Aspectos da Segurança da Informação: Sua Importância para as Organizações

Ronan Leandro Coelho dos Santos[1], Mário Rubens W Sott (Orientador)[1]

[1]Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Rua Palma Bageto Viol, s/n – Barbacena - MG.

Ronan_leandro@yahoo.com.br, mrws@powerline.com.br

Resumo. *Este artigo demonstra como é importante a segurança das informações para as organizações já que tal segurança está sendo deixada de lado por chefes de empresas e alguns técnicos em segurança. Para o perfeito funcionamento e continuidade dos trabalhos da empresa a segurança da informação deve estar em primeiro lugar. Mostra também a importância da utilização de Políticas de Segurança e como algumas ameaças estão dentro da própria empresa e que precisam se dar maior atenção a tais problemas de segurança. Este artigo tem como objetivo mostrar algumas técnicas básicas de segurança.*

Palavras chaves: Segurança, informação, política de segurança.

1 - Introdução

Desde que o ser humano deixou de fazer trabalhos braçais para serem substituídos por máquinas, a principal preocupação passou a ser com relação à segurança da informação. E ela é hoje a maior preocupação para quem tem ou quer montar uma empresa, e permanecer com suas informações seguras e integras. A informação tem valor maior que qualquer ativo na empresa e é ela a base de sobrevivência.

Quando as informações eram escritas em papéis havia a facilidade de se guardá-las já que ao trancá-las em um local seguro ninguém as tocaria. Mas com a evolução da tecnologia, as informações passaram a ser armazenadas em mídias digitais, fato que as tornam mais vulneráveis a roubos e perdas.

Com isso se torna uma necessidade crescente de implantação de políticas de segurança. Tornando assim possível a utilização dessas informações em tomadas de decisão pela empresa.

No decorrer do artigo serão abordadas regras e normas que deverão ser seguidas pelas empresas e seus funcionários para manter a confiabilidade e segurança das suas informações.

2 – Definições

2.1 - Segurança

No dia a dia o ser humano está sempre procurando segurança. Quando sai de casa, ao atravessar uma rua com os devidos cuidados, quando constrói uma casa num lugar mais tranqüilo e que não tenha violência, quando compra um carro com ótimos itens de segurança.

Já no mundo da informática a preocupação com segurança é com relação às informações. É necessário que elas estejam seguras e confiáveis para que tomadas de decisões de gestores da empresa sejam mais precisas e assim aumentar os lucros da empresa.

De acordo com o site da Scua o melhor conceito de segurança pode ser encontrado no Dicionário Aurélio:

> *"**Segurança**. S. f. 2. Estado, qualidade ou condição de seguro. 3. Condição daquele ou daquilo em que se pode confiar. 4. Certeza, firmeza, convicção."* [5]

O mesmo site menciona a definição de seguro:

> *"**Seguro**. [Do lat. securu.] Adj. 1. Livre de perigo. 2. Livre de risco; protegido, acautelado, garantido. 8. Em quem se pode confiar. 9. Certo, indubitável, incontestável. 10. Eficaz, eficiente. [Dicionário Aurélio] "*[5]

2.2 - Informação

O homem a cada dia quer mais informação e conhecimento, extraindo de livros, painéis, TV, jornal, internet. Enfim, aonde vai está adquirindo informação.

Informação é o conhecimento sobre um determinado assunto, sobre dados de uma pessoa ou organização. É algo importante, de valor, é o bem mais valioso para uma organização e se não for guardado trará grandes perdas. [1]

Atualmente a preocupação maior é em proteger as informações, já que há muitas pessoas e empresas concorrentes querendo roubá-las.

