A GESTÃO DA SEGURANÇA DA INFORMAÇÃO E SEU ALINHAMENTO ESTRATÉGICO NA ORGANIZAÇÃO

Marcelo Teixeira TORRES*
Marcelo Wilson ANHESINE**
Walther AZZOLINI JÚNIOR***

RESUMO

É inegável que a Tecnologia da Informação (TI) tem proporcionado às empresas, grandes ou pequenas, maior eficiência e rapidez na troca de informações e tomada de decisões. A TI evoluiu de um suporte administrativo para um papel estratégico dentro de uma organização. No entanto, esse ambiente é extremamente complexo, heterogêneo e distribuído, dificultando a gestão de questões referentes à Segurança da Informação. Este trabalho faz o levantamento histórico da Segurança da Informação e sua contextualização empresarial, discutindo os impactos que podem ser causados devido a sua falha. Os pontos críticos da Gestão da Segurança da Informação são apontados e ainda é proposta a aplicação de um código de boas práticas, no sentido de conscientizar as empresas no tocante à adoção de um Sistema de Gestão da Segurança da Informação. São discutidos, neste artigo, a análise e tratamento de riscos de segurança da informação; a adoção de uma política de segurança da informação; a gestão de ativos da informação e seus proprietários; a segurança da informação vinculada a recursos humanos; a segurança física do ambiente corporativo; o gerenciamento das operações e das comunicações; os controles de acesso físico e lógicos; a aquisição, desenvolvimento e manutenção dos sistemas de informação e a gestão de incidentes de segurança da informação. Ainda serão ponderados ao final do trabalho os aspectos legais da propriedade intelectual relacionados à proteção dos registros organizacionais.

PALAVRAS-CHAVE: Gestão da Segurança da Informação. Alinhamento Estratégico de TI. Tecnologia da Informação. Análise e avaliação de riscos de Segurança da Informação.

ABSTRACT

Clearly, the Information Technology (IT) has provided businesses, large or small, more efficient and rapid exchange of information and decision making. IT has evolved from an administrative support for a strategic role within an organization. However, this environment is extremely complex, heterogeneous and distributed, making the management of issues relating to Information Security. This

* Bacharel em Sistemas de Informação e Mestrando do curso de mestrado Profissional em Engenharia de Produção do Centro Universitário de Araraquara (UNIARA), marcelo@wai.com.br.

** Professor do Centro Universitário de Araraquara (UNIARA), coordenador do curso de Pós-graduação: MBA em Administração da Produção e Operações do Centro Universitário de Araraquara (UNIARA) e coordenador do curso de Engenharia Bioenergética do Centro Universitário de Araraquara (UNIARA), mwanhesine@uniara.com.br.

*** Pesquisador do GEOPE, Coordenador do Programa de Mestrado Profissional em Engenharia de Produção do Centro Universitário de Araraquara (UNIARA), e Coordenador do curso de Graduação em Engenharia de Produção do Centro Universitário de Araraquara (UNIARA), wazzolini@uniara.com.br.

work is the historical survey of Information Security and its business context, discussing the impacts that may be caused due to their failure. The critical points of the Management of Information Security are pointed out and yet it is proposed to implement a code of best practices in order to educate companies regarding the adoption of a Management System of Information Security. Are discussed in this article the analysis and processing of information security risks, the adoption of a policy of information security, asset management information and its owners, the security of information linked to human resources, physical security of the corporate environment ; management of operations and communications, physical access controls and software, acquisition, development and maintenance of information systems and management of information security incidents. Still be considered the final work on the legal aspects of intellectual property related to the protection of organizational records.

KEYWORDS: *Information Security Management. IT Strategic Alignment. Information Technology. Analysis and risk assessment of Information Security.*

INTRODUÇÃO

Segundo dados corporativos globais (PANDA SOFTWARE, 2010), os agentes ameaçadores aos ambientes computacionais estão em constante evolução, seja em número ou em forma. Novos vírus, mais potentes que seus antecessores, surgem a uma velocidade quase exponencial. A Figura 1 demonstra a curva de crescimento e tendência de crescimento dos vírus de computador desde 1983, data da classificação do primeiro vírus conhecido.

