UNIVERSIDADE CANDIDO MENDES
PÓS-GRADUAÇÃO "LATO SENSU"
PROJETO A VEZ DO MESTRE

SEGURANÇA DE INFORMAÇÕES: UMA QUESTÃO ESTRATÉGICA

Por: Rosemberg Faria Calheiros

Orientador
Prof. Ms. Marco A. Larosa

Rio de Janeiro
2004

UNIVERSIDADE CANDIDO MENDES
PÓS-GRADUAÇÃO "LATO SENSU"
PROJETO A VEZ DO MESTRE

SEGURANÇA DE INFORMAÇÕES: UMA QUESTÃO ESTRATÉGICA

Apresentação de monografia à Universidade Candido Mendes como condição prévia para a conclusão do Curso de Pós-Graduação "Lato Sensu" em Gestão Estratégica e Qualidade.

Por: . Rosemberg Faria Calheiros.

AGRADECIMENTOS

Á Deus em primeiro lugar, à minha esposa Antônia Aguiar Calheiros, que sempre me incentivou em todos os momentos e aos meus amigos e professores do Projeto “A Vez do Mestre”, pela marcante amizade.

RESUMO

Aborda a conscientização e a importância da Segurança de Informações na Gestão Estratégica das Empresas. Apresenta os recursos e medidas relacionadas à proteção da informação e os riscos relativos às vulnerabilidades.

Cita os principais obstáculos para a implementação da Segurança de informações como estratégia adotada. Enfoca a necessidade da capacitação técnica como medida primordial utilizada pelas Empresas.

Aponta os fatores determinantes e os controles adequados na proteção de incidentes, definindo soluções e ações práticas para minimizar impactos e perdas de informações estratégicas, que possam afetar o bom funcionamento da Gestão de uma Empresa ou Instituição.

METODOLOGIA

A metodologia de pesquisa utilizada para conclusão deste trabalho foram bibliografias e conceitos encontrados em livros, artigos e Internet ligados a assuntos sobre o tema proposto, onde, na busca de informações, apresentamos a importância da Segurança de Informações na Gestão Estratégica de uma Empresa.

SUMÁRIO

INTRODUÇÃO

A Segurança de Informações tem deixado de ser tratada como um assunto técnico da área de informática, e vem sendo considerada uma real necessidade nas empresas e nas instituições, como uma questão estratégica, visto que a informação é o bem ativo mais valioso da empresa.

O objetivo do processo de Segurança de Informações em uma organização é alcançar a disponibilidade, confidencialidade, integridade, legalidade e auditabilidade da informação. A segurança das informações é difícil, talvez até mesmo impossível, porém existe a necessidade da proteção da informação, fator primordial para própria sobrevivência da empresa, reduzindo assim, os impactos e os riscos de incidentes de segurança.

É necessário ter uma boa Política de Segurança, composta de regras claras, praticáveis e sintonizadas com a cultura do ambiente tecnológico da empresa. Deve não apenas proteger não só as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização e envolvimento de todos.

Garantir a segurança de informações é uma questão estratégica, um grande desafio, que passa por todas as pessoas envolvidas, direta e indiretamente.

CAPÍTULO I

CONCEITOS

Segundo alguns conceitos básicos de escritores para fundamentação do trabalho, a Segurança de informação é o conjunto de dados, imagens, textos e outras formas de representação usadas para os valores da Companhia, associados ao seu funcionamento e/ou manutenção das suas vantagens competitivas.

Conforme POLÍTICAS (2002, p. 1-4), os conceitos podem ser definidos como:

Recursos de Informação - são todos os meios usados para obtenção, geração, armazenamento e transporte das informações. Inclui: os recursos do ambiente de tecnologia da informação (instalações e equipamentos de informática e telecomunicações, sistemas operacionais, aplicativos e sistemas de informação usados nesses equipamentos) e outros recursos convencionais (arquivos, papel, microfilme, mapas etc.).

Sistema de Informação - é um conjunto de processos e recursos do ambiente de tecnologia da informação organizados para prover, de modo sistemático, informações para a Companhia.