De acordo com o Dicionário Aurélio, 2ª edição:

> ***"Informação.** [Do latin informatione.] S.f. 1. Ato ou efeito de informar (-se); informe. 2. Dados acerca de alguém ou de algo. [...] 4. Comunicação ou noticia trazida ao conhecimento de uma pessoa ou do publico. [...] 9. Proc. Dados. Coleção de fatos ou de outros dados fornecidos à máquina, a fim de se objetivar um processamento".*

O significado mais técnico de informação esta no site da Scua e diz:

> ***"Informação** é um recurso que, como outros importantes recursos de negócios, tem valor a uma organização e por conseguinte precisa ser protegido adequadamente [BS 7799 -1: 1999, British Standards Institute]."* [5]

3 - Segurança da Informação

Segurança da informação é quando todos os dados e informações importantes para uma pessoa ou organização estão livres de ameaças, sejam elas físicas ou lógicas.

O conceito de segurança da informação está mais bem definido no site wikipedia, e diz o seguinte:

> *“A **Segurança da Informação** refere-se à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto as informações corporativas quanto as pessoais.”* [4]

F.T. Grampp e R.H. Morris tem a seguinte definição de segurança da informação.

> *"É fácil ter-se um sistema de computação seguro. Você meramente tem que desconectar o seu sistema de qualquer rede externa, e permitir somente terminais ligados diretamente a ele. Pôr a máquina e seus terminais em uma sala fechada, e um guarda na porta."* [7]

Quando se pensa em Segurança da Informação é importante lembrar de manter a integridade, a disponibilidade, confidencialidade da informação e o não repúdio. Estes quatro princípios serão tratados mais a frente no item 3.1 deste artigo.

Fazendo o bom uso da Segurança da Informação a empresa terá muitos benefícios e com isso poderá dar continuidade a seus trabalhos. Com a evolução tecnológica o mundo pode-se conectar com mais facilidade e assim fazer a troca de informações. Porém o risco de perdê-las é maior, já que há muita gente com capacidade de invadir sistemas e roubar ou alterar tais informações.

Há uma grande necessidade de se pensar em segurança da informação ou caso contrário o prejuízo para a organização será considerável. Mas para isso todos os usuários e funcionários da empresa precisam estar cientes da importância da informação e assim zelar pela segurança.

3.1 - Objetivos da Segurança da Informação

A segurança da informação tem como objetivo manter protegido, seja de qual ameaça for, todos os dados e informações de uma empresa ou pessoa.

Basicamente será falado de 4 princípios: a confidencialidade da informação, a integridade dos dados, a disponibilidade e o não repúdio.

- **Confidencialidade**

O acesso às informações deverá ser feito apenas por pessoas autorizadas. Informações que nem todos os funcionários podem ter acesso. Um usuário qualquer não poderá ter acesso a informações que só os gerentes da empresa podem. Caso contrário dados valiosos poderão cair nas mãos de pessoas com o intuito de prejudicar a empresa. [1] [5]

- **Integridade**

As informações estarão sempre exatas e completas quando acessadas. Informações puras e integras caso contrário, todas as idéias e planos da empresa poderão não dar certo e assim causar grandes prejuízos. [1] [5]

- **Disponibilidade**

Certeza de que as pessoas que tenham permissão para acesso às informações possam acessá-las sem algum tipo de empecilho. A disponibilidade é importante para aquele funcionário que necessite acessar algum dado para executar uma tarefa, tenha a sua disposição tudo o que ele precisa. Caso contrário, uma boa negociação poderá estar sendo perdida. [1] [5]

- **Não repúdio**

Ao se enviar uma mensagem o emissor ou o receptor pode dizer que não enviou ou que não recebeu tal mensagem. O mesmo ocorre com quem faz uma negociação e depois nega ter feito. Para garantir que tal negociação ou que o envio da mensagem ocorreu é usada a técnica do não repúdio. [6]

O não repúdio colocado em um contrato visa proteger as partes de uma provável desistência sem pagamento de multas de rescisão e ainda caso alguém assine um contrato digital, e depois venha alegar que não fechou o negócio. [6]

No site Dicas-l tem a seguinte definição de Não Repúdio:

> *"Podemos definir o **não repúdio** com uma qualidade de determinada relação através da qual as partes são protegidas de uma alegação de inexistência, o que representa que a figura está presente para produzir efeitos legais nos contratos feitos por meio do computador. "* [6]

