidos. (ABNT, 2006, p.1)*

A política de segurança é um dos controles que deve ser considerado. Ela é um controle básico, pois é no regulamento de política que são declarados os demais controles, em maior ou menor nível de granularidade, que serão considerados pela organização.

c) Capítulo 2 – Referência normativa

Neste capítulo é indicado que para a aplicação desta Norma é indispensável a referência à NBR ISO/IEC 27002:2005 – Tecnologia da informação – técnicas de segurança – Código de prática para a gestão da segurança da informação.

d) Capítulo 3 – Termos e definições

Neste capítulo são definidos os termos e definições utilizados nesta Norma. Alguns termos também estão definidos na NBR ISO/IEC 27002:2005.

Dos termos considerados, destacam-se:

> *Sistema de gestão da segurança da informação - SGSI*
> *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.(ABNT, 2006, p.3)*

> *Declaração de aplicabilidade*
> *Declaração documentada que descreve os objetivos de controles e controles que são pertinentes e aplicáveis ao SGSI da organização*

e) Capítulo 4 – Sistema de Gestão de Segurança da Informação

Neste capítulo são definidas as atividades e etapas que a organização deve realizar para estabelecer, monitorar e analisar criticamente o seu SGSI.

Esta norma define que a política de segurança da informação é um controle fundamental. Ela considera a política de segurança da informação como uma das atividades chaves para o estabelecimento do SGSI da organização que inclusive estabelecerá critérios em relação aos riscos:

> *4.2.1 Estabelecer um SGSI*
> *A organização deve:*
>
> *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 de 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 risco da organização no qual o estabelecimento e manutenção do SGSI irão ocorrer;*
> >
> > *4. estabeleça critérios em relação aos quais os riscos serão avaliados*
> >
> > *5. tenha sido aprovada pela direção.*
>
> *c) Definir a abordagem de análise/avaliação de riscos da organização.*
>
> *d) Identificar os riscos.*
>
> *e) Analisar e avaliar os riscos*
>
> *f) Identificar e avaliar as opções para o tratamento de riscos.*
>
> *g) Selecionar os objetivos de controle e controles para o tratamento de risco.*
>
> *h) Obter aprovação da direção dos riscos residuais propostos*
>
> *i) Obter aprovação da direção para implementar e operar o SGSI.*
>
> *j) Preparar uma Declaração de Aplicabilidade.*

No item monitorar e analisar criticamente o SGSI, a política de segurança da informação é mencionada explicitamente:

> *b) realizar análises críticas regulares da eficácia do SGSI (incluindo o atendimento da política e dos objetivos do SGSI, e a análise crítica dos controles de segurança), levando em consideração os resultados de auditorias de segurança da informação, incidentes de segurança da informação, resultado das eficácias das medições, sugestões e realimentação de todas as partes interessadas. (ABNT, 2006, p.7)*

f) Capítulo 5 – Responsabilidades da direção

Neste capítulo são definidas as responsabilidades da direção da organização. São considerados:

- Comprometimento da direção
- Provisão de recursos
- Treinamento, conscientização e competência das pessoas.

Neste capítulo a política de segurança da informação é evidenciada:

> *5.1 – Comprometimento da direção*
> *A direção deve fornecer evidência do seu comprometimento com o estabelecimento,* 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;*
> >
> > *h) a condução de análises críticas do SGSI pela direção.*
> > *(ABNT, 2005, p.9-10)*

g) Capítulo 6 – Auditorias internas do SGSI

Neste capítulo são definidas as responsabilidades e ações para que a organização conduza auditorias internas do SGSI a intervalos planejados para determinar se os objetivos de controles, controles, processos e procedimentos do seu SGSI:

> *a) atendem aos requisitos desta Norma e à legislação ou regulamentações pertinentes;*
>
> *b) atendem aos requisitos de segurança da informação identificados;*
>
> *c) estão mantidos e implementados eficazmente; e*
>
> *d) são executados conforme esperado. (ABNT, 2005, p.11)*

De uma maneira indireta a política de segurança da informação foi citada no item (b), pelo motivo de que os requisitos de segurança da informação devem estar definidos na política.

h) Capítulo 7 – Análise crítica do SGSI pela direção

Neste capítulo são definidas as responsabilidades para a realização da análise crítica do SGSI pela direção.

A política de segurança da informação é citada como um dos elementos chaves dessa análise:

> *A direção deve analisar criticamente o SGSI da organização a intervalos planejados (pelo menos uma vez por ano) para assegurar a sua contínua pertinência, adequação e eficácia.*
>
> *Esta análise crítica deve incluir a avaliação de oportunidades para melhoria e a necessidade de mudanças do SGSI, incluindo a política de segurança da informação e objetivos de segurança da informação.*
>
> *Os resultados dessas análises críticas devem ser claramente documentados e os registros devem ser mantidos. (ABNT, 2006,* p.12)

i) Capítulo 8 – Melhoria do SGSI

Neste capítulo são definidas as responsabilidades para a realização da melhoria do SGSI através de medidas preventivas e corretivas.

A política de segurança da informação é referenciada como o elemento que permitirá esta melhoria do SGSI:

> *8.1 Melhoria contínua*
> *A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção. (ABNT, 2006, p.12)*

j) Anexo A – Normativo – Objetivos de controles e controles

Neste anexo normativo são definidos os objetivos de controles e controles derivados diretamente da NBR ISO/IEC 27002:2005. Estes objetivos de controles e controles não são exaustivos e a organização poderá considerar que objetivos de controles e controles adicionais são necessários. A lista final selecionada indicará os objetivos de controles e controles que farão parte do SGSI a ser estabelecido pela organização.

k) Anexo B – Informativo – Princípios da OECD e desta Norma

Neste anexo informativo identifica os princípios definidos pelas Diretrizes de OECD e esta Norma.

São considerados os seguintes princípios da OECD que são referenciados nesta norma:

- Conscientização
- Responsabilidade
- Respostas
- Análise/avaliação de riscos
- Arquitetura e implementação de segurança
- Gestão de segurança
- Reavaliação.

l) Anexo C – Informativo – Correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma

Neste anexo informativo identifica correspondência entre a ABNT NBR ISO 9001:2000, a ABNT NBR ISO 14001:2004 e esta Norma.

2.4 – Política de segurança da informação – Norma NBR ISO/IEC 27005:2008

Norma NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação, ABNT, 2008.

Esta Norma tem por objetivo fornecer "diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um SGSI de acordo com a ABNT NBR ISO/IEC 27001. Entretanto esta Norma não inclui uma metodologia específica para a gestão de riscos de segurança da informação." (ABNT, 2008, p.vi)

Esta Norma ao definir a gestão de riscos faz o seu relacionamento com o escopo do SGSI e com a política de segurança da informação.

Para um funcionamento adequado do SGSI é importante que a gestão de riscos e a política de segurança da informação sejam elementos que estejam bem definidos e explícitos.

No contexto da gestão de riscos, a política de segurança da informação é considerada na fase de definição do contexto, mais especificamente na definição de escopo e limites. No Capítulo 7 - Definição de contexto, no item 7.3 – Escopo e limites, esta Norma declara que "Convém que a organização defina o escopo e os limites da gestão de riscos de segurança da informação" (ABNT, 2008, p.8).

Para a definição do escopo e limites esta Norma cita a política de segurança da informação quando declara ainda no item 7.3 – Escopo e limites:

> *Ao definir escopo e limites, convém que a organização considere as seguintes informações:*
>
> *- Os objetivos estratégicos, políticas e estratégias da organização*
>
> *- Processo de negócio*
>
> *- As funções e estrutura da organização*
>
> *- Requisitos legais, regulatórios e contratuais aplicáveis à organização*
>
> *- A política de segurança da informação*
>
> *- A abordagem da organização à gestão de riscos*

- Ativos de informação

- Localidades em que a organização se encontra e características geográficas

- Restrições que afetam a organização

- Expectativas das partes interessadas

- Ambiente sócio cultural

- Interfaces (ou seja, a troca de informação com o ambiente)

A Norma ainda complementa com uma nota:

> *O escopo e os limites da gestão de riscos de segurança da informação estão relacionados ao escopo e aos limites do SGSI conforme requerido na ABNT ISO/IEC 27001 4.2.1.a. (ABNT, 2008, p. 9).*

A NBR ISO/IEC 27001:2006 indica no seu item 4.2.1 – Estabelecer o SGSI, os elementos necessários para que a organização estabeleça um SGSI e novamente aparece a política de segurança da informação como uma das atividades.

> *a) Definir o escopo e os limites do SGSI (Sistema de gestão de Segurança da Informação) nos termos das características do negócio, a organização, sua localização, ativos de tecnologia, incluindo detalhes 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 as ações relacionadas com a segurança da informação;*
>
> *2. considere os requisitos de negócio, legais e/ou regulamentares, e obrigações de segurança contratuais;*
>
> *3. esteja alinhada com o contexto estratégico de gestão de risco da organização no qual o estabelecimento e manutenção do SGSI irá ocorrer;*
>
> *4. estabeleça critérios em relação aos quais os riscos serão avaliados.*
>
> *c) Definir a abordagem de análise e avaliação de riscos da organização.*
> *(ABNT, 2006, p. 4-5)*
>
> *d) Identificar os riscos.*
>
> *e) Analisar e avaliar os riscos.*
>
> *f) Identificar e avaliar as opções para o tratamento de risco.*
>
> *g) Selecionar objetivos de controle e controles para o tratamento de riscos.*
>
> *h) Obter aprovação da direção dos riscos residuais propostos.*
>
> *i) Obter autorização da direção para implementar e operar o SGSI.*

j) Preparar uma Declaração de Aplicabilidade.

A política de segurança da informação relaciona-se com a gestão do risco na sua fase de definição de contexto. Ela deve conter elementos que explicitem o escopo e os limites que serão considerados no SGSI e conseqüentemente na gestão de riscos.

Esta Norma possui doze capítulos e seis anexos informativos.

a) Capítulo 1 – Escopo

Indica o contexto em que esta Norma se aplica. Ela declara que “Esta norma se aplica a todos os tipos de organização que pretendem gerir os riscos que poderiam comprometer a segurança da informação” (ABNT, 2008, p.1)

b) Capítulo 2 – Referências normativas

Define os documentos indispensáveis para a correta aplicação desta Norma:

- NBR ISO/IEC 27001:2006
- NBR ISO/IEC 27002:2005

c) Capítulo 3 – Termos e definições

Atribui definições aos termos utilizados nesta Norma.

d) Capitulo 4 – Organização da Norma

Indica como esta Norma está estruturada.

e) Capitulo 5 - Contextualização

Apresenta a necessidade de um visão sistêmica para a gestão de riscos.

f) Capítulo 6 – Visão geral do processo de gestão de riscos de segurança da informação.

Apresenta de uma forma concisa todo o processo de gestão de riscos.

Duas figuras são muito importantes para a compreensão da gestão de riscos e para o posicionamento da ligação com a política de segurança da informação na etapa de definição de contexto da gestão de riscos.

A Figura 3 indica as etapas do processo de gestão de risco em segurança da informação. A primeira etapa deste processo é definição do contexto e nesta etapa é que a política de segurança da informação se faz presente registrando e explicitando o que deverá ser considerado para o contexto da gestão de risco.

Em seguida a Figura 3 apresenta a etapa seguinte, análise/avaliação de riscos tendo em seguida a etapa de tratamento do risco, onde uma das opções é a aceitação do risco, isto é, nada será feito em relação ao risco e a organização define por aceitar o referido risco. Durante todo este processo existem duas etapas que existem continuamente: a comunicação dos riscos e o monitoramento e análise crítica dos riscos.

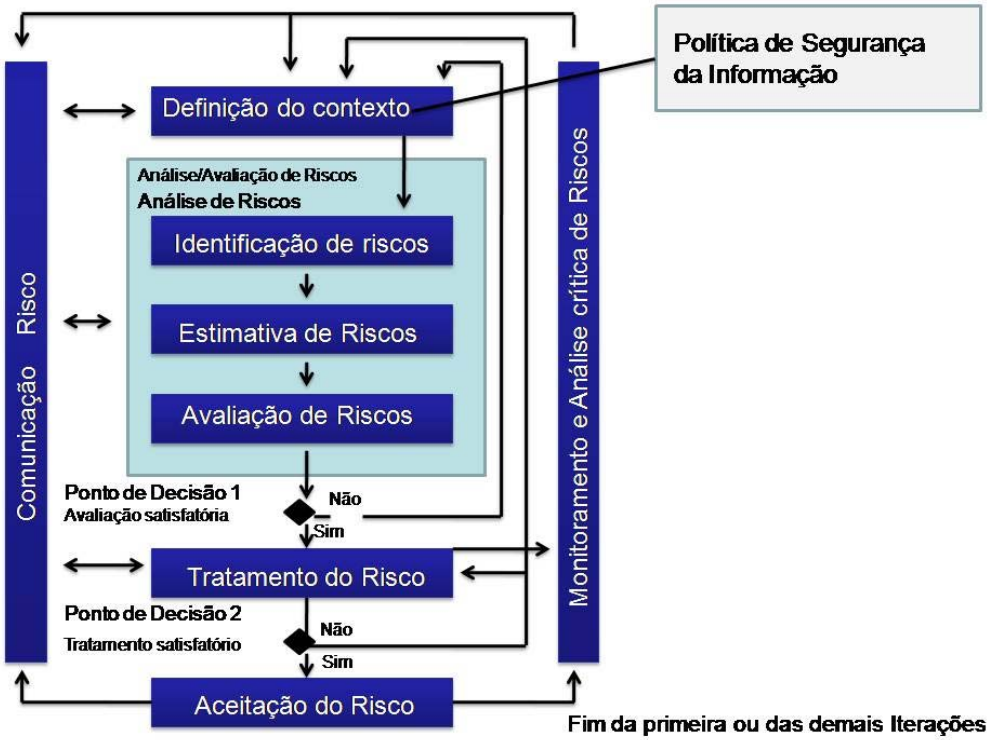


Figura 3 – Processo de gestão de risco de segurança da informação

Fonte: NBR ISO/IEC 27005:2008

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

Figura 4 – Relacionamento dos processos do SGSI e dos processos de gestão de riscos de TI
Fonte: NBR ISO/IEC 27005:2008

A Figura 4, acima, apresenta de uma maneira estruturada a as etapas do Modelo PDCA e o seu relacionamento com as etapas de um processo de gestão de riscos de segurança da informação.

g) Capítulo 7 - Definição do Contexto

Este capítulo indica os critérios básicos, escopo e limites e as responsabilidades para o processo de gestão de riscos.

É nesta definição do escopo e limites que a política de segurança da informação é considerada.

h) Capítulo 8 – Análise/avaliação de riscos de segurança da informação

Este capítulo descreve todo o processo de análise e avaliação dos riscos de segurança da informação, detalhando:

- Identificação de ativos
- Identificação de ameaças
- Identificação de controles existentes
- Identificação das vulnerabilidades

- Identificação das conseqüências
- Estimativa dos riscos (quantitativa, qualitativa)
- Avaliação da probabilidade dos incidentes
- Estimativa do nível de risco. ABNT (2008)

O assunto de análise/avaliação de riscos de segurança da informação relaciona-se à política do SGSI conforme a NBR ISO/IEC 27001:2006 no item 4.2.1. b e c, que indica que a política de do SGSI deve “estabeleça critérios em relação aos quais os riscos serão avaliados”, e “desenvolva critérios para que a aceitação de riscos e identifique os níveis aceitáveis de riscos”. (ABNT, 2008, p.4-5)

Conforme apresentado acima, a política do SGSI possibilita a análise/avaliação dos riscos.

i) Capítulo 9 – Tratamento do risco de segurança da informação

Este capítulo descreve todo o processo de tratamento dos riscos de segurança da informação, detalhando:

- Redução do risco
- Retenção do risco
- Ação de evitar o risco
- Transferência do risco

A Figura 5 apresenta graficamente o processo de tratamento do risco e facilita o seu entendimento. O tratamento de risco pode ser feito tomando quatro decisões: buscar reduzir o risco, evitar o risco, transferir o risco para outro elemento ou organização ou aceitar e reter o risco. Para qualquer uma destas quatro decisões sempre haverá o risco residual.

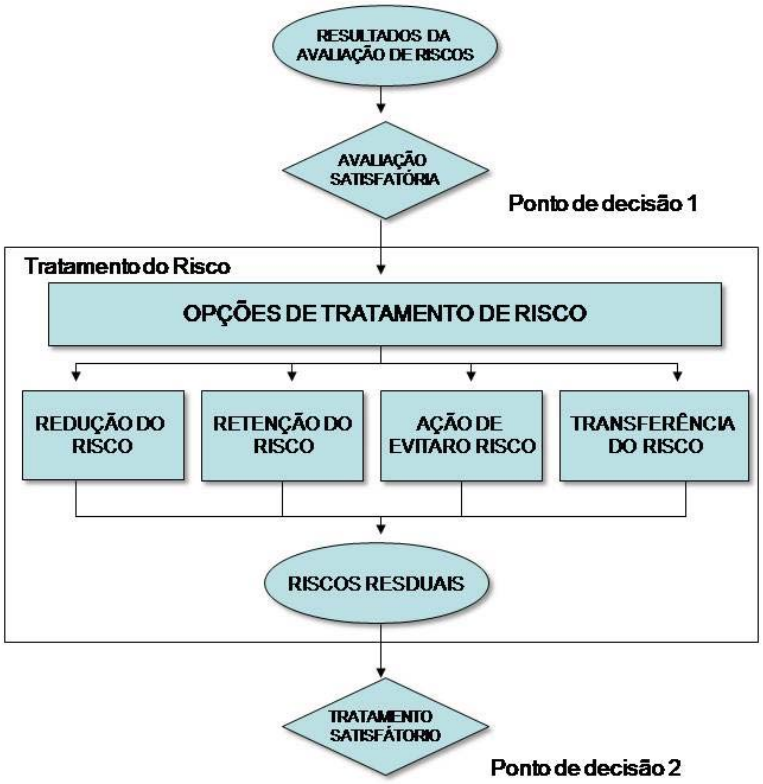


Figura 5 – Processo de tratamento do risco - Fonte: NBR ISO/IEC 27005:2008

O assunto de tratamento do risco de segurança da informação relaciona-se à política do SGSI conforme a NBR ISO/IEC 27001:2006 no item 4.2.1.b.4 e 4.2.1.c.2, que indica que a política do SGSI deve “estabelecer critérios em relação aos quais os riscos serão avaliados”, e deve “desenvolver critérios para que a aceitação de riscos e identifique os níveis aceitáveis de riscos”. (ABNT, 2006, p.4-5)

Conforme definido acima, a política do SGSI define elementos para possibilitar a realização do tratamento dos riscos de segurança da informação.

j) Capítulo 10 – Aceitação do risco de segurança da informação

Este capítulo descreve as responsabilidades quando da aceitação do risco ou a aceitação do risco residual.

k) Capítulo 11 – Comunicação do risco de segurança da informação

Este capítulo descreve as responsabilidades para a comunicação do risco de segurança da informação entre as partes interessadas e envolvidas no SGSI.

l) Capítulo 12 – Monitoramento e análise crítica de riscos de segurança da informação

Este capítulo descreve as responsabilidades e principais atividades de monitoramento dos riscos de segurança da informação com o objetivo de identificar o mais rapidamente possível eventuais mudanças no contexto da organização e garantir uma visão geral e verdadeira dos riscos.

Este capítulo sugere que no mínimo sejam considerados os seguintes elementos:

- Contexto legal e do ambiente
- Contexto da concorrência
- Método de análise/avaliação de riscos
- Valor e a categoria de ativos
- Critérios de impacto
- Critérios para a avaliação de riscos
- Critérios para a aceitação do risco
- Custo total de propriedade
- Recursos necessários. (ABNT, 2008, p.23)

m) Anexo A – Informativo

Definição do escopo e os limites do processo de gestão de riscos de segurança da informação.

n) Anexo B – Informativo

Identificação e valoração dos ativos e avaliação do impacto.

o) Anexo C – Informativo

Apresentação de exemplos de ameaças comuns

p) Anexo D – informativo

Definição de vulnerabilidades e métodos de avaliação de vulnerabilidades.

q) Anexo E – Informativo

Apresentação de diferentes abordagens para análise/avaliação de riscos de segurança da informação

r) Anexo F – informativo

Definição de restrições que afetam a redução do risco

2.5 – Política de segurança da informação – Futura Norma 27799

Projeto 78:000.00-19 – Informática em Saúde – Gestão de segurança da informação em saúde usando a ABNT NBR ISO/IEC 27002:2005, ABNT, 2009. Futura NBR ISO/IEC 27799.

Esta futura Norma tem por objetivo dar suporte e apoiar à interpretação e a implantação da NBR ISO/IEC 27002:2005 quando da implementação da segurança da informação em organizações de saúde ou organizações custodiantes de informação de saúde.

> *Esta Norma fornece orientação às Organizações de saúde e aos outros custodiantes de informações pessoais de saúde sobre a melhor maneira de proteger a confidencialidade, a integridade e a disponibilidade de tais informações pessoais de saúde através da implementação da ABNT NBR ISO/IEC 27002. (ABNT, 2009, p.5)*

Esta futura Norma deve ser utilizada em conjunto com a NBR ISO/IEC 27002:2005. Para alguns controles da NBR ISO/IEC 27002:2005, esta futura Norma complementa estes controles com regras mais rígidas. Juntas elas definem o que é necessário em termos de segurança da informação para organizações que tratam dados de saúde; entretanto não definem como estes requisitos devem ser atendidos. O que significa dizer que, na medida do possível, esta norma internacional é tecnologicamente neutra.

Esta futura NBR ISO/IEC 27799 se aplica à informação de saúde em todos os aspectos, seja qual for o formato da informação (letras e números, gravação de sons, vídeo e imagens médicas), seja qual for o meio de armazenamento (impresso ou escrito em papel, ou armazenamento eletrônico) e seja qual for o meio utilizado para transmissão (manual, fax, através de redes de computadores ou postagem), visto que a informação precisa estar sempre devidamente protegida.

Esta futura Norma dá um tratamento mais rígido a vários controles da Norma ISO/IEC 27002:2005.

Os dois controles relativos à política de segurança da informação foram complementados.

a) Controle (1): Documento da política de segurança da informação.

A NBR ISO/IEC 27002:2005 descreve a política de segurança da informação como algo desejável:

> *Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado para todos os funcionários e partes externas relevantes. (ABNT, 2005, p.8)*

Enquanto a Futura NBR ISO/IEC 27799 descreve a política de segurança da informação como mandatório:

> *Organizações processando informações de saúde, incluindo informação pessoal de saúde, devem possuir uma política de segurança da informação escrita que seja aprovada pela gerência, publicada, e comunicada para todos os funcionários e partes externas relevantes (ABNT, 2009, p.29)*

No caso deste controle é mandatório que as Organizações de saúde tenham uma política de segurança da informação.

b) Controle (2): Análise crítica da política de segurança da informação.

NBR ISO/IEC 27002:2005

> *Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua continua pertinência, adequação e eficácia. .(ABNT, 2005, p.9)*

Futura NBR ISO/IEC 27799

> *Convém que a política de segurança da informação da organização de saúde seja submetida ao processo contínuo de revisão de forma que a totalidade da política seja endereçada pelo menos anualmente.*
>
> *Convém que a política seja revisada após a ocorrência de um sério incidente de segurança.*

No caso deste controle é mandatório que as Organizações de saúde revisem a política de segurança da informação pelo menos em cada período de 12 (doze) meses ou quando da ocorrência de um sério incidente de segurança.

2.6 – Política de segurança da informação e o COBIT

COBIT (Control Objectives for Information and related Technology): Objetivos de Controle para a Informação e Tecnologia relacionada

Este item descreve a contextualização do controle política de segurança da informação quando da utilização da estrutura COBIT.

2.6.1 - Contextualização

O COBIT *(Control Objectives for Information and related Technology),* Objetivos de Controle para a Informação e Tecnologia relacionada foi publicado pela ISACA *(Information Systems Audit and Control Foundation)* em 1996. O COBIT está em sua quarta edição, inclusive com versão em português. Atualmente o COBIT é mantido pelo IT Governance Institute, órgão ligado à ISACA. O desenvolvimento do COBIT contou com a participação de especialistas de todo o mundo e foram consideradas várias e melhores práticas, metodologias, padrões profissionais para controle interno e requerimentos legais e governamentais de segmentos de mercado que dependem fortemente de tecnologia, como o setor financeiro e o setor de telecomunicação. (ISACA, 2010)

A Governança Corporativa gerou a necessidade da Governança de TI. Esta última tem como objetivo maior garantir que a área de TI da organização suporte o atendimento dos objetivos de negócio, no que diz respeito à informação processada e armazenada no ambiente de tecnologia da informação.

A Governança de TI é de responsabilidade dos executivos e da alta direção, consistindo em aspectos de liderança, estrutura organizacional e processos que garantam que a área de TI da organização suporte e aprimore os objetivos e as estratégias da organização. (ITGI, 2007)

Os executivos precisam aperfeiçoar o uso dos recursos de TI disponíveis, incluindo os aplicativos, informações, infra-estrutura e pessoas. Para cumprir essas responsabilidades bem como atingir seus objetivos, os executivos devem entender o estágio de sua arquitetura de TI e decidir que governança e controles devem ser considerados. O *Control Objectives for Information and related Technology* (COBIT) ajuda aos executivos, pois fornece boas práticas através de um modelo de domínios e processos e apresenta atividades em uma estrutura lógica e gerenciável. (ITGI, 2007)

O COBIT não define como os processos serão executados, porém, define controles que possibilitarão que TI cumpra seus objetivos estando alinhado aos objetivos de negócio.

Um dos fatores críticos da aceitação do COBIT nos diversos mercados e países é a sua orientação ao negócio. O COBIT consiste em objetivos de negócios ligados a objetivos de TI, provendo métricas e modelos de maturidade para medir a sua eficácia e identificando as responsabilidades relacionadas dos donos dos processos de negócios e de TI. (ITGI, 2007)

Portanto o COBIT é uma estrutura aceita mundialmente e possui vários controles. Em um desses grupos encontram-se os controles relacionadas à política de segurança da informação, motivo pelo qual consideramos o COBIT nesta pesquisa.