A maioria dos ataques é direcionada às empresas, com intenção de roubo de informações e identidades. Segundo a Symantec, em seu relatório anual sobre ameaças na Internet, o Brasil é o terceiro país no mundo em números de atividades maliciosas, atrás somente dos Estados Unidos e da China. O aumento significativo dos números do Brasil, no referido relatório, se deve ao crescimento da infraestrutura de Internet banda larga (Tabela 1). O nível crescente de atividades de códigos maliciosos que afetam o Brasil também resultou na proposta de uma nova lei do cibercrime[1] no país (SYMANTEC CORPORATION, 2010).

[1] [Neo.]. Designação geral para os delitos cometidos, mediante a utilização da Internet. Ex. invasão de servidores e computadores para alteração ou roubo de dados, desvio de dinheiro em contas bancárias, fraudes com cartão de crédito, violações de propriedade intelectual, pedofilia, protestos políticos com dimensões criminosas, etc.

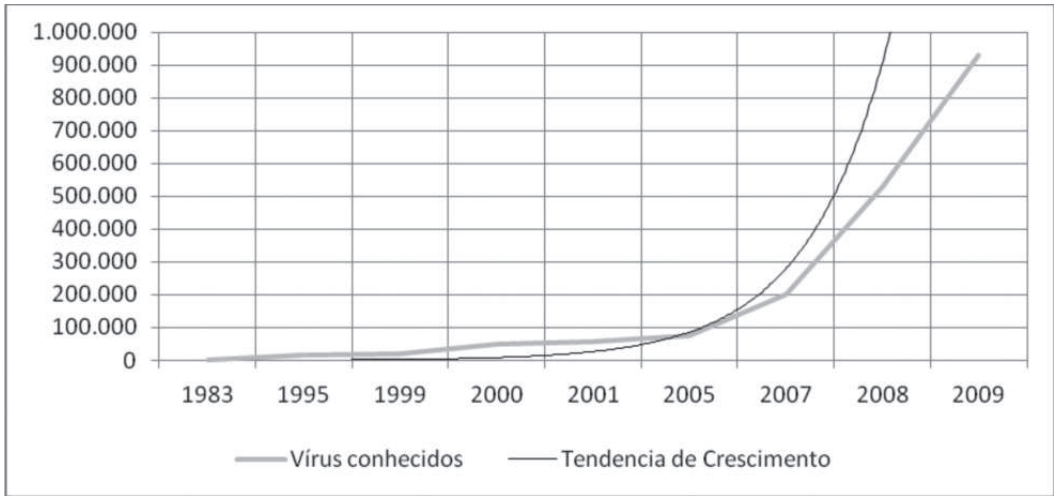


Figura 1 - Evolução dos vírus de computador
Fonte: Adaptado de (PANDA SOFTWARE, 2010)

Tabela 1 - Atividade Maliciosa por Países
Fonte: (SYMANTEC CORPORATION, 2010, p. 7)

Overall Rank 2009	Overall Rank 2008	Country	Percentage 2009	Percentage 2008	2009 Activity Rank: Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Sob constantes ataques de criminosos, cerca de 320 redes de computadores do governo federal – entre elas sistemas de grande porte, como o do Banco do Brasil e o Serviço de Processamento (Serpro), que cuida do coração da economia e do mercado financeiro – geraram uma nova demanda para os órgãos de segurança e de inteligência. Um inquérito que corre em segredo na Polícia Federal, em Brasília, investiga a atuação de uma quadrilha internacional que penetrou no servidor de uma estatal, destruiu os controles, trocou a senha e, depois de paralisar todas as atividades da empresa, exigiu um resgate de US$ 350 mil (FOLHA DE S. PAULO, 2009).