Órgão Proprietário da Informação - é o órgão da empresa responsável pelas informações de uma determinada área de atividade da Companhia.

Proprietário da Informação - empregado, designado pelo Órgão Proprietário da Informação, para responder perante a Companhia pela classificação das informações e definição das suas necessidades de segurança.

Comitê de Segurança de Informações - é o comitê constituído pela Diretoria Executiva da empresa com a finalidade de implantar e garantir o cumprimento da Política de Segurança de Informações no âmbito da Companhia.

Gerente de Segurança de Informações do Órgão - empregado designado pelo órgão da Companhia, como responsável pelo cumprimento da Política de Segurança de Informações no âmbito do órgão, servindo de interface entre gerentes, proprietários, usuários, custodiantes, Gerência de Tecnologia da Informação do Órgão e o Comitê de Segurança de Informações.

CAPÍTULO II

CLASSIFICAÇÃO DE INFORMAÇÕES

De acordo com POLÍTICA...(2002, p. 2), todo tipo de documento de uma corporação deve exibir, de maneira clara, o respectivo grau de acessibilidade ou seja seu grau de sigilo, o que requer classificar todas as informações segundo o seu grau de criticidade e âmbito de acesso:

a) Informações Confidenciais: só podem ser disseminadas para empregados previamente nomeados;

b) Informações Corporativas: sua divulgação restringe-se ao âmbito da Empresa.

c) Informações Públicas: podem ser disseminadas dentro e fora da Empresa.

Convém que informações e resultados de sistemas que processam dados classificados sejam rotulados de acordo com seu valor e sua sensibilidade para a organização. Também pode ser apropriado rotular a informação em termos de quão crítica ela é para a organização como, por exemplo, em termos de integridade e disponibilidade. A informação freqüentemente deixa de ser sensível ou crítica após um certo período de tempo, por exemplo quando a informação se torna pública. Convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar a custos adicionais desnecessários.

Convém que as regras de classificação previnam e alertem para o fato de que um determinado item de informação não tem necessariamente uma classificação fixa, podendo sofrer modificação de acordo com alguma política predeterminada.

CAPÍTULO III

OBJETIVOS DA SEGURANÇA DE INFORMAÇÕES

Quando se pensa em segurança de informações, a primeira idéia que nos vem à mente é a proteção da mesma, não importando onde ela esteja. Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado. Porém, segurança é um conceito que vai muito além disso. É expectativa de todos que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas tenham acesso a seu conteúdo. Ou seja, é expectativa de qualquer usuário que as informações estejam em local adequado, disponíveis no momento desejado, que sejam confiáveis, corretas e permaneçam protegidas contra acessos indesejados. Essas expectativas correspondem aos objetivos da segurança.

Destacam-se entre os objetivos da segurança, SEGURANÇA DA TECNOLOGIA..... (2002):

Confidencialidade ou privacidade – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia.
Integridade dos dados – evitar que dados sejam apagados, ou alterados sem a permissão do gestor da informação.

Legalidade - Estado legal da informação, em conformidade com os preceitos da legislação em vigor.

Disponibilidade – garantir o provimento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos/sistemas e *backup*. Um bom

exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar pane nos sistemas.

Consistência – certificar-se de que o sistema atua de acordo com a expectativa dos usuários.

Isolamento ou uso legítimo – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema.

Auditoria – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando.

Confiabilidade – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

Antes de implementar um programa de segurança de informações, é aconselhável responder às seguintes questões:

a) O que proteger?
b) Contra que ou quem?
c) Quais as ameaças mais prováveis?
d) Qual a importância de cada recurso?
e) Qual o grau de proteção desejado?
f) Quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança desejados?
g) Quais as expectativas dos usuários e clientes em relação à segurança de informações?

h) Quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?

Tendo a resposta a essas perguntas, é definida a política de segurança de informações e analisadas as ameaças, fazendo-se uma análise de riscos. A tecnologia de segurança a ser implantada deve atender aos requisitos da política. Por fim, para administrar os sistemas, é necessário implantar uma gerência de segurança.

Segurança de Informação é a conjugação de uma estratégia e de ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa. (COLTRO, 2002, p. 26).