Porém o próprio COBIT indica que em relação ao assunto segurança da informação, o usuário pode obter informações detalhadas consultando o padrão ISO 17799, que foi transformado na NBR ISO/IEC 27002:

> *Todos os usuários em potencial podem se beneficiar da utilização do conteúdo do CobiT como um enfoque geral para o gerenciamento e governança de TI em conjunto com os seguintes padrões mais detalhados:*
> *· ITIL para entrega de serviços*
> *· CMM para entrega de soluções*
> *· ISO 17799 para segurança da informação*
> *· PMBOK ou PRINCE2 para gerenciamento de projetos.*
> *(ITGI, 2007, p.30)*

De acordo com o ITGI (2007), os principais objetivos do COBIT são:

- Estabelecer relacionamentos com os requisitos do negócio;
- Organizar as atividades de TI em um modelo de processo;
- Identificar os principais recursos de TI;
- Definir os objetivos de controle que serão considerados para a gestão.

Os benefícios da implementação do COBIT como um modelo de governança de TI são, entre outros:

> *· Um melhor alinhamento baseado no foco do negócio*
> *· Uma visão clara para os executivos sobre o que TI faz*
> *· Uma clara divisão das responsabilidades baseada na orientação para processos*
> *· Aceitação geral por terceiros e órgãos reguladores*
> *· Entendimento compreendido entre todas as partes interessadas, baseado em uma linguagem comum*
> *· - Cumprimento dos requisitos do COSO para controle do ambiente de TI.*
> *(ITGI, 2007, p.10)*

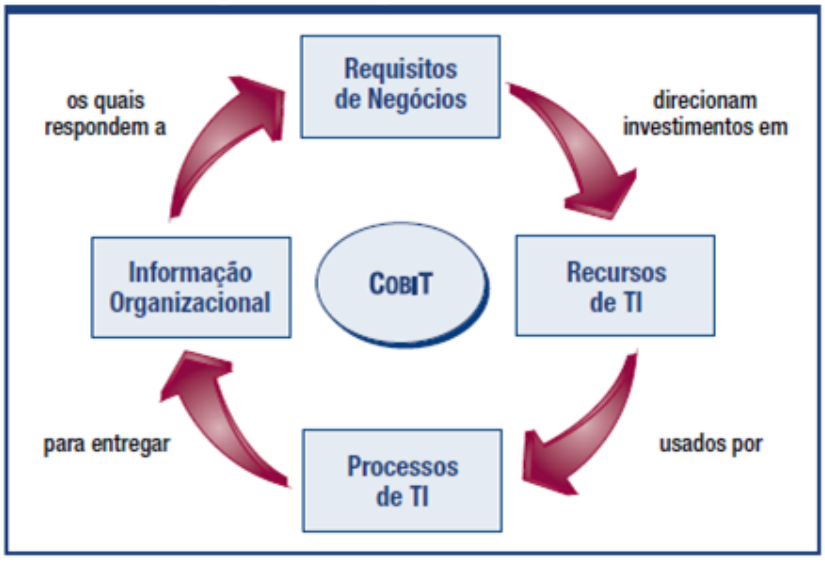


Figura 6 – Princípios básicos do COBIT Fonte: COBIT, Edição 4.1, 2007

A Figura 6, acima, mostra o ciclo dos princípios básicos do COBIT que começa com a identificação dos Requisitos de Negócio. Os investimentos para os recursos de TI vão acontecer após esta identificação dos requisitos de negócio. Os Recursos de TI

serão usados nos Processos de TI que entregarão Informação Organizacional para responder aos Requisitos de Negócio, origem de tudo.

2.6.2 – Os domínios do COBIT

O COBIT considera as atividades de TI em um modelo de processos:

PO – Planejar e Organizar.

AI – Adquirir e Implementar

DS – Entregar e Suportar

ME – Monitorar e Avaliar

A Figura 7 apresenta estes domínios e os seus relacionamentos.

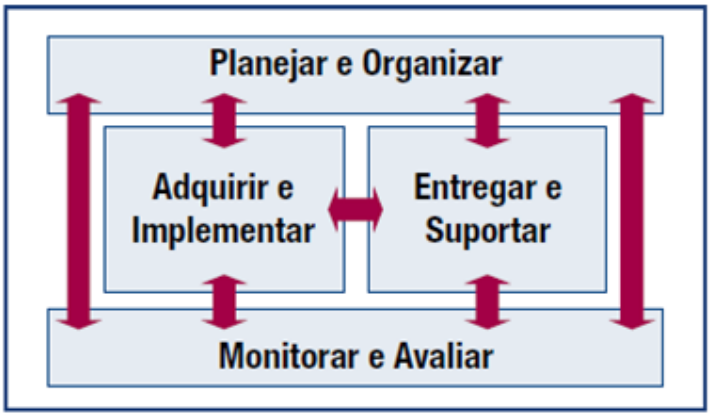


Figura 7 – Os quatro domínios inter-relacionados do COBIT
Fonte: COBIT, Edição 4.1, 2007

a) Domínio Planejar e Organizar – PO

Este domínio considera as ações de estratégia e as ações táticas. Seu objetivo é garantir que TI contribua para que os objetivos, metas e estratégias de negócio sejam atingidos.

Este domínio ajuda a responder as seguintes questões:

· As estratégias de TI e de negócios estão alinhadas?
· A empresa está obtendo um ótimo uso dos seus recursos?
· Todos na organização entendem os objetivos de TI?
· Os riscos de TI são entendidos e estão sendo gerenciados?
· A qualidade dos sistemas de TI é adequada às necessidades de negócios?

(ISACA, 2007, p.14)

b) Domínio Adquirir e Implementar - AI

Este domínio trata das soluções de TI que precisam ser desenvolvidas ou adquiridas, implementadas e integradas para o atendimento dos objetivos do negócio bem como a forma que estas soluções serão integradas aos processos de negócio. Este domínio também considera que as soluções adotadas devam continuar a atender os objetivos de negócio ao longo do tempo.

Este domínio ajuda a responder as seguintes questões:

· Os novos projetos fornecerão soluções que atendam às necessidades de negócios?
· Os novos projetos serão entregues no tempo e orçamento previstos?
· Os novos sistemas ocorreram apropriadamente quando implementado?
· As alterações ocorrerão sem afetar as operações de negócios atuais?
(ITGI, 2007, p.15)

c) Domínio Entregar e Suportar - DS

Este domínio trata da entrega dos serviços solicitados. Ele considera: entrega de serviço, gerenciamento de segurança, continuidade suporte aos usuários, gerenciamento de dados e gerenciamento de recursos operacionais.

Este domínio ajuda a responder as seguintes questões:

· Os serviços de TI estão sendo entregues de acordo com as prioridades de negócios?
· Os custos de TI estão otimizados?
· A força de trabalho está habilitada para utilizar os sistemas de TI de maneira produtiva e segura?
· Os aspectos de confidencialidade, integridade e disponibilidade estão sendo contemplados para garantir a segurança da informação?
(ITGI, 2007, p.15)

d) Domínio Monitorar e Avaliar – ME

Este domínio tem por objetivo garantir a revisão periódica da qualidade e aderência dos processos de TI aos requisitos de negócio. Também cuida do desempenho, monitoramento dos controles e aderência a normas e padrões.

Este domínio ajuda a responder as seguintes questões:

> *· A performance de TI é mensurada para detectar problemas antes que seja muito tarde?*
> *· O gerenciamento assegura que os controles internos sejam efetivos e eficientes?*
> *· O desempenho da TI pode ser associado aos objetivos de negócio?*
> *· Existem controles adequados para garantir confidencialidade, integridade e disponibilidade das informações?*
> *(ITGI, 2007, p.15)*

2.6.3 – Domínios do COBIT e os Processos de TI

Dentro destes quatro domínios, o COBIT identificou 34 (trinta e quatro) processos de TI que foram ligados a objetivos de negócio. Para cada um desses 34 processos de TI foram identificados objetivos de controle e controles. (ITGI, 2007)

Domínio Planejar e Organizar – Processos de TI

- PO1 Definir um Plano Estratégico de TI
- PO2 Definir a Arquitetura da Informação
- PO3 Determinar as Diretrizes de Tecnologia
- PO4 Definir os Processos, a Organização e os Relacionamentos de TI
- PO5 Gerenciar o Investimento de TI
- PO6 Comunicar Metas e Diretrizes Gerenciais
- PO7 Gerenciar os Recursos Humanos de TI
- PO8 Gerenciar a Qualidade
- PO9 Avaliar e Gerenciar os Riscos de TI
- PO10 Gerenciar Projetos

Domínio Adquirir e Implementar – Processos de TI

- AI1 Identificar Soluções Automatizadas
- AI2 Adquirir e Manter Software Aplicativo
- AI3 Adquirir e Manter Infraestrutura de Tecnologia

- AI4 Habilitar Operação e Uso
- AI5 Adquirir Recursos de TI
- AI6 Gerenciar Mudanças
- AI7 Instalar e Homologar Soluções e Mudanças

Domínio Entregar e Suportar – DS – processos de TI

- DS1 Definir e Gerenciar Níveis de Serviços
- DS2 Gerenciar Serviços Terceirizados
- DS3 Gerenciar o Desempenho e a Capacidade
- DS4 Assegurar a Continuidade dos Serviços
- DS5 Garantir a Segurança dos Sistemas
- DS6 Identificar e Alocar Custos
- DS7 Educar e Treinar os Usuários
- DS8 Gerenciar a Central de Serviço e os Incidentes
- DS9 Gerenciar a Configuração
- DS10 Gerenciar Problemas
- DS11 Gerenciar os Dados
- DS12 Gerenciar o Ambiente Físico
- DS13 Gerenciar as Operações

Domínio Monitorar e Avaliar – Processos de TI

- ME1 Monitorar e Avaliar o Desempenho de TI
- ME2 Monitorar e Avaliar os Controles Internos
- ME3 Assegurar a Conformidade com Requisitos Externos
- ME4 Prover Governança de TI

2.6.4 – Processo de TI – DS5 Garantir a Segurança dos Sistemas

Neste processo de TI o COBIT considera controles para garantir a segurança da informação com foco nos sistemas de TI.

O escopo deste processo é assim definido:

> *Para manter a integridade da informação e proteger os ativos de TI, é necessário implementar um processo de gestão de segurança.*

> *Esse processo inclui o estabelecimento e a manutenção de papéis, responsabilidades, políticas, padrões e procedimentos de segurança de TI.*
>
> *A gestão de segurança inclui o monitoramento, o teste periódico e a implementação de ações corretivas das deficiências ou dos incidentes de segurança.*
>
> *A gestão eficaz de segurança protege todos os ativos de TI e minimiza o impacto sobre os negócios de vulnerabilidades e incidentes de segurança. (ITGI, 2007, p.119)*

Neste processo é citada a política de segurança da informação como um dos seus elementos.

O COBIT definiu para este processo de TI, 11 controles (ITGI, 2007, p.120). São eles:

DS5.1 Gestão da Segurança de TI

Gerenciar a segurança de TI no mais alto nível organizacional da empresa de modo que a gestão das ações de segurança esteja em alinhamento com os requisitos de negócio.

DS5.2 Plano de Segurança de TI

Traduzir os requisitos de negócio, de risco e conformidade, em um plano abrangente de segurança de TI, que leve em consideração a infraestrutura de TI e a cultura de segurança.

O plano deve ser implementado em políticas e procedimentos de segurança, juntamente com investimentos adequados em serviços, pessoal, software e hardware.

Políticas e procedimentos de segurança devem ser comunicados aos usuários e partes interessadas.

DS5.3 Gestão de Identidade

Todos os usuários (internos, externos e temporários) e suas atividades nos sistemas de TI (aplicação de negócio, desenvolvimento, operação e manutenção de sistemas) devem ser identificáveis de modo exclusivo.

Os direitos de acesso dos usuários aos sistemas e dados devem estar em conformidade com as necessidades dos negócios e com os requisitos da função definidos e documentados.

Os direitos de acesso devem ser solicitados pela gestão de usuários, aprovados pelo proprietário do sistema e implementados pelo responsável pela segurança. As identidades e os direitos de acesso dos usuários devem ser mantidos em um repositório central.

É necessário implementar e manter atualizadas medidas técnicas e de procedimentos com boa relação custo-benefício para determinar a identificação dos usuários, implementar a devida autenticação e impor direitos de acesso.

DS5.4 Gestão de Contas de Usuário

Assegurar que a solicitação, a emissão, a suspensão, a modificação e o bloqueio de contas de usuário e dos respectivos privilégios sejam tratados por procedimentos de gestão de contas de usuário.

Incluir um procedimento de aprovação de concessão de direitos de acesso pelos proprietários dos dados ou sistemas. Esse procedimento deve ser aplicado a todos os usuários, inclusive aos administradores (usuários com privilégios), usuários internos e externos, para os casos normais ou emergenciais.

Os direitos e obrigações relativos ao acesso a sistemas e informações corporativos devem ser definidos em contrato para todos os tipos de usuários.

Devem ser feitas revisões freqüentes de todas as contas e os respectivos privilégios.

DS5.5 Teste de Segurança, Vigilância e Monitoramento

Garantir que a implementação de segurança de TI seja testada e monitorada proativamente.

A segurança de TI deve ser revalidada periodicamente para garantir que o nível de segurança aprovado seja mantido.

A função de monitoramento e registro de eventos *(logging)* deve possibilitar a prevenção e/ou detecção prematura de atividades anormais e incomuns que precisem ser tratadas, bem como a subseqüente geração de relatórios no tempo apropriado.

DS5.6 Definição de Incidente de Segurança

Definir e comunicar claramente as características de incidentes de segurança em potencial para que possam ser tratados adequadamente pelos processos de gestão de incidentes ou gestão de problemas.

DS5.7 Proteção da Tecnologia de Segurança

Garantir que as tecnologias de segurança importantes sejam invioláveis e que as documentações de segurança não sejam reveladas desnecessariamente.

DS5.8 Gestão de Chave Criptográfica

Assegurar que sejam estabelecidos políticas e procedimentos de geração, mudança, revogação, destruição, distribuição, certificação, armazenamento, inserção, uso e arquivamento das chaves criptográficas visando proteger contra sua modificação ou revelação pública não autorizada.

DS5.9 Prevenção, Detecção e Correção de Código de ProgramaçãoMalicioso

Assegurar que medidas preventivas, de detecção e corretivas sejam estabelecidas corporativamente, em especial correções de segurança *(patches)* e controles de vírus, para proteger os sistemas de informação e tecnologias contra código malicioso (vírus, *worms, spyware, spam.).*

DS5.10 Segurança de Rede

Garantir que técnicas de segurança e procedimentos de gestão relacionados (como *firewalls*, aplicativos de segurança, segmentação de rede e detecção de intrusão) sejam utilizadas para autorizar o acesso e controlar os fluxos de informação entre redes.

DS5.11 Comunicação de Dados Confidenciais

Assegurar que as transações de comunicação de dados confidenciais ocorram somente por um caminho confiável ou controlado de modo a fornecer autenticação de conteúdo, comprovante de envio, comprovante de recebimento e não-rejeição de origem.

2.6.5 – COBIT e a Política de segurança da informação

O processo de TI DS5 – Garantir a segurança dos sistemas atende ao requisito de negócio para TI manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança. (ITGI, 2007)

A política de segurança da informação está inserida neste processo de TI e está contemplada mais detalhadamente no objetivo de controle DS 5.2 – Plano de Segurança de TI. Quando de uma avaliação da Governança de TI realizada utilizando o COBIT, a política de segurança da informação será considerada.

Para as organizações, possuir uma política de segurança da informação incrementará o grau de maturidade deste processo de TI e conseqüentemente suportará melhor o requisito de negócio.

2.7 – Política de segurança da informação e o ITIL

ITIL - Information Technology Infrastructure Library: Biblioteca de Infraestrutura para a Tecnologia da Informação

2.7.1 - Contextualização

ITIL - *Information Technology Infrastructure Library* é uma estrutura que contém um conjunto de diretrizes e práticas recomendadas que visa ajustar pessoas, processos e tecnologia para aumentar a eficiência no gerenciamento de serviços. O ITIL foi desenvolvido pelo governo britânico no final da década de 80. Sua estrutura se

mostrou útil para diversos setores e o ITIL começou a ser utilizado em varias empresas no gerenciamento de serviços. (OGC, 2007)

Desde essa data, tem sofrido revisões, para acompanhar a evolução do mercado e as novas tecnologias. Destas revisões, houve duas que se destacam: A primeira revisão que deu origem à versão dois, ITIL V2, e a segunda revisão que deu origem à versão três, ITIL V3, versão atual.

2.7.2 – Estrutura do ITIL

A OGC (2007) dividiu o seu material para o ITIL V3 em cinco livros. Com exceção do livro *Continual Services Improvment* (Melhoria contínua de serviços), cada um dos demais possui um conjunto de funções.

a) *Service Strategy* (Estratégias de serviços)

Garante que todos os elementos do ciclo de vida do serviço são focados em resultados do cliente e se relaciona com todos os elementos do processo que se seguem.

Funções:

- Composição da Estratégia
- Gerenciamento Financeiro
- Gerenciamento Portifólio Serviços
- Gerenciamento da Demanda

b) *Service Design* (Desenho de serviços)

A fim de cumprir os requisitos de negócio atuais e futuros, fornece orientações sobre a produção e manutenção de políticas de TI, arquiteturas e documentos para o projeto de soluções de TI para infra-estrutura de serviços e processos.

Funções:

- Gerenciamento Catálogo Serviços
- Gerenciamento de Nível de Serviço
- Gerenciamento da Capacidade
- Gerenciamento da Disponibilidade

- Gerenciamento da Continuidade
- Gerenciamento Segurança Informação
- Gerenciamento de Fornecedores

c) *Service Transition* (Transição de serviços)

Transição de Serviço fornece orientações e atividades do processo de transição dos serviços no ambiente de negócios operacionais.

Funções:

- Planejamento
- Gerenciamento de Mudanças
- Gerenciamento da Configuração
- Gerenciamento da Liberação
- Validação e Teste
- Avaliação
- Gerenciamento Base Conhecimento

d) *Service Operation* (Operação de serviços)

Apresenta, explica e entrega os detalhes e as atividades de controle para alcançar a excelência operacional no dia-a-dia.

Funções:

- Gerenciamento de Eventos
- Gerenciamento de Incidentes
- Requisição
- Gerenciamento de Problemas
- Gerenciamento de Acessos

e) *Continual Services Improvment* (Melhoria contínua de serviços)

Juntamente com a entrega consistente, o ITIL enfatiza nesta função a importância da melhoria contínua, como parte da qualidade do serviço,

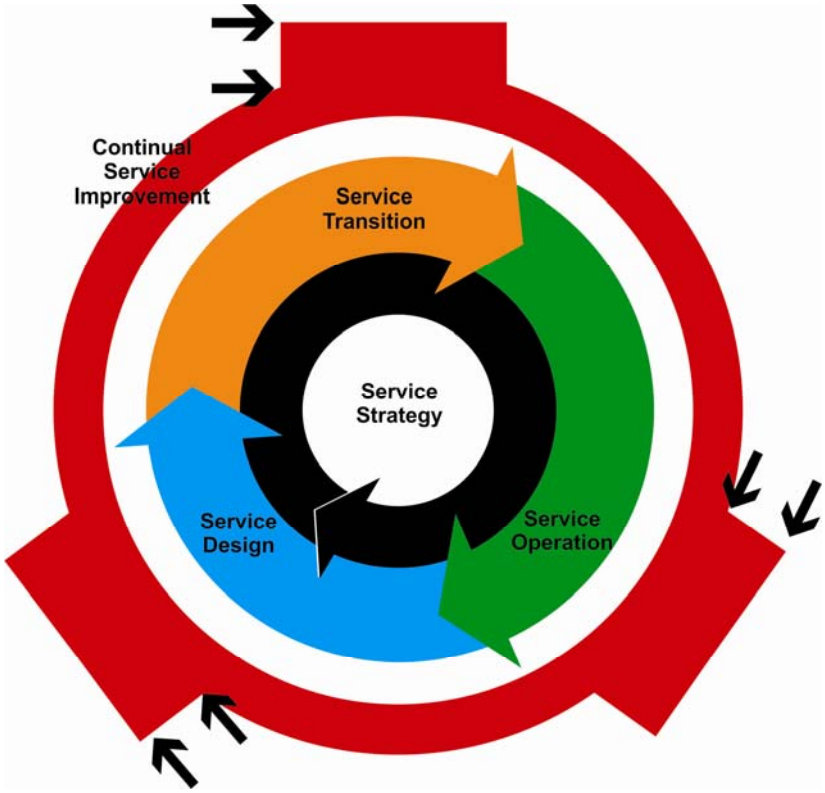


Figura 8 – Serviços do ITIL Fonte: ITIL V3, Service Design (OGC,2007)

A Figura 8 apresenta os Serviços do ITIL de uma maneira estruturada e como eles devem interagir. Como centro de todas as ações encontra-se as Estratégias do Serviço, garantindo que os demais elementos do ciclo de vida do serviço estarão focados em resultados do cliente. Ao redor de uma maneira contínua o Desenho de Serviços, a Transição de Serviços e a Operação de Serviços. Esse encadeamento demonstra a continuidade dessa seqüência, aprimorando sempre pois todo este ambiente está envolvido pela Melhoria Contínua de Serviços.

2.7.3 – ITIL e a Política de Segurança da Informação

O ITIL é uma estrutura voltada para o gerenciamento de serviço. Neste contexto a segurança da informação aparece nesta estrutura como uma função do *Service Design* (Desenho de Serviços).

Breternitz, Neto e Navarro (2009) descrevem a necessidade da qualidade nos serviços de tecnologia da informação das organizações e da existência do módulo de segurança da informação compondo este gerenciamento de serviços.

> *Em um ambiente no qual as organizações dependem cada vez mais da qualidade de seus serviços de Tecnologia da Informação para poderem prestar serviços e produzirem bens de forma adequada, torna-se vital adotar ferramentas que garantam essa qualidade. Uma das ferramentas mais utilizadas para esse fim é a biblioteca ITIL (Information Technology Infrastructure Library), que possui um módulo que trata de gerenciamento da segurança.(Breternitz, Neto e Navarro, 2009, p.1)*

Segundo a OGC (2007) o objetivo do Gerenciamento de Segurança da informação é alinhar a segurança de TI com a segurança do negócio e garantir que a segurança da informação está efetivamente gerenciada em todos serviços e atividades do Gerenciamento de Serviços.

Para o ITIL, o processo do Gerenciamento de Segurança da Informação contempla:

> *- A produção, manutenção, distribuição e melhoria de uma Política de Segurança da Informação e das demais políticas complementares.*
>
> *- A garantia da adequação dos requerimentos de negócio com a Política de Segurança do Negócio.*
>
> *- Implementação de um conjunto de controles que suportem a Política de Segurança da Informação e gerencie os riscos associados aos acessos aos serviços, informações e sistemas.*
>
> *- Documentação de todos os controles de segurança, juntos com a operação e manutenção dos controles e dos riscos associados.*
>
> *- Gerenciamento dos fornecedores e contratados em relação ao acesso aos sistemas e serviços, em paralelo com o Gerenciamento de Fornecedores.*
>
> *- Gerenciamento de todas as falhas e incidentes de segurança associados aos sistemas e serviços.*
>
> *- Melhoria proativa nos controles de segurança, gerenciamento de risco de segurança e na redução dos riscos de segurança.*
>
> *- Integração dos aspectos de segurança com os demais processos de gerenciamento de serviços de TI.*
> *(OGC, Service Design, p.245)*

O próprio documento do Service Design detalha mais um pouco sobre as Políticas de Segurança da Informação, quando indica quais políticas relativas à segurança da informação devem existir, OGC (2007):

- Uma Política de Segurança da Informação de mais alto nível.
- Política sobre o uso de recursos de TI
- Política de controle de acesso
- Política de uso de email
- Política de uso de Internet
- Política de uso de anti vírus
- Política de classificação de documento
- Política de acesso remoto
- Política de acesso a serviços de TI por fornecedores
- Política de uso de ativos

A política de segurança da informação aparece como um elemento importante na função de Gerenciamento da Segurança da Informação. Se uma organização desejar estar alinhada com o ITIL, precisará considerar fortemente a segurança da informação, e neste contexto precisará ter uma efetiva e estruturada Política de Segurança da Informação.

2.8 – Política de segurança da informação - Governança

2.8.1 – Governança Corporativa

A Governança Corporativa surgiu há algumas décadas quando os governos decidiram definir regras mais rígidas para a gestão das organizações em função de escândalos corporativos que levaram ao fechamento de grandes corporações aparentemente sólidas.

O IBGC (2009, p.19), em seu Código de Melhores práticas de governança corporativa define Governança Corporativa como:

> *Sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgão de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade.*

A governança corporativa possui quatro princípios e objetivos básicos (IBGC, 2009)

a) Transparência: prover informações relevantes, não apenas as obrigatórias por lei, de forma clara e tempestiva a qualquer interessado.

b) Equidade: tratamento, de forma justa, de todos os *stakeholders*, bem como não adoção de práticas ou políticas discriminatórias.

c) Prestação de Contas: prestação de contas de todos os sócios, conselheiros fiscais e auditores (agentes de governança), dos seus atos administrativos, assumindo toda e qualquer conseqüência pelos seus atos.

d) Responsabilidade corporativa: os agentes de governança corporativa devem tomar decisões visando à continuidade do negócio, de forma ética, sem se esquecerem da sociedade e meio ambiente.

Para atender a estes princípios a organização precisa de informação confiável. Por esta necessidade a informação tornou-se um recurso crítico.

O ITGI (2006, p.7) coloca bem esta questão quando indica:

> *Informação e sistemas que tratam esta informação são críticos para a operação de todas as organizações. O acesso confiável à informação se tornou um componente indispensável na condução do negócio; além do que para um crescente número de organizações, informação é o negócio.*
>
> *Esta crescente dependência pela informação foi identificada a cerca de uma década, quando Peter Drucker afirmou que "a difusão da tecnologia e a mercantilização da informação transformou o papel da informação em um recurso de igual importância à terra, trabalho e capital."*

Cresce a necessidade de uma orientação vinda do alto escalão da organização. Cresce a necessidade da existência de uma Governança para as organizações;.