Os ataques às instituições governamentais são frequentes ao redor do mundo. Em 2008, uma agência estrangeira de espionagem comandou um ataque digital ao Pentágono, sede do Departamento de Defesa dos Estados Unidos, causando a mais significativa violação já ocorrida na segurança digital das Forças Armadas norte-americanas. O ataque teve início depois que um *pendrive* contaminado foi

inserido em um *notebook* militar, em um quartel do Oriente Médio. O vírus contido nesse *pendrive* foi transferido até o Comando Central do Pentágono, penetrando sistemas sigilosos e não sigilosos. O ataque serviu de alerta ao Pentágono, que depois disso criou o Comando Cibernético e tomou medidas para reforçar suas defesas digitais (G1 TECNOLOGIA & GAMES, 2010).

Instituições financeiras sofrem prejuízos financeiros e de imagem consideráveis devido às violações de suas informações. Os prejuízos financeiros do setor bancário com crimes eletrônicos, incluindo Internet e cartões de crédito e débito, somaram cerca de R$ 450 milhões no primeiro semestre de 2010. O prejuízo total do setor bancário em 2009 foi de R$ 900 milhões. No ano passado, os investimentos em segurança na Internet atingiram R$ 1,94 bilhão. Os prejuízos na imagem dessas instituições não podem ser medidos, pois possuem desdobramentos em diferentes variáveis (G1 ECONOMIA e NEGÓCIOS, 2010).

Normalmente, esses ataques começam com algum reconhecimento por parte dos atacantes. Isso pode incluir pesquisar informações publicamente disponíveis sobre a empresa e seus empregados, como dos sites de relacionamento pessoal. Essa informação é então utilizada para criar métodos de captura, conhecidos como *phishing*, que induzem funcionários e pessoas comuns a clicar em links maliciosos, entrarem em sites contaminados, etc. De acordo com a Symantec (2010), 95% das exposições de identidade poderiam ser evitadas adotando alguma política de segurança da informação. O cenário atual sugere que a maioria das organizações deveria se preocupar mais em gerenciar seus recursos de informação do que controlar a execução de programas não autorizados (ANGELL e SPYRIDON, 2009).

Apesar de as empresas afirmarem informalmente que o assunto segurança da informação é importante, essa declaração fica muito distante das ações. A Figura 2 mostra que a 78% das violações de dados (*hacking*, política insegura e perda/roubo) possivelmente seriam evitadas com uma boa política de gestão da segurança da informação (SYMANTEC CORPORATION, 2010).

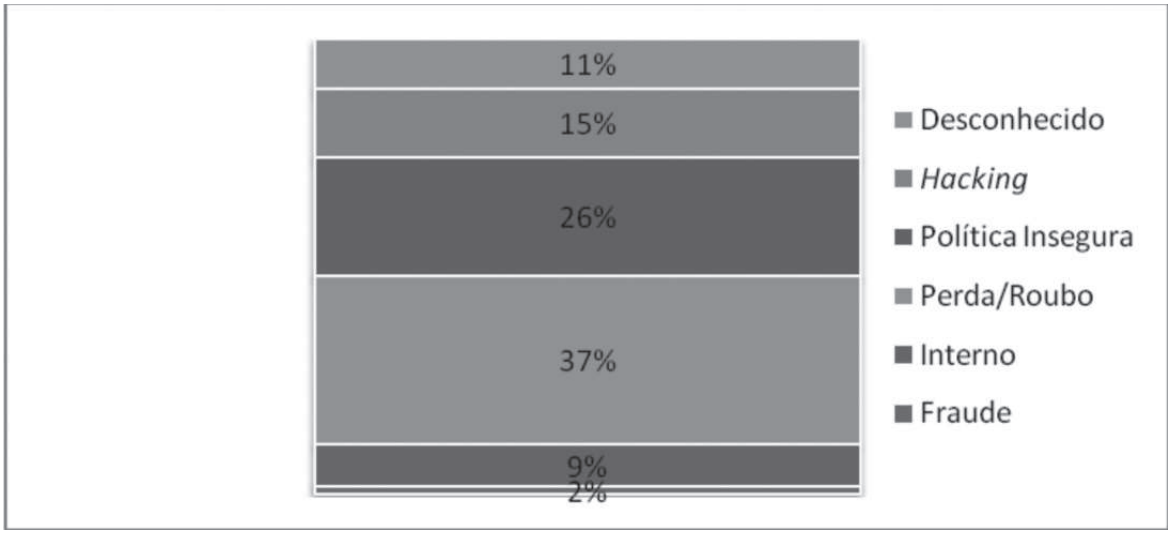


Figura 2 - Causa das violações de dados empresariais
Fonte: Adaptado de (SYMANTEC CORPORATION, 2010, p. 9)

