2º Contecsi – Congresso Internacional de Gestão da Tecnologia e Sistemas de Informação /
Internacional Conference on Information Systems and Technology Management
01-03 de Junho de 2005 São Paulo/SP Brasil

A Segurança em Sistemas de Informação

Jorge Rady de Almeida Junior (Prof. Dr. Associado da POLI/USP) - jorge.almeida@poli.usp.br

Os Sistemas de Informação têm representado, notadamente nos últimos anos, uma grande importância para a sociedade. O valor desses sistemas pode ser constatado pelas perdas que são sentidas quando os mesmos apresentam problemas em sua operação, ainda que tal comprometimento seja apenas uma queda temporária de desempenho. Além do mais, desativações em Sistemas de Informação podem representar perdas econômicas de vulto para as organizações. Algumas aplicações podem até mesmo resultar em riscos à segurança física de pessoas e de equipamentos. Dessa forma, o objetivo deste artigo é destacar os principais aspectos a serem verificados, tendo em vista a segurança dos Sistemas de Informação. Descrevem-se técnicas de projeto que visam garantir a segurança desses sistemas. A metodologia apresentada neste artigo inclui os planos de contingência e de recuperação de desastres, a importância fundamental de se ter uma cultura de segurança implantada na organização, além do papel vital da elaboração cuidadosa dos requisitos voltados para a segurança da informação. Ressalta-se ainda o papel primordial da análise de segurança dos Sistemas de Informação, bem como a necessidade de utilização de normas voltadas para a segurança da informação. Como resultados, destacam-se as principais conclusões e recomendações resultantes do estudo criterioso realizado.

Palavras-Chave: Segurança de Informação, Sistemas de Informação, Requisitos de Segurança.

A SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

1. INTRODUÇÃO

A informação e seus Sistemas de Informação associados vêm apresentando uma crescente relevância nas atividades desempenhadas pelas organizações. A informação deve, e de fato vem sendo, considerada como um ativo da maior relevância, cuja obtenção e posterior manutenção são extremamente necessárias. Desta forma, tornam-se vitais as atividades que visem garantir um gerenciamento eficaz desses Sistemas de Informação. As modernas organizações, através desse contínuo gerenciamento, tornam-se aptas a atuar no ambiente, cada vez mais competitivo, representado pelo atual panorama econômico e tecnológico (Laudon; Laudon, 2002).

Há um número muito grande de aplicações envolvendo Sistemas de Informação, as quais compreendem a prestação de serviços já fundamentais à sociedade moderna. Como exemplos dessas aplicações podem ser citados os sistemas bancários, os sistemas de reserva de passagens aéreas e todo o comércio eletrônico efetuado por meio da Internet, dentre outros.

Os Sistemas de Informação devem ter uma disponibilidade muito grande. Um problema nesses sistemas pode significar um prejuízo muito grande para as

atividades de uma organização. Pode-se citar alguns dados que corroboram para tal afirmação: em 1998, nos Estados Unidos, o custo de inatividade por hora, de alguns importantes sistemas computacionais estava estimado em: US$ 1.150.000,00 para o sistema *pay-per-view* de operadoras de TV a cabo, US$ 2.600.000,00 para operadoras de cartões de crédito e US$ 6.500.000,00 para operadoras de bolsa de valores. Deve-se frisar que esses números consideram apenas as perdas diretas, não incluindo efeitos negativos que consideram o aspecto psicológico, o qual envolve, por exemplo, a perda de credibilidade das instituições envolvidas (IBM, 1999).

Além da necessidade de se ter uma grande disponibilidade dos Sistemas de Informação, há ainda outros fatores a serem levados em conta, tais como a garantia de um desempenho compatível com as especificações, a segurança dos dados armazenados contra invasões ou furto de informação, a manutenção permanente da consistência dos dados e a facilidade de utilização.

Diferente de sistemas de supervisão e controle de Sistemas Críticos, tal como o sistema responsável pela operação de uma usina nuclear, onde há riscos físicos envolvidos, em Sistemas de Informação não há situações diretamente ligadas a eventos de calamidade ou de acidentes. Eventos que podem ocorrer, além da paralisação de um sistema, são a perda ou a adulteração de dados, ou ainda com a invasão do sistema por pessoas ou sistemas não autorizados.

O foco principal da segurança em Sistemas de Informação está voltado para a proteção e controle do ambiente computacional que o compõe. Através de mecanismos que visem proporcionar a proteção desses sistemas, também se busca a garantia da Segurança de Informação.

Pode-se dizer que o objetivo primordial da política de Segurança de Informação de uma organização está dirigido para que se evitem incidentes de segurança, sejam tais incidentes representados por acontecimentos intencionais ou não.

A estrutura deste trabalho contempla, em seu segundo item, uma descrição geral sobre os Sistemas de Informação. O item 3 apresenta conceitos sobre a segurança de Sistemas de Informação, abrangendo seus objetivos, os principais mecanismos utilizados para a sua garantia, além de destacar a importância da existência de uma cultura de Segurança de Informação. Também são destacados os papéis da Análise de Segurança e das Normas voltadas para Sistemas de Informação. No item 4 descrevem-se os resultados e recomendações resultantes do estudo realizado. Finalmente no item 5 são apresentadas as principais conclusões deste trabalho.

2. SISTEMAS DE INFORMAÇÃO

Um Sistema de Informação pode ser definido como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem informações para apoiar o processo de tomada de decisões e o controle de uma organização. Sistemas de Informação contêm informações sobre pessoas, lugares e coisas significativas dentro da organização ou do ambiente que a envolve (Laudon; Laudon, 2002).

O Sistema de Informação de uma organização deve contemplar todos os elementos que sejam úteis à condução dos negócios da mesma. Esses elementos podem abranger desde a forma como as atividades devem ser conduzidas, até o conhecimento geral possuído por essa organização. Tendo em vista a utilização

intensiva dos Sistemas de Informação, vem ocorrendo uma influência mútua entre estes últimos e as organizações. Tais sistemas devem ser projetados de forma a se adaptarem às organizações, gerando as informações necessárias e importantes ao desenvolvimento de suas atividades. Por sua parte, a organização deve estar aberta às influências geradas pelo Sistema de Informação, eventualmente alterando sua forma de trabalho.