2.8.2 – Governança de Segurança da Informação

A ISACA – *Information Security Audit and Control Association*, uma associação global formada na década de 1960 e atualmente com mais de 70.000 profissionais de controle, segurança e auditoria associados, define Governança como:

> *Um conjunto de responsabilidades e práticas exercidas pelos administradores do alto escalão da organização e pelos gerentes executivos com o objetivo de prover uma direção estratégica garantindo que os objetivos serão atingidos, certificando-se que os riscos são gerenciados adequadamente e verificando que os recursos corporativos estão sendo usados com responsabilidade.*
> *(ISACA, 2010)*

Até recentemente na maioria das corporações a segurança da informação estava restrita ao ambiente de TI, se preocupando basicamente na garantia de proteção para os dados processados e armazenados neste ambiente. Um dos principais motivos deste foco é a dependência das organizações nos recursos de tecnologia da informação e comunicação. (Bernardes e Moreira, 2005, p.1)

Com as exigências da Governança Corporativa, a segurança deixou de ser um controle específico de TI para ser um elemento do negócio e da gestão deste negócio Sempre considerando o gerenciamento de riscos e a prestação de contas no uso da informação ou no uso dos recursos de informação. Uma segurança da informação efetiva exige o envolvimento dos executivos da organização para participar da avaliação das novas ameaças e da definição de prioridades.

É responsabilidade da alta direção da organização e dos gerentes executivos:

> *1. Entender a criticidade da informação e da segurança da informação na organização.*
>
> *2. Rever o investimento da segurança da informação considerando o Alinhamento da segurança da informação com a estratégia de negócio da organização e com o perfil de risco definido pela organização.*
>
> *3. Dar efetivo apoio ao desenvolvimento e implantação de um abrangente programa de segurança da informação.*
>
> *4. Exigir relatórios periódicos da gerência sobre o desenvolvimento e efetividade dos requisitos definidos pela alta direção.*
> *(ITGI, 2006, p.9)*

Sem deixar de considerar também as seguintes questões:

> *- Crescente dependência em relação à informação, aos sistemas e aos recursos de comunicação que possibilitam o uso da informação na organização.*
>
> *- Dependência de outras entidades.*
>
> *- Crescente demanda de compartilhar informações com parceiros, fornecedores e clientes.*

> *- Impacto na reputação e no valor da companhia em função de falhas na segurança da informação.*
>
> *- Falha na dosagem da importância da segurança da informação para a alta direção.*
> *(ITGI, 2006, p.9)*

O ITGI define a Governança da Segurança da Informação como:

> *Um subconjunto da Governança Corporativa que fornece orientação estratégica assegura que os objetivos serão alcançados, gerencia os riscos adequadamente, garante o uso dos recursos organizacionais de maneira responsável e monitora o sucesso ou fracasso do programa corporativo de segurança da informação. (ITGI, 2006, p.17)*

Como estrutura básica para a Governança da Segurança da Informação o ITGI sugere a existência dos seguintes elementos:

> *- Uma metodologia para gerenciamento de riscos em segurança da informação.*
>
> *- Uma abrangente estratégia de segurança explicitamente conectada aos objetivos de negócio e aos objetivos de TI.*
>
> *- Uma estrutura organizacional de segurança da informação eficiente.*
>
> *- Uma estratégia de segurança da informação que explicite o valor da informação protegida e informação entregue.*
>
> *- Políticas de segurança da informação que direcione cada aspecto da estratégia e dos requisitos definidos em regulamentação.*
>
> *- Um completo conjunto de padrões de segurança para cada política definida, de maneira a garantir que os procedimentos e diretrizes estão coerentes com a política.*
>
> *- Um processo de monitoramento institucionalizado para garantir o cumprimento e dar o retorno sobre a eficácia da minimização do risco.*
>
> *- Um processo para assegurar uma avaliação contínua e atualizada das políticas de segurança, padrões, procedimentos e riscos.*
> *(ITGI, 2006, p.18)*

Verifica-se que nesta estrutura básica de Governança de Segurança que a política de segurança da informação tem uma presença importante.

É sempre dito que a Governança da Segurança da Informação para ser definida, implementada e mantida precisa do apoio da alta administração. Algumas entidades definiram formalmente esta exigência. A NACD *(The National Association of Corporate Directors)*, associação líder de profissionais do alto escalão e gerentes

executivos de corporações reconheceu a importância da segurança da informação. (ITGI, 2006)

A NACD recomenda a prática pela alta direção de quatro atitudes essenciais:

> *- Coloque a segurança da informação na agenda da alta direção.*
>
> *- Identifique líderes de segurança da informação, defina responsabilidades para eles e garanta suporte para eles exercerem as funções de segurança da informação.*
>
> *- Assegure a eficácia da política de segurança da informação da corporação através de revisões e aprovações periódicas.*
>
> *- Atribua a segurança da informação a um comitê importante na organização e garanta o adequado suporte a este comitê.*
> *(ITGI, 2006, p.12)*

Com esta recomendação fica explícita a necessidade de uma Política de Segurança da Informação quando da necessidade de utilizar a abordagem de Governança de Segurança da Informação.

Também quando se destaca a importância das pessoas no processo da Governança da Segurança da Informação a política de segurança da informação novamente é citada:

> *A Governança da Segurança da Informação requer o comprometimento da gerência sênior, uma cultura e conscientização em segurança, a promoção de boas práticas de segurança e o cumprimento da política de segurança da informação. É mais fácil comprar uma solução do que realizar uma mudança na cultura. Mas, até o sistema mais seguro não vai conseguir um significativo grau de segurança, caso seja utilizado por pessoas mal treinadas, inexperientes, descuidados ou indiferentes em relação à segurança da informação.*
> *(ITGI, 2006, p.16)*

O ITGI (2006, p.13) resume bem o ambiente para a Governança da Segurança:

> *Governança para a Segurança Corporativa significa uma visão adequada da segurança como um requerimento não negociável na realização do negócio. Se a gerencia de uma organização – incluindo a alta administração, diretores e gerentes executivos e todos os gerentes – não estabelecer e reforçar que o negócio precisa de uma efetiva segurança corporativa, o desejado estado de proteção não será desenvolvido, atingido e mantido ao longo do tempo. Para alcançar a capacidade de sustentabilidade empresarial, a organização deve fazer com que a segurança corporativa seja de responsabilidade dos líderes em nível de Governança e não de pessoas em outras funções organizacionais que não possuem: autoridade, responsabilidade, recursos para agir e poder para exigir a conformidade.*

A Figura 9 apresenta uma representação conceitual da governança de segurança da informação. A mensagem principal desta representação são os elementos do meio da figura, onde indica uma seqüência de prioridade. Primeiramente deve existir a Estratégia do Negócio (Business Strategy). Somente após o negócio definir sua estratégia, pode-se ser definido a Estratégia de Segurança da Informação e Gestão de Risco (Risk Management/Information Security Strategy). Em seguida é que são desenvolvidos os Planos de Ação, Políticas e Padrões (Security Action Plans, Policies and Stardards). Na figura, o grupo à esquerda indica o nível/hierarquia dos profissionais envolvidos e o grupo à direita indica os produtos elaborados.

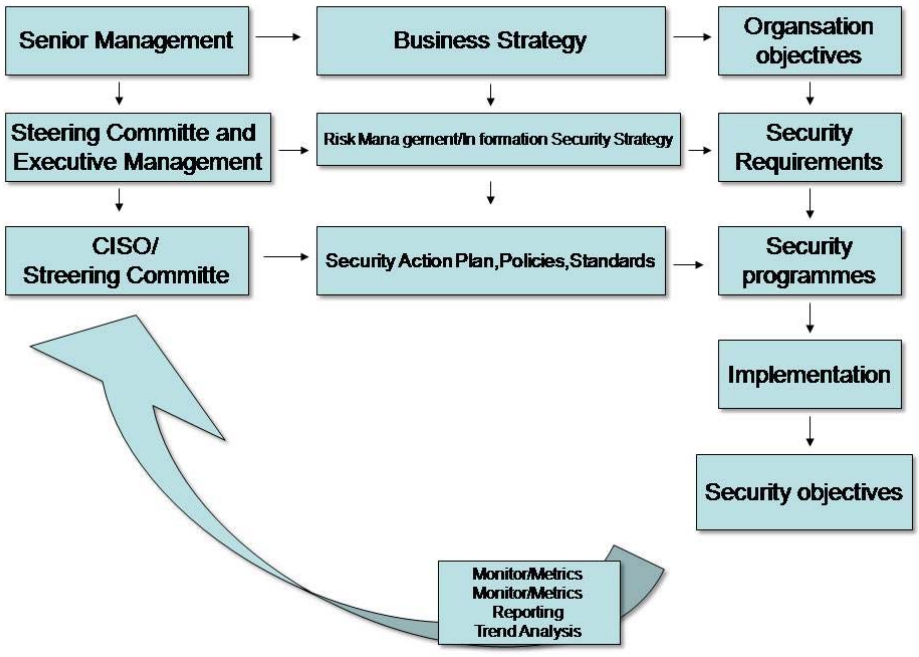


Figura 9 – Estrutura Conceitual da Governança de Segurança da Informação
Fonte: ITGI (2006)

2.9 – Política de Segurança da Informação – Alinhamento da Segurança da Informação ao negócio da organização – NBR ISO/IEC 27002:2005

Alinhamento da segurança da informação ao negócio da organização considerando os requisitos de segurança descritos na Norma NBR ISO/IEC 27002:2005

Várias estruturas e padrões que consideram a segurança da informação, e mais fortemente o tema Governança da Segurança da Informação, indicam a necessidade de que a segurança deva estar alinhada com os objetivos de negócio. A Política de segurança da informação deve indicar a participação das áreas de negócio ou da direção da organização em diferentes ações necessárias para a implantação e manutenção da segurança da informação na organização.

Neste capítulo são apresentados os requisitos de segurança da informação definidos pela NBR ISO/IEC 27002:2005 que exigem ou possibilitam a participação da direção ou das áreas de negócio. Cabe a cada organização definir se considerará estes requisitos quando da construção da sua política de segurança da informação.

A NBR ISO/IEC 27002:2005 declara que a informação é um ativo essencial para o negócio de uma organização e necessita ser adequadamente protegida ABNT (2005). Porém, a proteção da informação não deve acontecer por si só. A proteção deve acontecer porque existem os objetivos de negócio. Peltier (2004, 2005) enfatiza que a segurança da informação ajuda a organização a alcançar seus objetivos de negócio por intermédio de seus ativos tangíveis, de seus ativos intangíveis e deve dar suporte a realização da missão da organização. Ele continua destacando que a alta direção é exigida para proteger os ativos da organização e deve tomar decisões baseadas em informações confiáveis. Isto nos indica que o processo de segurança da informação precisa ser posicionado de uma maneira menos operacional. Wylder (2004) afirma que os programas de segurança da informação precisam se mover da implantação tática da tecnologia para se tornar parceiros estratégicos do negócio. Peltier (2004, 2005) complementa este pensamento quando afirma que só existem objetivos de negócio e a segurança da informação deve estar integrada em todos os processos de negócio. Calder e Watkins (2005) reforçam quando afirmam que as organizações devem garantir que qualquer processo que seja implantado deva ser apropriado e construído sob

medida para o ambiente da respectiva organização. Quando estivermos construindo uma arquitetura de segurança, Sherwood, Clark e Linas (2005) nos orientam indicando que a arquitetura corporativa de segurança deve ser guiada com base na perspectiva do negócio e deve considerar a variedade de requerimentos que inclusive podem conflitar entre si. E não podemos esquecer que a segurança da informação vai afetar cada funcionário da organização em função das políticas e dos controles implantados Maiwald e Sieglein (2002).

A governança da segurança da informação possibilita a sustentabilidade e transparência através da estrutura de relacionamentos e processos para controlar a organização de maneira que ela alcance seus objetivos e minimize os seus riscos de segurança da informação contando com o envolvimento dos executivos de negócio nas decisões relativas à segurança da informação e que afetam ao negócio da organização. IT Governance Institute (2008).

Alinhar a segurança da informação aos requisitos de negócio é um elemento necessário para um efetivo processo de segurança da informação. A Norma ISO/IEC 27002:2005 possui enraizada no seu texto a exigência deste alinhamento, como é dito no seu início: “Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável levando-se em conta os objetivos organizacionais” (ABNT, 2005, p. 7).

Este capítulo identifica as diretrizes que exigem o alinhamento da gestão de segurança com os objetivos das áreas de negócio.

Para cada uma das seções que dividem a NBR ISO/IEC 27002:2005, foi analisado o seu texto e foram identificadas aquelas diretrizes, considerando o conjunto de diretrizes, que exigem a participação das áreas de negócio.

Seção 5: Política de Segurança da Informação, ABNT (2005, p.8-9).

> *- O documento de segurança da informação deve ser aprovado pela direção.*
>
> *- O documento de segurança da informação deve conter uma declaração do comprometimento da direção alinhada com os objetivos e a estratégia de negócio.*

> *- A revisão periódica da política de segurança da informação deve considerar as mudanças e as circunstâncias do negócio.*

Estas diretrizes exigem o comprometimento da direção da organização e desta forma garantem que as orientações básicas do processo de segurança da informação estarão alinhadas com os objetivos de negócio e da organização.

Seção 6: Organizando a segurança da informação, ABNT (2005, p.10-20):

> *- A direção deve apoiar ativamente o processo de segurança da informação através de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação.*
>
> *- A direção deve fornecer um claro direcionamento e apoio para as iniciativas de segurança da informação.*
>
> *- Dependendo do tamanho da organização a direção pode definir um fórum de gestão (exclusivo ou já existente) para o acompanhamento e coordenação dos resultados da implantação do processo de segurança da informação.*
>
> *- As atividades do processo de segurança da informação devem envolver representantes de diferentes partes da organização.*
>
> *- Os novos recursos de processamento de informação devem ter a autorização adequada por parte da administração dos usuários (área de negócios) permitindo seus propósitos e uso.*
>
> *- Quando da proteção do recurso de informação deve-se definir requisitos para a continuidade dos serviços de acordo com as prioridades do negócio da organização.*

Estas diretrizes reforçam o comprometimento da direção e explicitam a participação e conseqüente comprometimento das diversas áreas da organização (áreas de negócio): na participação de atividades do processo de segurança da informação, na autorização de uso de novos recursos de processamento da informação e na definição do nível de disponibilidade. Desta forma as ações e o nível de rigidez do processo de segurança da informação serão direcionados pelos requisitos das áreas de negócio.

Seção 7: Gestão de ativos, ABNT (2005, p.21-24):

> *- As informações e os ativos associados com os recursos de processamento da informação devem ter um proprietário por uma parte definida da organização.*
>
> *- A classificação da informação e seus respectivos controles devem considerar os impactos nos negócios.*

Estas diretrizes indicam que:

a) diferente do que historicamente ocorreu (ou ocorre) onde a área de TI assumia a função de proprietária da informação, é exigido que o proprietário da informação seja

das diversas áreas da organização, isto é, o proprietário da informação deve ser da área (de negócio ou de apoio) que é responsável pela informação;

b) a classificação da informação existirá em função dos impactos nas áreas de negócio, isto é, os objetivos de negócio serão a razão do nível de classificação da informação.

Seção 8: Segurança em Recursos Humanos, ABNT (2005 p. 25-31):

> *- As responsabilidades em relação à segurança da informação existem em todos os cargos da organização. Os papéis e responsabilidades em relação ao processo de segurança da informação dos funcionários, fornecedores e terceiros precisam estar definidos e documentos quando da contratação dessas pessoas.*
>
> *- É conveniente a existência de um código de conduta que contemple as responsabilidades dos funcionários, fornecedores ou terceiros em relação à ética e a proteção dos dados.*
>
> *- A conscientização, educação e treinamento em segurança da informação devem ser adequados aos papéis, responsabilidade e das pessoas*.

Estas diretrizes explicitam que todos os cargos (e conseqüentemente todas as pessoas) possuem responsabilidades com o processo de segurança da informação e que orientações corporativas, como o código de ética, devem falar da proteção da informação, indicando dessa maneira que a segurança da informação deve ser uma preocupação da organização. Como preocupação organizacional, os objetivos de negócio deverão ser considerados no processo de segurança da informação.

Seção 9: Segurança física e do ambiente (ABNT (2005).
Para esta seção não foram identificadas diretrizes que explicitamente reforçam o alinhamento da Gestão da Segurança da Informação com os objetivos de negócio.

Seção 10: Gerenciamento das operações e comunicações, ABNT (2005, p. 40-64):

> *- Todas as pessoas envolvidas em cada mudança devem ser comunicadas dos detalhes das mudanças.*
>
> *- Convém que sejam estabelecidos os procedimentos e responsabilidades gerenciais formais para garantir que haja um controle satisfatório de todas as mudanças.*
>
> *- As mudanças em sistemas devem ser realizadas apenas quando houver uma razão de negócio válida para tal.*
>
> *- As funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.*

> *- Os recursos que possuem um ciclo de renovação ou custo maior devem ser monitorados pelos gestores que devem identificar as tendências de utilização, particularmente em relação às aplicações do negócio, com o objetivo de identificar e evitar os potenciais gargalos e a dependência em pessoas chaves que possam representar ameaças à segurança dos serviços.*
>
> *- Quando de novos sistemas, atualizações e novas versões a aceitação formal deve considerar s requisitos de continuidade dos negócios.*
>
> *- Na proteção contra códigos maliciosos devem-se preparar planos de continuidade do negócio.*
>
> *- As cópias de segurança devem refletir os requisitos de negócio da organização e para tanto devem ter o nível necessário para a existência dessas cópias.*
>
> *- Deve-se prevenir contra a divulgação não autorizada, remoção ou destruição de recursos de informação que podem causar interrupção das atividades do negócio e as mídias as mídias removíveis devem estar habilitadas somente se houver uma necessidade de negócio.*
>
> *- Devem-se ter diretrizes de retenção e descarte para toda a correspondência de negócios.*
>
> *- Convém que os aspectos de segurança contidos nos acordos de troca de informação reflitam a sensibilidade das informações envolvidas no negócio.*
>
> *- Convém que as políticas e procedimentos sejam desenvolvidos e implantados para proteger as informações associadas com a interconexão de sistemas de informações do negócio.*
>
> *- Deve existir uma Gestão de Mudança que garanta um rígido controle das alterações que serão feitas no ambiente de processamento das informações, considerando os impactos potenciais e a comunicação dos detalhes das mudanças para todas as pessoas envolvidas.*

Estas diretrizes são variadas, mas todas têm como base a participação das áreas de negócio além da exigência de definições de segregação de função.

Seção 11: Controle de acessos, ABNT (2005, p. 65-83):

> *- Convêm que a política de controle de acesso seja estabelecida documentada e analisada criticamente tomando-se como base os requisitos de acesso dos negócios.*
>
> *- O acesso do usuário deve ser permitido apenas onde existe necessidade do negócio ou razões operacionais.*
>
> *- O nível de acesso concedido ao usuário deve ser apropriado ao propósito do negócio.*
>
> *- Para o usuário ter acesso ao sistema é necessário a autorização do proprietário do sistema.*
>
> *- O estabelecimento de perfis de acesso para usuário deve ser baseado nos requisitos dos negócios.*

O acesso a informação exige que as áreas de negócio sejam as responsáveis para a liberação da informação do negócio para todas as áreas da organização.

Seção 12: Aquisição, desenvolvimento e manutenção sistemas, ABNT (2005, p.84-97):

> *- Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas ou melhorias dos sistemas existentes.*
>
> *- Convém que requisitos de segurança e controles reflitam o valor para o negócio dos ativos de informação envolvidos e os danos potenciais ao negócio que poderiam resultar de uma falha ou ausência de segurança.*

Desde a etapa de desenvolvimento ou aquisição de sistemas de informação, as áreas de negócio precisam ser envolvidas. Os sistemas e posteriores controles de segurança existem para a realização do negócio.

Seção 13: Gestão de incidentes de segurança da informação, ABNT (2005, p. 98-102):

> *- Convêm que os eventos de segurança da informação sejam relatados através dos canais da direção, o mais rápido possível.*
>
> *- Deve existir um ponto de contato de conhecimento de toda a organização para receber as notificações de segurança da informação.*

Neste item temos o uso de canal da direção e a ênfase para que toda a organização conheça o ponto de contato para relato da gestão de incidentes.

Seção 14: Gestão de continuidade de negócio, ABNT (2005, p. 103-107):

> *- Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização.*
>
> *- Quando do entendimento dos riscos que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, deve-se considerar a identificação e prioridade dos processos críticos de negócio.*
>
> *- Devem-se identificar os ativos dos processos críticos de negócio.*
>
> *- Deve-se entender o impacto que os incidentes de segurança da informação terão sobre os negócios.*
>
> *- Deve-se buscar garantir que a gestão da continuidade do negócio está incorporada aos processos estruturais da organização.*
>
> *- Convém que as análises/avaliações de riscos de continuidade de negócio sejam realizadas com total envolvimento dos responsáveis pelos processos e recursos do negócio.*
>
> *- Convém que a análise/avaliação de riscos identifique, quantifique e priorize os critérios baseados nos riscos e os objetivos pertinentes à organização.*
>
> *- Deve-se ser definida uma abordagem estratégica para a continuidade dos negócios e a mesma deve ser validada com a direção da organização.*

> *- Ao ser desenvolvido o plano de continuidade de negócios deve-se ser dada atenção especial à avaliação de dependências externas ao negócio e de contratos existentes.*
>
> *- Convém que o processo de planejamento foque nos objetivos requeridos do negócio.*

Este é o item da norma que mais fortemente exige a participação da área de negócio. Fica bastante claro que um plano de continuidade deve existir para possibilitar a continuidade do negócio.

Seção 15: Conformidade, ABNT (2005, p. 108-114):

> *- Convém que a direção aprove o uso de recursos de processamento de informação.*
>
> *- Os recursos de processamento da informação de uma organização são destinados básica ou exclusivamente para atender aos propósitos do negócio.*
>
> *- Se qualquer não-conformidade for encontrada como um resultado da análise crítica convém que os gestores determinem as causas da não conformidade; avaliem ações para que a não conformidade se repita; determinem e implementem ação corretiva apropriada e analisem a ação corretiva tomada.*

Este item tem como foco principal a necessidade da organização cumprir os regulamentos, a legislação e seus contratos. De uma maneira indireta, tudo que torna a organização não cumpridora das suas obrigações afetará a área de negócio. Sendo assim a área de negócio deve ser a unidade organizacional que mais deseje a garantia do cumprimento legal e contratual.

Seção 4: Análise/avaliação e tratamento de risco, ABNT (2005 p. 6-7):

> *- Convém que as análises/avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para a aceitação dos riscos e dos objetivos relevantes para a organização.*
>
> *- Convém que os controles assegurem que os riscos sejam reduzidos a um nível aceitável, levando-se me conta os objetivos organizacionais.*

Foram identificados em onze categorias, das doze categorias existentes na norma, cinqüenta e uma diretrizes que exigem a participação das áreas de negócio e conseqüentemente possibilitam o alinhamento da gestão da segurança da informação com as mesmas, desde que definidas na política de segurança da informação.

3. UMA REVISÂO DO ESTADO DA ARTE

A literatura existente, considerando trabalhos acadêmicos e livros, aborda a aplicação das normas de segurança da informação (desde a BS-7799 até a NBR ISO/IEC 27002:2005) na organização e os seus impactos. Pouco se pesquisa como elaborar as políticas, como estruturar os níveis de detalhamento de cada assunto, quais são os controles necessários e a necessidade de amadurecimento da organização em segurança da informação. A organização que necessita implantar políticas de segurança da informação encontrará dificuldade quando buscar ajuda na literatura para identificar como fazer, por onde começar, como priorizar e o que contemplar. Tal realidade aponta para a relevância e pioneirismo desta pesquisa.

Estudando dissertações e teses no ambiente acadêmico brasileiro, foram encontrados poucos documentos tratando diretamente o tema política de segurança da informação. Contudo os que foram encontrados não abordam a identificação de um padrão mínimo para a política de segurança da informação.

No segundo semestre de 2010, foi feito um levantamento junto ao Portal de Periódico da CAPES, com foco no Banco de Teses e Dissertações. Após algumas dificuldades de estabelecimento de acesso, foi identificado o Novo Banco de Teses e Dissertações. Pesquisando com base no tema deste trabalho, “Política de segurança da informação: uma contribuição para o estabelecimento de um padrão mínimo”, foram selecionados pela ferramenta de busca 600 (seiscentos) trabalhos. A maioria desses trabalhos tinha alguma palavra chave do tema, mas não estavam relacionados à esta pesquisa. Após uma primeira seleção, o número de trabalhos foi reduzido para 150 trabalhos e posteriormente com mais rigor no tema e abordagem do tema, foram selecionados 49 (quarenta e nove) trabalhos. Considerando este conjunto foram analisados 8 (oito) trabalhos que tinham no tema tratado ou na abordagem alguma relação mais forte com o tema desta pesquisa. Eles estão relacionados abaixo, porém, nenhum deles fala especificamente sobre um padrão mínimo de política de segurança da informação, tema central desta dissertação.

Tal fato ressalta a importância desta pesquisa e aumenta o seu grau de novidade no tema de segurança da informação.

Lorens (2007) em sua Dissertação de Mestrado, intitulada *Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação*, apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília, concentra-se na implantação da segurança da informação no âmbito da organização considerando o usuário como elemento fundamental e a integração dessa implantação com o planejamento estratégico da organização.

Ellwanger (2009) em sua Dissertação de Mestrado, intitulada *Impactos da utilização das técnicas de endomarketing na efetividade das políticas de segurança da informação,* defendida no Programa de Pós Graduação em Engenharia de Produção da Universidade Federal de Santa Maria, investiga por meio de uma pesquisa em duas unidades de um hospital, o impacto da utilização de técnicas de endomarketing para a melhor conscientização dos usuários dos sistemas de informação.