Em 2009, 98% das ameaças à confidencialidade das informações teve algum componente de acesso remoto. Este foi um aumento de 83% em relação aos números de 2008. O contínuo aumento é provavelmente devido à adição de funcionalidades de acesso remoto (bem como outras ameaças de informações confidenciais) nos softwares empresariais e sistemas operacionais. A sofisticação e eficácia de kits de ferramentas de criação de softwares maliciosos também contribuíram para o aumento desse número.

Dos ataques bem sucedidos, ou seja, com captura de alguma informação e onde dados confidenciais e estratégicos das empresas foram expostos, 72% obtiveram acesso a dados de sistema das empresas e 86% instalaram programas espiões, como *keyloggers*[2] (SYMANTEC CORPORATION, 2010).

Na contramão do crescimento das ameaças, o interesse global por segurança da informação vem reduzindo lentamente, ano a ano, conforme dados do Google (2010). Em fevereiro de 2004, ano em que o Google iniciou a tabulação de seus dados, das pesquisas mundiais categorizadas com interesse em computadores e aparelhos eletrônicos, as buscas por *information security* representaram 100% das palavras-chave. Em maio de 2010, essas palavras aparecem em apenas 37% das pesquisas, como mostra a Figura 3 (GOOGLE, 2010).

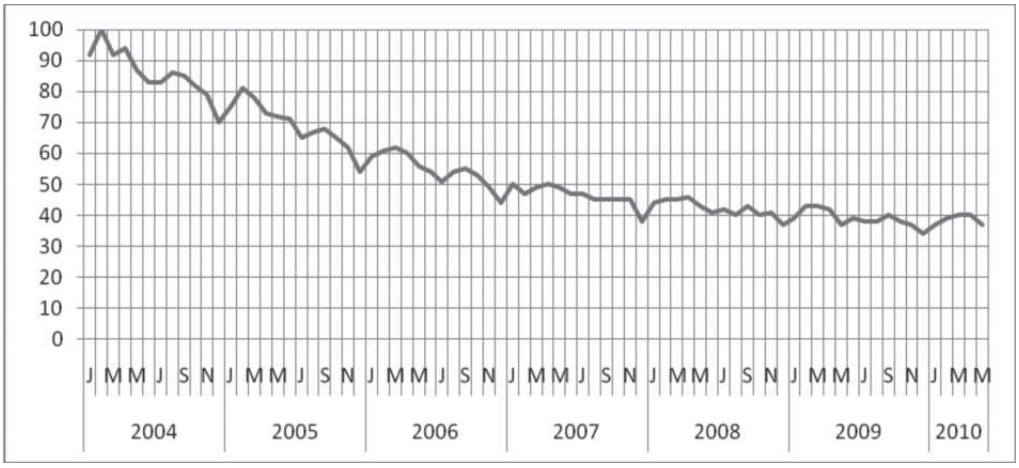


Figura 3 - Interesse mundial por *information security*
Fonte: Adaptado de (GOOGLE, 2010)

O Brasil ainda demonstra relativo interesse pelo assunto segurança da informação, se comparado à média mundial, devido principalmente ao aumento da atividade maliciosa na Internet, como relatado no anual da Symantec, subir da 5ª para a 3ª posição no ranking mundial e da 5ª para a 2ª posição no ranking dos países que mais enviam *spam*[3], coforme Tabela 2 (SYMANTEC CORPORATION, 2010).

[2] Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2006).

[3] Termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, essa mensagem também é referenciada como UCE - do Inglês *Unsolicited Commercial E-mail* (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2006).