Todo o esforço representado pela criação e manutenção dos Sistemas de Informação tem sua origem na importância que a informação tem representando, justificando todo o empenho realizado, visando garantir sua proteção e segurança, assegurando a continuidade das atividades que deles dependam.

Segundo um estudo realizado pela SIMS – *School of Information Management and Systems* da Universidade da Califórnia, Berkeley, no ano de 2001 a humanidade produziu o equivalente a 6 exabytes de informação, sendo que esse número vem dobrando a cada ano e inclui apenas uma versão original, não contabilizando réplicas (Berkeley, 2002), (Winter, 2002). Para se ter idéia de quão grande é esse número, considere-se que o tamanho médio de um documento seja de 1 MB, isto significa que, em média, cada ser humano, seja homem, mulher ou criança, gerou 1.000 documentos de 1 MB cada um, no ano de 2001, considerando-se uma população mundial de 6 bilhões de pessoas. É claro que o número de pessoas, que de fato geram informações e seus documentos associados, é muito inferior a este último valor apresentado.

Há uma linha de pesquisa que aponta para uma tendência de que alguns Sistemas de Informação possam ser considerados como sistemas críticos (Almeida, 2003). Segundo essa linha de raciocínio, um sistema pode ser dito crítico quando uma falha causada pelo mesmo possa levar o sistema a apresentar conseqüências inaceitáveis. Como exemplos podem ser citados os casos de falhas em um sistema de crédito, a qual pode levar a grandes perdas financeiras, falhas em uma central de atendimento, que pode tornar indisponível o atendimento a clientes atuais e a possíveis novos clientes, e assim por diante.

Um fator a ser considerado é que a maioria das aplicações tem sido desenvolvida para ambientes distribuídos e heterogêneos, principalmente para a Internet. Por outro lado, esse tipo de implementação sujeita as organizações a uma maior exposição, aumentando os riscos relacionados com as possibilidades do uso indiscriminado de informações consideradas segredos de negócios.

É importante destacar que uma aplicação distribuída não é sinônimo de uma aplicação insegura. Devem ser utilizados os mecanismos apropriados para que o nível de Segurança de Informação seja mantido em patamares aceitáveis, tendo em vista que não é possível se obter uma segurança absoluta (Dias, 2000).

3. METODOLOGIA PARA GARANTIA DA SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

A metodologia apresentada neste trabalho, no tocante à garantia da segurança da informação consiste de alguns passos. O primeiro deles refere-se à avaliação dos riscos e dos impactos a que os Sistemas de Informação podem estar submetidos. O segundo passo inclui a realização de uma comparação com entre os níveis de segurança exigidos e os níveis de segurança obtidos para o Sistema de Informação. O terceiro passo reside no estudo das diversas técnicas existentes, visando a garantia da segurança nesses sistemas. Finalmente, seguem-se os passos da

implementação das técnicas consideradas mais adequadas e a avaliação após a sua implementação.

O ambiente computacional, no qual se inserem os Sistemas de Informação, deve ser controlado e protegido contra todas as causas previsíveis que possam prejudicar sua operação: desastres naturais (incêndios, terremotos), falhas estruturais (interrupções no fornecimento de energia), sabotagens, fraudes e acessos não autorizados. Isso significa que deve haver um esquema eficiente de proteção da informação nesses sistemas, ou seja, deve ser implementado um esquema para se garantir a Segurança de Informação.

A Segurança de Informação pode ser definida como a proteção de informações e de seu respectivo sistema computacional contra intervenções não autorizadas, falhas e desastres, de forma a reduzir a probabilidade de incidentes. Por incidente entende-se a perda de consistência dos dados, a sua alteração ou ainda o furto de informações por pessoas ou sistemas não autorizados (Almeida, 2003).

Desta forma, pode-se dizer que os principais objetivos de uma política de Segurança de Informação são: a redução da probabilidade de ocorrência de incidentes de segurança, a redução de danos causados por tais incidentes, além da recuperação em caso de problemas de segurança (Moreira, 2001).

A realização de pesquisas em empresas que vendem produtos ou serviços pela Internet demonstrou que 60% delas acusaram, em um ano, um ou mais ataques a seus sites (Price, 2002). Esse número aponta para a necessidade de se prover mecanismos adequados e eficazes para a proteção da informação, tendo em vista a gravidade do problema.

Resumidamente, a atividade de garantia da Segurança de Informação se inicia com a definição de uma política global de segurança da organização, passando pela análise de risco, pelos controles de acesso físico e lógico aos recursos computacionais, pelo treinamento e conscientização de funcionários, e finalizando com a existência de um plano de contingência e recuperação de desastres.

3.1. Objetivos da Segurança de Informação

A manutenção da disponibilidade, da confidencialidade e da integridade da informação representa o objetivo fundamental da Segurança de Informação. Um usuário, ao buscar informações, espera que as mesmas estejam disponíveis no momento que ele necessitar, não possam ser acessadas por pessoas ou sistemas não autorizados e ainda que seu conteúdo não possa ter sido alterado indevidamente (Dias, 2000).

A manutenção da disponibilidade representa a medida da probabilidade de um sistema estar sem falha em um determinado instante de tempo. A manutenção da confidencialidade aponta para a necessidade de se prover proteção às informações contra o acesso de pessoas ou programas não autorizados, mantendo o sigilo e a privacidade das informações. Finalmente, manter íntegras as informações de um Sistema de Informações tem a finalidade de protegê-las contra alterações não autorizadas pelo proprietário ou do responsável pelas mesmas.

A prioridade relativa de cada uma dessas propriedades varia conforme o Sistema de Informação, podendo-se atribuir prioridades relativas às mesmas, cujos pesos serão determinados em função da natureza de cada aplicação, das ameaças e riscos a

que se esteja sujeito e de prováveis impactos resultantes de violações da Segurança de Informação.

É importante que se proceda à definição de qual deve ser a parcela de informação a ser protegida, além de se determinar o tipo de indivíduo ou de sistema que possa representar ameaças à informação. Outra etapa na manutenção da segurança de informação consiste na identificação das ameaças mais prováveis, determinando-se também o nível de proteção mais adequado.