CAPÍTULO IV

POLÍTICA DE SEGURANÇA

Uma política de segurança é um conjunto de regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.

A política de segurança deve incluir regras detalhadas, definindo como as informações e os recursos da organização devem ser manipulados. Deve definir, também, o que é e o que não é permitido em termos de segurança, durante a operação de um dado sistema.

Existem dois tipos de políticas:

Política baseada em regras: as regras deste tipo de política utilizam os rótulos dos recursos e processos para determinar o tipo de acesso que pode ser efetuado. No caso de uma rede de computadores, os dispositivos que implementam os canais de comunicação, quando é permitido transmitir dados nesses canais, etc.

Política baseada em segurança: o objetivo deste tipo de política é permitir a implementação de um esquema de controle de acesso que possibilite especificar o que cada indivíduo pode ler, modificar ou usar para desempenhar suas funções na organização.

4.1 - Desenvolvimento de uma Política de Segurança

- Pesquisar o conteúdo que terá a política;
- Minutar o texto que descreve a política;
- Obter a aprovação dos altos escalões da administração da organização;
- Disseminar a política de segurança em todos os escalões da organização.

4.2 - A Política de Segurança define o que precisa ser protegido

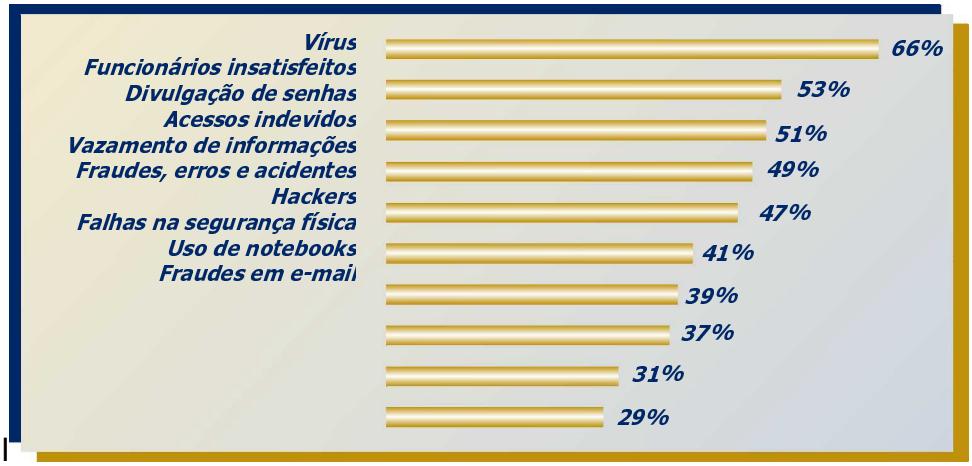
As Políticas de Segurança definem os “o que” precisam ser protegidos, mas são Procedimentos de Segurança que irão dizer “como” estes serão protegidos. O documento das Políticas de Segurança tende a ser uma documentação de mais alto nível, ficando a responsabilidade do maior detalhamento para documentação que irá tratar dos procedimentos de segurança.

CAPÍTULO V

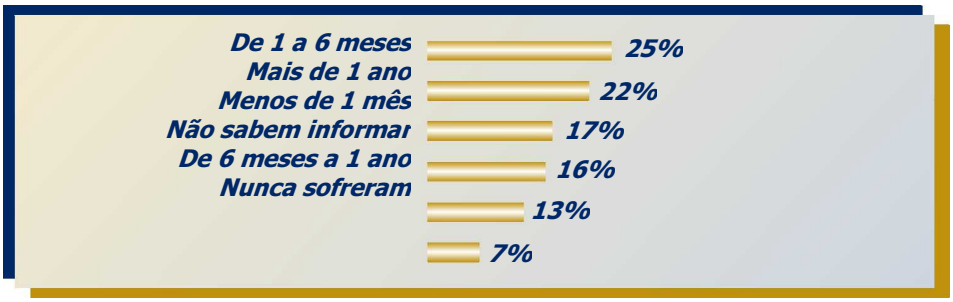
PESQUISAS SOBRE SEGURANÇA DE INFORMAÇÕES NAS EMPRESAS