Benz (2008) em sua Dissertação de Mestrado intitulada *Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI: estudo de casos em instituições financeiras*, apresentada no Programa de Pós Graduação em Administração da Universidade Federal do Rio Grande do Sul tem como foco no seu trabalho o alinhamento da política de segurança da informação com o planejamento da tecnologia da informação, pois, segundo ele caso isso não ocorra o planejamento de TI estará comprometido.

Cavalcante (2002) em sua Dissertação de Mestrado intitulada *Segurança da informação no correio eletrônico baseada na ISO/IEC 17799: um estudo de caso em uma instituição de ensino superior, com foco no treinamento*, submetida ao Programa de Engenharia de Produção da Universidade Federal do Rio Grande do Norte, demonstra os resultados de uma pesquisa que teve por objetivo identificar a importância que o treinamento do usuário têm sobre as políticas de segurança das informações nas empresas através de um estudo de caso em uma instituição de ensino superior.

Menezes (2005) em sua Dissertação de Mestrado intitulada *Gestão da segurança da informação: análise em três organizações brasileiras,* apresentada ao Núcleo de Pós Administração em Administração da Universidade Federal da Bahia analisa o grau de conhecimento e adoção da política de segurança da informação por parte dos funcionários através de pesquisa em três organizações brasileiras.

Roza (2010) em seu Trabalho de Conclusão de Curso de Graduação de Tecnologia em Segurança da Informação, intitulado *Política de segurança da informação em ambientes hospitalares*, apresentado na Faculdade de Tecnologia de São Caetano do Sul, apresenta uma pesquisa sobre política de segurança em onze hospitais da Cidade de São Paulo.

Ribas (2010) em sua Dissertação de Mestrado intitulada *Sistema de gestão da segurança da informação em organizações da área de saúde* descreve o processo de implantação de um sistema de gestão de segurança da informação em uma organização da área de saúde e faz uma avaliação dessa implantação. Sua conclusão é que no estudo feito, a implantação do sistema de gestão da segurança da informação trouxe melhorias para a organização com melhorias significativas no nível de conformidade com a Norma NBR ISO/IEC 27001:2006 além da redução de riscos aos ativos da organização por meio da implantação de controles. Em relação às normas de segurança da informação, Ribas (2010) indica:

> *As normas desempenham um papel essencial para a elaboração de um plano de segurança da informação. Elas fornecem uma abordagem sistemática de gestão para adotar as melhores práticas em controles, quantificar o nível de risco aceitável e implantar as medidas adequadas que protejam a confidencialidade, integridade e disponibilidade das informações. (RIBAS, 2010, p. 17)*

Nesta dissertação, Ribas (2010) adotou uma estrutura normativa com três níveis hierárquicos, assim relacionados:

> *a) Políticas – definem a estrutura, as diretrizes e as obrigações referentes à segurança da informação.*
>
> *b) Normas – estabelecem obrigações e procedimentos definidos de acordo com as políticas.*
>
> *c) Procedimentos – instrumentalizam o disposto nas Normas e nas Políticas, permitindo a direta aplicação nas atividades da organização.*
> *(RIBAS, 2010, p.34)*

Venturini (2006) na sua Tese de Doutorado intitulado *Modelo Ontológico de segurança para negociação de política de controle de acesso em multidomínios*, trata do tema política de segurança, porém com o objetivo de propor um modelo de segurança para a negociação e composição dinâmica de políticas de segurança para controle de acessos em ambientes de domínios distintos que precisam compartilhar parcialmente seus recursos para a realização de trabalho colaborativo.

Foram identificados artigos científicos publicados em periódicos que estivessem relacionados ao tema e alguns deles foram considerados nesta pesquisa para a introdução ao tema e a fundamentação teórica do tema. Nenhum dos artigos trata da identificação de um padrão mínimo de elementos para uma política de segurança da informação. Este fato reforça a importância desta pesquisa e seu grau de novodade no tema segurança da informação.

4. ESTUDO DE CASO

4.1 – Etapas da metodologia

A metodologia utilizada neste estudo considerou o estudo de caso integrado (unidades múltiplas de análise) utilizando a pesquisa exploratória. A metodologia considerou as seguintes etapas:

a) Levantamento da literatura sobre o assunto política de segurança da informação, considerando fontes acadêmicas e empresariais.

b) Estudo teórico do tema política de segurança da informação.

c) Desenvolvimento de um estudo de caso múltiplo de modo a analisar políticas de segurança da informação já implantadas em dez organizações e identificar elementos comuns que possam estabelecer um padrão mínimo de política de segurança da informação.

Foi utilizado o estudo de caso para esta pesquisa exploratória por ser a estratégia que melhor atende às características da mesma. Segundo Yin (2010) o estudo de caso é utilizado para examinar acontecimentos contemporâneos e também para contribuir ao nosso conhecimento os fenômenos individuais, grupais, organizacionais, sociais, políticos e relacionados. Complementa que as aplicações de estudo de caso podem ser feitas para explorar situações em que a intervenção que está sendo avaliada não apresenta um conjunto simples e claro de resultados.

Yin (2010) ainda declara:

> *O estudo de caso é uma investigação empírica que investiga um fenômeno contemporâneo em profundidade e em seu contexto na vida real, especialmente quando os limites entre o fenômeno e o contexto não são claramente evidentes. (YAN, 2010).*

4.2 – Protocolo de aplicação do estudo de caso

Este protocolo descreve os procedimentos e as regras gerais da condução e realização do estudo de caso.

4.2.1 – Visão geral do projeto de estudo de caso

4.2.1.1 - Objetivo da pesquisa

Esta pesquisa teve como objetivo principal propor a construção de um padrão mínimo para a política de segurança da informação de uma organização.

Contemplou, ainda, os seguintes objetivos específicos:

- realização de uma pesquisa exploratória em organizações que possuem políticas de segurança da informação;

- análise da política (diretriz) de segurança da informação de cada uma dessas organizações;

- identificação da existência de requisitos de segurança comuns nestas políticas;
- estabelecimento do conjunto de requisitos que comporão o padrão mínimo para a política de segurança da informação.

4.2.1.2 - Questão da pesquisa

A principal questão desta pesquisa foi:

- Quais são os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização?

4.2.1.3 - Tipo da pesquisa, tipo do projeto e unidade de análise

Esta foi uma pesquisa exploratória utilizando um projeto de estudo de caso integrado (unidades múltiplas de análise) e tem como unidade de análise as políticas de segurança da informação de diferentes organizações.

Esta pesquisa teve como delimitação, o estudo de políticas de segurança da informação em três organizações.

4.2.2. – Procedimentos de campo

Fontes gerais de informação – Coleta dos dados

Foram utilizadas como fonte de evidencia para a coleta de dados:

- Documentação.
- Entrevista.

4.2.3 – Documentação e questões para o estudo de caso

4.2.3.1 - Documentação

Foram considerados os documentos de políticas de segurança da informação, das organizações. O foco do trabalho diz respeito aos documentos de políticas e não considerou os documentos de procedimentos ou de regras detalhadas que indicam como executar o que as políticas definem.

O trabalho foi baseado no conjunto de controles definidos pela Norma NBR ISO/IEC 2007:2005 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação.

Cada política de cada organização foi analisada e foram identificados os controles definidos pela Norma que foram considerados na política. Depois foram identificados os requisitos comuns existentes na maioria das políticas analisadas.

A partir dos dados acima identificados foram estruturados os elementos que devem compor um padrão mínimo para a política de segurança da informação.

A utilização da documentação foi o fator fundamental para a identificação dos elementos que serão indicados para compor o padrão mínimo para a política de segurança da informação.

4.2.3.2 - Entrevista

As informações coletadas nas entrevistas tiveram como finalidade identificar algumas características do ambiente onde a política foi construída e publicada. Essas características podem influenciar a política e ajudam a conhecer melhor cada organização pesquisada, no que diz respeito à política de segurança da informação.

A entrevista foi realizada com o profissional que tem a responsabilidade pela Segurança da Informação e suas questões ajudarão a compreender a estruturação e características do processo de segurança da informação.

As perguntas foram abertas para garantir que o respondente não se guiaria por opções de resposta.

Foram coletadas informações sobre o respondente e foram considerados quatro eixos para um melhor entendimento sobre a organização e fatores que podem ter norteado a criação de políticas de segurança da informação.

O Anexo 4 apresenta o questionário submetido aos entrevistados.

4.3 – Análise de dados

Foi realizada uma análise descritiva dos dados coletados com o objetivo de organizar este estudo.

5. RESULTADOS

Inicialmente a pesquisa tinha o compromisso de analisar três políticas de segurança da informação de três organizações. Para alcançar este fim foi solicitada a doze organizações a disponibilização de suas políticas para a realização desta pesquisa. Nesta solicitação sempre foi informado que o nome da organização não seria divulgado no documento de dissertação e nem na apresentação verbal da pesquisa.

Das organizações solicitadas, duas declinaram da participação da pesquisa. Das dez organizações que disponibilizaram as suas políticas, oito responderam o questionário.

Desta maneira os percentuais referentes às políticas de segurança da informação se referem às dez organizações participantes e os percentuais referentes aos profissionais e a prioridade dos riscos se refere às oito organizações cujos questionários foram completamente respondidos.

5.1 – Análise das organizações

As dez organizações participantes estão distribuídas, sem grande concentração, em nove segmentos de negócios. A Figura 10 apresenta esta distribuição.

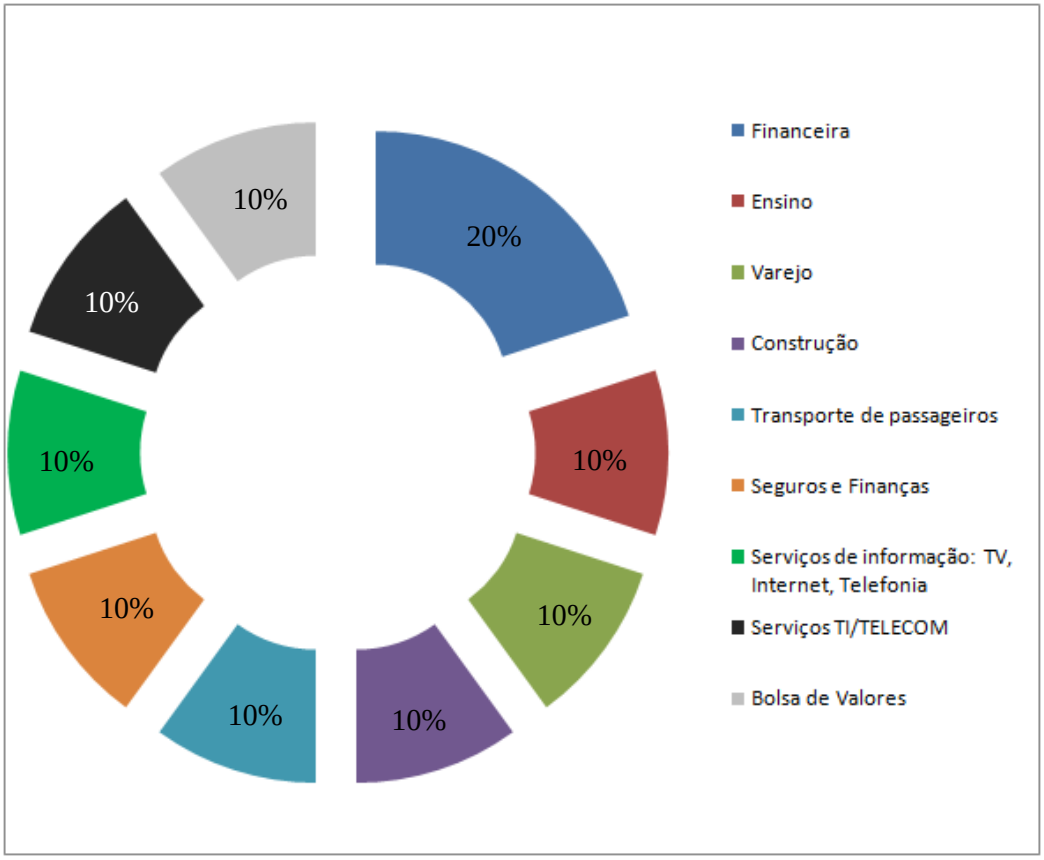


Figura 10 – Percentual das organizações pesquisadas por segmento de negócio.
Fonte: Elaborado pelo autor.

Todas as organizações possuem políticas há vários anos. Noventa por cento das organizações pesquisadas possuem políticas há mais de cinco anos e apenas dez por cento das organizações pesquisadas possuem políticas há menos de cinco anos (Figura 11, abaixo). Porém se considerarmos um tempo menor, todas as organizações possuem políticas há mais de quatro anos.

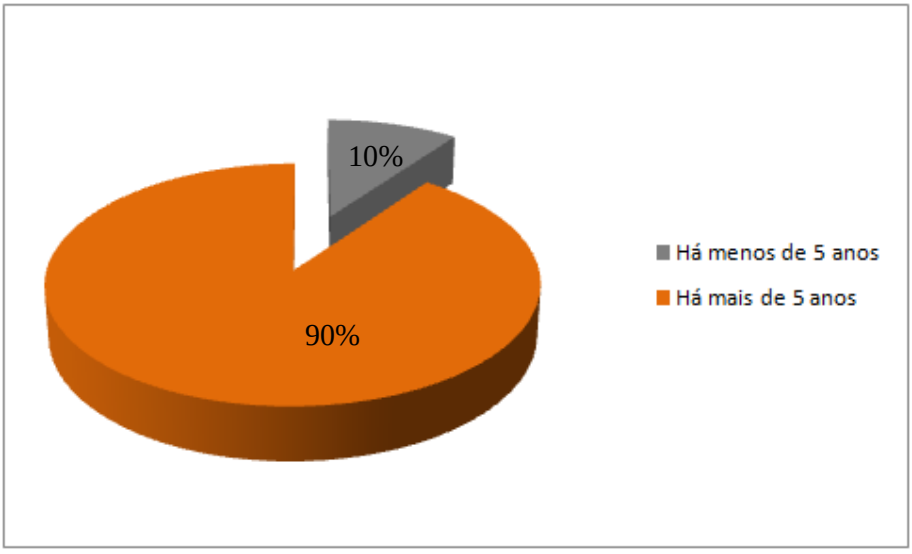


Figura 11 – Percentual das organizações pesquisadas considerando o tempo de publicação da primeira política de segurança da informação.
Fonte: Elaborado pelo autor.

O fato da existência de políticas há vários anos é importante para esta pesquisa porque indica que a grande maioria das organizações consideradas possui políticas de segurança da informação maduras e consolidadas. Por conseqüência os controles utilizados por cada política são considerados importantes para a respectiva organização.

Outra informação que reforça a maturidade das políticas consideradas é o fato de que todas as organizações tiveram suas políticas de segurança da informação assinadas por um nível hierárquico de diretoria. Sendo que, 30% foram aprovadas por um Comitê Executivo e 30% assinadas pelo presidente ou vice-presidente. Este nível de aprovação indica que o assunto segurança da informação, representado pela sua diretriz, a política de segurança da informação, é formalmente tratado, mesmo que inicialmente, em grau estratégico pela organização.

Outro fator importante é que 70% das organizações possuem uma área específica para a segurança da informação. Nesta pesquisa não foi investigado o grau hierárquico desta unidade organizacional referente à segurança da informação, porém, a existência de uma área com a responsabilidade explícita de tratar a

segurança da informação indica um início de entendimento da criticidade da proteção da informação para que a organização atinja os seus objetivos.

Ainda nesta abordagem da segurança da informação para a organização, todas as políticas pesquisadas indicam, de maneira direta ou indireta, que a proteção da informação deve contemplar a informação no ambiente de tecnologia da informação e no ambiente convencional. Outro fato importante identificado em todas as políticas analisadas, é o escopo considerado para os tipos de usuários: funcionários, estagiários e prestadores de serviço. Sendo assim, a responsabilidade para com a informação da organização exercida pelo funcionário da organização é semelhante a responsabilidade do prestador de serviço.

A quantidade de usuários afetados pela política de segurança da informação de cada organização considerada nesta pesquisa é outro fator de confirmação de que as políticas consideradas são representativas. Oitenta por cento das organizações desta pesquisa possuem políticas que afetam mais de 1.000 usuários (Figura 12), sendo que uma das organizações pesquisadas possui no Brasil cerca de 35.000 usuários que são afetados por sua política e outra organização possui 24.000 usuários.

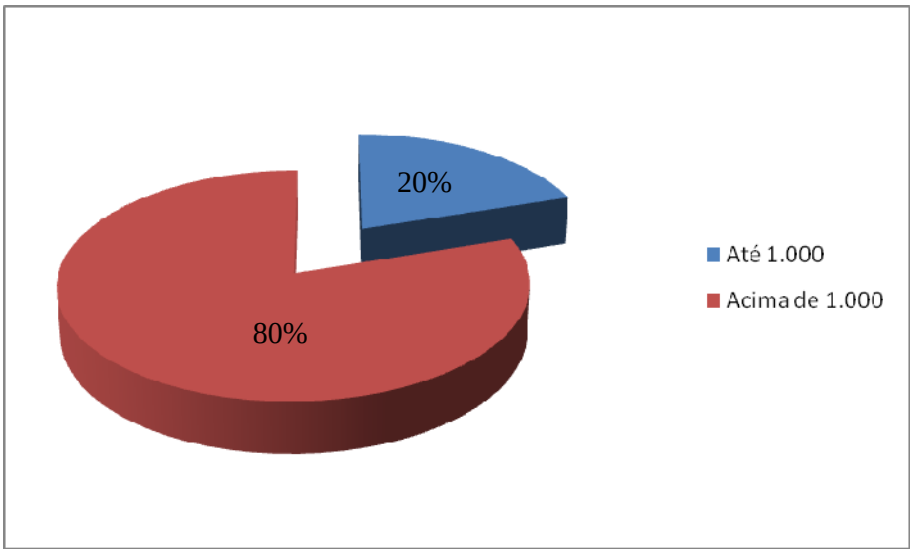


Figura 12 – Percentual das organizações pesquisadas considerando a quantidade de usuários afetados pela política de segurança da informação.
Fonte: Elaborado pelo autor.

A pesquisa demonstrou que as organizações consideradas ainda não são rigorosas com a exigência do controle de política de segurança da informação para os seus fornecedores de serviços ou produtos. Apenas 20% das organizações pesquisadas consideram este controle para os seus fornecedores. Outras 20% indicam que consideram a exigência do controle política de segurança para fornecedores críticos, porém fica em aberto o que é fornecedor crítico, assunto que deve ultrapassar o escopo da segurança da informação e adentrar no ambiente de risco operacional. Porém, um dado importante é que metade das organizações estudadas informou que analisam caso a caso. Este fato indica que o assunto política de segurança da informação está se consolidando como um elemento crítico para que uma organização preste serviço para outra organização.

Uma resposta comum em todas as organizações pesquisadas foi o fato de tomarem como base a Norma ISO 27002. Esta é uma norma internacional e no Brasil ela foi publicada pela ABNT como NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Tal fato muito corrobora para o presente estudo uma vez que esta norma foi tomada por base para a análise dos controles nas políticas das organizações com o objetivo de identificar um padrão mínimo para a política de segurança da informação de uma organização.

5.2 – Análise dos entrevistados

Todos os profissionais que foram entrevistados são do sexo masculino.

Um dado importante para esta pesquisa é o fato de que 100% dos profissionais que deram o retorno do questionário possuem mais de cinco anos de experiência profissional em atividades de segurança da informação. Mais detalhadamente: 75% dos profissionais que responderam o questionário possuem mais de 10 anos de experiência em segurança da informação (Figura 13). Isto demonstra que estes profissionais participam de maneira consciente no processo de segurança da informação da organização em que trabalham e também indica que as respostas e

opiniões dadas por estes profissionais são frutos de uma boa experiência profissional.

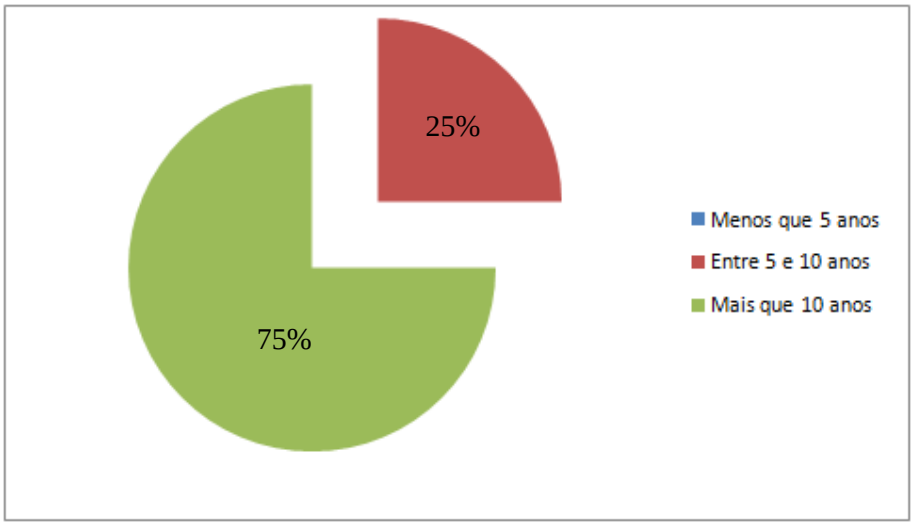


Figura 13 – Percentual dos profissionais em relação ao seu tempo de experiência em segurança da informação. Fonte: Elaborado pelo autor.

Em relação ao processo formal de especialização na área de segurança da informação, 50% dos profissionais possuem certificações internacionais de reconhecida credibilidade: CISM, CISA, CISSP. (Figura 14 abaixo)

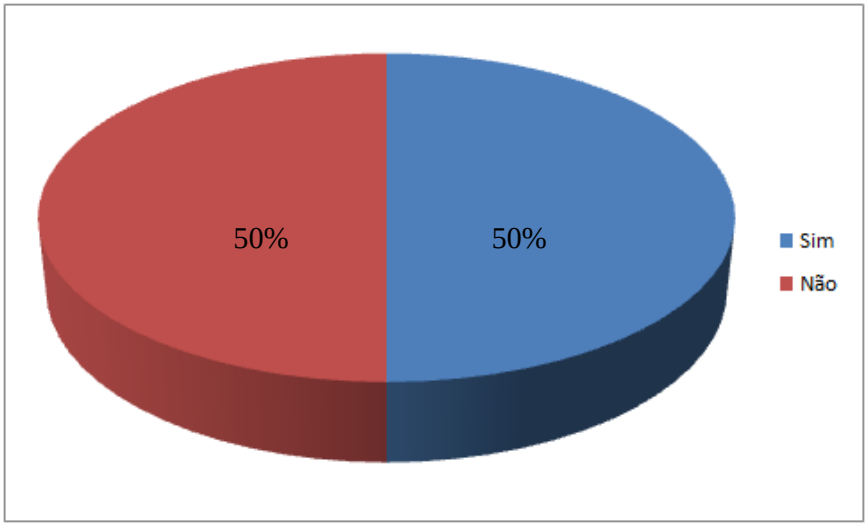


Figura 14 – Percentual dos profissionais que possuem certificação internacional.
Fonte: Elaborado pelo autor.

O dado de que metade dos profissionais de segurança da informação pesquisado possui certificação profissional, aponta para a importância das mesmas. Vale salientar que estas certificações são pessoais e estão atreladas ao profissional. Para se ter uma das certificações indicadas é necessário que o profissional preste um exame teórico sobre o assunto, prove seu tempo de experiência em segurança da informação e realize atividades no assunto controle de segurança da informação de maneira que seja possível a renovação anual desta certificação.

Para esta pesquisa este fato é muito importante, pois indica formalmente que metade dos profissionais que responderam o questionário estudou diversas normas e em especial a Norma NBR ISO/IEC 27002:2005, base e referência desta pesquisa. Conseqüentemente são profissionais com conhecimento prático e teórico sobre o assunto segurança da informação.

Em relação às ameaças e riscos que mais preocupam a organização, sob a visão do seu profissional de segurança da informação, tem-se o seguinte quadro (Figura 15), onde 1-Maior prioridade e 8-Menor prioridade:

3. ADMINISTRAÇÃO DO RISCO	
Organizações =>	**Prioridade**
e) Roubo de informação por concorrente desleal ou por criminosos que podem vender esta informação	1
f) Vazamento de informação por erro, descuido/negligência	2
a) Contingencia que indisponibiliza o ambiente de tecnologia	3
d) Invasão do ambiente de tecnologia por criminosos externos	4
g) Virus e demais códigos maliciosos	5
c) Incapacidade de responder questionamentos da Justiça	6
b) Fraude realizada por usuário interno	7
h) Falha em sistema aplicativo	8

Figura 15 – Quadro indicando a prioridade de ameaças e risco para a Organização.
Fonte: Elaborado pelo autor.

O roubo da informação é a ameaça que mais preocupa as organizações, conforme indica a resposta dos questionários fornecida pelos seus profissionais de segurança da informação. Roubo de informação acarreta impactos financeiros e de imagem da organização e afeta diretamente os objetivos de negócio da organização.

Em segundo lugar continua a preocupação com o sigilo da informação: Vazamento da informação por erro, descuido ou negligencia. Seja por má fé ou por descuido, as organizações não querem que pessoas e organizações não autorizadas tenham acesso às suas informações.

Em terceiro lugar foi considerada a ameaça de uma situação de contingência que indisponibilize o ambiente de tecnologia.. Todas as organizações pesquisadas dependem fortemente dos recursos de tecnologia da informação e uma indisponibilidade desses recursos atinge diretamente aos objetivos de negócio da organização.

A invasão por criminosos do mundo virtual é a quarta ameaça mais prioritária. Este fato indica que o gestor do processo de segurança da informação está ciente de que é necessário uma proteção técnica eficiente.

Vírus e código maliciosos formam a quinta preocupação dos profissionais de segurança da informação e podem levar a destruição da informação, a indisponibilidade da informação ou a quebra de sigilo dessa informação. Para minimizar o risco desta ameaça, serão realizadas ações técnicas, porém as conseqüências da concretização dessa ameaça acarretam impacto para o negócio.

A sexta ameaça foi a incapacidade de responder a questionamentos da justiça e por último a única ameaça técnica colocada no questionário: falha em sistema aplicativo. Este fato indica que a proteção técnica é considerada mais eficiente do que proteção contra ações de erro ou má fé das pessoas.