Deve ser bem explicitada a quantidade de recursos disponíveis para o desenvolvimento e implantação de políticas de Segurança de Informação, bem como o tempo disponível ao seu desenvolvimento. Esses recursos devem fazer parte do planejamento geral das empresas.

Finalmente, é necessário que se conheçam quais são as expectativas de usuários e clientes em relação à Segurança de Informação e quais são as conseqüências para a organização em caso de violação das condições de segurança.

Através da obtenção de todos esses parâmetros, torna-se possível a definição das linhas gerais da política de Segurança de Informação de uma organização. As medidas preventivas a serem adotadas devem ser definidas de forma a atender aos requisitos da política de segurança, tendo sempre em mente a manutenção do equilíbrio entre os fatores custo da implementação de medidas de segurança e os respectivos benefícios associados.

O apoio da alta direção de uma organização é um fator primordial para que sua política de Segurança de Informação possa ser bem sucedida. Tal apoio não deve se restringir apenas à liberação de recursos, incluindo-se também o aspecto de se atribuir à Segurança de Informação uma alta prioridade dentro da organização.

O ideal é que as ações que visem a garantia da Segurança de Informação sejam projetadas e implementadas nas fases iniciais do desenvolvimento do sistema, de maneira que quando o Sistema de Informação entrar no ar, todas os mecanismos de proteção já estejam implementados, evitando-se adicionar mecanismos apenas após a ocorrência de incidentes relacionados à Segurança de Informação.

Tendo em vista que o ambiente computacional é muito dinâmico, não faz sentido a adoção de uma política inflexível no que diz respeito à Segurança de Informação. Pelo contrário, deve ser possível a adaptação da política adotada, conforme se altere o ambiente em que o Sistema de Informação estiver inserido. A política de segurança implantada deve ter ampla divulgação na organização, inserindo-se em sua política global de condução dos negócios.

Um aspecto que deve constar dessa política de Segurança da Informação, é a definição das responsabilidades de todos os membros da organização, atribuindo-se direitos e deveres a cada um.

3.2. Mecanismos de Segurança de Informação

Os mecanismos utilizados para implementar a Segurança de Informação englobam o controle físico do ambiente computacional, o controle lógico, através de autenticações e controle de acesso, chegando até o controle humano, representado pelo treinamento de funcionários e pela realização de auditorias.

Os principais objetos de proteção incluem programas aplicativos, arquivos de dados, utilitários, sistema operacional, arquivos de senha e arquivos de histórico de uso (Dias, 2000).

O objetivo de proteger programas aplicativos (programas fonte ou programas executáveis) é o de impedir sua alteração ou ainda sua execução indevida. De forma a evitar consultas e alterações indevidas em dados vitais ao negócio da organização, deve-se proteger os arquivos de dados.

Um aspecto de fundamental importância na questão da Segurança de Informação refere-se ao sistema operacional dos computadores, o qual se constitui em um ponto chave do controle do esquema de segurança. Uma possível fragilidade no sistema operacional pode permitir o acesso de pessoas ou sistemas não autorizados às informações da organização.

Como exemplo, o acesso aos arquivos de senha de um Sistema de Informação, pode representar a obtenção de todas as senhas desse sistema, abrindo a possibilidade de acesso livre e irrestrito aos seus recursos.

Há diversos mecanismos utilizados, visando a manutenção da Segurança de Informação: uso de criptografia na transmissão de mensagens, certificação digital para acesso a informações, segurança física, existência de um plano de contingência, detecção de invasões, realização de auditorias e existência de programas antivírus (Dias, 2000).

Esses mecanismos podem ser classificados em três tipos implementação: controles de acesso físico, controles de acesso lógico e a segurança na comunicação.

A utilização dos controles de acesso físico tem com objetivo impedir o acesso físico de pessoas não autorizadas a certos objetos. Por objetos entendem-se os equipamentos que compõem o sistema computacional que aloja o Sistema de Informação. Normalmente, obtém-se a segurança física escondendo-se ou ocultando-se a localização dos objetos, ou ainda isolando-os e protegendo-os, dificultando ainda mais o acesso aos mesmos.

Pode-se dizer que, através dos controles de acesso físico, apenas as pessoas autorizadas obtenham acesso ao ambiente físico que contém os recursos computacionais do Sistema de Informação.

Os controles de acesso lógico são implementados, tendo em vista que os controles de acesso físico não são suficientes para garantir a segurança de informações de um sistema computacional. Os controles de acesso lógico são implementados por intermédio de hardware e de software.

O controle de acesso lógico visa restringir o acesso ao sistema computacional apenas a usuários autorizados, sendo que esse acesso deve se restringir somente aos recursos realmente necessários à execução de suas tarefas. Isto significa que, usuários devem ser impedidos de executar transações incompatíveis com suas funções ou além de suas responsabilidades.

Praticamente não faz mais sentido a utilização de um sistema computacional completamente isolado dos demais, ou seja, há a necessidade de comunicação e a conseqüente troca de informações com outros sistemas computacionais. É nessa comunicação que surgem os principais problemas de segurança em Sistemas de Informação.

Usuários não autorizados podem se conectar e passar por usuários autorizados. Se um invasor conseguir se fazer passar como um usuário legítimo, provavelmente terá o acesso facilitado a todas as informações que desejar furtar ou adulterar. Mesmo usuários autorizados têm restrições de acesso. Eles podem tentar burlar os controles e executar operações ou obter dados a que não teriam direito.

Com o objetivo de fixar algumas normas mínimas de segurança, o governo britânico estabeleceu uma diretriz, cujo objetivo é o de conter ou minimizar ataques a sistemas computacionais (Hunter, 2001). Essa diretriz estabelece que, se qualquer parte de um sistema ou rede de computadores transportar informações sigilosas sobre o andamento de projetos e negócios de uma empresa, e for acessível por áreas não controladas (por ex. rede pública de telefonia), a comunicação deve ser protegida por métodos de criptografia.

A criptografia é uma das principais formas de se incrementar a segurança na comunicação e no armazenamento de dados. A criptografia compreende a codificação, pelo sistema que estiver gerando mensagens ou dados, e a decodificação, pelo sistema destinatário das mensagens ou dados.