Tabela 2 - Classificação de países com maior envio de *spam*
Fonte: (SYMANTEC CORPORATION, 2010, p. 80)

Overall Rank 2009	2008	Country	Percentage 2009	2008
1	1	United States	23%	25%
2	5	Brazil	11%	4%
3	13	India	4%	2%
4	12	South Korea	4%	2%
5	9	Poland	4%	3%
6	4	China	3%	4%
7	3	Turkey	3%	5%
8	2	Russia	3%	6%
9	32	Vietnam	3%	1%
10	19	Colombia	2%	1%

A Figura 4 mostra o interesse do Brasil em pesquisas sobre "segurança da informação" no Google, com dados até maio de 2010, baseado nas pesquisas relacionadas à categoria computadores e aparelhos eletrônicos. O auge da busca pelo tema foram os meses de abril e maio de 2004, quando as palavras "segurança" e "informação" estavam presentes em 100% das pesquisas. No mês de maio de 2010, essa porcentagem foi de 53% (GOOGLE, 2010).

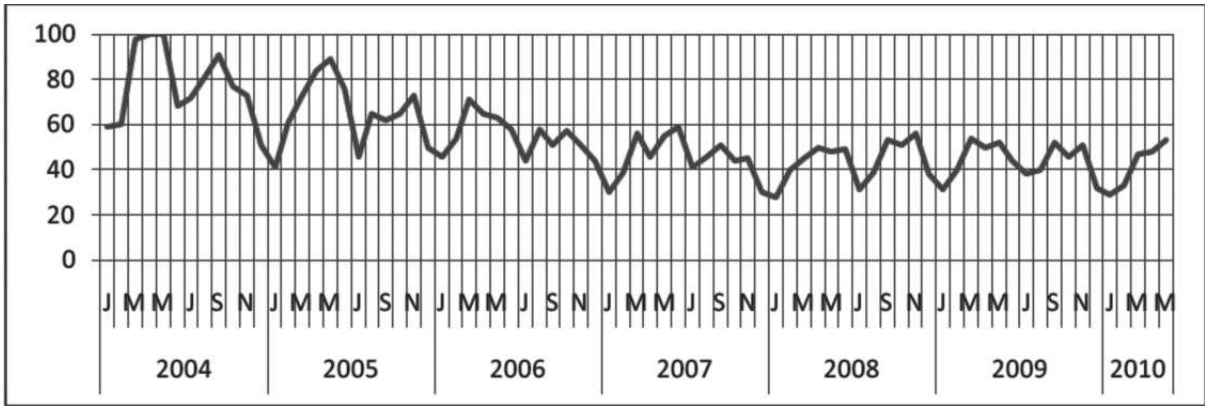


Figura 4 - Interesse nacional em "segurança da informação"
Fonte: Adaptado de (GOOGLE, 2010)

Sistemas de gestão da segurança da informação

Nos dias atuais, a informação e os processos de apoio, sistemas internos e redes de dados são ativos essenciais a uma organização, seja ela pública ou privada. Protegê-las tornou-se algo indispensável, principalmente em um ambiente cada dia mais interconectado. Como resultado do aumento dessa interconectividade, a informação se expõe a um infindável número de ameaças e vulnerabilidades. Definir, alcançar e manter a segurança da informação se tornou atividade vital para estabelecer a com-

petitividade, o fluxo de caixa, a lucratividade, os requisitos legais e uma boa imagem da organização junto ao mercado (LAHTI e PETERSON, 2006).

Segurança da Informação é a proteção da informação contra vários tipos de ameaças, com finalidade de garantir a continuidade do negócio, minimizando seus riscos e maximizando o retorno sobre os investimentos. A Segurança da Informação é obtida através da adoção de um conjunto de controles adequados, que devem ser estabelecidos, implantados, monitorados, analisados e melhorados constantemente, a fim de garantir que os objetivos estratégicos do negócio e da segurança da informação sejam atendidos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Muitos sistemas de informação não foram projetados para serem seguros, uma vez que a Segurança da Informação não pode ser alcançada apenas por meios técnicos. Para ser plenamente eficaz, a Segurança da Informação deve estar apoiada por uma gestão e por procedimentos apropriados. Os mecanismos de controle devem ser detalhadamente implementados. A implantação deve acontecer de cima para baixo (arquitetura *Top-Down*[4]), atingindo desde a mais alta direção, passando por todos os funcionários e abrangendo clientes, fornecedores e acionistas. Uma consultoria externa especializada pode ser útil no momento de sua implantação (LAHTI e PETERSON, 2006).