3.2 – Segurança física

O objetivo da segurança física é restringir o acesso de pessoas não autorizadas a ambientes que contenham os equipamentos de armazenamento de dados. Mas deve-se, também, dar atenção ao acesso lógico, eles devem ser implementados juntos para que não haja falhas na segurança. Não adianta implementar apenas um deles e querer total segurança aos dados. [5]

Um item determinante na segurança física é com relação à localização. O CPD (Centro de Processamento de Dados) deve ser construído em um local que não haja risco de desabamento, inundações, excesso de calor, poeira e umidade, que não tenha risco de serem danificados em caso de vandalismo, magnetismo, entre outros. [5]

O acesso ao CPD deve ser feito somente por pessoal autorizado. Restringindo assim a entrada de pessoas mal intencionadas. Esse controle pode ser feito por ferramentas de controle de acesso como: crachás, senhas, trancas, planta da mão, identificação pela íris, câmeras de vídeo, cartões magnéticos. Ferramentas de Segurança são equipamentos específicos pra a segurança física, são dispositivos usados para proteger e controlar o acesso ao local onde estão guardadas as informações. [5]

Os crachás, senhas, cartões magnéticos e trancas impedem que pessoas não autorizadas acessem locais não permitidos a elas. E ainda que apenas funcionários da empresa tenham acesso a suas dependências.

Planta da mão, identificação pela íris são mais confiáveis porem mais caros, mas com certeza a segurança será maior nas dependências da empresa, já que só poderá ter acesso aquele que for funcionário da empresa.

As câmeras de vídeo ajudam no monitoramento de quem entra e sai da empresa.

É importante se ter atenção especial com as portas e janelas, elas têm que ter boas trancas. No caso das janelas o uso de grades ajuda bem. [5]

O acesso e permanência de pessoas que não sejam funcionários do CPD devem ser registrados e feitos somente com acompanhamento de algum funcionário do setor. [5]

O que tem sido deixado de lado por técnicos em segurança é: o acesso físico a dispositivos de rede e de armazenamento. Por isso, a importância de saber guardar o *Backup*[1].

Os principais objetivos da segurança física é garantir a continuidade das rotinas, manter a integridade das informações e garantir a confidencialidade dos dados.

3.3 – Segurança lógica

Esse tipo de segurança visa proteger as informações. Tem por finalidade impedir a alteração, divulgação ou destruição das informações, seja ela intencional ou não, dando maior atenção à criação e utilização de senhas. É importante que apenas pessoas que necessitem de tais informações tenham a senha de acesso.

Há a necessidade de se fazer o controle de acesso assim como na segurança física. A diferença é que o controle de acesso lógico visa proteger dados e programas contra tentativas de acesso não autorizados. Seja o acesso feito por pessoas ou programas. [1]

A proteção dos recursos é feita de acordo com a permissão e a necessidade de cada usuário. Tal acesso é feito com uso de ID e senha. [1]

A proteção deve ser feita desde os aplicativos e dados até o sistema operacional. O sistema operacional por ser bastante frágil com relação à segurança, é o principal alvo de invasores o que pode comprometer a segurança.

O controle de acesso lógico procura garantir que: [1]

- Somente pessoas autorizadas tenham acesso às informações e recursos;
- Que o acesso do usuário será feito somente a recursos que ele tem permissão;
- O acesso a recursos mais importantes será feito apenas por pessoas autorizadas e se feito por outros usuários, tal acesso será monitorado;
- Que usuários os quais não tenham permissão para fazer determinadas transações não as façam. [1]

O controle de acesso lógico pode ser feito tanto por gerentes da empresa quanto por proprietário de aplicativos. Eles devem controlar o acesso a rede, ao sistema operacional e seus recursos. E tem por obrigação proteger os recursos contra invasores e outros funcionários. [1]

Para a perfeita implantação dos controles de acesso lógico o usuário deve estar ciente de suas responsabilidades com relação a manutenção de senhas e a segurança dos equipamentos de informática utilizados por ele. [1]

Existem vários tipos de ferramentas que ajudam na segurança. Elas podem ser classificadas quanto ao seu escopo:

- Ferramentas de segurança de hosts: voltadas para análise, correção, implementação de controles em sistemas computacionais;

[1] Backup – “Refere-se à cópia de dados de um dispositivo para o outro com o objectivo de posteriormente os recuperar, caso haja algum problema”. Disponivel em: pt.wikipedia.org

- Ferramentas de segurança de rede: Estão centradas na verificação e implementação de controles de acesso e trafego a rede. Ex: filtro de pacotes;
- Verificação da integridade e vulnerabilidade: são programas que controlam e analisam sistemas, relacionando serviços disponíveis, erros de permissão, mudança em programas;
- Autenticação: esta ferramenta esta relacionada com a identificação de usuários em um sistema;
- Privilégios: sua relação é com um ambiente de operação, fazendo assim, restrições de usuários ao mínimo necessário para que ele possa executar suas tarefas;
- Criação de programas seguros: bibliotecas com funções que deixam os sistemas mais difíceis de serem invadidos com as técnicas mais comuns de invasões. [8]

Existem inúmeras ferramentas para segurança da informação, o melhor é fazer um estudo de caso pra ver qual delas poderá estar sendo instaladas na empresa, de acordo com a necessidade e com disponibilidade financeira.

4 – Ameaças e Vulnerabilidades

Ameaça é tudo aquilo que coloca em risco seus dados e suas informações. Tais ameaças podem ser de duas origens: internas e externas.

As Ameaças Internas estão presentes no dia a dia da organização mesmo estando ou não conectado a internet. [2]

Como exemplo de ameaças internas tem-se:

Contaminação por vírus de computador através de um simples disquete – o uso de disquetes infectados por vírus poderá fazer com que o computador, ao ser infectado não funcione corretamente atrapalhando o rendimento dos trabalhos;

Incêndios – podem ocorrer em qualquer local, basta uma fagulha. Os prejuízos poderão ser enormes se não tiver medidas para conter ou evitar os incêndios. Pode haver além de perda de todas as informações, danos na estrutura do prédio da empresa.

Funcionários mal treinados – o funcionário sem treinamento para manusear os equipamentos da empresa podem, mesmo sem querer, danificar as aparelhagens causando a perda das informações.

Divulgação das senhas dos funcionários – alguns funcionários ainda anotam suas senhas em pedaços de papel ou em arquivos texto no computador. Uma pessoa que invada a empresa terá facilidade para roubar ou danificar informações que estejam em computadores.

Lixo informático – documentos com informações da empresa ou com planos de trabalho não devem ser apenas “jogados no lixo”, pois qualquer pessoa que entre na sala poderá encontrar e fazer mal uso deles.

Uso indevido dos serviços de Internet em nome da empresa – funcionários que acessam seus e-mails, paginas pornográficas, orkut, MSN, com certeza estão deixando

mais vulneráveis os sistemas da empresa, além de estarem usando o serviço de internet da empresa de forma errada e atrasando seus trabalhos. [2]

As Ameaças Externas são todos os ataques que provém de fora do ambiente físico da empresa. É o principal responsável por perdas de informações da empresa.

Como exemplo de Ameaças externas tem os Invasores, que são pessoas que utilizam de seus dons para burlarem as técnicas de segurança das empresas. São vários os tipos, mas os mais comuns são:

- *Hacker* – são indivíduos que invadem sistemas com falhas para se apropriarem de informações alheias.
- *Cracke*r – ao contrário do hacker ele invade e altera os computadores desviando conexões e até tirando alguns serviços do ar.
- *Phreaker* – são indivíduos com grandes conhecimentos em telefonia e que usam tais dons para fazerem ligações sem pagar.
- *Lammer* – são pessoas que utilizam programas para invadir *sites* de internet. [2]

Esses indivíduos não costumam invadir sistemas só por diversão, geralmente tem o intuito de roubar informações seja por vingança, para roubar dinheiro, espionagem industrial.

São várias as ameaças contra a segurança da informação, como é possível ver na figura 2. Os mais comuns são os populares vírus com 66%, os funcionários insatisfeitos com 53% e a divulgação de senhas com 51%. É possível perceber o quanto estas ameaças têm ligação com o ser humano, o principal causador de perdas às organizações.

