

GERENCIAMENTO ESTRATÉGICO DE SEGURANÇA DA INFORMAÇÃO

RESUMO DO ARTIGO

Este artigo se propõe a apresentar uma panorâmica do uso da Segurança da Informação e sua importância como diferencial competitivo para as organizações e a sua capacidade em manter o nível mínimo necessário de segurança na gestão da informação e garantia de continuidade do negócio.

A implementação de um Sistema de Gerenciamento de Segurança da Informação não se resume na instalação de softwares. Sua abrangência vai além deste tipo de ação (MOREIRA, 2001). Como exemplo, pode-se citar outros dispositivos de controle e gestão que compõem o sistema de segurança da informação: Análise de Risco; Política de Segurança; Controle de Acesso Físico e Lógico; Treinamento e Conscientização para a Segurança da Informação; Plano de Contingência ou Continuidade do Negócio. A Segurança da Informação pode e deve ser tratada como um conjunto de mecanismos conforme acima exposto, devendo ser adequada à necessidade de cada empresa.

Alguns pontos são importantes determinar, e a empresa deve sempre tê-los em mente:

- O que deve ser protegido?
- Contra o que será necessário proteger?
- Como será feita a proteção?

É necessário determinar que nível de segurança é mais adequado para as organizações, bem como avaliar a questão custo X benefício. Ou seja, se o custo da implementação de um sistema de segurança justifica os benefícios obtidos com a proteção dos ativos tratados.

Uma pergunta fica sempre no ar quando se trata deste assunto - Qual a finalidade do uso da Segurança da Informação nas organizações? Um sistema de segurança da informação tem a finalidade de diminuir o nível de exposição aos riscos em todos os ambientes para que a empresa possa estender a segurança

aos seus produtos e serviços, resultando em uma satisfação maior por parte dos clientes.

Outra questão relevante é - Qual a importância da Segurança nos Negócios ? A importância e os benefícios são evidentes. Como exemplo, podemos citar: Redução de riscos contra vazamento de informações confidenciais e / ou sigilosas; Redução da probabilidade de fraudes; Diminuição de erros devido a treinamento e mudança de comportamento; Manuseio correto de informações confidenciais;

Os principais objetivos de um Sistema de Segurança da Informação são(MOREIRA, 2001):

- Redução da probabilidade de ocorrência de incidentes de segurança;
- Redução dos danos/perdas causados por incidentes de segurança;
- Recuperação dos danos em caso de desastre/incidente.

A segurança da informação busca proteger a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, visando minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. O sistema de proteção da informação deve considerar aspectos ligados a: segurança física da informação, segurança lógica, segurança das relações financeiras, garantia da reputação e imagem da organização, aspectos legais, comportamento dos funcionários, e para com os funcionários, e todos os ativos tangíveis e intangíveis (PELTIER,2001).

A segurança da informação é caracterizada pela preservação de:

- a) confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
- b) integridade: salvaguarda da exatidão e completude da informação e métodos de processamento;
- c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Alguns questionamentos devem ser feitos pelas empresas antes de efetuarem investimentos em segurança da informação:

- ✓ Que ativos devem ser protegidos?
- ✓ Quais ativos críticos deverão ter proteção adicional?
- ✓ Quais serviços na rede deverão estar disponíveis para os funcionários?
- ✓ Quem terá acesso a esses serviços?
- ✓ Quem poderá conceder autorização e privilégios para o acesso aos sistemas?
- ✓ Que software permitir nas estações de trabalho?
- ✓ Como proceder quando programas não-aprovados/piratas forem encontrados nas estações de trabalho?

Abrangência do Sistema de Segurança da Informação

O processo de análise das medidas de segurança pode ser aplicado onde seja necessário avaliar riscos potenciais, independente da área desejada.

São eles:

- Controle de acesso aos sistemas críticos da empresa;
- Análise da segurança das estações de trabalho e notebooks;
- Análise da segurança física e lógica dos servidores de rede;
- Análise da segurança contra contaminação por vírus;
- Avaliação da configuração do firewall X Política de Segurança;
- Criptografia de dados (e-mails e informações confidenciais);
- Análise da Política de Backup;
- Análise da segurança do acesso físico aos locais críticos da empresa;
- Análise da exigência de prevenção contra softwares piratas na empresa;
- Plano de Contingência;
- Análise da Política de Acesso dos funcionários à Internet;
- Política de Instalação de Software nas estações e na rede;
- Processo de conscientização de funcionários.