É fundamental a uma organização identificar seus requisitos de Segurança da Informação, os quais são identificados por meio de análises sistemáticas dos riscos da Segurança da Informação. Todos os investimentos com controles precisam ser ponderados conforme os danos causados aos negócios gerados pelas potenciais falhas de segurança. Os resultados das análises de risco ajudarão a direcionar e estabelecer as ações apropriadas e as prioridades gerenciais dos riscos da Segurança da Informação, na implementação dos controles definidos para proteção contra esses riscos. A análise de riscos deve ser periodicamente repetida para atender a e prever quaisquer mudanças que podem modificar os resultados da gestão da Segurança da Informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Uma vez identificados os requisitos de Segurança da Informação, seus riscos e tenham sido definidas as decisões para o tratamento dos riscos, devem ser escolhidos e implementados controles apropriados a cada risco, para que eles sejam reduzidos a níveis toleráveis dentro da estratégia organizacional. Tais controles podem ser selecionados a partir de uma norma vigente ou criados em separado, visando a atender a uma necessidade específica. A decisão de cada controle de segurança da informação depende da decisão estratégica da organização, devendo estar em conformidade com a legislação e regulamentações específicas, nacional e internacional, relevante à área de atuação (ANGELL e SPYRIDON, 2009).

Experiências na adoção de um plano de gestão da segurança da informação têm mostrado alguns fatores críticos de sucesso, dentro de uma organização. Entre eles, destacam-se: boas políticas de segurança da informação são aquelas que se mostram alinhadas com as estratégias de negócios; a estrutura de implementação, manutenção, análise e melhoramento da segurança da informação deve ser agregada à cultura organizacional; a implantação e adoção devem ocorrer em todos os níveis organi-

[4] Mostra o sentido que alguma ordem, implementação ou mudança é realizada dentro da empresa, neste caso, da direção para os funcionários. Seu inverso é *Botton-up*.

zacionais; a organização deve conhecer todos os requisitos de segurança da informação, seus riscos e procedimentos a serem adotados em casos de não conformidade; divulgação das normas de segurança da informação e a conscientização de sua adoção a todos os níveis da organização e terceiros envolvidos; provimento de recursos financeiros para todas as atividades relacionadas à gestão da segurança da informação e à implementação de um sistema de medição de eficiência da gestão da segurança da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Normas ABNT

Na tentativa de normatizar a Gestão da Segurança da Informação, a ABNT (Associação Brasileira de Normas Técnicas) elaborou, em parceria com a ISO (*International Organization for Standardization*), um conjunto de normas técnicas que: definem um código de prática para Gestão da Segurança da Informação; estabelecem alguns requisitos para construção de Sistemas de Gestão de Segurança da Informação; estabelecem diretrizes para gestão de riscos de Segurança da Informação e desenvolvem métricas para aferição da eficácia de um Sistema de Gestão de Segurança da Informação.

As normas que abordam o tema deste trabalho são:

- ABNT NBR ISO/IEC 27002:2005 – Código de prática para gestão de segurança da informação, em vigor desde 30/09/2005. Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação em uma organização. Os objetivos definidos nessa norma proveem diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.

- ABNT NBR ISO/IEC 27001:2006 Versão Corrigida:2006 – Sistemas de gestão de segurança da informação – Requisitos, em vigor desde 20/04/2006. Esta norma cobre todos os tipos de organizações (empreendimentos comerciais, agências governamentais, organizações sem fins lucrativos, etc.). Esta norma especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI documentado dentro do contexto dos riscos de negócios globais da organização. Ela especifica requisitos para a implementação de controles de segurança personalizados para as necessidades individuais de organizações ou suas partes.

