Política de Segurança da Informação nas Organizações: desafio de elaboração para os gestores.

Edison Luiz Gonçalves Fontes
Centro Estadual de Educação Tecnológica Paula Souza/CEETEPS – SP - Brasil
edison@pobox.com

Prof. Dr. Napoleão Verardi Galegale
Centro Estadual de Educação Tecnológica Paula Souza/CEETEPS - SP- Brasil
nvg@galegale.com.br

Resumo – Este artigo apresenta os resultados da pesquisa de Mestrado que teve como objetivo identificar os controles que devem compor um padrão mínimo para as políticas de segurança da informação das organizações. Foi realizado um estudo de caso múltiplo em dez organizações de nove segmentos de negócio e foram identificados os controles comuns destas políticas. Este conjunto de elementos compõe o padrão mínimo recomendado. Os cento e trinta e três controles da Norma NBR ISO/IEC 27002:2005 foram tomados por base nesta pesquisa. A existência de um padrão mínimo de controles para a elaboração de uma política de segurança da informação ajuda as organizações a desenvolverem as suas políticas de proteção da informação.

Palavras chave: segurança da informação, política de segurança, NBR ISO/IEC 27002.

Abstract – This article presents the results of Masters research that aimed to identify the controls that should comprise a minimum standard for information security policies of organizations. We conducted a multiple case study of ten organizations in nine business segments and identified the common controls of these policies. This set of elements make up the minimum recommended standard. The one hundred thirty-three controls of the NBR ISO/IEC 27002:2005 has been taken based on this research. The existence of a minimum standard of controls for the development of a policy of information security helps organizations develop policies on protection of information.

Keywords: information security, security policy, NBR ISO/IEC 27002.

Introdução

Atualmente as organizações precisam proteger a sua informação em função de que este recurso é fundamental para o atendimento de seus objetivos. Silva e Tomaél (2007) consideram a importância da informação para organizações 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. [1]*

Sendo a informação um bem para a organização, é necessária a existência de um processo de segurança da informação. Para tanto a 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. [2]*

A NBR ISO/IEC 27002:2005 define 133 controles de segurança da informação e as organizações, personificadas nos seus gestores, sentem dificuldades em definir sua política de segurança da informação, principalmente as organizações que estão começando seu processo de proteção da informação.

Com o objetivo de facilitar estas organizações surgiu a seguinte indagação: seria possível elaborar e formalizar uma política de segurança da informação para um primeiro estágio de maturidade em segurança considerando apenas alguns desses controles? Esta situação é considerada na NBR ISO/IEC 27001:2006 quando afirma:

> *É esperado que a implementação de um Sistema de Gestão de Segurança da Informação seja escalada conforme as necessidades da organização. [3]*

Desta maneira a pesquisa considerou a seguinte questão problema: quais são os elementos que devem compor um padrão mínimo para a política de segurança da informação de uma organização?

Baseado neste cenário foi realizada uma pesquisa nas políticas de segurança da informação de dez organizações de nove seguimentos de negócio, com o objetivo de identificar controles comuns nestes regulamentos.

Na pesquisa realizada [4] foi utilizado o termo política, significando a orientação básica para o assunto segurança da informação. Define Maximiniano [5]:

> *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.*

Complementando, a própria NBR ISO/IEC 27002:2005 tem a sua definição do termo política [2]:

> *2. Termos e definições*
> *2.8 Política*
> *Intenções e diretrizes globais formalmente expressas pela direção.*

A pesquisa realizada [4] considerou 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

Metodologia

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

No estudo realizado a metodologia considerou as seguintes etapas [4]:

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 podiam estabelecer um padrão mínimo de política de segurança da informação.

Resultados [4]

Foram consideradas nesta pesquisa dez organizações. Destas dez organizações, duas não responderam ao questionário sobre o ambiente de segurança da organização. 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.

Resultado - Análise das organizações

As dez organizações participantes estão distribuídas, sem grande concentração, em nove segmentos de negócios. Duas organizações pertencem ao segmento financeiro e cada uma das demais organizações pertence a um desses segmentos: Ensino, Varejo, Construção, Transporte de passageiros, Seguros, Serviços de informação (TV, Internet, telefonia), Serviços TI/Telecom e Bolsa de Valores,

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. Porém se considerarmos um tempo menor, todas as organizações possuem políticas há mais de quatro anos.

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.

Setenta por cento das organizações possuem uma área específica para a segurança da informação. Na 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 indicaram, 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 na 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, 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.

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.

Resultado - Análise dos entrevistados

Como ponto a destacar na análise realizada temos 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. 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.

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.

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, isto é, elas 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 a pesquisa este fato foi 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. Consequentemente 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, 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) 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

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.

Resultados - Análise dos controles das políticas

A análise dos controles das políticas estudadas considerou os controles da Norma NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação que define 133 controles.

Para que um controle fosse considerado para o padrão mínimo de segurança da informação para esta pesquisa, foi obrigatório que ele fosse referenciado por pelo menos 70% das políticas 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. Foi considerado pela pesquisa que estes controles formam o padrão mínimo de controles que devem compor um padrão mínimo de política de segurança da informação. O quadro a seguir indica estes controles, o percentual de organizações que considera este

controle, a quantidade de controles referenciados na norma e ligados ao controle citado e a identificação do item da norma referente a este controle.

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%**

Discussão e Conclusões

A pesquisa realizada [4] identificou os elementos recomendados para 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.

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 [4] 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 [4] 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.

Agradecimentos

Agradecemos as dez organizações que disponibilizaram suas políticas de segurança da informação e possibilitaram a realização da pesquisa. Pelo acordo realizado o nome das organizações e dos seus profissionais não seriam divulgados. Desta maneira, não podemos explicitar seus nomes.

Referências

Artigos Científicos

[1] SILVA, Terezinha Elisabeth; TOMAÉL, Maria Inês. (2007), "**Gestão da Informação nas Organizações"** Revista Informação & Informação, No. 12, p.1. Londrina: Universidade Estadual de Londrina.

Livros e Teses

[2] ABNT – Associação Brasileira de Normas e Técnicas (2005) "Tecnologia da informação – Técnicas de segurança – Código de Prática para a gestão da segurança da informação – NBR ISO/IEC 27002", p.8, p.2, ABNT, Brasil.

[3] ABNT – Associação Brasileira de Normas e Técnicas (2006) "Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação - Requisitos – NBR ISO/IEC 27001", p.v, ABNT, Brasil.

[4] Fontes E.L.G., "Política de Segurança da Informação: uma contribuição para o estabelecimento de um padrão mínimo". (2011) Centro Estadual de Educação Tecnológica Paula Souza, Dissertação de Mestrado, Orientador: Prof.Dr. Napoleão Galegale, São Paulo.

[5] Maximiniano, A. C. A., "Introdução à Administração". (2010), p.86, São Paulo: Editora Atlas.

Contato

Edison Luiz Gonçalves Fontes, Alameda Santos, 1.293, Conjunto 84 – Cerqueira César – São Paulo, SP, CEP 01419-001. Agosto/2011. edison@pobox.com

Napoleão Verardi Galegale, R. Dr. Cândido Espinheira, 560, Conj. 81, Perdizes, São Paulo, SP, CEP 05004-000. Agosto/2011.