5.3 - Análise dos controles das políticas de segurança da informação

A NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação define 133 controles. Estes controles estão descritos no Anexo 2 – Controles da Norma NBR ISO/IEC 27002:2005.

Foi tomado por base que um controle seria considerado para o padrão mínimo de segurança da informação, quando este controle fosse referenciado por pelo menos 70% das organizações.

Considerando as dez políticas de segurança da informação de organizações distintas, foram identificadas as seguintes referencias de controles:

a) Dezesseis controles (12%) da norma são citados por mais de 80% dos documentos de política de segurança da informação. Doze destes controles são citados por 100% das organizações.

b) Vinte e quatro controles (18%) da norma são citados por mais de 70% dos documentos de política de segurança.

Desta maneira, quarenta controles (30%) da norma são citados por 70% a 100% das organizações pesquisadas.

A Figura 16 abaixo apresenta estes percentuais.

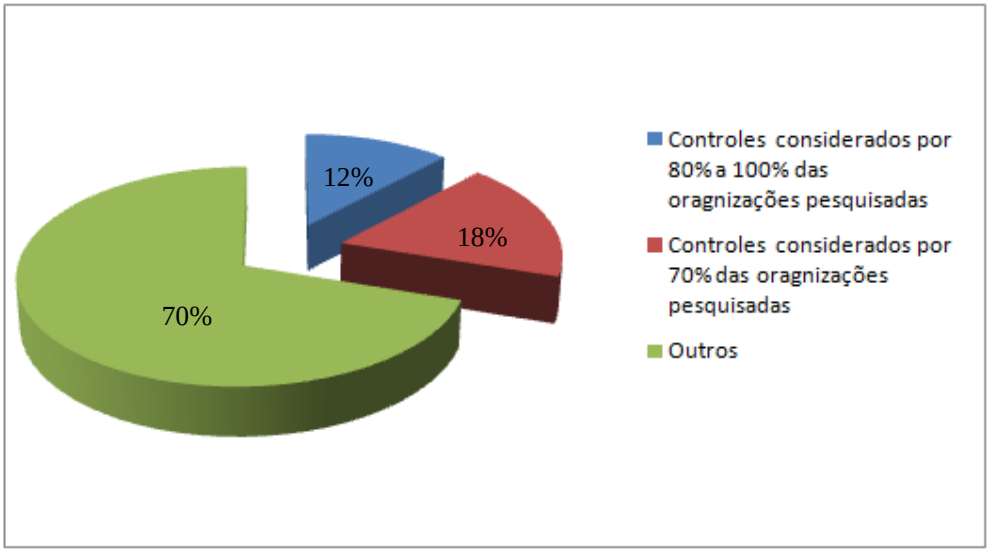


Figura 16 – Percentual da quantidade de controles referenciados em comum pela política de segurança da informação das organizações pesquizadas.
Fonte: Elaborado pelo autor.

A Figura 17 abaixo possui um quadro que detalha todos os controles da norma e a sua referência pelas organizações quando da política de segurança da informação.

Controles em comum nas Políticas	Percentual de Organizações	Quantidade de Controles envolvidos	Controle principal
Controle de acesso à informação	100%	11	11.1.1
Gestão de ativos: Internet, Equipamentos inteligentes, email, outros	100%	1	7.1.3
Classificação da informação	90%	2	7.2.1
Cópias de segurança	90%	1	10.5.1
Monitoramento de uso de sistema	80%	1	10.10.2
Total (80% - 100%)		**16**	**12%**
Política de segurança da informação	70%	2	5.1.1
Conscientização, educação e treinamento	70%	1	8.2.2
Encerramento de atividades: corte de acesso à informação	70%	3	8.3.1
Trabalho remoto	70%	1	11.7.2
Aquisição, Desenvolvimento e Manutenção de sistemas	70%	16	12.1.1
Processo Disciplinar	70%	1	8.2.3
Total (70%)		**24**	**18%**
Total (70% - 100%)		**40**	**30%**
Total de Controles na NBR 27002:2005		**133**	**100%**

Figura 17 – Quadro indicando os controles ou conjunto de controles que são referenciados por 80% a 100% e/ou são referenciados por 70% a 100% das organizações.

Fonte: Elaborado pelo autor.

O Anexo 13 apresenta um quadro detalhado contendo os controles da Norma NBR ISO/IEC 27002:2005 e as referencias existente nas políticas de segurança da informação das organizações pesquisadas.

5.4 – Discussão dos resultados

A pesquisa identificou 40 controles (30%) de controles que devem compor um padrão mínimo de política de segurança da informação.

Esta pesquisa indica que como um Padrão Mínimo de Política de Segurança da Informação, a política da organização deve considerar os elementos descritos no item abaixo.

5.4.1 – Controles que devem compor um Padrão Mínimo de Política de Segurança da Informação.

5.4.1.1 - Controles de acesso lógico à informação

Este controle foi referenciado em 100% pelas políticas consideradas nesta pesquisa. O detalhamento deste controle (itens abaixo) foi citado nas políticas das organizações.

Item Norma	*Descrição*
11.1.1.	Política de controle de acesso.
11.2.1.	Registro de usuário.
11.2.2.	Uso de privilégio – Restrito e controlado
11.2.3.	Gerenciamento de senha do usuário.
11.3.1.	Uso de senhas.
11.4.2.	Autenticação para conexão externa do usuário
11.5.1.	Procedimentos seguros de entrada nos sistema (log on).
11.5.2.	Identificação e autenticação do usuário
11.5.3.	Sistema de gerenciamento de senha
11.5.5.	Limite de tempo de sessão
11.6.1.	Restrição de acesso à informação

5.4.1.2 - Controle de Gestão de ativos

(Internet, Equipamentos inteligentes, email, outros)

Este controle foi referenciado em 100% pelas políticas consideradas nesta pesquisa. Em cada uma das políticas das organizações ficava claro a importância que determinado ativo estava tendo no momento da elaboração da política de segurança. Na medida em que o documento de política detalha mais este controle, indicando o nome da tecnologia do ativo, tipo modelo e fabricante, o documento de política que deveria ser uma diretriz se torna uma norma de um produto.

Porém tona-se evidente que as novas tecnologias geram novos tipos de ativo que são uma preocupação para a proteção da informação e necessitarão de controles específicos.

Todas as organizações definiram regras para a utilização destes tipos de ativo.

Item Norma	*Descrição*
7.1.3.	Uso aceitável dos ativos. (Email e Internet, Mídia portátil, *SmartPhone)*.

5.4.1.3 - Controles de Classificação da informação

Este controle de classificação da informação é citado por 90% das políticas consideradas nesta pesquisa e tem por objetivo possibilitar uma melhor gestão para o sigilo e acesso autorizado da informação.

Item Norma	*Descrição*
7.2.1.	Classificação da informação – Recomendações para classificação.
7.2.2.	Classificação da informação – Rótulos e tratamento da informação.

5.4.1.4 - Controle de Cópias de segurança

Este controle de cópias de segurança da informação é citado por 90% das políticas consideradas nesta pesquisa e tem por objetivo garantir que a organização possua cópias das informações em local alternativo. Em caso de alguma indisponibilidade das informações utilizadas no ambiente principal, existirá uma cópia que possa minimizar a perda de informação.

Uma questão a ressaltar é que este controle é citado em 90% das políticas, porém o controle de continuidade de negócio, que necessita de cópias de segurança, foi citado por 50% das políticas e conseqüentemente não foi selecionado para a o padrão mínimo de política de segurança da informação.

Item Norma	*Descrição*
10.5.1.	Cópias de segurança da informação

5.4.1.5 - Controle de Monitoramento de uso de sistema

Este controle de Monitoramento de uso de sistemas é citado por 80% das políticas consideradas nesta pesquisa e tem por objetivo explicitar, para o usuário, que o acesso feito no ambiente de tecnologia da informação da organização pode ser gravado e monitorado.

No Brasil não existe uma legislação sobre o assunto e a jurisprudência jurídica possibilita que a organização monitore os acessos de seus usuários no seu ambiente, desde que exista uma formalização indicando isto (política de segurança da informação, por exemplo) e que o usuário conheça esta regra. Em função deste fato existe a grande possibilidade deste controle ser no futuro referenciado por todas as organizações.

Item Norma	*Descrição*
10.10.2.	Monitoramento do uso do sistema

5.4.1.6 - Controle da Política de segurança da informação

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa. Ele tem por objetivo explicitar o documento política de segurança da organização e os seus controles de atualização e as responsabilidades em relação a esta política.

Item Norma	*Descrição*
5.1.1.	Documento da política de segurança da informação.
5.1.2.	Análise crítica da política de segurança da informação

5.4.1.7 - Conscientização, educação e treinamento em segurança da informação

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa e tem por objetivo garantir a exigência de um processo de conscientização e treinamento em segurança da informação para todos os usuários.

Item Norma	*Descrição*
8.2.2.	Conscientização, educação e treinamento em SI.

5.4.1.8 - Controle de Encerramento de atividades: corte de acesso à informação

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa e tem por objetivo garantir que quando do encerramento das atividades do usuário com a organização, todos os recursos referentes a este usuário não podem mais ser utilizados por ele. Em comum as políticas que citaram este controle, definem uma diretriz sobre este assunto.

Item Norma	*Descrição*
8.3.1.	Encerramento das atividades.
8.3.2.	Devolução de ativos.
8.3.3.	Retirada de direitos de acesso

5.4.1.9 - Controle de Processo disciplinar

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa e tem por objetivo explicitar que o não cumprimento das regras definidas nas políticas e em outros regulamentos é passível de punição administrativa, contratual, cível e até penal.

Item Norma	*Descrição*
8.2.3.	Processo disciplinar.

5.4.1.10 - Controle de Trabalho remoto

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa e tem por objetivo garantir que o acesso remoto possua o mesmo nível de proteção do acesso local. Este controle deve ser cada vez mais referenciado na medida em que as organizações precisam que seus usuários acessem remotamente as suas informações.

Item Norma	*Descrição*
11.7.2.	Trabalho remoto

5.4.1.11 - Controle de Aquisição, Desenvolvimento e Manutenção de sistemas

Este controle de Política de segurança da informação é citado por 70% das políticas consideradas nesta pesquisa e tem por objetivo cuidar para que a Aquisição, desenvolvimento e manutenção de sistemas aconteçam de uma maneira segura. Este item sempre foi referenciado nas políticas consideradas em forma de diretriz. Porém a definição da diretriz referencia indiretamente os controles da Norma NBR ISO/IEC 27002:2005.

Item Norma	*Descrição*
12.1.1.	Análise e especificação dos requisitos de segurança
12.2.1.	Validação dos dados de entrada.
12.2.2.	Controle do processamento interno
12.2.3.	Integridade de mensagens

12.2.4. Validação dos dados de saída
12.3.1. Política para uso de controles criptográficos
12.3.2. Gerenciamento de chaves.
12.4.1. Controle de software operacional
12.4.2. Proteção dos dados para teste de sistema
12.4.3. Acesso ao código fonte de programa
12.5.1. Procedimentos para controle de mudanças.
12.5.2. Análise crítica técnica aplicações após mudanças s.o.
12.5.3. Restrições sobre mudanças em pacotes de software
12.5.4. Vazamento de informações
12.5.5. Desenvolvimento terceirizado de software
12.6.1. Controle de vulnerabilidades técnicas

5.4.2 – Estrutura dos Elementos que devem compor um Padrão Mínimo de Política de Segurança da Informação.

Tomando por base a ordem dos controles descritos na Norma NBR ISO/IEC 27002:2005, segue abaixo uma estrutura dos elementos que devem compor um Padrão Mínimo de Política de Segurança da Informação:

* Considerações sobre a Política de segurança da informação
* Conscientização, educação e treinamento em segurança da informação
* Gestão de ativos (Internet, equipamentos inteligentes, email, outros)
* Acesso lógico à informação
* Gestão para o trabalho remoto
* Encerramento de atividades do usuário
* Classificação da informação
* Controle de Cópias de segurança
* Aquisição, Desenvolvimento e Manutenção de sistemas
* Monitoramento de uso de sistema
* Responsabilidades e processo disciplinar

6. CONCLUSÃO

Esta pesquisa identificou os elementos que devem compor um padrão mínimo para uma política de segurança da informação de uma organização, tomando por base os elementos comuns de políticas já implantadas em outras organizações. Trinta por cento dos controles definidos na Norma NBR ISO/IEC 27002:2005, de um total de 133 controles são referenciados por mais de dois terços (70%) das políticas pesquisadas.

Considerando este fato, o conjunto destes controles constitui o padrão mínimo de política de segurança da informação de uma organização e responde a questão problema desta pesquisa:

- Quais são os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização?

A pesquisa realizada em dez políticas de segurança da informação referentes a dez organizações de nove segmentos de negócio possibilitou atingir o objetivo proposto neste estudo:

- Identificar os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização tomando por base elementos comuns existentes em políticas de organizações distintas.

Além dos 30% dos controles referenciados por mais de 2/3 das organizações pesquisadas, ficou evidenciado na pesquisa realizada que alguns dos controles da norma são prioridade de todas as organizações. Dois assuntos foram referenciados por 100% das organizações pesquisadas:

- o acesso lógico da informação e
- o uso de recursos (Internet, correio eletrônico, telefones inteligentes, similares).

Os resultados da pesquisa realizada são consistentes em função do porte das organizações consideradas, da variedade dos segmentos de negócio destas

organizações, do tempo de existência da política de segurança em cada uma das organizações e da maturidade dos profissionais responsáveis pelo processo de proteção da informação na organização.

Quando do convite das organizações para a participação da pesquisa, o compromisso da não divulgação do nome da organização e do nome do profissional de segurança da informação, foi fator decisivo para a aceitação da participação. Este fato foi comum para todas as organizações. Todas as organizações que aceitaram participar da pesquisa enviaram suas políticas, porém apenas 80% enviaram as informações sobre o profissional de segurança e sobre a priorização das ameaças.

Com o resultado desta pesquisa as organizações que precisam desenvolver suas políticas de segurança da informação podem começar as mesmas em um patamar avançado ao tomarem como referência o padrão mínimo de política de segurança da informação identificado nesta pesquisa.

A pesquisa contribui com as organizações na medida em que considera que este padrão mínimo seja sempre considerado e que os demais 70% dos controles da Norma devem ser utilizados considerando as peculiaridades de cada organização.

Os profissionais de segurança da informação que tem a responsabilidade de desenvolver a política de segurança da informação para uma organização, contam com esta pesquisa para lhes ajudar na tarefa de construção e implantação da política de segurança da informação baseada na Norma NBR ISO/IEC 27002:2005.

O campo da ciência que estuda as organizações possui com este trabalho uma referência para todos os pesquisadores que precisam desenvolver ações no segmento da segurança da informação para a organização.

Esta pesquisa é relevante para as organizações, pois tratou de um assunto pouco explorado no campo da segurança da informação. Ela possibilita que a Norma NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação, seja tratada de maneira mais

prática pelas organizações que precisam desenvolver a sua política de segurança da informação.

Ficam postas novas questões para futuras pesquisas no campo de políticas de segurança da informação:

* Analisar a relação das organizações que são obrigadas a seguirem legislação nacional ou de outros países e os controles considerados na política de segurança da informação da organização.

* Analisar os controles considerados na política de segurança da informação na organização e o seu grau de maturidade em segurança da informação.

* Pesquisar a relação dos controles descritos na política de segurança da informação e a sua implantação prática na organização.

* Pesquisar o entendimento pelos usuários dos controles considerados na política de segurança da informação da organização.

* Pesquisar a utilização do padrão mínimo de política de segurança da informação descrito nesta pesquisa, em organizações de diferentes portes e atividades.

* Analisar o atendimento a requisitos legais quando a organização utilizar este padrão mínimo de política de segurança da informação.

* Pesquisar o nível de entendimento dos usuários de organizações que utilizem este padrão mínimo de política de segurança da informação em comparação com usuários de organizações que utilizem desde o início um padrão completo de política de segurança da informação.

REFERÊNCIAS

ABNT, **NBR ISO/IEC 27001 Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

____, **NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

____, **NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2008.

____, **NBR ISO/IEC Guia 73 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

____, **NBR 15999-1 – Gestão de continuidade de negócios – Parte 1: Código de prática.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2008.

____, **NBR 15999-2 – Gestão de continuidade de negócios – Parte 2: Requisitos**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2008.

____, **Projeto 78:000.00-19 – Informática em Saúde – Gestão de segurança da informação em saúde usando a ABNT NBR ISO/IEC 27002.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2009.

ALBERTIN, Alberto Luiz; PINOCHET, Luis Hernan Contreras. **Política de Segurança de Informações.** Rio de Janeiro: Elsevier Editora, 2010.

ALBERTIN, Alberto Luiz; MOURA, Rosa Maria (Organizadores). **Tecnologia de Informação**. São Paulo: Editora Atlas, 2004.

ASSIS, Wilson Martins. **Metodologia para a construção de produtos de informação nas organizações.** Belo Horizonte: Universidade Federal de Minas Gerais, Dissertação de Mestrado, Programa de Pós graduação da Escola de Ciência da Informação, 2006

BACIK, Sandy. **Building na Effective Information Security Policy Architecture**. Boca Raton: CRC Press, 2008.

BARMAN, Scott. **Writing Information Security Polices**. Indianapolis: New Riders, 2002.

BEAL, Adriana**. Segurança da Informação**. São Paulo: Editora Atlas, 2005

BENZ, Karl Heinz. **Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI: estudo de casos em**

instituições financeiras. Porto Alegre: Universidade Federal do Rio Grande do Sul, Dissertação de Mestrado, Programa de Pós Graduação em Administração, 2008.

BERNARDES, Mauro Cesar; MOREIRA, Edson dos Santos. **Um Modelo para Inclusão da Governança da Segurança da Informação no Escopo da Governança Organizacional**. In: Simpósio Segurança em Informática - SSI'2005, 2005, São José dos Campos. Anais do Simpósio Segurança em Informática. São José dos Campos: CTA/ITA/IEC, 2005.

BISHOP, Matt**. Introduction to Computer Security.** Boston: Addison-Wesley, 2006.

BRETERNITZ, Vivaldo José; NAVARRO NETO, Francisco; NAVARRO, Alexandre Franco. **Gerenciamento de segurança segundo ITIL: um estudo de caso em uma organização industrial de grande porte.** Revista Eletrônica de Sistemas de Informação, v. 8, n. 2, artigo 4. Curitiba: Editoria Universidade Tecnológica do Paraná, 2009.

BRITO, Mozart José; ANTONIALLI, Luiz Marcelo; SANTOS, Antonio Carlos. **Tecnologia da Informação e Processo Produtivo de Gestão em uma Organização Cooperativa: Um Enfoque Estratégico**. RAC – Revista de Administração Contemporânea, v.1, n.3, Set./Dez., p. 77-95. Rio de Janeiro: ANPAD, 1997.

BROTBY, Krag**. Information Security Governance.** New Jersey: Wiley, 2009.

CALDER, Alan; WATKINS, Steve **IT Governance – A Manager´s Guide to Data Security and BS17799**. London: Editora Kogan Page, 2005.

CARVALHO, Júlio Luiz Nunes. **O Problema da Proteção e Controle de Acesso à Informação – Proteção Digital e Vigilância do Ambiente Operacional de um Módulo Criptográfico.** Rio de Janeiro: Universidade Federal do Rio de Janeiro-UFRJ, Tese de Doutorado, Programa de Pós Graduação em Engenharia Civil, 2007.

CAVALCANTE, Sayonara de Medeiros. **Segurança da informação no correio eletrônico baseada na ISO/IEC 17799: um estudo de caso em uma instituição de ensino superior, com foco no treinamento.** Natal: Universidade Federal do Rio Grande do Norte, Dissertação de Mestrado, Programa de Engenharia de Produção, 2003.

CARUSO, Carlos; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações.** São Paulo: Editora SENAC, 1999.

CHIAVENATTO, Idalberto. **Administração – Teoria, Processo e Prática**. Rio de Janeiro: Elsevier Editora, 2010.

DOMENEGHETTI, Daniel; MEIR, Roberto. **Ativos Intangíveis**. Rio de Janeiro: Elsevier Editora, 2009.

DEY M. **Information security management – a practical approach**. In: Africon 2007 – 8th IEEE Africon Conference 2007. p. 1-6.

ELLWANGER, Cristiane. **Impacto da utilização das técnicas de endomarketing na efetividade das políticas de segurança da informação**. Santa Maria: Universidade Federal de Santa Maria, Dissertação de Mestrado, Programa de Pós Graduação em Engenharia de Produção, 2009.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu. **Política de Segurança da Informação.** Rio de Janeiro: Editora Ciência Moderna, 2008.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna, 2003

FREITAS, Henrique; KLADIS, Constantin Metaxa. **Da informação à política informacional das organizações: um quadro conceitual.** São Paulo: RAP, v.29, n. 03, Junho-Setembro 1995, p. 73-86.

GIL, Antonio Loureiro. **Segurança em Informática**. São Paulo: Editora Atlas, 1994.

HANSCHE, Susan; BERTI, John; HARE, Chris. **Official Guide to CISSP Exam**. USA: Auerbach, 2004.

HEROLD, Rebecca. **Managing Information Security and Privacy**. USA: Auerbach, 2005.

IBGC, **Código das melhores práticas de governança corporativa**. São Paulo: Instituto Brasileiro de Governança Corporativa, 4a ed. 2009.

IKENAGA, Cristiane Yayoko. **Gestão da terceirização dos serviços de TI: um estudo de caso.** São Paulo: Centro Estadual de Educação Tecnológica Paula Souza, Dissertação de Mestrado, Programa de Pós Graduação em Tecnologia, 2008.

ISACA**, Information System Audit and Control Association**, http://www.isaca.org/ acesso em 27/12/2010.

ITGI, **COBIT – Control Objectives for Information and related Technology**, 4th edition, Rolling Meadows, Ilinois – USA: Information Technology Governance Institute, 2007.

____, **Information Security Governance: Guidance for Board Directors and Executive Management**, 2nd Edition, Rolling Meadows, Ilinois – USA: Information Technology Governance Institute, 2006.

____, **Information Security Governance: Guidance for Information Security Managers**, 2nd Edition, Rolling Meadows, Ilinois – USA: Information Technology Governance Institute, 2008.

KARABACAK B., SOGUKPINAR I. Isram: **Information risk security analysis method**. J Comput Secur. 2005.

LANDOLL, Douglas. **The Security Risk Assessment Handbook**. USA: Auerbach, 2006.

LAUREANDO, Marcos Aurélio Pchek; MORAES, Paulo Eduardo Sobreira. **Segurança como estratégia de gestão da informação**. Revista Economia & Tecnologia, v. 08, f. 03, p 38-44. São Paulo: FATEC, 2005.

LOBO, Maria Celeste Reis; JAMIL, George Leal. **Proteção do conhecimento: análise dos impactos positivos e negativos do vazamento de conhecimento de empresas no Brasil e no Reino Unido.** Revista Perspectiva em Ciência da Informação, v.13, n.3, p. 96-115, set/dez. Belo Horizonte: Escola de Biblioteconomia – UFMG, 2008.

LORENS, Evandro. **Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação.** Brasília: Universidade de Brasília, Dissertação de Mestrado, Departamento de Ciência da Informação e Documentação, 2007.

MARTINS, Alaíde Barbosa; SANTOS, Carlos Alberto Saibel. **Uma metodologia para implantação de um sistema de gestão de segurança da informação.** Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 2, No. 2, p. 121-136. São Paulo: FEA-USP, 2005.

MAXIMINIANO, Antonio Cesar Amaru**. Introdução à Administração**. São Paulo: Editora Atlas, 2010.

MENEZES, Josué das Chagas**. Gestão da segurança da informação: análise em três organizações brasileiras.** Salvador: Universidade Federal da Bahia, Dissertação de Mestrado, Núcleo de Pós Administração em Administração, 2005.

NEVES, Geraldo de Oliveira Santos. **Código Civil Brasileiro De 2002-Principais Alterações.** Curitiba: Editora Juruá, 2003.

OCG, **ITIL - Information Technology Infrastructure Library – Service Design**, 3rd edition, London: OCGE, 2007.

OLIVEIRA Jr., Renato Salatiel. **Utilizando a norma ISO 27002 para atender os requisitos da SOX que exigem proteção da informação no ambiente de TI.** São Paulo: Faculdade de Informática e Administração Paulista, Pós-Graduação em Gestão de Segurança da Informação, 2010.

PAGE, Stephen. **Achieving 100% Compliance of Policies and Procedures**. Westerville: Process Improvement Publishing, 2000.

_____. **Estabilishing a System of Policy and Procedures**. Westerville: Process Improvement Publishing, 2002.

PELTIER, Thomas. **Information Security Fundamentals.** USA: Auerbach, 2005.

_____. **Information Security Policies and Procedures.** USA: Auerbach, 2004.

_____. **Information Security Risk Analysis**. USA: Auerbach, 2001.

PEREIRA, Anísio Cândido; NASCIMENTO, Wesley Souza. **Um estudo sobre a atuação da auditoria interna na detecção de fraudes nas empresas do setor privado do Estado de São Paulo.** Revista Brasileira de Gestão de Negócios. FECAP, ano 7, n. 19, set-dez. São Paulo: FECAP, 2005.

PRICEWATERHOUSECOOPERS**. Pesquisa Global de Segurança da Informação 2011.** São Paulo: PricewaterhouseCoopers, 2010.

RIBAS, Carlos Eduardo. **Sistema de gestão da segurança da informação em organizações na área de saúde.** São Paulo: Universidade de São Paulo-USP, Dissertação de Mestrado, Faculdade de Medicina, 2010.

ROZA, Fabiana Freitas Furtado. **Política de segurança da informação em ambientes hospitalares.** São Caetano do Sul: Faculdade de Tecnologia,Trabalho de Conclusão de Curso de Graduação de Tecnologia em Segurança da Informação, 2010.

SALES, Rodrigo; ALMEIDA, Patrícia Pinheiro. **Avaliação de fontes de informação na Internet: avaliando o site NUPILL/UFSC.** Revista Digital de Biblioteconomia e Ciência da Informação, Campinas, v. 4, n. 2, p. 67-87, jan./jun. 2007 – ISSN: 1678-765X. Campinas: Unicamp, 2007.

