

## **A importância e a implementação da segurança da informação no âmbito das atividades de negócios**

**Mônica Cassa**

O que se pode perceber nos dias atuais é que os negócios das organizações - sejam elas empresas privadas ou instituições públicas - são, na grande maioria dos casos, sustentados pela informática. Estamos na era da Tecnologia da Informação. Diante desse fato podemos afirmar que a informação é um bem, e que o seu valor é perfeitamente possível de ser medido. Portanto, a informação deve ser mantida em segurança, assim como os ambientes e os equipamentos utilizados para o seu processamento. As organizações sabem da necessidade de se praticar Segurança da Informação. E sabem que deve fazê-lo o quanto antes.

Nesse sentido, abordar a prática de Segurança da Informação significa implementar mecanismos e ferramentas de segurança que se fundamentem nos seguintes princípios:

- O princípio da Confidencialidade, que se caracteriza pela proteção da informação contra acessos não autorizados;
- O princípio da Disponibilidade, que se estabelece como a prevenção contra interrupções na operação de sistemas e no acesso à informação nos momentos em que houver necessidade;
- O princípio da Integridade, que se traduz na proteção contra manipulações e alterações indevidas;
- O princípio da Autenticidade, que reflete a identificação daquele que tem acesso à informação ou que realiza qualquer operação que a utilize;
- O princípio da Legalidade, que se conceitua como proteção da informação, no sentido de garantir a sua preservação, em conformidade com preceitos legais;
- O princípio da Auditabilidade, que significa a configuração de sistemas e bases de dados de forma a possibilitar o rastreamento de atividades físicas e lógicas.

Para que se possa compreender a abrangência da Segurança da Informação é necessário observar os principais aspectos desse cenário:

- Físico - instalações, equipamentos, infra-estrutura, insumos de várias espécies;
- Lógico - informações, sistemas, armazenamentos, construção de sistemas e bancos de dados;
- Ambiental - de TI, locais, lay-outs, conexões, segregações de ambientes;
- Organizacional - atividades, pessoas, segregação de funções, conhecimento, consciência, compromisso;
- Comunicação - internet, intranet, e-business, e-mail.

A implementação da prática de Segurança da Informação no âmbito da organização compreende uma seqüência de ações importantes e indispensáveis:

Inicialmente é necessário identificar e examinar as atividades de negócio da organização e a influência que as informações e respectivos meios e ambientes em que são tratadas exercem junto a essas atividades, visando o dimensionamento do nível de Segurança da Informação necessário.

Em seguida, deve-se avaliar o nível de Segurança da Informação existente e praticada na organização, identificando mecanismos e ferramentas utilizadas e realizando os necessários testes de vulnerabilidades.

O próximo passo será então o dimensionamento do grau de risco ao qual está exposta a organização, considerando o nível de Segurança da Informação constatado e os respectivos recursos envolvidos, tais como ambientes, hardware, software, dados, pessoas, documentação e materiais.

Identificado o nível de segurança praticado e dimensionados os riscos a que a organização está

exposta, segue-se a definição, o planejamento e a execução de ações prioritárias e emergenciais a serem executadas, visando a proteção das informações de sua propriedade ou que estão sob sua responsabilidade.

Disparada a execução das ações emergenciais, deve-se cuidar da elaboração da Política e das Diretrizes de Segurança da Informação, que caracterize o conjunto de princípios, valores e propósitos da organização, traduzidos em regras específicas para proteger as informações que são de sua propriedade ou que estão sob sua responsabilidade.

Este documento deve fundamentar-se nas normas internacionais, emanadas por organismos reconhecidamente competentes e aceitos pela comunidade de Tecnologia e Segurança da Informação, bem como nos principais mecanismos de segurança utilizados e aplicados no âmbito dessa comunidade e nas ferramentas disponíveis no mercado.

Formalizada a Política e as Diretrizes de Segurança da Informação, é imperativo que sejam realizadas definição, especificação, dimensionamento e instalação de ferramentas e soluções destinadas à prática de Segurança da Informação no âmbito da organização. Paralelamente a isso, deve-se realizar o desenvolvimento e implantação de processos - gerenciais, técnicos e de controle - para viabilizar a prática da Política e das Diretrizes de Segurança da Informação formalizadas.

Durante a realização desses trabalhos que levam à implementação da prática de Segurança da Informação na organização, deve-se realizar a atividade mais importante dessa empreitada: a conscientização das pessoas. Trata-se de programas de treinamento e desenvolvimento de pessoal destinados a funcionários, colaboradores, prestadores de serviços, fornecedores, entre outros, para que possam entender a importância e a necessidade do engajamento de todos nesta causa comum e do comprometimento com a prática efetiva de Segurança da Informação.

Muito se pode fazer implementado normas, mecanismos e ferramentas de segurança. Entretanto, sem o comprometimento dos indivíduos, pouco resultado se pode alcançar.

A partir de então, pode-se considerar implementada a prática de Segurança da Informação na organização. Resta agora fazer o gerenciamento, manutenção e atualização constante daquilo que foi implementado.

Além disso, o que se tem verificado em muitas organizações são soluções pontuais e específicas. Normalmente elas são baseadas em aplicações de ferramentas ou, na melhor das hipóteses, na implementação de certos mecanismos isolados como pequenos planos para contingências pontuais ou adotando políticas de segurança absolutamente incipientes. Isto sem qualquer amparo por processos e controles adequados. Na maioria dos casos, verifica-se aplicações de soluções inadequadas ou insuficientes para a necessidade da organização, o que pode caracterizar investimentos desnecessários ou não prioritários, com a permanência agravante de situações de risco.

A implementação efetiva de Segurança da Informação demanda conjuntos de fatores completos, adequados e ajustados às necessidades da organização, compreendendo política, diretrizes, processos, mecanismos, ferramentas, documentação e ações planejadas.

Essa atividade abrange um cenário com extensão tal que o dimensionamento e o planejamento daquilo que deve ser realizado no tocante a Segurança da Informação é tão importante quanto a implementação propriamente dita.