- ABNT NBR ISO/IEC 27005:2008 – Gestão de riscos de segurança da informação, em vigor desde 07/08/2008. Esta norma fornece diretrizes para o processo de gestão de riscos de segurança da informação.

- ABNT NBR ISO/IEC 27004:2010 – Gestão da segurança da informação – Medição, em vigor desde 01/05/2010. Esta norma fornece diretrizes para o desenvolvimento e uso de métricas e medições a fim de avaliar a eficácia de um Sistema de Gestão de Segurança da Informação (SGSI) implementado e dos controles ou grupos de controles, conforme especificado na ABNT ISSO/IEC 27001.

Gestão da Segurança da Informação

A primeira etapa para adoção de um Sistema de Gestão da Segurança da Informação (SGSI) é levantar os riscos de quebra da segurança da informação. A análise de riscos deve ser estabelecida pelo comando da empresa, em conjunto com o departamento de TI. Essa análise deve incluir sistemas para estimar o impacto do risco e sua significância. Para cada risco identificado deve ser estabelecida uma decisão para seu tratamento (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Após o levantamento dos riscos, deve-se elaborar um documento, aprovado pela direção, que descreva para todos os funcionários e pessoas externas relevantes, a política de segurança da informação. Esse documento deve declarar o comprometimento da organização na gerência da segurança da informação. Essa política de gestão da segurança deve ser analisada, de forma criteriosa, em intervalos de tempo predefinidos ou quando houver mudanças críticas que comprometam sua pertinência ou eficácia (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Todos os ativos de informação devem ser identificados, assim como seus respectivos proprietários. Aos proprietários desses ativos deve ser atribuída a responsabilidade pela manutenção da sua segurança. Os ativos de informação estão classificados, de acordo com a ABNT (2005), em: ativos de informação, ativos de software, ativos físicos, serviços, pessoas e intangíveis.

Os papéis de responsabilidade pela segurança da informação de funcionários, fornecedores e terceiros envolvidos devem ser documentados conforme a política do SGSI, a fim de reduzir o risco de furto, fraude ou mau uso dos recursos. Essas responsabilidades devem ser estabelecidas antes da contratação, estabelecendo um termo de uso da informação. Recomenda-se que funcionários com acesso a informações sensíveis sejam adequadamente analisados e testados antes de sua contratação. Deve ser prevista também uma forma de retirar direitos de acesso e de devolução de ativos, caso o contrato de um funcionário ou terceiro seja encerrado (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Prevenir o acesso físico não autorizado aos ativos previne danos e interferências nas informações. O processamento de informações críticas ou sensíveis deve ser mantido em áreas seguras, com perímetro definido e com controle de acesso apropriado. Toda proteção física deve ser compatível com o risco identificado. Deve ser estabelecida também a proteção contra ameaças externas e do meio ambiente, como proteção contra incêndios e enchentes ou outras formas de desastres naturais ou causados pelo homem (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Proteger a integridade dos sistemas de software e da informação por eles manipulados também deve fazer parte da política de gestão da Segurança da Informação. O SGSI deve ser capaz de identificar a introdução de códigos maliciosos ou códigos móveis não autorizados. Os usuários devem ser conscientizados sobre os perigos dos códigos maliciosos. Os gestores dos ativos devem estar capacitados a prevenir, detectar e remover qualquer código malicioso que penetrar o sistema. O SGSI deve permitir gerar cópias de segurança dos dados e sua respectiva restauração em tempo aceitável, a fim de não prejudicar o bom andamento das atividades da empresa (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

O acesso à informação, seus recursos de processamento e os processos críticos de negócio devem ser controlados e criteriosamente autorizados para uso. Todas as regras de usuário e grupos devem ser expressamente claras, fornecendo aos usuários e provedores uma visão nítida do controle de acesso. Todo equipamento com acesso a rede e/ou sistemas organizacionais devem ser identificados física e logicamente, de modo que sejam facilmente localizados em caso de incidentes (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