SCUDERE, Leonardo. **Risco Digital**. Rio de Janeiro: Elsevier Editora, 2007

SEMOLA, Marcos. **Gestão da Segurança da Informação**. São Paulo. Editora Campos, 2003.

SHERWOOD, John; CLARK, Andrew; LYNAS, David. **Enterprise Security Architecture.** USA: CMP Books, 2005.

SHOSTACK, Adam; STEWART, Andrew. **A Nova Escola da Segurança da Informação.** Rio de Janeiro: Alta Books, 2008.

SILVA, Terezinha Elisabeth; TOMAÉL, Maria Inês. **Gestão da Informação nas Organizações.** Revista Informação&Informação, No. 12. Londrina: Universidade Estadual de Londrina, 2007.

SILVA NETTO, Abner; SILVEIRA, Marco Antonio Pinheiro**. Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas.** Revista de Gestão da Tecnologia e Sistemas de Informação, Vol. 4, No. 3, 2007, p. 375-397. São Paulo: FEA-USP, 2007.

TÉBOUL, James. **A era dos serviços – Uma abordagem de gerenciamento**.

São Paulo: Quality Market, 1999.

VENTURINI, Yeda Regina. **Modelo Ontológico de segurança para negociação de política de controle de acesso em multidomínios**. São Paulo: Universidade de São Paulo-USp, 2006.

VIANEZ, Marcos S.; SEGOBIA, Roberta H.; CAMARGO, Vander. **Segurança de Informação: Aderência à Norma ABNT NBR ISO/IEC N. 17.799:2005**. Revista de Informática Aplicada (Journal of Applied Computing), Vol. IV - Nº 01 - Jan/Jun, São Caetano do Sul: USCS, 2008.

YIN, Robert. **Estudo de Caso**. São Paulo: Bookman, 2010.

WERTHEIN, Jorge**. A sociedade da informação e seus desafios**. Revista Eletrônica de Sistemas de Informação, v. 29, n. 2, p. 71-77, maio/agosto. Brasília: C.Inf., 2000.

WYLDER, John. **Strategic Information Security**. USA: Auerbach, 2004.

WOOD, Charles. **Information Security Policies Made Easy**. Houston: Information Shild, 2005.

ANEXO 1 - Quarenta e nove trabalhos selecionados.

Instituição	Tipo	Ano	Título	Autor(es)	Prioridade	Observações
Presidência da República	Decreto 3505	2000	Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal	Casa Civil	1	
FGV-RJ	Mestrado	2009	CULTURA DE SEGURANÇA DA INFORMAÇÃO: UM PROCESSO DE MUDANÇA ORGANIZACIONAL NA PETROBRAS	Patricia dos Santos Vieira	3	
Fundação João Pinheiro-MG	Mestrado	2002	SEGURANÇA DA INFORMAÇÃO UM MAPEAMENTO TEÓRICO E A PRÁTICA NAS EMPRESAS DE TELECOMUNICAÇÕES NO BRASIL	Caio Julio Martins Veloso	3	
Fundação João Pinheiro-MG	Mestrado		REGULAMENTAÇÃO DA POLÍTICA DE SEGURANAÇA DA INFORMAÇÃO DO GOVERNO ELETRÔNICO FEDERAL: ESTUDO COMPARADO BRASIL e CANADÁ. (3)	Kamila Araújo Rola Fontes Moreir		Texto não disponível. Link com problema. Governo eletronico
METROSUL IV – IV Congresso Latino-Americano de Metrologia	Artigo	2004	O CONTROLE DE DOCUMENTOS MANTIDOS EM MEIO ELETRÔNICO E OS REQUISITOS DA NBR ISO/IEC 17025	Anselmo Ferreira de Castro, Glória Maria Pereira da Silva, Silvio Francisco dos Santos	3	
IPEN-USP	Doutorado	2009	GESTÃO DA SEGURANÇA DA INFORMAÇÃO – UMA PROPOSTA PARA POTENCIALIZAR A EFETIVIDADE DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DE PESQUISA CIENTIFICA	João Carlos Soares de Alexandria	2	
Instituto Superior de Ciencias do trabalho e da Empresa - Portugal	Mestrado	2008	FACTORES DE SUCESSO NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO NAS EMPRESAS PORTUGUESAS	Luis Manuel Franco dos Santos	2	
Universidade Presbiteriana Mackenzie	Mestrado	2008	UM MÉTODO DE CLASSIFICAÇÃO EM GRUPOS DE INFORMAÇÕES VISANDO SUA SEGURANÇA	José Antonio Corrales Torres	3	
Universidade Católica de Brasília	Mestrado	2007	A PERCEPÇÃO GERENCIAL SOBRE UM MODELO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO DE UMA EMPRESA PÚBLICA DE TIC: PERSPECTIVA DE EVOLUÇÃO PARA UM MODELO DE GOVERNANÇA.	Maria do Carmo Soares de Mendonça	2	
PUC-CAMP	Mestrado	2009	GESTÃO DA SEGURANÇA DA INFORMAÇÃO: UM OLHAR A PARTIR DA CIÊNCIA DA INFORMAÇÃO	Claudete Aurora da Silva	3	
PUC-CAMP	Mestrado	2007	CONTRIBUIÇÃO DA CIÊNCIA DA INFORMAÇÃO PARA A CRIAÇÃO DE UM PLANO DE SEGURANÇA DA INFORMAÇÃO	Isaías de Queiroz Ramos	3	
PUC-RS	Mestrado	2008	INSTRUMENTO DE AVALIAÇÃO DE MATURIDADE EM PROCESSOS DE SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO EM INSTITUIÇÕES HOSPITALARES.	Luis Antonio Janssen	2	Editora Saraiva
SBC	Artigo	2008	CORESEC: UMA ONTOLOGIA COMO FERRAMENTA EDUCACIONAL PARA O APIO NO ENSINO DE DISCIPLINAS DE SEGURANÇA DA INFORMAÇÃO	Ryan Ribeiro de Azevedo e outros	3	
PUC-Brasília	Mestrado	2008	GESTÃO SEGURA DO CONHECIMENTO: DIRETRIZES ORGANIZACIONAIS PARA A PROTEÇÃO DO CONHECIMENTO	Américo Borghi Moreira Jacinto	3	
Caderno Pesquisas NPGA-Salvador/BA	Artigo	2006	CLIMA ORGANIZACIONAL DO PLANEJAMENTO ESTRATÉGICO CORPORATIVO: ESTRATÉGIA NA OBTENÇÃO DE RESULTADOS	Paulo Roberto Pereira Ruchinski	3	
UFBA	Mestrado	2005	A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES EM SALVADOR	Bianca Capelato Lucas	2	
UFBA	Mestrado	2005	GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ANÁLISE DE TRÊS ORGANIZAÇÕES BRASILEIRAS(2)	Josué das Chagas Menezes	2	Percepção dos empregados. Considera a política de SI
UFF	Mestrado	2008	SUBSÍDIOS PARA UMA POLÍTICA DE GESTÃO DA INFORMAÇÃO DA EMBRAPA SOLOS - À LUZ DO REGIME DE INFORMAÇÃO	Claudia Regina Delaia	2	
UFPB	Mestrado	2009	DIMENSÕES DA GESTÃO DA INFORMAÇÃO NO CAMPO DA CIENCIA DA INFORMAÇÃO: UMA REVELAÇÃO DA PRODUÇÃO CIENTÍFICA DO ENANCIB	Irma Gracielle dos Santos Carvalho de Oliveira	3	
UFRS	Mestrado	2004	SITEMA DE GERENCIAMENTO DE SEGURANÇA DE INFORMAÇÕES: PROCESSO DE AUDITORIA	Fábio Natonio Pizzoli	3	
UFRS	Mestrado	2006	GESTÃO DE SEGURANÇA DA INFORMAÇÃO: IMPLEMENTAÇÃO DA NORMA BS7799-2:2002 EM UMA INSTITUIÇÃO FINANCEIRA	Guilherme Gonçalves Lessa	2	
UFRS	Mestrado	2008	ALINHAMENTO ESTRATÉGICO ENTRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E AS ESTRATÉGIAS E PRÁTICAS ADOTADAS NA TI: ESTUDOS DE CASOS EM INSTITUIÇÕES FINANCEIRAS (1)	Karl Heinz Benz	2	
UFSC	Artigo	2009	CONTROLES DE GESTÃO: UMA CONTRIBUIÇÃO AO ESTUDO DOS PRINCIPAIS MODELOS	Marcelo Dutra e Outros	3	
UFSM	Artigo	2009	O CONTROLE DE ACESSO NA PERCEPÇÃO DOS PROFISSIONAIS DE ARQUIVO: UMA QUESTÃO DE SGURANÇA DAS INFORMAÇÕES INSTITUCIONAIS	Josiane Ayres Sfreedo e Daniel Flores	3	
UFSM	Mestrado	2009	IMPACTO DA UTILIZAÇÃO DE TÉCNICAS DE ENDOMARKETING NA EFETIVIDADE DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (5)	Cristiane Ellwanger	3	Investiga o impacto do uso de técnicas de endo marketing na efetividade da PSI Política de Segurança da Informação. Utiliza uma pesquisa experimental em duas unidades de hospital. Cita meu livro Editora Saraiva.
UFSM	Mestrado	2009	IMPLANTAÇÃO DE UMA GESTÃO DE SEGURANÇA DA INFORMAÇÃO ATRAVÉS DA ABORDAGEM SEIS SIGMA	Maria Angélica Figueredo Oliveira	2	
UFSM	Mestrado	2010	UM MODELO CONCEITUAL PARA ESPECIFICAÇÃO DA GESTÃO DE RISCOS DE SEGURANÇA EM SISTEMNAS DE INFORMAÇÃO	Josiane Kroll	3	
Universidade do Minho - Portugal	Mestrado	2008	FRAMEWORK DE SEGURANÇA DE UM SISTEMA DE INFORMAÇÃO	José Carlos Lourenço Martins	2	
UNB	Artigo	2006	O ENFOQUE SOCIAL DA SEGURANÇA DA INFORMAÇÃO	João Luiz Marciano e Mamede Lima Marques	3	
UNB	Artigo	2007	GERENCIAMENTO ESTRATÉGICO DA INFORMAÇÃO: A CONVERGÊNCIA A PARTIR DA SOCIEDADE DA INFORMAÇÃO	Rogério henrique de Araújo Junior e Lilian Alvares	2	
UNB	Doutorado	2009	A SEGURANÇA DO CONHECIMENTO NAS PRÁTICAS DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E DA GESTÃO DO CONHECIMENTO	Wagner Junqueira de Araújo	3	
UNB	Mestrado	2007	O DIREITO À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO	Tatiana Malta Vieira	3	
UNB	Mestrado	2004	POLÍTICA DE PRESERVAÇÃO DE INFORMAÇÃO DIGITAL EM BIBLIOTECAS UNIVERSITÁRIAS BRASILEIRAS	Sonia Araújo de Assis Boeres	1	
UNB	Mestrado	2007	ASPECTOS NORMATIVOS DA SEGURANÇA DA INFORMAÇÃO: UM MODELO DE CADEIA DE REGULAMENTAÇÃO(6)	Evandro Mário Lorens	1	Preocupa-se com a implantação da segurança da informação.
UNB	Mestrado	2008	PROPOSTA DE METODOLOGIA DE GESTÃO DE RISCO EM AMBIENTES CORPORATIVOS NA ÁREA DE TI	Laerte Peotta de Melo	2	
UNB	Mestrado	2008	UM MODELO FASEADO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO	Leandro Ramalho Frósio	2	
UNB	Mestrado	2008	SEGURANÇA DA INFORMAÇÃO PARA O SISTEMA DE MEDIÇÃO DE FATURAMENTO NO SETOR ELÉTRICO	Wilson Miranda Junior	3	
UNB	Mestrado	2008	PROTEÇÃO DO CONHECIMENTO: UMA PROPOSTA DE FUNDAMENTAÇÃO TEÓRICA	Marta Sianes Oliveira Nascimento	3	
UNB	Pós Graduação	2009	SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: CONCEITO APLICÁVEL EM ORGANIZAÇÕES GOVERNAMENTAIS	Reinaldo Silva Simeão	2	
UNINOVE - EccoS Revista Científica	Artigo	2000	RESENHA DE SEGURANÇA DA INFORMAÇÃO: UM CAMINHO ESTRATÉGICO PARA A CONTINUIDADE DE NEGÓCIO	Waldir Antonio da Silva	3	
USP	Doutorado	2009	ESTUDO DAS PRÁTICAS DE GOVERNAÇA ELETRÔNICA: INSTRUMENTO DE CONTROLADORIA PARA A TOMADA DE DECISÕES NA GESTÃO DOS ESTADOS BRASILEIROS.	Gilmar Ribeiro de Mello	3	
USP	Mestrado	1981	SEGURANÇA EM PROCESSAMENTO DE DADOS	Edson Luiz Riccio	3	
Universidade de Taubaté	Mestrado	2008	O GERENCIAMENTO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO: APLICABILIDADE DA NORMA ISO 20000 EM UMA INSTITUIÇÃO PÚBLICA DE ENSINO	Carlos Kóji Morikane	4	
UFRN	Mestrado	2004	PUPSI: UMA PROPOSTA DE PROCESSO UNIFICADO PARA POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO	Ivano Miranda dos Santos	1	
UFRN	Mestrado	2009	FATORES QUE INFLUENCIA A ACEITAÇÃO DE PRÁTICAS AVANÇADAS DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO COM GESTORES ESTADUAIS DO BRASIL	Anna Claudia dos Santos Nobre	1	
UFRN	Mestrado	2003	FATORES INFLUENCIADORES NA IMPLANTAÇÃO DE AÇÕES DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO COM EXECUTIVOS E GERENTES DE TECNOLOGIA DA INFORMAÇÃO DO ESTADO DO RIO GRANDE DO NORTE	Max Simon Gabbay	1	
UFRN	Mestrado	2009	ASPECTOS DO GERENCIAMENTO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO NAS EMPRESAS: UM ESTUDO DE CASO MÚLTIPLOS	Alexandre Thiago de Santana	3	
UFRN	Mestrado	2003	SEGURANÇA DA INFORMAÇÃO NO CORREIO ELETRÔNICO BASEADA NA ISSO/IEC 17799: UM ESTUDO DE CASO EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR COM FOCO NO TREINAMENTO.(4)	Sayonara de Medeiros Cavalcante	2	Identifica a importancia que o treinamento do usuário tem sobre as políticas de segurança das informações nas empresas, através de um estudo de caso.
Instituto Superior Tupy - Joinville-SC	Bacharelado	2004	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - DESENVOLVIMENTO DE UM MODELO VOLTADO PARA INSTITUIÇÃO DE ENSINO (7)	Francini Reitz Spanceski		

ANEXO 2 - Controles da NBR ISO/IEC 27002:2005

Capítulo 5 – Política de segurança da informação

(1) Controle: Documento da política de segurança da informação.

> *5.1.1*
> *Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado para todos os funcionários e partes externas relevantes.(ABNT, 2005, p.8)*

(2) Controle: Análise crítica da política de segurança da informação.

> *5.1.2*
> *Convém que a política de segurança da informação seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua continua pertinência, adequação e eficácia. .(ABNT, 2005, p.9)*

Capítulo 6 – Organizando a segurança da informação

Estabelece uma estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação dentro da organização.

Controles definidos neste capítulo:

(3) Controle: Comprometimento da direção com a segurança da informação.

> *6.1.1*
> *Convém que a direção apóie ativamente a segurança da informação dentro da organização por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação. .(ABNT, 2005, p.10)*

Este controle tem relação direta com a política de segurança da informação, pois é pelo direcionamento da direção da organização que a política pode ser definida e estabelecida.

(4) Controle: Coordenação da segurança da informação.

> *6.1.2*
> *Convém que as atividades da segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes. (ABNT, 2005, p.11)*

(5) Controle: Atribuição de responsabilidades para a segurança da informação.

> *6.1.3*
> *Convém que todas as responsabilidades pela segurança da informação estejam claramente definidas. (ABNT, 2005, p.11)*

(6) Controle: Processo de autorização para os recursos de processamento da informação.

> *6.1.4*
> *Convém que seja definido e implementado um processo de gestão de autorização para novos recursos de processamento de informação. (ABNT, 2005, p.12)*

(7) Controle: Acordos de confidencialidade.

> *6.1.5*
> *Convém que os requisitos para a confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação sejam identificados e analisados criticamente de forma regular. (ABNT, 2005, p.12)*

(8) Controle: Contato com autoridades.

> *6.1.6*
> *Convém que contatos apropriados com autoridades pertinentes sejam mantidos. (ABNT, 2005, p.13)*

(9) Controle: Contato com grupos especiais.

> *6.1.7*
> *Convém que sejam mantidos contatos apropriados com grupos de interesses especiais ou outros fóruns especializados de segurança da informação e associações profissionais. (ABNT, 2005, p.14)*

(10) Controle: Análise crítica independente de segurança da informação.

> *6.1.8*
> *Convém que o enfoque da organização para gerenciar a segurança da informação e a sua implementação (por exemplo, controles, objetivos dos controles, políticas, processos e procedimentos para a segurança da*

> *informação) seja analisado criticamente de forma independente, a intervalos planejados, ou quando ocorrerem mudanças significativas relativas à implementação da segurança da informação. (ABNT, 2005, p.14)*

(11) Controle: Identificação dos riscos relacionados às partes externas.

> *6.2.1*
> *Convém que os riscos para os recursos de processamento da informação e da informação da organização oriundos de processos do negócio que envolva as partes externas sejam identificados e controles apropriados implementados antes de se conceder o acesso. (ABNT, 2005, p.15)*

(12) Controle: Identificando a segurança da informação, quando tratando com os clientes.

> *6.2.2*
> *Convém que todos os requisitos de segurança da informação identificados sejam considerados antes de conceder aos clientes o acesso aos ativos ou às informações da organização. (ABNT, 2005, p.17)*

(13) Controle: Identificando a segurança da informação nos acordos com terceiros.

> *6.2.3*
> *Convém que os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação cubram todos os requisitos de segurança da informação relevantes. (ABNT, 2005, p.18)*

Capítulo 7 – Gestão de ativos

Estabelece responsabilidades pelos ativos da organização.

Controles definidos neste capítulo:

(14) Controle: Inventário dos ativos.

> *7.1.1*
> *Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido. (ABNT, 2005, p.21)*

(15) Controle: Proprietário dos ativos.

> *7.1.2*
> *Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário designado por uma parte definida pela organização.*
> *Obs: O termo "proprietário" identifica uma pessoa ou organismo que tenha uma responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança dos ativos. O termo "proprietário" não significa que a pessoa realmente tenha qualquer direito de propriedade do ativo. (ABNT, 2005, p.22)*

(16) Controle: Uso aceitável dos ativos.

> *7.1.3*
> *Convém que sejam identificadas, documentadas, e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação. (ABNT, 2005, p.22)*

(17) Controle: Classificação da informação – Recomendações para classificação.

> *7.2.1*
> *Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização. (ABNT, 2005, p.23)*

(18) Controle: Classificação da informação – Rótulos e tratamento da informação.

> *7.2.2*
> *Convém que um conjunto apropriado de procedimentos para a rotulação e tratamento da informação seja definido e implementado de acordo com o esquema de classificação adotado pela organização. (ABNT, 2005, p.24)*

Capítulo 8 – Segurança em recursos humanos

Estabelece responsabilidades para assegurar que os funcionários, fornecedores e terceiros entendam as suas responsabilidades em segurança da informação para com a organização.

Controles definidos neste capítulo:

(19) Controle: Segurança em recursos humanos – Papéis e responsabilidades.

> *8.1.1*
> *Convém que papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros, sejam definidos e documentados de acordo com a política de segurança da informação. (ABNT, 2005, p.25)*

(20) Controle: Segurança em recursos humanos – Seleção.

> *8.1.2*
> *Convém que verificações do histórico de todos os candidatos a emprego, fornecedores e terceiros sejam realizados de acordo com a ética, as leis e as regulamentações pertinentes, e proporcionais aos requisitos do negócio, à classificação das informações a serem acessadas e aos riscos percebidos. (ABNT, 2005, p.26)*

(21) Controle: Segurança em recursos humanos – Termos e condições de contratação.

> *8.1.3*
> *Como parte de suas obrigações contratuais, convém que os funcionários, fornecedores e terceiros concordem e assinem os termos e condições de sua contratação para o trabalho, os quais devem declarar as suas responsabilidades e a da organização para a segurança da informação. (ABNT, 2005, p.26)*

(22) Controle: Segurança em recursos humanos – Responsabilidades da direção.

> *8.2.1*
> *Convém que a direção solicite aos funcionários, fornecedores e terceiros que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização. (ABNT, 2005, p.28)*

(23) Controle: Segurança em recursos humanos – Conscientização, educação e treinamento em segurança da informação.

> *8.2.2*
> *Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriados em conscientização e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções. (ABNT, 2005, p.28)*

(24) Controle: Segurança em recursos humanos – Processo disciplinar.

> *8.2.3*
> *Convém que exista um processo disciplinar formal para os funcionários que tenham cometido uma violação da segurança da informação. (ABNT, 2005, p.29)*

(25) Controle: Segurança em recursos humanos – Encerramento das atividades.

> *8.3.1*
> *Convém que responsabilidades para realizar o encerramento ou a mudança de um trabalho sejam claramente definidas e atribuídas. (ABNT, 2005, p.30)*

(26) Controle: Segurança em recursos humanos – Devolução de ativos.

> *8.3.2*
> *Convém que todos os funcionários, fornecedores e terceiros devolvam todos os ativos da organização que estejam em sua posse, após o encerramento de suas atividades, do contrato ou acordo. (ABNT, 2005, p.30)*

(27) Controle: Segurança em recursos humanos – Retirada de direitos de acesso.

> *8.3.3*
> *Convém que os direitos de acesso de todos os funcionários,fornecedores e terceiros às informações e aos recursos de processamento de informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustados após a mudança destas atividades. (ABNT, 2005, p.30)*

Capítulo 9 – Segurança física e do ambiente

Estabelece responsabilidades para o ambiente físico de maneira que este ambiente seja protegido de maneira compatível com os riscos identificados.

Controles definidos neste capítulo:

(28) Controle: Segurança física – Perímetro de segurança física.

> *9.1.1*
> *Convém que sejam utilizados 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. (ABNT, 2005, p.32)*

(29) Controle: Segurança física – Controles de entrada física.

> *9.1.2*
> *Convém que as áreas seguras sejam protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso. (ABNT, 2005, p.33)*

(30) Controle: Segurança física – Segurança em escritórios, salas e instalações.

> *9.1.3*
> *Convém que seja projetada e aplicada segurança física para escritórios, salas e instalações. (ABNT, 2005, p.33)*

(31) Controle: Segurança física – Proteção contra ameaças externas e do meio ambiente.

> *9.1.4*
> *Convém que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem. (ABNT, 2005, p.34)*

(32) Controle: Segurança física – Trabalhando em áreas seguras.

> *9.1.5*
> *Convém que seja projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras. (ABNT, 2005, p.34)*

(33) Controle: Segurança física – Acesso do público, áreas de entrega e de carregamento

> *9.1.6*
> *Convém que os pontos de acesso, tais como de entrega e de carregamento e outros pontos em que pessoas não autorizadas possam entrar nas instalações, sejam controladas e, se possível, isoladas das suas instalações de processamento da informação, para evitar o acesso não autorizado. (ABNT, 2005, p.35)*

(34) Controle: Segurança física – Instalação e proteção de equipamento.

> *9.2.1*
> *Convém que os equipamentos sejam colocados no local ou protegidos para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizados. (ABNT, 2005, p.35)*

(35) Controle: Segurança física – Utilidades.

> *9.2.2*
> *Convém que os equipamentos sejam protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas das utilidades. (ABNT, 2005, p.36)*

(36) Controle: Segurança física – Segurança do cabeamento

> *9.2.3*
> *Convém que cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações seja protegido contra a interceptação ou danos. (ABNT, 2005, p.37)*

(37) Controle: Segurança física – Manutenção dos equipamentos

> *9.2.4*
> *Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanentes. (ABNT, 2005, p.38)*

(38) Controle: Segurança física – Segurança de equipamentos fora das dependência da organização.

> *9.2.5*
> *Convém que sejam tomadas medidas de segurança para equipamentos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização. (ABNT, 2005, p.38)*

(39) Controle: Segurança física – Reutilização e alienação segura de equipamentos.

> *9.2.6*
> *Convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobre gravados com segurança. (ABNT, 2005, p.39)*

(40) Controle: Segurança física – Remoção de propriedade

> *9.2.7*
> *Convém que equipamentos, informações ou softwares não sejam retirados do local sem autorização prévia. (ABNT, 2005, p.39)*

Capítulo 10 – Gerenciamento das operações e comunicações

Estabelece responsabilidades para garantir que a operação dos recursos de processamento de informação aconteça de maneira segura e correta.

Controles definidos neste capítulo:

(41) Controle: Operações e Comunicações – Documentação dos procedimentos.

> *10.1.1*
> *Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem. (ABNT, 2005, p.40)*

(42) Controle: Operações e Comunicações – Gestão de mudanças.

> *10.1.2*
> *Convém que modificações nos recursos de processamento da informação e sistemas sejam controlados. (ABNT, 2005, p.41)*

(43) Controle: Operações e Comunicações – Segregação de funções.

> *10.1.3*
> *Convém que funções e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização. (ABNT, 2005, p.41)*

(44) Controle: Operações e Comunicações – Separação dos recursos de desenvolvimento, teste e de produção.

> *10.1.4*
> *Convém que recursos de desenvolvimento, teste e produção sejam separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais. (ABNT, 2005, p.42)*

(45) Controle: Operações e Comunicações – Entrega de serviço.

> *10.2.1*
> *Convém que seja garantido que os controles de segurança, as definições de serviço e os níveis de entrega incluídos no acordo de entrega de serviços terceirizados sejam implementados, executados e mantidos pelo terceiro. (ABNT, 2005, p.43)*

(46) Controle: Operações e Comunicações – Monitoramento e análise crítica de serviços terceirizados.