3.3. Planos de Contingência e de Recuperação de Desastres

Pode-se afirmar que não há mecanismos que proporcionem a proteção completa de um Sistema de Informação. Considerando-se tal situação, faz-se necessário que, além das medidas de proteção, exista um plano de contingência e um plano de recuperação de desastres.

A finalidade do plano de contingência é manter a operação do Sistema de Informação, ainda que tenham ocorrido problemas, como, por exemplo, uma invasão com adulteração de dados, ou um acidente natural, como um incêndio no sistema computacional.

Se for registrado algum problema que impeça a operação completa do Sistema de Informação, deve ser possível ainda operá-lo com um certo grau de degradação, sempre na dependência da extensão do problema ocorrido.

No que se refere a perdas financeiras, pode-se dizer que os planos de contingência e de recuperação de desastres não contribuem, diretamente, para um aumento da lucratividade da instituição, mas sim possibilitam que se evitem maiores perdas em decorrência de incidentes que possam ocorrer.

Tendo em vista que a disponibilidade de um Sistema de Informação e a confiabilidade em seus dados influem diretamente na credibilidade da instituição proprietária do Sistema, quanto mais tempo este estiver indisponível, maiores serão os impactos nos negócios. Dessa forma, um dos principais objetivos de um plano de contingência é minimizar o tempo de parada dos sistemas.

a) Fases do Plano de Contingência

As fases que compõem um plano de contingência são (Maiwald; Siegleim, 2002):

- Análises Preliminares: nesta fase realiza-se de um estudo preliminar, envolvendo a identificação das funções e recursos críticos ao Sistema de Informação. Outro objetivo é o de envolver e conscientizar a alta direção da empresa sobre a importância da implementação de um plano de contingência, tendo em vista que tal tarefa compreende, invariavelmente, a aplicação de recursos financeiros.

Funcionários também devem ser conscientizados a respeito da importância deste tipo de atividade.

- Análise de Impacto: compreende a identificação de impactos sobre a instituição, o que significa avaliar os danos potenciais que uma ameaça possa causar, ao ser concretizada. Realiza-se a avaliação do tempo que cada atividade, sistema ou recurso possa ficar indisponível ou com funcionalidade reduzida.
- Análise das Alternativas de Recuperação: compreende a realização de um estudo sobre possíveis as alternativas de operação, tendo como objetivo a recuperação dos serviços computacionais ligados ao Sistema de Informação. Uma alternativa que apresenta significativa eficiência é representada pela manutenção do chamado *hot site*, que se constitui em um local alternativo de processamento paralelo que, em caso de qualquer problema no site principal, está capacitado para assumir imediatamente o comando do sistema.
- Desenvolvimento do Plano de Contingência: nesta fase é feito o detalhamento do plano, identificando-se os recursos necessários à sua implementação. Os principais passos a serem executados em resposta a um desastre são: identificação e compreensão do problema, contenção dos danos, limitando ou resolvendo o problema, determinação dos danos causados, restauração dos sistemas à sua operação normal e eliminação das causas, para que o problema não ocorra novamente.

b) Recuperação de Desastres

Após a ocorrência de um problema, considerando-se a operação degradada ou não do Sistema de Informação, vem a fase de recuperação do desastre. Nesta etapa ocorre a substituição dos recursos computacionais, provavelmente danificados, por outros recursos previamente reservados para essa função, possibilitando o retorno a um funcionamento normal e com todas as funções originalmente previstas para o sistema.

O objetivo da recuperação de desastres é manter a disponibilidade especificada de um Sistema de Informação. A capacidade recuperação de um Sistema de Informação representa a habilidade de uma empresa em se recuperar de um incidente de segurança. A empresa deve estar apta a continuar operando seus Sistemas de Informação mesmo após a ocorrência de um problema desse tipo. O nível de recuperação é determinado pelos tipos de incidentes que possam afetar a empresa e pelos impactos potenciais de um incidente de Segurança de Informação (Massiglia; Marcus, 2002).

Tendo em vista que a eficiência de um negócio pode ser entendida como fazer o que deve ser feito, utilizando o mínimo possível de recursos, podem ocorrer conflitos na implantação de mecanismos de recuperação, os quais sempre levam à utilização de mecanismos e equipamentos adicionais àqueles estritamente necessários ao funcionamento sem falhas do sistema (Byrnes; Kutnick, 2002).

Em um plano de recuperação de desastres há dois problemas básicos a serem resolvidos. O primeiro problema refere-se à forma como uma função tornada inoperante, em decorrência de um incidente, deve ser restaurada. O segundo problema que se coloca é, se durante a recuperação de um incidente, outro incidente ocorrer, levando uma segunda função a se tornar inoperante, como serão resolvidos eventuais conflitos de demanda requeridos para recobrar as duas funções afetadas.

Desta forma, em um plano de recuperação, é importante que se identifiquem as prioridades de cada aspecto do funcionamento do sistema, bem como as formas de resolução de conflitos, possivelmente existentes, para que a recuperação seja viável.

3.4. Cultura de Segurança em Sistemas de Informação

Pode-se dizer que, através da aplicação de uma única técnica que vise garantir a Segurança da Informação, não é possível assegurar a solução de todos os problemas a ela relacionados.

Portanto, faz-se necessária a existência de um programa de conscientização que torne possível a preparação dos envolvidos com a operação e manutenção de um Sistema de Informação, de forma que todos estejam capacitados a compreender e participar do processo de implementação da Segurança de Informação.

Os envolvidos na operação e manutenção de um Sistema de Informação devem receber o treinamento adequado, no que se refere à Segurança de Informação. Tal treinamento deve ser contínuo, buscando manter todo o corpo de funcionários atualizado quanto aos conceitos e normas implementados, bem como obter sua consciência e o comprometimento com o processo de garantia da Segurança de Informação.

A equipe encarregada do projeto da Segurança de Informação deve ser capacitada, de forma a transmitir confiança e credibilidade, antes, durante e após o processo de implementação de garantia da Segurança de Informação.