É recomendável que apenas os sistemas internos da empresa sejam capazes de ler e gravar informações nos arquivos de dados. A adoção de política de controle de autenticidade, confidencialidade ou integridade deve ser estabelecida por meio de criptografia das informações. O acesso aos códigos-fonte dos sistemas de informação deve ser estritamente controlado e restrito apenas à equipe de desenvolvimento a fim de que sejam evitadas mudanças não autorizadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

Quando ocorrerem incidentes de segurança, as ações de recuperação estabelecidas no documento de políticas de gestão da segurança da informação devem ser implementadas em tempo hábil. Todos os funcionários, fornecedores e terceiros envolvidos devem estar cientes dos procedimentos de recuperação. Um plano de recuperação eficiente deve ser capaz de minimizar o impacto sobre a organização (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

O SGSI deve evitar violações de quaisquer obrigações legais, estatutárias ou contratuais. A implantação de um SGSI e da política de gestão da segurança da informação deve contar com suporte jurídico ou de profissionais qualificados sobre os aspectos legais e seus requisitos. Toda a legislação aplicável à regra de negócios da empresa deve ser identificada como forma de garantir os direitos de propriedade da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005).

CONSIDERAÇÕES FINAIS

A informação passou a ser o eixo central das empresas a partir das últimas décadas do século XX. Para alcançar o sucesso competitivo, as organizações precisam cumprir novas exigências no ambiente da informação. Investir, gerenciar e explorar o conhecimento passou a ser um fator crítico de desenvolvimento.

Proteger a informação significa proteger o patrimônio organizacional. Na atual formação mercadológica a Segurança da Informação desenha um degrau sutil entre o sucesso e o fracasso. A perda de informações pode causar prejuízos irreparáveis, sejam financeiros ou de imagens, às instituições afetadas. Cada vez mais a Gestão da Segurança da Informação deve fazer parte da estratégia da empresa.

Este artigo propôs a adoção da Gestão da Segurança da Informação, através das normas regulatórias descritas pela ABNT, como forma viável de proteger um dos ativos intangíveis mais importantes das organizações. Com uma breve descrição sobre as boas práticas para a gestão da segurança da informação, este trabalho sugere que cada vez mais empresas protejam seus patrimônios intelectuais e de informação.

REFERÊNCIAS

ANGELL, I. O.; SPYRIDON, S. The Risk of Computerised Bureaucracy. *Journal of Information System Security*, 2009. 3 - 25.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 27002:2005.* São Paulo, p. 120. 2005.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de Segurança. *cert.br*, 2006. Disponível em: <http://cartilha.cert.br/glossario/>. Acesso em: 20 jun. 2010.

FOLHA DE S. PAULO. *Folha on line*, 25 ago. 2009. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u614597.shtml>. Acesso em: 13 jun. 2010.

G1 ECONOMIA E NEGÓCIOS. *Globo.com*, 2010. Disponível em: <http://g1.globo.com/economia-e-negocios/noticia/2010/08/crimes-eletronicos-dao-prejuizo-de-r-450-milhoes-para-bancos-em-2010.html>. Acesso em: 31 ago. 2010.

G1 TECNOLOGIA & GAMES. *Globo.com*, 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/08/espioes-usaram-virus-em-pendrive-para-atacar-rede-do-pentagono.html>. Acesso em: 27 ago. 2010.

GOOGLE. *Google Insights*, 2010. Disponível em: <http://www.google.com/insights/search/#q=information%20security&cmpt=q>. Acesso em: jun. 2010.

LAHTI, C. B.; PETERSON, R. *Sarbanes-Oxley:* Conformidade TI usando COBIT e ferramentas open source. Rio de Janeiro: Alta Books, 2006.

PANDA SOFTWARE. *List of Viruses*, 13 jun. 2010. Disponível em: <http://www.cloudantivirus.com/en/listofviruses/>. Acesso em: 15 abr. 2010.

SYMANTEC CORPORATION. *Symantec Global Internet Security Threat Report - Trends for 2009.* Mountain View, CA - EUA, p. 98. 2010.