A gestão da segurança da informação necessita, da participação de todos os funcionários da organização. Pode ser que seja necessária também a participação de fornecedores, clientes e acionistas. Entretanto, as metas, objetivos, direção, incentivos e definição dos papéis e responsabilidades em relação à consecução

segurança da informação, devem vir da alta direção (da diretoria, ou fórum de segurança da informação) da organização, a quem compete a:

- análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;
- monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;
- análise crítica e monitoração de incidentes de segurança da informação;
- aprovação das principais iniciativas para aumentar o nível da segurança da informação;

De acordo com o tamanho da organização, pode ser nomeado um RD (representante da direção), que será o líder de uma equipe destinada a coordenar a segurança da informação, e também pode ser chamado de Security Officer. Esta gerência é responsável por:

- Gestão do Sistema de Segurança da Informação, com responsabilidade pelo desenvolvimento e implementação da segurança e responsabilidade pelo suporte e à identificação dos controles;
- Assegurar que o Sistema de Segurança da Informação da organização seja mantido em conformidade com a Norma de Segurança da Informação específica ou a Norma BS 7799.
- Relatar o desempenho e manutenção do Sistema de Segurança da organização à Alta Direção para sua análise crítica como base para garantia da segurança e continuidade do negócio.

Para gestão estratégica da segurança deve-se considerar 8 elementos do sistema de proteção da informação (PELTIER,2001):

- ✓ O sistema de proteção da informação deve estar alinhado com as estratégias e objetivos de negócios da organização;
- ✓ A proteção da informação requer comprometimento da alta direção em manter alinhados os objetivos de segurança com os níveis de segurança desejados para o negócio;

- ✓ Os investimentos em segurança da informação devem ser compatíveis com o nível de segurança e proteção da informação esperada pela organização, ou melhor, necessário para suportar os negócios;
- ✓ As responsabilidades com a segurança e a proteção da informação, devem estar explícitas para todos os funcionários, clientes e fornecedores e as consequências advindas do não cumprimento das políticas, normas e procedimentos devem ser claramente divulgados e conhecidos por todos;
- ✓ Os proprietários (responsáveis pela guarda, monitoramento e administração) das informações têm responsabilidades sobre a manutenção da integridade, confidencialidade e disponibilidade, podendo dar permissões de acesso ou retirá-las de acordo com as necessidades do negócio;
- ✓ A proteção da informação deve fazer parte de um sistema com análise, revisões e correções permanentes que devem incluir a análise de risco e de impacto no negócio, e a classificação da informação, visando garantir a manutenção do nível esperado de segurança pela organização;
- ✓ O sistema de segurança da informação deve ser periodicamente auditado e testado, considerando as disposições ou ações corretivas para desvios ou falhas de funcionamento encontrados, e realimentando assim todo o sistema com a verificação de novas vulnerabilidades que possam ter surgido ao longo de seu funcionamento;
- ✓ A segurança da informação é um sistema eficiente de proteção dos ativos, deve ser construída com base na cultura da organização e nas necessidades de proteção identificadas, preservando as devidas regionalidade e propriedades inerentes aos países onde as mesmas existem ou suas filiais estão instaladas.

A proteção da informação deve ser um meio para organização alcançar seus objetivos e não deve significar um fim em si mesma. (PELTIER, 2001)

A implementação do sistema de proteção da informação deve transpor as fronteiras da implantação de dispositivos de hardware ou software, que protegem o que está armazenado nos bancos de dados e arquivos da empresa, e muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de

funcionamento ou de parametrização e instalação (PELTIER, 2001). O sistema deve considerar o grau de dependência da organização da utilização da informática como ferramenta de trabalho no seu dia-a-dia, as necessidades de manutenção dos sistemas ativos em caso de desastre e o comprometimento de áreas críticas da organização, com problemas de vazamento de informações, entre outros. Para resolver estes problemas será necessário, e pode-se dizer fundamental a definição da Política de Segurança da Informação, que é o conjunto de diretrizes do sistema de gestão de segurança da informação.