Devem ser estabelecidos e amplamente divulgados a toda organização, um conjunto de normas e diretrizes, as quais devem descrever os objetos a serem protegidos, contra quem e contra o que proteger, além das principais medidas a serem acionadas em caso de incidentes de segurança.

Apenas a utilização de modernas tecnologias não é suficiente para a proteção da informação. Práticas de segurança não são simples mecanismos da Tecnologia da Informação implementados através de hardware e de software. Tais práticas são resultado de experiências adquiridas em processos de garantia da segurança. Atos isolados não são suficientes para garantir a Segurança de Informação, mas sim um conjunto de diretrizes e procedimentos.

Alguns autores afirmam que o ponto mais vulnerável da Segurança de Informação é constituído pelos funcionários da empresa, tornando vital sua conscientização. Os próprios funcionários podem cometer erros, utilizar indevidamente os sistemas ou mesmo realizar atos de sabotagem.

Além dos próprios funcionários da organização detentora do sistema, a outra fonte de risco que se apresenta a um Sistema de Informação é constituída por invasores externos e pelo ambiente do sistema computacional.

Invasores externos podem ocasionar todos os tipos de problemas já citados, tais como roubo de informações, destruição ou alteração deliberada de informações ou ainda inclusão de informações com o intuito de sabotar ou confundir usuários autorizados do sistema. No que se refere ao ambiente do sistema computacional, há o risco de interferências eletromagnéticas, bem como de desastres naturais, tal como um incêndio (Almeida, 2003).

Assim como em outras áreas, o desenvolvimento de práticas adequadas de Segurança de Informação também tem um ciclo, composto pela identificação e a avaliação das melhores práticas de acordo com determinados critérios, a adoção e a documentação das práticas selecionadas e eventuais adaptações ou melhorias que se façam necessárias, em virtude de constantes inovações tecnológicas e de alterações do ambiente.

3.5. Requisitos de Segurança de Informação

Um dos aspectos de maior relevância dentro de uma cultura de Segurança de Informação se constitui na definição dos requisitos de segurança aplicáveis a tais sistemas.

Os requisitos de segurança de um Sistema de Informação devem incluir a proteção contra todos os riscos identificados, incluindo-se riscos internos e externos.

A segurança dos primeiros Sistemas de Informação restringia-se ao controle de acesso físico aos locais onde se situavam os sistemas computacionais. Evoluções desse panorama passaram a considerar a identificação e autenticação para o acesso lógico aos recursos dos sistemas. A comunicação entre computadores também passou a integrar os requisitos de Segurança de Informação.

Pode-se dizer que os ataques terroristas ocorridos nos últimos anos também foram um fator propulsor dessa maior preocupação com a Segurança de Informação, visto que há diversos sistemas, muitos deles governamentais, que despertam grande cobiça por pessoas ligadas a grupos terroristas (Ghosh, 2002).

A falta de confiança e o receio de existência de pontos vulneráveis na Segurança de Informação constituem-se na grande fonte de resistência à utilização do comércio eletrônico. Um ataque a uma rede de computadores pode afetar a milhares ou mesmo milhões de pessoas, como por exemplo, a invasão de computadores de bolsas de valores, de instituições financeiras, de monitoramento de pacientes em um hospital, de vendas de passagens, etc.

Alguns sistemas, buscando uma maior segurança a seu acesso, já incluem, em seus requisitos de segurança, a necessidade do uso da identificação através de características físicas de seus usuários, tais como a impressão digital, a voz ou a íris, dentre outros.

Outro ponto bastante importante é a especificação da utilização de técnicas de criptografia de dados. Praticamente não se concebe mais a existência de comunicação de dados de valor sem a utilização da criptografia para a sua proteção.

A especificação de requisitos deve abranger os requisitos comuns a todos os Sistemas de Informação: a existência de um plano de contingência, de um plano de recuperação de desastres e minimização de conseqüências em virtude de um problema de segurança.

Também devem constar dos requisitos a especificação das manutenções preventiva e corretiva. Na manutenção preventiva, devem ser estabelecidos intervalos mínimos necessários à realização desse tipo de manutenção, visando manter a disponibilidade desejada. Com relação às manutenções corretivas, devem ser estabelecidos tempos máximos para que a equipe de manutenção consiga reparar todos os módulos que possivelmente tenham apresentado problemas, restaurando o sistema à sua condição inicial.

Requisitos não diretamente ligados à Segurança de Informação também devem ser especificados, como, por exemplo, o desempenho e a capacidade de armazenamento de dados.

3.6. Análise de Segurança de Sistemas de Informação

A Análise de Segurança de Sistemas de Informação é feita observando-se as ameaças, riscos e impactos que possíveis invasões ou problemas nos sistemas possam causar à sua operação.

Em uma Análise de Segurança de Sistemas de Informação, as principais etapas a serem cumpridas são: a classificação das informações, a análise de ameaças e a análise de riscos e impactos, a seguir descritos.

a) Classificação das Informações

O grau de proteção exigido para uma aplicação varia de acordo com o tipo de informação processada, tornando necessário o estabelecimento de uma classificação dos tipos de informações existentes em uma organização. Uma das classificações mais utilizadas é a seguinte (Dias, 2000):

- Públicas ou de Uso Irrestrito: são informações que podem ser divulgadas livremente a qualquer pessoa, sem nenhuma implicação para a instituição, como por exemplo material de divulgação institucional da empresa;
- Internas: tal tipo de informação não deve ser divulgado fora da instituição, mas se isso ocorrer, as conseqüências não são críticas, como, por exemplo, informações gerais internas;
- Confidenciais: representam informações sigilosas sobre o andamento de projetos e negócios da empresa, sendo que mesmo o acesso interno é controlado, como, por exemplo, dados de clientes e de projetos; e
- Secretas: constituem-se em informações altamente confidenciais e de acesso extremamente controlado, mesmo dentro da empresa, como, por exemplo, arquivos de senhas e de dados financeiros.

b) Ameaças a um Sistema de Informação

Ameaças representam perigos potenciais aos recursos de um sistema computacional e a seu Sistema de Informação. Desta forma, torna-se necessário conhecer as ameaças potenciais a um Sistema de Informação para que se possam tomar as medidas necessárias à proteção de suas informações. O furto de informações, a ocorrência de um incêndio ou o ataque por um vírus de computador são possíveis tipos de eventos ou atividades indesejáveis que compõem uma ameaça.

