28 – Janeiro de 2001

Sei O QUE fazer com a segurança da informação, mas COMO?

Esse questionamento deve estar na cabeça de pelo menos 80% dos executivos ou funcionários responsáveis por gerir a segurança da informação, da parcela de empresas que estão sensibilizadas para o problema e buscam a redução dos riscos corporativos.

Diariamente lemos, ouvimos e infelizmente, muitas vezes, somos vítimas da falta de segurança e da carência de controles que efetivamente reduzam os riscos do manuseio, armazenamento, transporte e descarte de informações. Esses fatos acabam galgando os degraus do organograma corporativo e atingindo igualmente o corpo diretor. O impacto acaba por delinear ações emergenciais e prioritárias em busca do aumento do nível de segurança da informação da empresa e de seus processos de negócio, provocando comumente a criação de um Comitê de Segurança que irá assumir o grande desafio.

O Comitê passa a ser o principal elemento para o sucesso da iniciativa, assumindo o papel de maestro, acompanhando e coordenando as diversas ações que inevitavelmente ocorrerão paralelamente, objetivando apoiar a construção de uma solução integrada, que agregue valor à empresa.

Neste momento, um novo questionamento surge – agora nesta camada/esfera – tornando o objetivo ainda mais distante e complexo. O que fazer!?

Quando estamos diante de um desafio como este, o primeiro passo é tomar consciência do tamanho, amplitude e complexidade das questões relacionadas à Segurança da Informação. Para o Comitê esta tarefa não deverá ser difícil, bastando analisar a reação do mercado – e de sua própria empresa - diante da invasão tecnológica, percebendo a veloz evolução da automação de processos, digitalização de dados e principalmente a crescente dependência que as empresas têm da informação.

Apoiando este estágio, surgem normas de segurança focadas em nortear os entusiastas e "aventureiros". Com extrema competência, estas normas enumeram os desafios, etapas e processos que os ajudarão a responder a pergunta anterior, apontando o que fazer.
Assumindo a liderança e credibilidade de grande parte do mercado, a norma européia BS7799 aparece como a grande bússola. Ela trata os assuntos correlatos, dividindo-os em: "Código de Conduta para o Gerenciamento da Segurança da Informação" e "Especificações para Sistemas de Gerenciamento de Segurança da Informação".

Código de Conduta para o Gerenciamento da Segurança da Informação:

- Escopo
- Política de Segurança
- Organização de Segurança
- Classificação e controle de ativos
- Segurança aplicada a recursos humanos

- Segurança física e de ambiente
- Gerenciamento de operações e comunicações
- Controle de Acesso
- Manutenção e Desenvolvimento de Sistemas
- Gerenciamento da Continuidade do Negócio
- Conformidade

A forma como os assuntos são abordados permite o entendimento das diversas dimensões do problema e nos leva a concluir que segurança da informação extrapola a esfera tecnológica, enveredando pelos problemas e vulnerabilidades associadas à infra-estrutura, ambientes físicos, aplicações, a própria tecnologia e as pessoas. Ratificando a mensagem de que segurança é a gestão inteligente da informação em todos os ambientes.

Em função da velocidade com que estas normas vão ganhando terreno e reconhecimento, muitas iniciativas governamentais isoladas vão ocorrendo ao redor do mundo. A própria ISO – International Organization for Standartization, reconhecido organismo que subsidia os certificados ISO9001, ISO14000 etc, já está se mexendo e estudando a norma européia a fim de criar a norma ISO 17799-1 (prevista para o ano 2001). Alguns representantes de empresas privadas especializadas em segurança e organismos governamentais apoiam esta iniciativa, propondo – através de estudos paralelos - mudanças e complementos à norma européia identificados em reuniões freqüentes.

Voltando ao desafio do Comitê de Segurança, percebemos agora que já é possível iniciar as atividades de mapeamento de segurança, definição da estratégia, planejamento de segurança e até mesmo projetar de forma macro as ações de implementação. Eis então que surge um novo e ainda mais inquietante questionamento: Como fazer!?

Parece que voltamos à estaca inicial, mas ao menos há de se tirar um ensinamento de tudo isso: “As normas apenas apontam o que é preciso fazer. A Metodologia é que tem o papel de dizer como fazer”.

Diante disso, só me resta deixar uma pergunta no ar. Você que está à frente desse desafio na sua empresa, que integra o Comitê de Segurança ou que conta com o importante apoio de uma consultoria especializada em Segurança da Informação, já sabe o que fazer!?

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente de Produto e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br