> *10.2.2*
> *Convém que os serviços, relatórios e registros fornecidos por terceiros sejam regularmente monitorados e analisados criticamente, e que auditorias sejam executadas. (ABNT, 2005, p.43)*

(47) Controle: Operações e Comunicações – Gerenciamento de mudanças para serviços terceirizados.

> *10.2.3*
> *Convém que mudanças no provisionamento dos serviços, incluindo manutenção e melhoria da política de segurança da informação, procedimentos e controles existentes, sejam gerenciadas levando-se em conta a criticidade dos sistemas e processos de negócios envolvidos e a reanálise/reavaliação de riscos. (ABNT, 2005, p.44)*

(48) Controle: Operações e Comunicações – Gestão de capacidade.

> *10.3.1*
> *Convém que a utilização dos recursos seja monitorada e ajustada, e as projeções feitas para necessidades de capacidade futura, para garantir o desempenho requerido sistema. (ABNT, 2005, p.45)*

(49) Controle: Operações e Comunicações – Aceitação de sistemas.

> *10.3.2*
> *Convém que sejam estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e que sejam efetuados testes apropriados do(s) sistemas(s) durante o desenvolvimento e antes da sua aceitação. (ABNT, 2005, p.45)*

(50) Controle: Operações e Comunicações – Proteção contra códigos maliciosos e códigos móveis.

> *10.4.1*
> *Convém que sejam implantados controles de detecção, prevenção e recuperação para proteger contra códigos maliciosos, assim como procedimentos para a devida conscientização do usuário. (ABNT, 2005, p.46)*

(51) Controle: Operações e Comunicações – Controles contra códigos móveis.

> *10.4.2*
> *Onde o uso de códigos móveis é autorizado, convém que a configuração garanta que o código móvel autorizado opere de acordo com uma política de segurança da informação claramente definida e códigos móveis não autorizados tenham sua execução impedida. (ABNT, 2005, p.47)*

(52) Controle: Operações e Comunicações – Cópias de segurança da informação.

> *10.5.1*
> *Convém que as cópias de segurança da informação e dos softwares sejam efetuadas, testadas regularmente conforme a política de geração de cópias de segurança definida. (ABNT, 2005, p.48)*

(53) Controle: Operações e Comunicações – Controles de redes.

> *10.6.1*
> *Convém que as redes sejam adequadamente gerenciadas e controladas, de forma a protegê-las contra ameaças e manter a segurança de sistemas e aplicações que utilizam estas redes, incluindo a informação em trânsito. (ABNT, 2005, p.49)*

(54) Controle: Operações e Comunicações – Segregação dos serviços de rede.

> *10.6.2*
> *Convém que as características de segurança, níveis de serviço e requisitos de gerenciamento de serviços de rede sejam identificados e incluídos em qualquer acordo de serviços de rede, tanto para serviços de rede providos internamente ou terceirizados. (ABNT, 2005, p.50)*

(55) Controle: Operações e Comunicações – Gerenciamento de mídias removíveis.

> *10.7.1*
> *Convém que existam procedimentos implementados para o gerenciamento de mídias removíveis. (ABNT, 2005, p.50)*

(56) Controle: Operações e Comunicações – Descarte de mídias.

> *10.7.2*
> *Convém que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias, por meio de procedimentos formais. (ABNT, 2005, p.51)*

(57) Controle: Operações e Comunicações – Procedimentos para tratamento de informação.

> *10.7.3*
> *Convém que sejam estabelecidos procedimentos para o tratamento e o armazenamento de informações, para proteger tais informações contra a divulgação não autorizada ou uso indevido. (ABNT, 2005, p.52)*

(58) Controle: Operações e Comunicações – Segurança da documentação dos sistemas.

> *10.7.4*
> *Convém que a documentação dos sistemas seja protegida contra acessos não autorizados. (ABNT, 2005, p.52)*

(59) Controle: Operações e Comunicações – Políticas e procedimentos para troca de informações.

> *10.8.1*
> *Convém que políticas, procedimentos e controles sejam estabelecidos e formalizados para proteger a troca de informações em todos os tipos de recursos de comunicação. (ABNT, 2005, p.53)*

(60) Controle: Operações e Comunicações – Acordos para trocas de informações.

> *10.8.2*
> *Convém que sejam estabelecidos acordos para a troca de informações e softwares entre organizações e entidades externas. (ABNT, 2005, p.55)*

(61) Controle: Operações e Comunicações – Mídias em trânsito.

> *10.8.3*
> *Convém que mídias contendo informações sejam protegidas contra acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização. (ABNT, 2005, p.56)*

(62) Controle: Operações e Comunicações – Mensagens eletrônicas.

> *10.8.4*
> *Convém que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas. (ABNT, 2005, p.56)*

(63) Controle: Operações e Comunicações – Sistemas de informações de negócio.

> *10.8.5*
> *Convém que políticas e procedimentos sejam desenvolvidos e implementados para proteger as informações associadas com interconexão de sistemas de informações do negócio. (ABNT, 2005, p.57)*

(64) Controle: Operações e Comunicações – Serviços de comércio eletrônico.

> *10.9.1*
> *Convém que as informações envolvidas em comércio eletrônico transitando sobre redes públicas sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas. (ABNT, 2005, p.58)*

(65) Controle: Operações e Comunicações – Transações on-line.

> *10.9.2*
> *Convém que informações envolvidas em transações on-line sejam protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada. (ABNT, 2005, p.59)*

(66) Controle: Operações e Comunicações – Informações publicamente disponíveis.

> *10.9.3*
> *Convém que a integridade das informações disponibilizadas em sistemas publicamente acessíveis seja protegida para prevenir modificações não autorizadas. (ABNT, 2005, p.60)*

(67) Controle: Operações e Comunicações – Registros de auditoria.

> *10.10.1*
> *Convém que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso. (ABNT, 2005, p.61)*

(68) Controle: Operações e Comunicações – Monitoramento do uso do sistema.

> *10.10.2*
> *Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente de forma regular. (ABNT, 2005, p.61)*

(69) Controle: Operações e Comunicações – Proteção das informações dos registros (log).

> *10.10.3*
> *Convém que os recursos de informações de registros (log) sejam protegidos contra a falsificação e acesso não autorizado. (ABNT, 2005, p.63)*

(70) Controle: Operações e Comunicações – Registro (log) de administrador e operador.

> *10.10.4*
> *Convém que as atividades dos administradores e operadores de sistemas sejam registradas. (ABNT, 2005, p.63)*

(71) Controle: Operações e Comunicações – Registro (log) de falhas..

> *10.10.5*
> *Convém que as falhas ocorridas sejam registradas e analisadas, e que sejam adotadas ações apropriadas. (ABNT, 2005, p.64)*

(72) Controle: Operações e Comunicações – Sincronização dos relógios.

> *10.10.6*
> *Convém que os relógios de todos os sistemas de processamento de informações relevantes, dentro da organização ou do domínio de segurança, sejam sincronizados com uma fonte de tempo precisa, acordada. (ABNT, 2005, p.64)*

Capítulo 11 – Controle de acessos

Estabelece responsabilidades e regras para que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.

Controles definidos neste capítulo:

(73) Controle: Acesso – Política de controle de acesso.

> *11.1.1*
> *Convém que a política de controle de acesso seja estabelecida e analisada criticamente, tomando-se como base os requisitos de acesso dos negócios e segurança da informação. (ABNT, 2005, p.65)*

(74) Controle: Acesso – Registro de usuário.

> *11.2.1*
> *Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços. (ABNT, 2005, p.66)*

(75) Controle: Acesso – Uso de privilégio – Restritos e controlados.

> *11.2.2*
> *Convém que a concessão e o uso de privilégios sejam restritos e controlados. (ABNT, 2005, p.67)*

(76) Controle: Acesso – Gerenciamento de senha do usuário.

> *11.2.3*
> *Convém que a concessão de senhas seja controlada através de um processo de gerenciamento formal. (ABNT, 2005, p.68)*

(77) Controle: Acesso – Análise crítica dos direitos de acesso de usuário.

> *11.2.4*
> *Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal. (ABNT, 2005, p.68)*

(78) Controle: Acesso – Uso de senhas.

11.3.1
Convém que os usuários sejam solicitados a seguir as boas práticas de segurança da informação na seleção e uso de senhas. (ABNT, 2005, p.69)

(79) Controle: Acesso – Equipamento de usuário sem monitoração.

11.3.2
Convém que os usuários assegurem que os equipamentos não monitorados tenham proteção adequada. (ABNT, 2005, p.70)

(80) Controle: Acesso – Política de mesa limpa e tela limpa.

11.3.3
Convém que seja adotada uma política de mesa limpa de papéis e mídias de armazenamento removível e política de tela limpa para os recursos de processamento da informação, (ABNT, 2005, p.70)

(81) Controle: Acesso – Política de uso de serviços de rede

11.4.1
Convém que os usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar, (ABNT, 2005, p.71)

(82) Controle: Acesso – Autenticação para conexão externa do usuário

11.4.2
Convém que métodos apropriados de autenticações sejam usados para controlar o acesso de usuários remotos, (ABNT, 2005, p.72)

(83) Controle: Acesso – Identificação de equipamentos em redes

11.4.3
Convém que sejam consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos, (ABNT, 2005, p.73)

(84) Controle: Acesso – Proteção de portas de configuração e diagnóstico remotos

11.4.4
Convém que sejam controlados os acessos físico e lógico a portas de diagnóstico e configuração, (ABNT, 2005, p.73)

(85) Controle: Acesso – Segregação de redes

11.4.5
Convém que grupos de serviços de informação, usuários e sistemas de informação sejam segregados em redes. (ABNT, 2005, p.73)

(86) Controle: Acesso – Controle de conexão de redes

> *11.4.6*
> *Para redes compartilhadas, especialmente essas que se estendem pelos limites da organização, convém que a capacidade dos usuários para conectar-se à rede seja restrita, alinhada com a política de controle de acesso e os requisitos das aplicações do negócio. (ABNT, 2005, p.74)*

(87) Controle: Acesso – Controle de roteamento de redes

> *11.4.7*
> *Convém que seja implementado controle de roteamento na rede, para assegurar que as conexões de computador e fluxos de informação não violem a política de controle de acesso das aplicações do negócio. (ABNT, 2005, p.75)*

(88) Controle: Acesso – Procedimentos seguros de entrada nos sistema (log on).

> *11.5.1*
> *Convém que o acesso aos sistemas operacionais seja controlado por um procedimento seguro de entrada no sistema (log on). (ABNT, 2005, p.75)*

(89) Controle: Acesso – Identificação e autenticação do usuário

> *11.5.2*
> *Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário. (ABNT, 2005, p.77)*

(90) Controle: Acesso – Sistema de gerenciamento de senha

> *11.5.3*
> *Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senha de qualidade. (ABNT, 2005, p.77)*

(91) Controle: Acesso – Uso de utilitários de sistema

> *11.5.4*
> *Convém que o uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações seja restrito e estritamente controlado. (ABNT, 2005, p.78)*

(92) Controle: Acesso – Limite de tempo de sessão

> *11.5.5*
> *Convém que sessões inativas sejam encerradas após um período definido de inatividade. (ABNT, 2005, p.79)*

(93) Controle: Acesso – Limitação de horário de conexão

> *11.5.6*
> *Convém que restrições nos horários de conexão sejam utilizados para proporcionar segurança adicional para aplicações de alto risco. (ABNT, 2005, p.79)*

(94) Controle: Acesso – Restrição de acesso à informação

> *11.6.1*
> *Convém que o acesso à informação e às funções dos sistemas de aplicações por usuários e pessoal de suporte seja restrito de acordo com o definido na política de controle de acesso. (ABNT, 2005, p.80)*

(95) Controle: Acesso – Isolamento de sistemas sensíveis

> *11.6.2*
> *Convém que sistemas sensíveis tenham um ambiente computacional dedicado (isolado). (ABNT, 2005, p.80)*

(96) Controle: Acesso – Computação e comunicação móvel

> *11.7.1*
> *Convém que uma política formal seja estabelecida e que medidas de segurança apropriadas sejam adotadas para a proteção contra os riscos do uso de recursos de computação e comunicação móveis. (ABNT, 2005, p.81)*

(97) Controle: Acesso – Trabalho remoto

> *11.7.2*
> *Convém que uma política, planos operacionais e procedimentos sejam desenvolvidos e implementados para atividades de trabalho remoto. (ABNT, 2005, p.82)*

Capítulo 12 – Aquisição, desenvolvimento e manutenção de sistemas de informação.

Estabelece responsabilidades e regras para que todos os requisitos de segurança da informação sejam identificados e acordados antes do desenvolvimento e/ou implementação de sistemas de informação.

Controles definidos neste capítulo:

(98) Controle: Análise e especificação dos requisitos de segurança

> *12.1.1*
> *Convém que sejam especificados os requisitos para controles de segurança nas especificações de requisitos de negócios, para novos sistemas de informação ou melhorias em sistemas existentes. (ABNT, 2005, p.84)*

(99) Controle: Validação dos dados de entrada.

> *12.2.1*
> *Convém que os dados de entrada de aplicações sejam validados para garantir que são corretos e apropriados. (ABNT, 2005, p.85)*

(100) Controle: Controle do processamento interno

> *12.2.2*
> *Convém que sejam incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas. (ABNT, 2005, p.86)*

(101) Controle: Integridade de mensagens

> *12.2.3*
> *Convém que requisitos para garantir a autenticidade e proteger a integridade das mensagens em aplicações sejam identificados e os controles apropriados sejam identificados e implementados. (ABNT, 2005, p.87)*

(102) Controle: Validação dos dados de saída

> *12.2.4*
> *Convém que os dados de saída das aplicações sejam validados para assegurar que o processamento das informações armazenadas está correto e é apropriado às circunstâncias. (ABNT, 2005, p.87)*

(103) Controle: Política para uso de controles criptográficos

> *12.3.1*
> *Convém que seja desenvolvida e implementada uma política para uso de controles criptográficos para a proteção da informação. (ABNT, 2005, p.88)*

(104) Controle: Gerenciamento de chaves.

> *12.3.2*
> *Convém que um processo de gerenciamento de chaves seja implantado para apoiar o uso de técnicas criptográficas pela organização. (ABNT, 2005, p.89)*

(105) Controle: Controle de software operacional

> *12.4.1*
> *Convém que procedimentos para controlar a instalação de software em sistemas operacionais sejam implementados. (ABNT, 2005, p.90)*

(106) Controle: Proteção dos dados para teste de sistema

> *12.4.2*
> *Convém que os dados de teste sejam selecionados com cuidado, protegidos e controlados. (ABNT, 2005, p.92)*

(107) Controle: Acesso ao código fonte de programa

> *12.4.3*
> *Convém que o acesso ao código fontes de programas seja restrito. (ABNT, 2005, p.92)*

(108) Controle: Procedimentos para controle de mudanças.

> *12.5.1*
> *Convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças. (ABNT, 2005, p.93)*

(109) Controle: Análise crítica técnica das aplicações após mudanças no sistema operacional.

> *12.5.2*
> *Convém que as aplicações críticas do negócio sejam analisadas criticamente e testadas quando sistemas operacionais são mudados, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança. (ABNT, 2005, p.94)*

(110) Controle: Restrições sobre mudanças em pacotes de software

> *12.5.3*
> *Convém que modificações em pacotes de software sejam desencorajadas e limitadas às mudanças necessárias e que todas as mudanças sejam estritamente controladas. (ABNT, 2005, p.95)*

(111) Controle: Vazamento de informações

> *12.5.4*
> *Convém que oportunidades para vazamento de informação sejam prevenidas. (ABNT, 2005, p.95)*

(112) Controle: Desenvolvimento terceirizado de software

> *12.5.5*
> *Convém que a organização supervisione e monitore o desenvolvimento terceirizado de software. (ABNT, 2005, p.96)*

(113) Controle: Controle de vulnerabilidades técnicas

> *12.6.1*
> *Convém que seja obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados. (ABNT, 2005, p.96)*

Capítulo 13 – Gestão de incidentes de segurança da informação.

Estabelece responsabilidades e regras para que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados permitindo a tomada de ação corretiva em tempo hábil.

Controles definidos neste capítulo:

(114) Controle: Notificação de eventos de segurança da informação.

> *13.1.1*
> *Convém que os eventos de segurança da informação sejam relatados através dos canais apropriados da direção, o mais rapidamente possível. (ABNT, 2005, p.98)*

(115) Controle: Notificando fragilidades de segurança da informação.

> *13.1.2*
> *Convém que os funcionários, fornecedores e terceiros de sistemas e serviços de informação sejam instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade em sistemas ou serviços. (ABNT, 2005, p.99)*

(116) Controle: Responsabilidades e procedimentos

> *13.2.1*
> *Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de segurança da informação. (ABNT, 2005, p.100)*

(117) Controle: Aprendendo com os incidentes de segurança da informação.

> *13.2.2*
> *Convém que sejam estabelecidos mecanismos para permitir que tipos, quantidades e custos dos incidentes de segurança da informação sejam quantificados e monitorados. (ABNT, 2005, p.101)*

(118) Controle: Coletas de evidência

> *13.2.3. Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição (ões) pertinente(s). (ABNT, 2005, p.102)*

Capítulo 14 – Gestão da continuidade do negócio.

Estabelece responsabilidades e regras para que o processo de continuidade de negócio seja implementado para minimizar o impacto sobre a organização e recuperar perdas de ativos da informação a um nível aceitável através da combinação de ações de prevenção e recuperação

Controles definidos neste capítulo:

(119) Controle: Incluindo a segurança da informação no processo de gestão de continuidade de negócio.

> *14.1.1*
> *Convém que um processo de gestão seja desenvolvido e mantido para assegurar a continuidade do negócio por toda a organização e que contemple os requisitos de segurança da informação necessários para a continuidade do negócio na organização. (ABNT, 2005, p.103)*

(120) Controle: Continuidade de negócios e análise/avaliação de riscos

> *14.1.2*
> *Convém identificar os eventos que podem causar interrupções aos processos de negócio, junto a probabilidade e impacto de tais interrupções e as conseqüências para a segurança da informação. (ABNT, 2005, p.104)*

(121) Controle: Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação.

> *14.1.3*
> *Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio. (ABNT, 2005, p.104)*

(122) Controle: Estrutura do plano de continuidade do negócio

> *14.1.4*
> *Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para teste e manutenção. (ABNT, 2005, p.105)*

(123) Controle: Testes, manutenção e reavaliação dos planos de continuidade do negócio

> *14.1.5*
> *Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade. (ABNT, 2005, p.106)*

Capítulo 15 – Conformidade.

Estabelece responsabilidades e regras para evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

Controles definidos neste capítulo:

(124) Controle: Identificação da legislação aplicável

> *15.1.1*
> *Convém que todos os requisitos estatutários, regulamentares e contratuais pertinentes, e o enfoque da organização para atender a esses requisitos, sejam explicitamente definidos, documentados e mantidos atualizados para cada sistema de informação da organização. (ABNT, 2005, p.108)*

(125) Controle: Direitos de propriedade intelectual.

> *15.1.2*
> *Convém que procedimentos apropriados sejam implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e sobre o uso de produtos de software proprietários. (ABNT, 2005, p.108)*

(126) Controle: Proteção de registros organizacionais

> *15.1.3*
> *Convém que registros importantes sejam protegidos contra perda, destruição e falsificação, de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio. (ABNT, 2005, p.109)*

(127) Controle: Proteção de dados e privacidade de informações pessoais

> *15.1.4*
> *Convém que a privacidade e a proteção de dados sejam asseguradas conforme exigido nas legislações, regulamentações e, se aplicável, nas cláusulas contratuais pertinentes. (ABNT, 2005, p.110)*

(128) Controle: Prevenção de mau uso de recursos de processamento de informação

> *15.1.5*
> *Convém que os usuários sejam dissuadidos de usar os recursos de processamento da informação para propósitos não autorizados. (ABNT, 2005, p.111)*

(129) Controle: Regulamentação de controles de criptografia

> *15.1.6*
> *Convém que controles de criptografia sejam usados em conformidade com todas as leis, acordos e regulamentações pertinentes. (ABNT, 2005, p.111)*

(130) Controle: Conformidade com as políticas e normas de segurança da informação.

> *15.2.1*
> *Convém que os gestores analisem criticamente, a intervalos regulares, a conformidade do processamento da informação dentro de sua área de responsabilidade com as políticas de segurança da informação, normas e quaisquer outros requisitos e segurança. (ABNT, 2005, p.112)*

(131) Controle: Verificação com a conformidade técnica.

> *15.2.2*
> *Convém que os sistemas de informação sejam periodicamente verificados em sua conformidade com as normas de segurança da informação implementadas. (ABNT, 2005, p.113)*

(132) Controle: Controles de auditoria de sistemas de informação

> *15.3.1*
> *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 de negócio. (ABNT, 2005, p.113)*

(133) Controle: Proteção de ferramentas de auditoria de sistemas de informação

> *15.3.2*
> *Convém que o acesso às ferramentas de auditoria de sistema de informação seja protegido, para prevenir qualquer possibilidade de uso impróprio ou comprometimento. (ABNT, 2005, p.114)*

ANEXO 3 – Termos descritos na norma e utilizados nesta pesquisa.

Os seguintes termos são utilizados nesta pesquisa e estão descritos na NBR ISO/IEC 27002:2005. (ABNT, 2005, p.1-3):

> *Controle*
> *Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.*
>
> *Segurança da informação*
> *Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidos.*
>
> *Política*
> *Intenções e diretrizes globais formalmente expressas pela direção.*
>
> *Risco*
> *Combinação da probabilidade de um evento e suas conseqüências.*
>
> *Análise de risco*
> *Uso sistemático de informações para identificar fontes e estimar o risco*
>
> *Análise/avaliação de risco*
> *Processo completo de análise/avaliação de riscos*
>
> *Gestão de risco*
> *Processo de comparar o risco estimado com critérios de risco pré-definidos para determinar a importância do risco.*
>
> *Tratamento do risco*
> *Processo de seleção e implementação de medidas para modificar um risco.*
> *(ABNT, 2005, p.1-3)*

ANEXO 4 – Questionário

1 – DADOS DO RESPONDENTE

1.1 - Gênero: ( ) Masc. ( ) Fem.

1.2 - Cargo que ocupa na Organização:

1.3 - Tempo de trabalho na Organização: _____ Anos.

1.4 - Tempo de trabalho relacionado à segurança da informação:_____ Anos

1.5 - Possui alguma certificação internacional em segurança da informação:

Sim (Qual?): _____ Não: _____

2 – SOBRE O DOCUMENTO DE POLÍTICA DE SEGURANÇA

2.1 - Como o documento de politica de segurança é comunicado aos usuários?

2.2 - Quais são os tipos de usuários considerados pela política?

- Funcionário: Sim_____ Não _____
- Prestador de serviço, terceiros: Sim_____ Não _____
- Estagiário, Aprendiz: Sim_____ Não _____
- Outros (Quais?)

2.3 - Quantos usuários são afetados por esta política?

2.4 - Quando foi publicada a primeira versão da política? Mês-Ano

2.5 - Qual a área organizacional responsável pelo processo de segurança da informação?

2.6 - Alguma norma foi tomada por base para a elaboração da política de segurança da informação?

2.7 – Qual o cargo da pessoa que assinou a política de segurança da informação?

2.8 – Que ambientes a política de segurança da informação contempla?

- Ambiente de tecnologia: Sim-Não
- Ambiente convencional: Sim-Não

3 – ADMINISTRAÇÃO DE RISCO

3.1 – Considerando as ameaças que a organização recebe, atribua uma ordem de prioridade (1 para o mais crítico e 10 para o menos crítico) para os riscos abaixo, que estão em ordem alfabética:

a) Contingencia que indisponibiliza o ambiente de tecnologia ( )

b) Fraude realizada por usuário interno ( )

c) Incapacidade de responder questionamentos da Justiça sobre uso e guarda da informação. ( )

d) Invasão do ambiente de tecnologia por criminosos externos ( )

e) Roubo de informação por concorrente desleal ou por criminosos que podem vender esta informação? ( )

f) Vazamento de informação por erro, descuido/negligência do usuário e que coloque a organização exposta na mídia ( )

g) Vírus e demais códigos maliciosos ( )

h) Falha em sistema aplicativo ( )

4 – SOBRE A ORGANIZAÇÃO

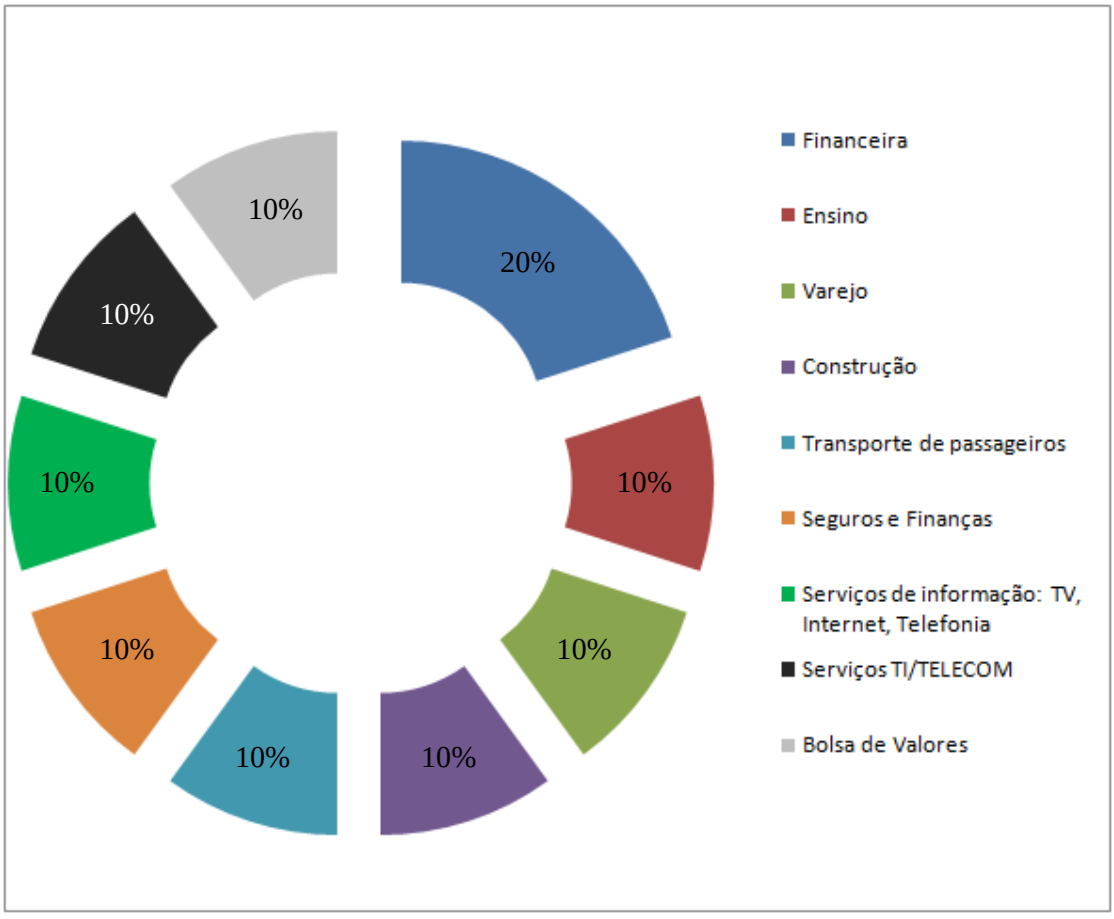
4.1 - Setor de atuação

- Serviço: financeiro, transporte, educação, construção.
- Indústria:
- Comércio:
- Outro (Descreva):

4.2 - A Organização exige que seus fornecedores de tecnologia da informação (todos ou alguns) possuam política de segurança da informação?