A concretização de uma ameaça pode desabilitar, danificar ou excluir um recurso computacional do Sistema de Informação, seja esse recurso constituído pela informação em si ou por qualquer componente de hardware ou software do sistema computacional (Almeida, 2003).

O alvo das ameaças se concentra em explorar as deficiências ou vulnerabilidades de um sistema, que podem ser classificadas da seguinte forma (Dias, 2000):

- Humanas: estão ligadas à falta de treinamento e de comprometimento de funcionários para com a organização, bem como a possíveis compartilhamentos de informações entre seus próprios funcionários;
- Físicas: referem-se ao não policiamento de salas e à não existência de barreiras físicas com relação ao local onde está instalado o hardware do Sistema de Informação;
- Naturais: são provocadas por eventos tais como terremotos, enchentes e condições de temperatura e umidade inadequadas do ambiente computacional;
- Software: ficam por conta de problemas no sistema operacional e nos programas aplicativos; e
- Comunicação de Dados: está ligada à não existência de mecanismos de proteção na comunicação de dados entre máquinas.

As barreiras de proteção de um Sistema de Informação devem ser analisadas, de forma a se verificar a possibilidade de potenciais ameaças conseguirem superá-las. Aí estarão identificados os pontos vulneráveis do Sistema de Informação, tornando necessária a realização de uma análise do impacto decorrente da concretização das ameaças.

Uma forma de classificação das ameaças é dividi-las em duas categorias: acidentais e deliberadas. Falhas no hardware, erros de programação ou ainda desastres naturais representam ameaças do tipo acidental. Tentativas de acesso não autorizado ao sistema constituem ameaças do tipo deliberado ou proposital.

c) Análise de Riscos e de Impactos

O risco a um Sistema de Informação representa a probabilidade da ocorrência de qualquer evento que possa vir a afetar as atividades de uma organização, impedindo que se atinjam os objetivos planejados em termos dos negócios a serem realizados.

Por sua vez, a análise de risco compreende a análise das ameaças que possam estar presentes, das vulnerabilidades de um sistema e dos impactos decorrentes da concretização de ameaças.

Só é possível adotar corretamente as medidas preventivas desde que se conheçam as ameaças potenciais, como tais ameaças podem explorar as vulnerabilidades do sistema e quais são os possíveis impactos, tendo em vista as ameaças existentes. ✓

Os principais impactos a que os sistemas computacionais estão sujeitos são: modificação dos dados, indisponibilidade de sistemas vitais, divulgação de informações confidenciais, perda de credibilidade da instituição, possibilidade de abertura de processos legais contra a mesma, além da perda de clientes para a concorrência (Byrnes; Kutnick, 2002). ✓

A análise de risco constitui-se no processo de identificação e avaliação dos fatores de risco presentes, de forma antecipada, possibilitando uma visão do impacto negativo, possivelmente causado aos negócios. A realização da análise de risco possibilita a identificação do valor e do tipo de investimento necessário para a prevenção de ataques contra a informação.

O custo é um dos fatores a ser considerado quando da análise de risco, pois se o custo para se combater uma ameaça potencial for superior a um possível dano decorrente dessa ameaça, talvez não seja aconselhável tomar as medidas preventivas necessárias.

Não é possível a eliminação total dos riscos de um Sistema de Informação. No entanto, os riscos podem ser reduzidos através da adoção de medidas de segurança, diminuindo-se a probabilidade de sua ocorrência, mas nunca os anulando por completo (Dias, 2000).

3.7. Normas Utilizadas em Sistemas de Informação

Neste item são apresentadas algumas das normas existentes na área de Tecnologia da Informação, e que abrangem o aspecto da Segurança de Informação. Essas normas têm como objetivo fornecer linhas de ação especialmente concebidas para o projeto e implementação de Sistemas de Informação.

a) Norma NBR ISO/IEC 17799

Esta norma da ABNT (Associação Brasileira de Normas Técnicas) tem sua origem na norma ISO/IEC 17799:2000, que por sua vez se originou da primeira parte da norma britânica BS7799, do *British Standard Institute*. A ABNT homologou a NBR ISO/IEC 17799 - Tecnologia da Informação: Código de Prática para a Gestão da Segurança de Informação - em 2001 (ABNT, 2001). A segunda parte da norma britânica BS7799 refere-se à especificação de sistemas de gestão para a Segurança de Informação e vem sendo objeto de estudos por parte do ISO (*International Standards Organization*) para a sua adoção a nível mundial.

O objetivo desta norma é o de fornecer recomendações para a gestão da Segurança de Informação, para assegurar a continuidade da operação de sistemas computacionais e minimizar danos aos negócios, prevenindo e diminuindo o impacto de incidentes de segurança. Outros objetivos são o de prover uma base comum para o desenvolvimento de práticas de segurança nas organizações, bem como prover segurança nos relacionamentos entre empresas.

Na NBR ISO/IEC 17799, a Segurança de Informação é caracterizada pela preservação dos atributos de confidencialidade, integridade e disponibilidade. Por confidencialidade a norma se refere às informações cujo acesso só pode ser feito por parte de quem possuir autorização para tal. A integridade refere-se à garantia da precisão das informações e a disponibilidade está relacionada à garantia de que os usuários autorizados tenham acesso, quando necessário, à informação.

A norma NBR ISO/IEC 17799 define a Segurança de Informação como a proteção contra ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimento e oportunidades.

b) Norma ISO/IEC 15408-1

Esta norma - *Information Technology – Security Techniques – Evaluation Criteria for IT Security* - é editada pelo ISO/IEC (*International Organization for Standardization/International Electrotechinical Commision*), tendo sido aprovada em 1999 (IEC, 1999). Sua finalidade é a de definir como os chamados Critérios Comuns (*Common Criteria* - CC) devem ser usados para a avaliação de propriedades de segurança de informação em produtos e sistemas que envolvam Tecnologia da Informação.

Esses Critérios Comuns provêm um conjunto comum de requisitos às funções de segurança da Tecnologia de Informação, abrangendo, dentre outros, proteção contra acessos indevidos, modificações ou exclusões não autorizadas de informações.

