

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

"Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento."

Artigo 4.15 da Política de Segurança do SPB - Sistema de Pagamentos Brasileiro

Qualquer política deve cobrir os três objetivos principais da segurança da informação:

Confidencialidade

Integridade

Disponibilidade

Confidencialidade – assegura que os dados confidenciais (e no fundo todos os dados são confidenciais) sejam lidos somente pelos interessados, devidamente autorizados, e que não sejam abertos para outros, não autorizados ou para o público em geral.

Integridade – garante que os dados (ou os programas) não sofram modificações não autorizadas (fraude, sabotagem infecção por vírus, etc.)

Disponibilidade – assegura que os sistemas, a rede, as aplicações e os dados estejam on-line e que sejam acessíveis quando os usuários, autorizados, deles necessitarem.

O nível de confidencialidade, integridade e disponibilidade, varia em função do tipo de aplicação ou usuário. Por exemplo, pesquisas nucleares exigem um alto nível de confidencialidade, mas a disponibilidade não precisa ser muito alta (down times de várias horas podem ser aceitáveis). Os sistemas de difusão das informações de bolsas de valores tem necessidades mínimas de confidencialidade, mas altíssima disponibilidade e integridade. Nos bancos o Sistema de Contas Correntes tem nível elevado de confidencialidade e integridade e não muito elevado de disponibilidade. O SPB (Sistema Pagamentos Brasileiro) que deverá estar implantado ainda em 2001 pelos bancos, tem um altíssimo grau de Disponibilidade, Integridade e Confidencialidade, o que o torna bastante mais crítico que os outros sistemas bancários.

Os objetivos a seguir, embora secundários, garantem que os três acima sejam respeitados:



www.servnet.inf.br

Serviços Especializados

Consultores em Segurança da Informação, Planos de Continuidade,
Diagnostico de Segurança, Suporte a Redes, Help Desk.

O log é mais importante do que normalmente se acredita.

Accountability (Trilha de auditoria) — é a capacidade de identificar quem fez o que, o que é muito importante, de um lado como dissuasão das atividades criminosas e do outro para verificar a adequação da atividade com os objetivos da política de segurança (compliance).

Controle de Recursos— é proteger os equipamentos (computadores, servidores e estações) de danos acidentais, naturais ou dolosos (deliberados) e restringir o acesso a esses equipamentos somente ao pessoal autorizado.

Segregar tudo que for possível.

O hardware do software.

A execução do controle.

Segregação de Funções é um conceito fundamental em segurança da informação. O segredo é que o poder não deve estar concentrado nas mãos de um único indivíduo. Segregar responsabilidades, é implantar, naturalmente, um sistema de controle (checks and balances) pois passa a ser necessária a participação de mais de um indivíduo em qualquer violação da segurança. Como exemplo, os seguintes tipos de tarefas devem ser segregados:

- **Recursos dos Dados**— o responsável pelo almoxarifado não é o mesmo que faz controle do estoque.
- **Origem da Aprovação**— quem assina os cheques é diferente de quem os preenche.
- **Criação da Manutenção**— quem cria as contas de fornecedores, é diferente de quem faz os lançamentos a débito e a crédito.
- **Procedimentos dos dados** – os programadores e analistas nunca devem entrar os dados nas aplicações que desenvolveram.

Mesmo que você não se interesse pela concorrência, a concorrência se interessa por você.

Nas grandes empresas, a classificação das informações em tipos deve ser efetuada pelo menos uma vez, pois será a base de qualquer política futura. Dessa forma fica muito mais fácil desenvolver uma política fazendo referencia a tipos de dados. A implicação lógica é que os empregados ou parceiros devem também ser classificados em grupos, para poderem ter as permissões necessárias que lhes permitam acessar esses dados.

Muitas informações empresarias envolvem segredos de negócios, e devem ser classificadas como confidenciais e só serem acessíveis pelos mais altos níveis da organização. A política de segurança deve indicar o procedimento para classificar os dados e funcionários, permitindo que os funcionários acessem só e somente o que tenham direito. Mesmo empresas que julguem não precisar dessa classificação podem classificar as informações por função (p.ex. informações financeiras) e os funcionários por “papel” (contador, tesoureiro, etc.).