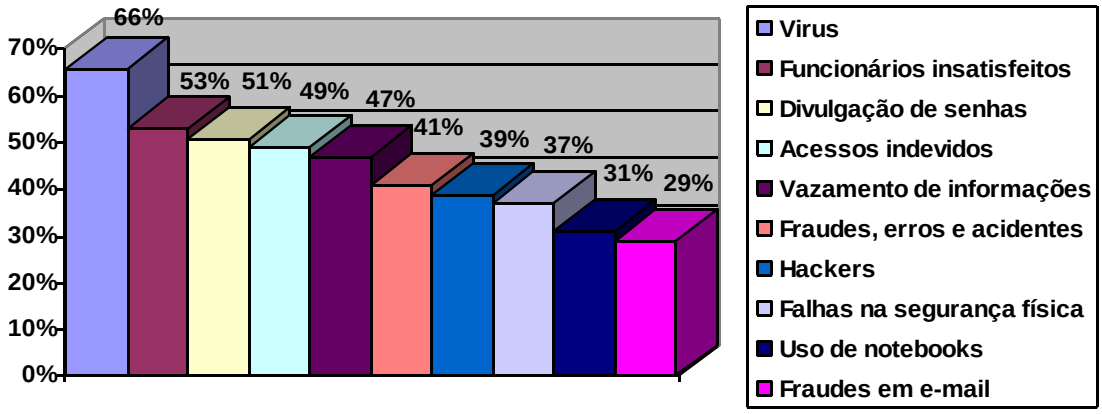

Figura 2 – Gráfico – Principais Ameaças à Segurança da Informação
Fonte: Adaptado da pesquisa da Modulo [2]

Alguns exemplos de vulnerabilidades:

- **Físicas** - Mau planejamento de salas de CPD e segurança fora dos padrões. Sala de CPD construídas em locais de risco de desabamento ou sem a segurança necessária poderá ser destruída ou invadida;
- **Naturais** - Quando os ativos da empresa estão propensos a sofrerem danos com enchente, poeira, tempestade, umidade, temperatura. As

aparelhagens de armazenamento de informação podem se danificar facilmente com poeira ou água e a perda das informações poderá ser irrecuperável;

- **Software** – Instalação e configuração mal feita. A instalação ou configuração mal feita pode causar a perda de dados importantes ou possibilitar a entrada de invasores no sistema;
- **Mídias** – Disquetes, CDs, DVDs são mídias frágeis e se danificam facilmente com impactos, arranhões ou magnetismo causando assim, a perda das informações;
- **Comunicação** – Causadas por perda da comunicação ou por acessos não autorizados. Perdas temporárias de comunicação causadas por mal funcionamento de aparelhagens e funcionários que acessam áreas não autorizadas podem danificar as informações ou atrasar o acesso, envio e recebimento de dados.
- **Humanas** – Causadas por imperícia, falta de treinamento, por falta de conscientização. Profissionais que ao acessar as informações as danificam ou perdem por não saberem usar os softwares e aparelhagens. [3]