O público alvo para esta norma é composto por consumidores, desenvolvedores e avaliadores. Os consumidores ou usuários podem utilizar resultados de avaliações para decidir qual ou quais produtos irão incorporar em seus sistemas. Desenvolvedores utilizam a norma para preparar seus produtos de forma adequada aos requisitos mínimos de Segurança de Informação. Finalmente, avaliadores utilizam a norma para poderem exercer os julgamentos necessários sobre produtos desenvolvidos.

A norma é dividida em três partes, a primeira com uma introdução e a apresentação de um modelo geral de avaliação, a segunda estabelece um conjunto de requisitos funcionais e a terceira um conjunto de requisitos de segurança.

c) Norma NIST 800-30

Esta norma - Risk Management Guide for Information Technology Systems - é editada pelo NIST (*National Institute of Standards and Technology*), órgão americano, tendo sido aprovada em 2001 (NIST, 2001). Sua finalidade é a de prover uma base para o desenvolvimento de um programa de gerenciamento de risco, contendo definições e um guia prático para detectar e diminuir riscos em Sistemas de Informação.

O público alvo desta norma vai desde a alta gerência de uma organização, até o grupo encarregado da garantia da qualidade, passando por todo o pessoal técnico.

A norma NIST 800-30 fornece uma visão geral sobre o gerenciamento de riscos, sua importância e sua integração no ciclo de desenvolvimento de sistemas. A norma estabelece ainda as funções de cada um dos responsáveis pelo sistema, no que diz respeito ao gerenciamento de risco.

Na NIST 800-30 são descritos nove passos para a determinação dos riscos: caracterização do sistema, identificação de ameaças, identificação de vulnerabilidades, análise dos controles de segurança, determinação das probabilidades das ameaças identificadas, análise de impacto, determinação do nível de risco, geração de recomendações e geração de documentação com os resultados.

A norma apresenta também um questionário para a realização de entrevistas, cuja finalidade é a detecção de áreas de risco na organização.

d) Orange Book

No fim dos anos 70 a *National Security Agency* (NSA), agência americana estabeleceu requisitos formais a serem cumpridos para a Segurança de Informação, publicados em uma série de documentos conhecidos como *Rainbow Books*. O mais significativo desses é o *Orange Book*, que teve sua primeira edição em 1983 e uma revisão em 1986 (Hunter, 2001). A denominação oficial do Oran*ge Book* é TCSEC (*Trusted Computer System Evaluation Criteria*).

O *Orange Book* apresenta as características requeridas para sistemas computacionais, onde a Segurança de Informação é uma exigência. O *Orange Book* apresenta 27 propriedades desejáveis para a Segurança de Informação, dentre elas auditoria, gerenciamento de configurações, documentação, especificação e verificação, controle de acesso, identificação e autenticação, testes de segurança e recuperação. O *Red Book* interpreta os princípios e critérios do *Orange Book* para ambientes do tipo cliente/servidor.

O *Orange Book* define 7 níveis de segurança: D, C1, C2, B1, B2, B3 e A1. O nível D, chamado de Proteção Mínima, não requer nenhuma característica especial de segurança. O nível mais exigente é o A1, chamado de Projeto Verificado, que exige identificação de usuários através de senhas, com níveis de acesso individualizados, além de processos de validação do projeto de segurança perante suas especificações.

Seguindo a linha do *Orange Book*, a comunidade européia criou o padrão ITSEC – IT *Security Evaluation Criteria*, relativo à Segurança de Informação, formulado por França, Alemanha, Holanda e Reino Unido.

e) SSP - System Security Policy

Esta é uma recomendação do governo britânico, visando a proteção nas fases de processamento, armazenamento e transmissão de informações em sistemas computacionais que tratem de informações consideradas secretas. Os sistemas que realizam essa tarefa são regulamentados pelo DSO (*Departamental Security Officer*), que verifica se os mesmos não representam riscos à segurança nacional. Para que se obtenha a permissão de operação, o responsável pelo sistema computacional deve fornecer dados relativos ao escopo do sistema, aos requisitos de Segurança de Informação, às medidas para a implementação de tais requisitos, bem como a alocação de responsabilidades. A esse conjunto de tópicos dá-se o nome de *System Security Policy* – SSP (Hunter, 2001).

Pode ser requerida a avaliação, por consultores independentes, visando a certificação dos aspectos da Segurança de Informação. Tais consultores necessitam de informações sobre:

- Detalhamento dos aspectos técnicos do SSP, também conhecido como *System Electronic Information Security Policy* – SEISP;
- Documento de projeto do sistema das partes referentes à segurança de informações; e
- Código fonte das seções críticas, ou seja, partes do código que contenham funções de Segurança de Informação.

O propósito da certificação é assegurar que o projeto reflita os requisitos SEISP e que o código implemente corretamente as especificações do projeto.

4. RESULTADOS E RECOMENDAÇÕES

Tendo em vista o panorama apontado pelos itens anteriores, torna-se possível destacar as principais constatações e recomendações referentes ao projeto e operação de Sistemas de Informação, no que diz respeito à Segurança das Informações envolvidas.

No tocante ao processo de garantia da segurança, este deve começar com uma compreensão clara de qual informação necessita ser protegida, de forma a possibilitar um projeto seguro para uma base de dados.

Existem muitas aplicações que se preocupam com a Segurança de Informação. Este fenômeno ocorre principalmente pelo fato de que os principais usuários de grandes Sistemas de Informação são instituições bancárias. Do ponto de vista de tais instituições, a disponibilidade é um fator essencial, porém um erro em um dado não implica em risco de vida como em uma Aplicação Crítica. Por outro lado, em sistemas do tipo aeronáutico, que também utilizam grandes quantidades de dados,

qualquer falha pode levar a situações de perigo, com possibilidades de ocasionar vítimas fatais.

Uma meta a ser buscada está em procurar mostrar possíveis caminhos para que se possa garantir que um Sistema de Informação possa ser confiável, seguro e ao mesmo tempo disponível.