Segurança da Informação como Diferencial Competitivo

Michael Porter (PORTER, 1986) apresenta a idéia de posicionamento estratégico a partir de uma diferenciação específica, na liderança de custo ou no enfoque, que é também defendida por Philip Kotler em seu vídeo para HSM, Como Construir Marcas Fortes, de 2000. Estas são consideradas estratégias genéricas pois são métodos que muitas das empresas de um segmento específico de indústria podem adotar para superar seus concorrentes. Como cada uma destas abordagens funciona, veremos a seguir:

A diferenciação é uma estratégia que consiste diferenciar seu produto ou serviço o mais possível dos oferecidos pelos concorrentes. Criar um conceito de produto ou serviço que possa parecer único aos olhos do cliente. Os métodos aplicados para diferenciação são inúmeros, podemos citar: projeto ou imagem da marca, tecnologia aplicada, grau de inovação, serviços personalizados (sob encomenda).

A liderança de custo está pautada na busca permanente da redução dos custos de fabricação dos produtos ou serviços, na utilização da curva de experiência, no controle rígido de custos e no controle das margens.

A posição de redução de custos traz com resultados a redução de preços e por consequência uma diferenciação perante os concorrentes. Este posicionamento pode trazer mudanças radicais em um segmento da indústria, ilustrando ações ligadas a concorrência que evidenciam outras estratégias aplicadas pelos concorrentes. A estratégia chamada enfoque, está relacionada em manter o foco em determinado grupo de compradores, segmento de linha de produtos, ou mercado específico. Para implementação das estratégias genéricas é necessário

que as empresas observem alguns requisitos comuns, aloquem recursos e desenvolvam habilidades específicas, tais como: investimento de capital, boa capacidade de engenharia de processo para liderança em custo, tino criativo e forte coordenação entre funções de pesquisa, para desenvolvimento de produto, na estratégia diferenciação; combinar as políticas de fortalecimento da marca e fortalecer a reputação da empresa em qualidade ou tecnologia para estratégia de enfoque. A implementação destas estratégias demanda alguns riscos como: velocidade de mudança tecnológica, redução de demanda por parte dos consumidores que compram o seu fator de diferenciação.

Identificamos que a utilização dos dispositivos de segurança da informação de forma sistemática e organizada, poderão trazer à estratégia de diferenciação do produto aplicada pelas empresas, maior credibilidade e inovação, pois a segurança da informação trata do bem mais preciso das organizações no atual momento da gestão empresarial, e portanto precisa de manutenção e diferenciação de tratamento tanto internamente quanto perante o seu cliente.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBUQUERQUE, RICARDO E RIBEIRO, BRUNO. Segurança no desenvolvimento de software : como garantir a segurança do sistema para seu cliente usando a ISO/IEC. Rio de Janeiro, Ed. Campus, 2002.

AMARAL, MARCOS P. Segurança da Informação em Ambientes Computacionais Complexos: uma abordagem baseada na gestão de projetos. Minas Gerais, CEFET-MG, 2001.

ANÔNIMO. Segurança Máxima, Campus, Rio de Janeiro, 2000.

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

BRITISH STANDARD. Information security management – Part 2: Specification for information security management systems, BS 7799-2:1999. London: BSI, 1999.

CARUSO, CARLOS A. A.; STEFFEN, Flávio Deny. Segurança em informática e de Informações. São Paulo: Senac, 1999.

GHEMAWAT, PANKAJ. A Estratégia e o Cenário dos Negócios; textos e casos. BookMan / IBMEC, Porto Alegre, 2000.

MÓDULO SECURITY SOLUTIONS S.A. 7ª pesquisa sobre segurança de informação, 2001. Disponível em: <http://www.modulo.com.br>. Acesso em 01 dez. 2001.

MOREIRA, NILTON S. Segurança Mínima - uma visão corporativa da segurança de informações. Rio de Janeiro, Axcel Books, 2001.

PELTIER, THOMAS. Information Security Policies, Procedures, and Standards – Guideline for effective Information Security Management, Florida, Auerbach, 2001.

PORTER, MICHAEL E. Competição: estratégias competitivas essenciais, Rio de Janeiro, Ed. Campus, 1999.

PORTER, MICHAEL E. Vantagem Competitiva, Rio de Janeiro, Ed. Campus, 1986.

QUINTELLA, HEITOR M. Tecnologia da Informação e Avaliação da Competitividade no Brasil. Revista Suma Econômica, Rio de Janeiro, p. 46-47, ago. 1998.

STEPHENSON, PETER. Investigating Computer-Related Crime. New York, CRC Press, 2000.

TIPTON, HAROLD F. KRAUSE, MICKI. Information Security Management Handbook. Volume 1, 2, 3 e 4. Flórida, Auerbach, 1998.