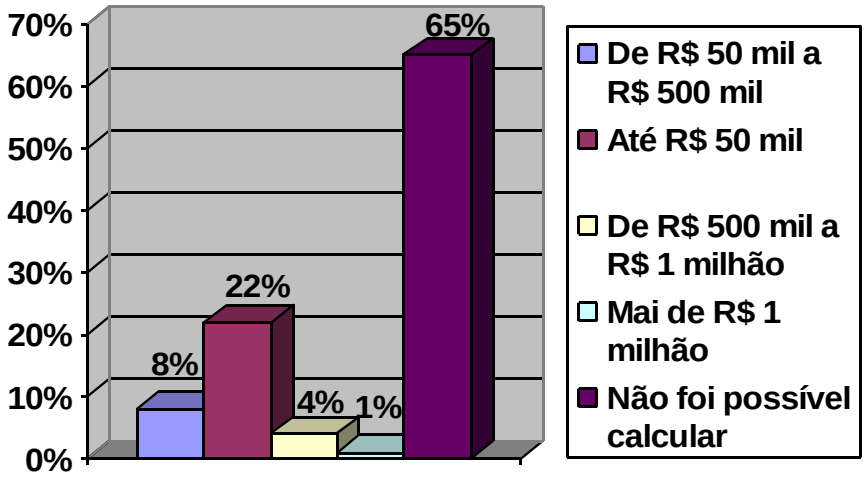

Figura 4 – Gráfico - Prejuízo nas Empresas Devido a Perda de Informações
Fonte: Adaptado da pesquisa da Modulo [2]

O gráfico acima mostra alguns valores de prejuízos causados por problemas com segurança. É possível ver que são valores altos e que dependendo da empresa os prejuízos podem levar a falência.

5 - Como se defender

Vírus – os vírus podem danificar ou alterar sistemas e informações, para resolver o uso de antivírus pode ajudar, porém ele precisa estar configurado corretamente e sempre atualizado.

É preciso ter cuidado com e-mails, disquetes infectados. Se você não conhece o remetente do e-mail não o abra. Se não conhecer a procedência de programas baixados na internet não os execute.

Procure não navegar em sites que considere suspeito. Sites de hacker ou sites pornográficos costumam ter muitos vírus. [5]

Incêndios – o risco de se perder as informações por causa de incêndio é grande, por isso a necessidade de aparelhagem anti incêndio a fim de evitar queimas parciais ou totais da aparelhagem de armazenamento de dados.

O local deve ser de fácil acesso ao carro do corpo de bombeiros. Tem que ser longe de locais que contenham objetos explosivos. Deve possuir sistemas de combate a incêndio. As paredes, piso e teto devem ser construídos com matérias de resistência ao fogo.

Funcionários sem treinamento ou mal treinados – investir em cursos para treinamento com relação ao uso de equipamentos que armazenam as informações. Treina-los a fim de que possam manusear tais equipamentos com segurança assegurando que não ocorrerão perdas de informações.

Senhas - as senhas merecem atenção especial, já que muitos funcionários não se preocupam em memorizá-las e acabam as deixando anotadas em papeis ou em arquivos texto no computador.

É preciso ter um cuidado maior com elas:

- Não as deixar escritas em papéis sobre a mesa, colados em monitores, em teclados ou salvar em arquivos texto no computador.
- Jamais passá-la a alguém seja pelo telefone ou de outra forma qualquer e qual for a necessidade.
- Fazer a troca das senhas periodicamente.
- Procurar usar caracteres variados nas senhas. Não usar apenas letras, colocar também números e símbolos.

A senha é de uso pessoal e intransferível.

Lixo – o que não for mais ser utilizado pela empresa é preciso ser inutilizado ao ir para o lixo. Os papeis precisam ser de preferência, queimados, más podem também ser picotados em vários pedaços e jogados em várias lixeiras diferentes. Os disquetes, CDs, DVDs, fitas magnéticas devem ser destruídos, inutilizados.

Uso indevido dos serviços de Internet em nome da empresa – fazer uso de programas que bloqueie o acesso a sites e programas que não são necessários para o funcionário ao exercer suas funções dentro da empresa.

Invasões – o uso de firewall pode evitar que pessoas mal intencionadas invadam os sistemas da empresa via rede. O firewall precisa estar configurado e atualizado a fim de se fazer um melhor uso da ferramenta.

Para se defender melhor de ameaças e evitar vulnerabilidades, medidas de segurança precisam ser tomadas. Medidas como as Políticas de Segurança ajudam a evitar ou resolver problemas caso seja necessário.

5.1 - Políticas de Segurança

São normas para melhores práticas de transporte, manuseio, descarte, armazenamento das informações.