Um aspecto de grande importância consiste no treinamento sobre o sistema. Um treinamento eficaz se constitui em um dos aspectos primordiais a serem observados, tendo influência na maneira como o sistema é utilizado e na cultura geral sobre a segurança.

Outro ponto a ser observado em qualquer sistema em que a segurança seja um fator importante é o envolvimento da alta direção das organizações. Esse envolvimento é necessário, não apenas pelo fator econômico da liberação de recursos destinados à manutenção da segurança em geral, mas também pelo incentivo que a direção deve proporcionar a todos os funcionários, no sentido de sempre zelarem pela segurança de seus sistemas.

Também deve ser encarado como um fator de grande importância, a existência e a conseqüente divulgação da política de segurança adotada pela empresa. Essa política de segurança deve abranger todos os pontos identificados como críticos, de forma a cobrir todas as ameaças e perigos potenciais aos sistemas. Uma ampla divulgação é necessária para que todos estejam conscientes da forma de agir, no caso da ocorrência de qualquer tipo de problema relativo à segurança.

Deve-se estar consciente de que a tecnologia é importante, ou seja, sem a tecnologia não existiriam muitas das formas de proteção atualmente utilizadas. No entanto, talvez mais importante que os aspectos tecnológicos, há a necessidade de que todos na organização mantenham uma preocupação constante com o aspecto segurança. Apenas com a junção da tecnologia com a vigilância permanente de funcionários, é que se pode ter sucesso em um plano de garantia da segurança.

O objetivo principal para o estabelecimento dos Requisitos de Segurança é o de evitar as condições perigosas ou vulneráveis, prevenir a ocorrência de acidentes ou de invasões que possam vir a ocorrer em função dessas condições perigosas, e finalmente minimizar as conseqüências advindas em função de um eventual acidente ou invasão. Para que isso seja possível, é necessário que se identifiquem todas as condições perigosas que possam vir a ocorrer, classificar tais condições dentro de uma escala de prioridades e determinar os métodos mais apropriados para o tratamento dessas condições.

Finalmente, deve-se considerar que nos Sistemas de Informação não há ações físicas diretamente associadas à sua operação, ou seja, a aplicação é computacional. Em grande parte das aplicações há o uso intensivo de bases de dados e de ferramentas de software utilizadas para o processamento desses dados.

5. CONCLUSÕES

Considerando-se a crescente importância da informação nas modernas organizações, torna-se uma tarefa vital realizar a proteção, e dessa forma garantir a segurança, do conjunto de informações vitais à continuidade dos negócios das empresas.

A manutenção da segurança em um Sistema de Informação é uma tarefa que justifica todos os esforços realizados, bem como todos os recursos empregados para o seu projeto e implementação.

As ameaças e riscos a um Sistema de Informação vêm se constituindo em uma das maiores fontes de preocupação das empresas que fazem uso intensivo da Tecnologia da Informação.

Para que seja possível viabilizar a adoção de mecanismos de segurança dos Sistemas de Informação, há a necessidade de se implantar mecanismos de proteção desse conjunto de informações vitais. Tais mecanismos são constituídos por uma série de medidas, representadas tanto por meio da implantação de novos sistemas, quanto pelo treinamento e conscientização dos funcionários responsáveis pela manutenção das informações dentro da empresa.

A adoção de normas e procedimentos padronizados, a análise dos riscos presentes na implantação e manutenção dos Sistemas de Informação, a avaliação dos impactos decorrentes de invasões a tais sistemas, bem como a adoção de planos consistentes de contingência e recuperação de desastres, constituem as principais providências a serem tomadas para a proteção dos mesmos.

Finalmente, deve-se ter em mente que problemas que afetem a operação e a disponibilidade de um Sistema de Informação causam tanto repercussões diretas e de curto prazo, representadas pela perda imediata de negócios, quanto indiretas e de longo prazo, representadas pela perda de confiabilidade por parte de clientes e parceiros, para com a organização detentora de tais sistemas.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT – Associação Brasileira de Normas Técnicas. Tecnologia da Informação – Código de Prática para a Gestão da Segurança de Informação. NBR ISO/IEC 17799. São Paulo, 2001.

Almeida Junior, J.R., Segurança em Sistemas Críticos e em Sistemas de Informação – Um Estudo Comparativo. 191p. Tese (Livre Docência) – Escola Politécnica da Universidade de São Paulo. São Paulo, 2003.

Berkeley - School of Information Management & Systems, University of California. How Much Information? Executive Summary. Disponível em: <http://sims.berkeley.edu/research/projects/how-much-info/summary.html>. Aceso em 27 out. 2002.

Byrnes, F.C.; Kutnick, D. Securing Business Handbook, Indianapolis: Addison Wesley, 2002. 237p.

Dias, C. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books, 2000. 218p.

Ghosh, A. Addressing New Security and Privacy Challenges. IT Pro, p.10-11, May/June 2002.

Hunter, J.M.D. An Information Security Handbook,Spriger Verlag, 2001. 226p.

IBM – International Business Machine. Arriving at the upside of uptime: How people, process and technology work together to build high availability computing solutions for e-business. USA, 1999. 16p.

IEC International Eletrotechnical Commission. Information Technology – Security Techniques – Evaluation Criteria for IT Security, Parts 1 to 3. ISO/IEC 15408,

Laudon, K.C.; Laudon, J.P. Management Information Systems, 6.ed. New York: Prentice Hall, 2002.

Maiwald, E.; Siegleim, W. Security Planning & Disaster Recovery, New York: Mc Graw / Osborne, 2002. 299p.

Massiglia, P.; Marcus E. (Ed.) The Resilient Enterprise – Recovering Information Services from Disasters. Mountain View: Veritas Software Corporation, 2002. 527p.

Moreira, N.S. Segurança Mínima – Uma Visão Corporativa da Segurança de Informação. Rio de Janeiro: Axcel Books, 2001. 240p.

NIST – National Institute of Standards and Technology. Risk Management Guide for Information Technology Systems. National Institute of Standards Technology – NIST 800-30, Washington, 2001. 49p.

Price Waterhouse Coopers. Disponível em: <http://www.betrusted.com>. Acesso em 22 Out. 2002.

Winter Corporation. Disponível em: http://www.wintercorp.com. Acesso em: 27 Nov. 2002.