ANEXO 5 – Tipos de organizações pesquisadas

Tipo de Organizações Pesquisadas	Quantidade
Financeira	2
Ensino	1
Varejo	1
Construção	1
Transporte de passageiros	1
Seguros e Finanças	1
Serviços de informação: TV, Internet, Telefonia	1
Serviços TI/TELECOM	1
Bolsa de Valores	1
TOTAL	10

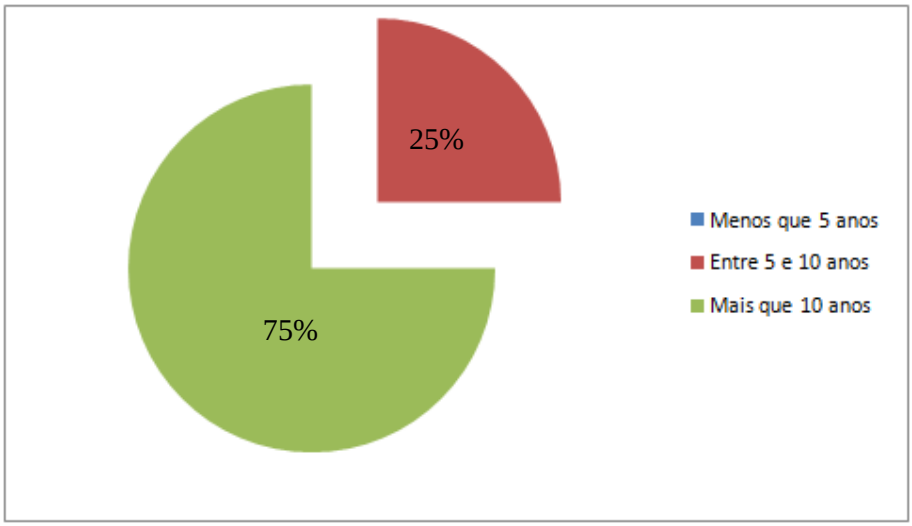


ANEXO 6 – Quadro resumo – Respostas do questionário.

1. DADOS DO RESPONDENTE										
1.1 - Gênero		M	M	M	M	M	M	M		M
1.2 - Cargo que ocupa na Organização		Gerente S.I.	Gerente S.I.	Coordenador Segurança da Informação	Assessor Tecnico	Gerente de Segurança da Informação	Analista Seguranca			Security Officer
1.3 - Anos de trabalho na Organização		11	3	29	36	5	5	10		1
1.4 - Tempo de trabalho em SI		16	8	6	12	15	12	17		22
1.5 - Possui Certificação Internacional em SI		CISM	CISSP	Não	Não	Não	Não	CISP, CGIH		CISM, CISA
2. DOCUMENTO POLÍTICA DE SEGURANÇA										
2.1 - Como é comunicado aos usuários	Email, Intranet	Palestras, Intranet, Intrgracao	Intranet, Email e Campanha Anual de Conscientização	Email, Intranet, Palestras	Email, Intranet, Novos funcionários	Intranet, Email, Manual, Integracao	Intranet, Email, Manual, Integracao	Intranet, Email, Cartilha, Integracao	Intranet, Email, Manual, Integracao	Intranet, E-Leraning, Novos Funcionarios
2.2 - Quais os tipos de usuários considerados	Funcionarios, Prestador Seviços, Estagiarios, Outros	Funcionarios, Prestador Seviços, Estagiario	Funcionário, Prestador de Seviço, Estagiário	Funcionario, Prestador de Serviço, Estagiário	Funcionario, Prestador de Serviço, Estagiário	Funcionário, Prestador de Seviço, Estagiário	Intranet, Email, Manual, Integracao	Funcionario, Prestador de Serviço, Estagiario	Funcionario, Prestador de Serviço, Estagiario	Funcionario, Prestador de Serviço, Estagiario
2.3 - Quantos usuários são afetados por esta política	Mais de 1 000	850	24.000	1.500	9.700	35.000	3000	2000	1000	200
2.4 - Quando foi publicada a primeira versão da política? Mes-Ano	Há mais de 5 anos	2002	2004	2006	2007	2005	2004	2003	Há mais de cinco anos	2005
2.5 - Qual a área organizacional responsável pelo processo de segurança da informação?	Tecnologia da Informação	Chief Operational Offcicer	Área de Segurança da Informação	Área de Segurança da Informação	Gerencia de Auditoria e Segurança da Informação	Gerencia de Segurança da Informação	Tecnologia da Informação	Coordenação de Segurança da Informação	Gerencia de Segurança da Informação	Area de Segurança da Informação
2.6 - Alguma norma foi tomada por base para a elaboração da política de segurança da informação?	ISO 27002	Codigo de Ética	ISO 27001/27002, SANS	ISO 27001/27002	ISO 27002	ISO 27002	ISO 27001/27002	ISO 27002/27001	ISO27002	ISO 27002
2.7 – Qual o cargo da pessoa que assinou a política de segurança da informação?	Diretor	Vice Presidente (COO)	Diretor	Diretor	Diretoria	Presidente	Comitê Executivo (Presidente e Diretores)	Presidente	Comitê de Segurança	Comitê Segurança
2.8 – Que ambientes a política de segurança da informação contempla? *- Ambiente de tecnologioa: Sim-Não* *- Ambiente convencional: Sim-Não*	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convenciaonal	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convencional	Tecnologia e Convencional
3. ADMINISTRAÇÃO DO RISCO										
3.1 – Considerando as ameaças que a organização recebe, atribua uma ordem de prioridade (1 é maior)										
a) Contingencia que indisponibiliza o ambiente de tecnologia		1	5	1	3	1	2	6		4
b) Fraude realizada por usuário interno		1	3	1	7	2	6	5		2
c) Incapacidade de responder questionamentos da Justiça		3	10	5	6	1	8	4		3
d) Invasão do ambiente de tecnologia por criminosos externos		2	8	1	5	1	3	3		5
e) Roubo de informação por concorrente desleal ou		2	1	1	4	1	4	2		1
f) Vazamento de informação por erro, descuido/negligência		2	3	1	1	1	5	1		6
g) Virus e demais códigos maliciosos		1	4	1	2	1	1	7		7
h) Falha em sistema aplicativo		4	7	1	8	3	7	10		8

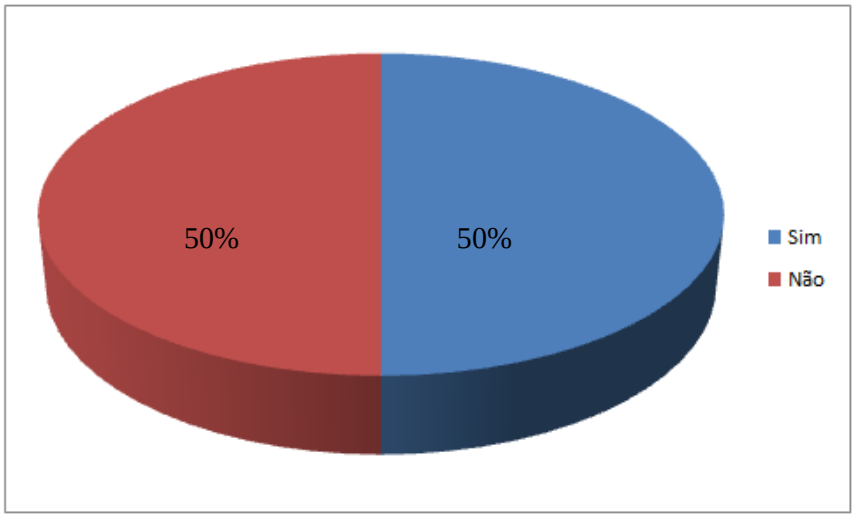
ANEXO 7 – Profissional – Experiência em segurança da informação

Tempo de experiência em segurança informação	Quantidade
Menos que 5 anos	0
Entre 5 e 10 anos	2
Mais que 10 anos	6



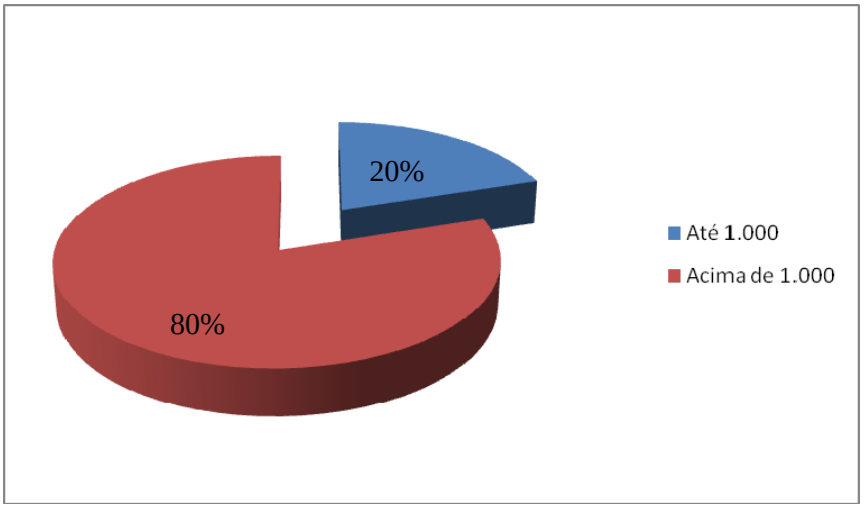
ANEXO 8 – Profissional – Certificação internacional em segurança da informação

Certificação internacional em segurança da informação	Quantidade
Sim	4
Não	4



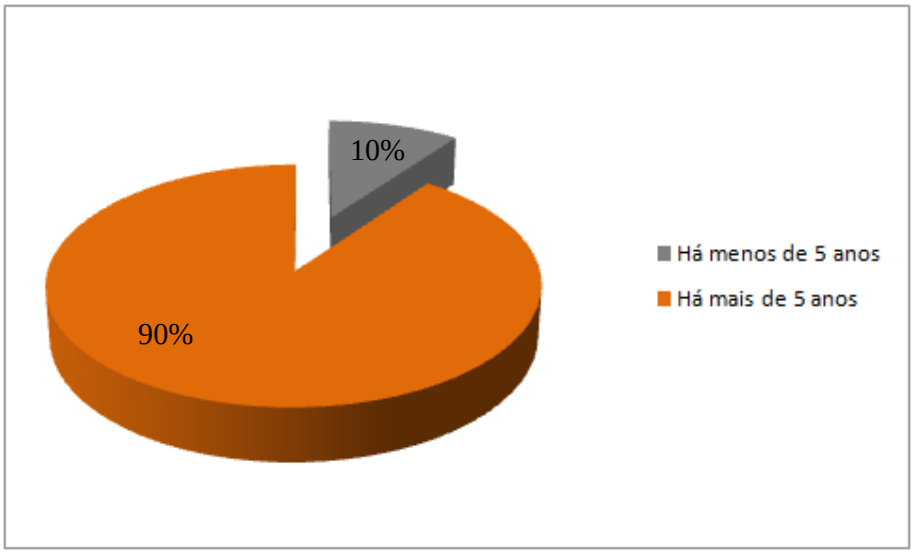
ANEXO 9 – Usuários impactados pela política

Numero de usuários impactados pela política	Quantidade
Até 1.000	2
Acima de 1.000	8



ANEXO 10 – Publicação da primeira versão da política de segurança da informação

Publicação da primeira versão da politica S.I.	Quantidade
Há menos de 5 anos	**1**
Há mais de 5 anos	**9**



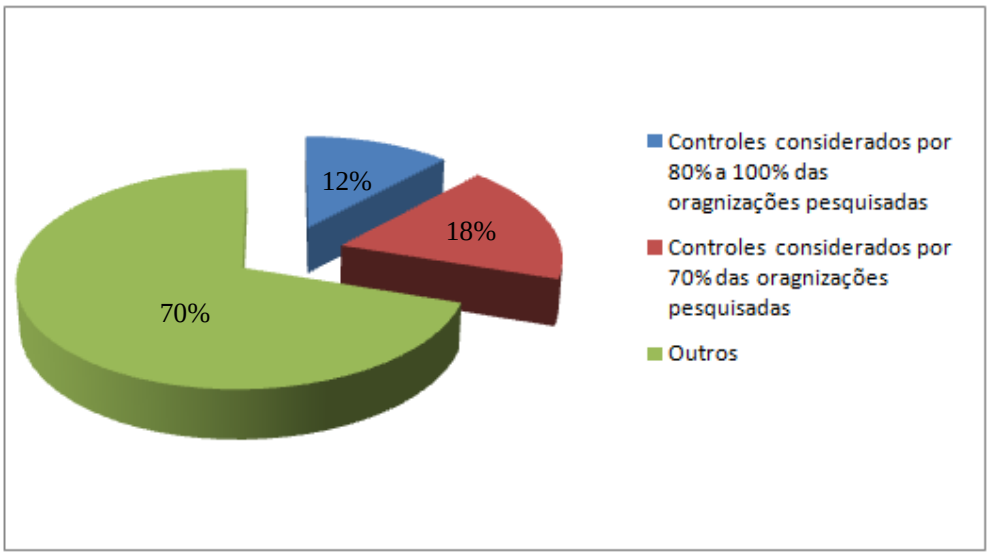
ANEXO 11 – Questionário – Analise de Risco

Resultado pelas Organizações – Prioridade Final

3. ADMINISTRAÇÃO DO RISCO	
Organizações =>	**Prioridade**
e) Roubo de informação por concorrente desleal ou por criminosos que podem vender esta informação	1
f) Vazamento de informação por erro, descuido/negligência	2
a) Contingencia que indisponibiliza o ambiente de tecnologia	3
d) Invasão do ambiente de tecnologia por criminosos externos	4
g) Vírus e demais códigos maliciosos	5
c) Incapacidade de responder questionamentos da Justiça	6
b) Fraude realizada por usuário interno	7
h) Falha em sistema aplicativo	8

ANEXO 12 – Controles comuns nas políticas.

Controles em comum nas Políticas	Percentual de Organizações	Quantidade de Controles envolvidos	Controle principal
Controle de acesso à informação	100%	11	11.1.1
Gestão de ativos: Internet, Equipamentos inteligentes, email, outros	100%	1	7.1.3
Classificação da informação	90%	2	7.2.1
Cópias de segurança	90%	1	10.5.1
Monitoramento de uso de sistema	80%	1	10.10.2
Total (80% - 100%)		**16**	**12%**
Política de segurança da informação	70%	2	5.1.1
Conscientização, educação e treinamento	70%	1	8.2.2
Encerramento de atividades: corte de acesso à informação	70%	3	8.3.1
Trabalho remoto	70%	1	11.7.2
Aquisição, Desenvolvimento e Manutenção de sistemas	70%	16	12.1.1
Processo Disciplinar	70%	1	8.2.3
Total (70%)		**24**	**18%**
Total (70% - 100%)		**40**	**30%**
Total de Controles na NBR 27002:2005		**133**	**100%**


12%
18%
70%
Controles considerados por 80% a 100% das oragnizações pesquisadas
Controles considerados por 70% das oragnizações pesquisadas
Outros

ANEXO 13 – Controles da Norma NBR ISO/IEC 27002:2005 e os controles encontrados nos documentos de políticas das organizações.

80% à 100%

70%

ORGANIZAÇÕES =>	1	2	3	4	5	6	7	8	9	10
5. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	X				X	X	X		X	X
5.1.1. Documento da política de segurança da informação.	X				X	X	X		X	X
5.1.2. Análise crítica da política de segurança da informação	X				X	X	X			X
6. ORGANIZANDO A SEGURANÇA DA INFORMAÇÂO			X	X	X	X			X	X
6.1.1.Comprometimento da direção com a segurança da informação				X					X	
6.1.2. Coordenação da segurança da informação				X	X				X	X
6.1.3. Atribuição de responsabilidades para a segurança da informação.				X						
6.1.4. Processo de autorização para os recursos de processamento info										
6.1.5. Acordos de confidencialidade.			X	X						
6.1.6. Contato com autoridades.										

6.1.7. Contato com grupos especiais.										
6.1.8. Análise crítica independente de segurança da informação.				X						
6.2.1. Identificação dos riscos relacionados às partes externas				X						
6.2.2. Identificando a segurança da informação,tratando com os clientes.										
6.2.3. Identificando a segurança da inform, nos acordos com terceiros			X							
7. GESTÃO DE ATIVOS	X	X	X	X	X	X	X	X	X	X
7.1.1. Inventário dos ativos.	X	X	X				X		X	X
7.1.2. Proprietário dos ativos.	X	X	X				X			
7.1.3. Uso aceitável dos ativos. OBS. Email e Internet, Midia portátil	X	X	X	X	X	X	X	X	X	X
7.2.1. Classificação da informação – Recomendações para classificação.	X	X	X		X	X	X	X	X	X
7.2.2.Classificação da informação – Rótulos e tratamento da informação.	X	X	X				X			X
8. SEGURANÇA EM RECURSOS HUMANOS	X	X	X	X	X	X			X	X
8.1.1. Papéis e responsabilidades										
8.1.2. Seleção										
8.1.3. Termos e condições de contratação.										X

8.2.1. Responsabilidades da direção										
8.2.2. Conscientização, educação e treinamento em SI.			X	X	X	X			X	X
8.2.3. Processo disciplinar.	X	X	X			X	X			X
8.3.1. Encerramento das atividades.	X	X				X	X		X	X
8.3.2. Devolução de ativos.										
8.3.3. Retirada de direitos de acesso	X	X				X	X			X
9. SEGURANÇA FÍSICA E DO AMBIENTE			X	X	X	X	X			
9.1.1. Perímetro de segurança física.						X				
9.1.2. Controles de entrada física.			X			X	X			
9.1.3. Segurança em escritórios, salas e instalações		X	X							
9.1.4. Proteção contra ameaças externas e do meio ambiente.										
9.1.5. Trabalhando em áreas seguras.		X	X							
9.1.6. Acesso do público, áreas de entrega e de carregamento										
9.2.1. Instalação e proteção de equipamento.						X				X

9.2.2. Utilidades.										
9.2.3. Segurança do cabeamento										
9.2.4. Manutenção dos equipamentos										
9.2.5. Segurança de equipamentos fora das dependência da organização.										
9.2.6. Reutilização e alienação segura de equipamentos										
9.2.7. Remoção de propriedade										
10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES		**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**	**X**
10.1.1. Documentação dos procedimentos.										
10.1.2. Gestão de mudanças.							**X**			**X**
10.1.3. Segregação de funções		**X**								**X**
10.1.4. Separação dos recursos de desenvolvimento, teste e produção.										**X**
10.2.1. Entrega de serviço.										**X**
10.2.2. Monitoramento e análise crítica de serviços terceirizados.		**X**								**X**
10.2.3. Gerenciamento de mudanças para serviços terceirizados.										**X**
10.3.1. Gestão de capacidade.										

10.3.2. Aceitação de sistemas							X			X
10.4.1. Proteção contra códigos maliciosos e códigos móveis.						X				X
10.4.2. Controles contra códigos móveis.										
10.5.1. Cópias de segurança da informação		X	X	X	X	X	X		X	X
10.6.1. Controles de redes.	X									X
10.6.2. Segregação dos serviços de rede.										X
10.7.1. Gerenciamento de mídias removíveis				X			X			X
10.7.2. Descarte de mídias.	X			X	X		X		X	X
10.7.3. Procedimentos para tratamento de informação.										X
10.7.4. Segurança da documentação dos sistemas.		X	X							
10.8.1. Políticas e procedimentos para troca de informações.				X						
10.8.2. Acordos para trocas de informações.				X			X			
10.8.3. Mídias em trânsito	X			X			X	X		X
10.8.4. Mensagens eletrônicas.										X

10.8.5. Sistemas de informações de negócio										X
10.9.1. Serviços de comércio eletrônico.										X
10.9.2. Transações on-line.										X
10.9.3. Informações publicamente disponíveis										
10.10.1. Registros de auditoria.					X		X	X	X	X
10.10.2. Monitoramento do uso do sistema	X	X	X			X	X	X	X	X
10.10.3. Proteção das informações dos registros (log).									X	X
10.10.4. Registro (log) de administrador e operador.					X				X	X
10.10.5. Registro (log) de falhas..					X				X	X
10.10.6. Sincronização dos relógios.					X					X
11. CONTROLE DE ACESSOS	X	X	X	X	X	X	X	X	X	X
11.1.1. Política de controle de acesso.	X	X	X	X	X	X	X	X	X	X
11.2.1. Registro de usuário.	X	X	X	X		X	X	X		X
11.2.2. Uso de privilégio – Restritos e controlados	X	X	X				X		X	X

11.2.3. Gerenciamento de senha do usuário.	X	X	X				X	X	X	X
11.2.4. Análise crítica dos direitos de acesso de usuário.		X					X		X	X
11.3.1. Uso de senhas.	X	X	X			X	X		X	X
11.3.2. Equipamento de usuário sem monitoração.										X
11.3.3. Política de mesa limpa e tela limpa.		X					X	X		X
11.4.1. Política de uso de serviços de rede	X						X			X
11.4.2. Autenticação para conexão externa do usuário		X					X			X
11.4.3. Identificação de equipamentos em redes	X	X					X			X
11.4.4. Proteção de portas de configuração e diagnóstico remotos										
11.4.5. Segregação de redes								X		
11.4.6. Controle de conexão de redes		X				X	X			X
11.4.7. Controle de roteamento de redes										
11.5.1. Procedimentos seguros de entrada nos sistema (log on).		X	X				X			
11.5.2. Identificação e autenticação do usuário	X	X	X				X		X	X

11.5.3.Sistema de gerenciamento de senha			X				X			
11.5.4. Uso de utilitários de sistema	X						X			
11.5.5. Limite de tempo de sessão										
11.5.6. Limitação de horário de conexão										
11.6.1. Restrição de acesso à informação		X	X					X		
11.6.2. Isolamento de sistemas sensíveis										
11.7.1. Computação e comunicação móvel										
11.7.2. Trabalho remoto	X	X				X	X	X	X	X
12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	X	X	X			X	X		X	X
12.1.1. Análise e especificação dos requisitos de segurança	X	X	X			X	X		X	X
12.2.1. Validação dos dados de entrada.										
12.2.2. Controle do processamento interno										
12.2.3. Integridade de mensagens										
12.2.4. Validação dos dados de saída										
12.3.1. Política para uso de controles criptográficos		X				X				X

12.3.2. Gerenciamento de chaves.		**X**								**X**
12.4.1. Controle de software operacional										**X**
12.4.2. Proteção dos dados para teste de sistema										**X**
12.4.3. Acesso ao código fonte de programa		**X**								
12.5.1. Procedimentos para controle de mudanças.										**X**
12.5.2. Análise crítica técnica aplicações após mudanças s.o.										
12.5.3. Restrições sobre mudanças em pacotes de software										**X**
12.5.4. Vazamento de informações										
12.5.5. Desenvolvimento terceirizado de software		**X**					**X**			**X**
12.6.1. Controle de vulnerabilidades técnicas							**X**			
13. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃo		**X**		**X**				**X**	**X**	**X**
13.1.1. Notificação de eventos de segurança da informação.		**X**								**X**
13.1.2. Notificando fragilidades de segurança da informação.										**X**
13.2.1. Responsabilidades e procedimentos										

13.2.2. Aprendendo com os incidentes de segurança da informação										
13.2.3. Coletas de evidência		X		X						
14 - GESTÃO DA CONTINUIDADE DO NEGÓCIO			X	X		X				X
14.1.1. Incluindo a segurança da informação no processo de GCN										
14.1.2. Continuidade de negócios e análise/avaliação de riscos			X			X				X
14.1.3. Desenvolvimento e implementação de planos de continuidade - S.I.			X							
14.1.4. Estrutura do plano de continuidade do negócio										
14.1.5. Testes, manutenção e reavaliação dos planos de continuidade negócio										
15. CONFORMIDADE			X	X	X					X
15.1.1. Identificação da legislação aplicável			X		X					X
15.1.2. Direitos de propriedade intelectual.		X	X		X					X
15.1.3. Proteção de registros organizacionais					X					X
15.1.4. Proteção de dados e privacidade de informações pessoais										X
15.1.5. Prevenção de mau uso - recursos de processamento informação		X								X
15.1.6. Regulamentação de controles de criptografia										X

15.2.1. Conformidade com as políticas e normas de si					**X**					**X**
15.2.2. Verificação com a conformidade técnica.										**X**
15.3.1. Controles de auditoria de sistemas de informação		**X**			**X**					**X**
15.3.2. Proteção de ferramentas de auditoria de sistemas de informação										**X**