Há um documento do Tribunal de Contas da União que explica melhor o significado da Política de Segurança: [1]

> ***"Política de segurança de informações** é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos."*

A Política de Segurança deve ser clara e objetiva. E tem que ser elaborada por pessoas experientes e comprometidas com a empresa. Devem-se estabelecer regras e punições a quem não as cumprir. [1]

Algumas etapas devem ser seguidas a fim de se estabelecer uma boa Política de Segurança: [1] [5]

Definir a equipe responsável pela implantação e manutenção - Primeiramente é necessário definir quem será o responsável pela elaboração, implantação e manutenção da Política de Segurança. Ao se definir os responsáveis é importante lembrar que cada um tem sua responsabilidade e que todos os funcionários devem participar até mesmo os administradores.

Analisar as necessidades de segurança da empresa - Nessa etapa deve ser levado em conta todas as necessidades da empresa com relação a segurança. Todos os processos devem ser observados, informatizados ou não, pois podem afetar a segurança.

Identificar recursos e processos críticos – Os processos críticos devem ser identificados e receber tratamentos diferenciados.

Classificar as informações – As informações precisam ser classificadas para poderem receber um nível de proteção apropriado. Deve-se utilizar um método para determinar tais níveis. De acordo com os níveis é importante estabelecer procedimentos para manipulação das informações.

Elaborar normas para funcionários e usuários – Nessa fase é que se estabelecem as normas para melhor segurança das informações. Essa fase é estabelecida de acordo com as informações coletadas nas fases anteriores.

Definir um plano de contingência – São planos que a empresa deve seguir caso haja algum problema. Ajuda a resolver mais rapidamente os problemas causados diminuindo o tempo de retomada de trabalho.

Definir penalidades ao não cumprimento das normas de segurança - É necessário definir punições para aqueles funcionários que não cumprirem as Políticas de Segurança. Tem por finalidade conscientizar os funcionários da importância da segurança da informação. As punições são determinadas de acordo com as culturas da organização.

Elaborar termo de compromisso – O termo de compromisso serve para além de comprovar que os funcionários e usuários estão cientes das Políticas de Segurança, garantir que eles as cumprirão, já que ocorrendo o descumprimento estarão sujeitos a penalidades.

Divulgar a política de segurança - Para que se tenha sucesso ao implantar a Política de Segurança, é importante que a divulgação seja feita a todas as pessoas que direta ou indiretamente utilizam e dependam da organização.

É preciso também que tais pessoas tenham acesso permanente à Política de Segurança, pois ela fornece orientação básica às pessoas que, direta ou indiretamente interagem com a empresa. Além de dar instruções básicas de somo proceder.

Sempre que houver mudança organizacional há a necessidade de se fazer uma revisão na Política de Segurança da empresa. Ela também deve ser feita periodicamente, visando estar sempre pronto a quaisquer novas ameaças.

Implantação - A implantação é algo demorado e é um processo que deve ser formal, além de ser ajustável. Para uma implantação bem sucedida devem-se seguir algumas etapas: elaboração, aprovação, implementação, divulgação e manutenção.

A implantação do processo de segurança é muito importante, porém tem algumas dificuldades. Alguns exemplos de tais dificuldades estão no gráfico abaixo.

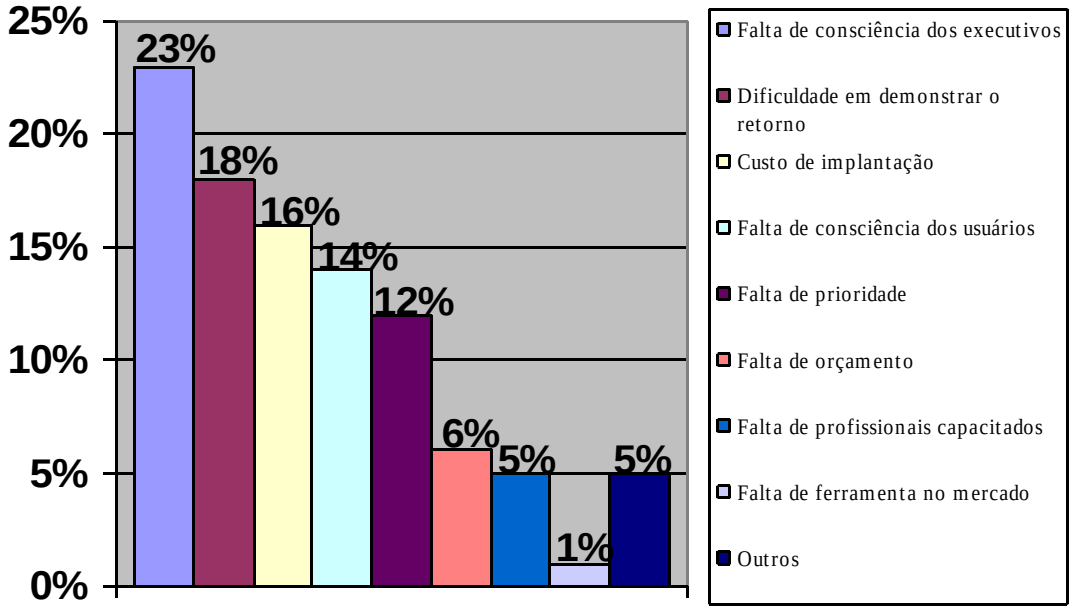

Figura 3 – Gráfico – Principais Obstáculos para Implementação da Segurança
Fonte: Adaptado da pesquisa da Modulo [2]

Revisão – A Política de Segurança deve ser revisada periodicamente a fim de deixá-las sempre atualizadas e diminuir os riscos de falha. Deve ser estabelecer um prezo para fazer as revisões. Mas também pode ser feitas quando algo de errado acontecer, com o intuito de corrigir tais erros.

Cada empresa tem suas necessidades de segurança que variam de empresa para empresa, por isso para cada uma é preciso fazer o estudo de caso a fim de determinar quais os melhores métodos para se implementar uma melhor Políticas de Segurança.

Conclusão

Após ver que prejuízos quase incalculáveis ocorrem em empresas por conta de erros ou sabotagens, observa-se a necessidade de estar implantando sistemas de segurança mais eficazes. Foi possível ver em pesquisas realizadas por uma entidade especializada em segurança da informação, a Modulo Security que no Brasil muita gente ainda ta precisando se conscientizar para que se tenha total segurança.

Como atualmente as informações são guardadas em meios digitais há a facilidade de perdê-las, porem é preciso usar ferramentas de segurança pra garantir que tais informações não caiam nas mãos de concorrentes ou de pessoa com o intuito de ganhar dinheiro ilegalmente.

Normas precisam ser seguidas dentro da organização por todos os funcionários, do faxineiro ao proprietário, afim de que seus dados e informações estejam sempre confiáveis.

A implementação da Política de Segurança é vista como fator primordial para a sobrevivência da empresa. E estando ela bem implementada e utilizada, a empresa terá suas informações mais seguras e confiáveis.

Quando ocorre a perda das informações todos os funcionários da empresa serão prejudicados. Mas o pior de todos os problemas é a falência da empresa.

Referências Bibliográficas

[1] Tribunal de Contas da União. Boas práticas em segurança da informação. Disponível em:http://www.cqgp.sp.gov.br/downloads/Boas_Praticas_em_Seguranca_da_Informacao.pdf , Acesso em: 18 ago. 2006.

[2] Calheiros, Rosemberg Faria. (2002) Segurança de Informações nas Empresas: uma prioridade corporativa. Disponível em: http://www.modulo.com.br/pdf/rosemberg.pdf, Acesso em 18 ago. 2006.

[3] Peixoto, Mário César Pintaudi. (2004) Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações. Unitri, Uberlândia.

[4]http://pt.wikipedia.org/wiki/Seguran%C3%A7a#Pol.C3.ADticas_de_seguran.C3.A7a Acesso em 11 out. 2006.

[5] http://www.scua.com.br/site/seguranca/conceitos/seguranca.htm Acesso em 30 nov. 2006

[6] http://www.dicas-l.com.br/dicas-l/20030813.php Acesso em 30 nov. 2006

[7] http://archives.neohapsis.com/archives/postfix/2006-02/0000.html Acesso em 30 nov. 2006

[8] http://www.rnp.br/newsgen/9711/seguranca.html Acesso em 07 dez. 2006