Segundo 9ª Pesquisa Nacional de Segurança da Informação nas empresas, realizada em 2003, elaborada pela empresa Modulo Security, especializada em segurança de informações, os principais dados encontrados são:

5.1 - Principais Ameaças à Segurança da Informação



5.6 - Incidência de Ataques e Invasões

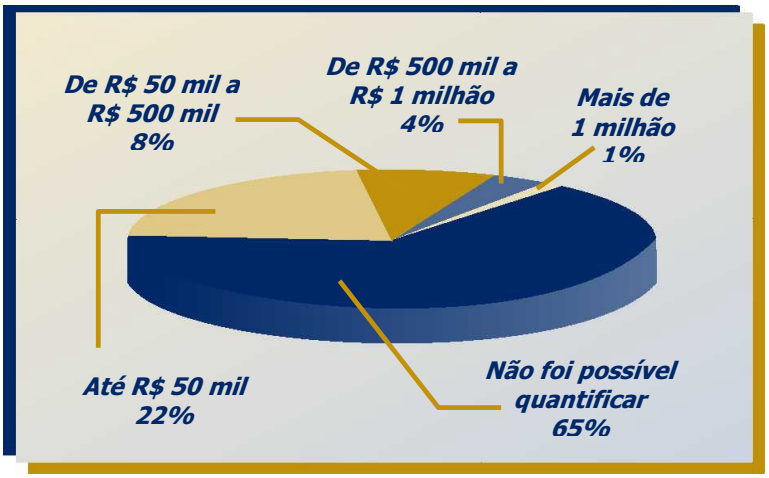


> **Principais Ameaças:** Vírus, Funcionário insatisfeito, Divulgação de senhas, Acessos indevidos e Vazamento de informações.

> **Ameaças consideradas como Fator Crítico:** 29% dos entrevistados apontaram as fraudes por e-mail como uma das principais ameaças.

5.3 - Prejuízos Contabilizados

> 35% das empresas no Brasil tiveram perdas financeiras;
> 22% das empresas acima registraram perdas de até R$ 50 mil, 8% entre R$ 50 mil e R$ 500 mil e 4% de R$ 500 mil a R$ 1 milhão;
> 65% não conseguem quantificar o valor dos prejuízos.



5.4 - Medidas adotadas após Ataques e Invasões

> 28% => Limitaram-se à correção do problema
> 28% => Optaram por providências internas
> 15% => Adotaram medidas legais
> 7% => Não tomaram nenhuma attitude

5.5 - Principais Responsáveis

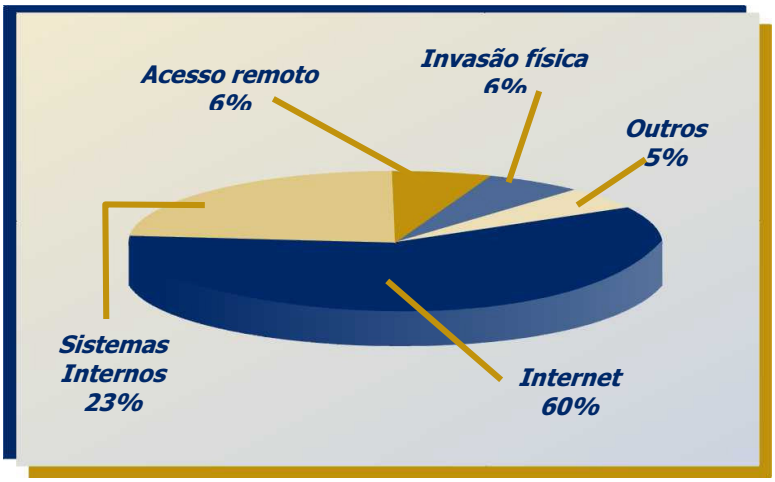
> Pelo terceiro ano consecutivo, os hackers são apontados como os principais responsáveis por ataques e invasões de sistemas corporativos.

> Outro fator negativo é que 26% das empresas não conseguem sequer identificar a origem dos ataques e invasões.

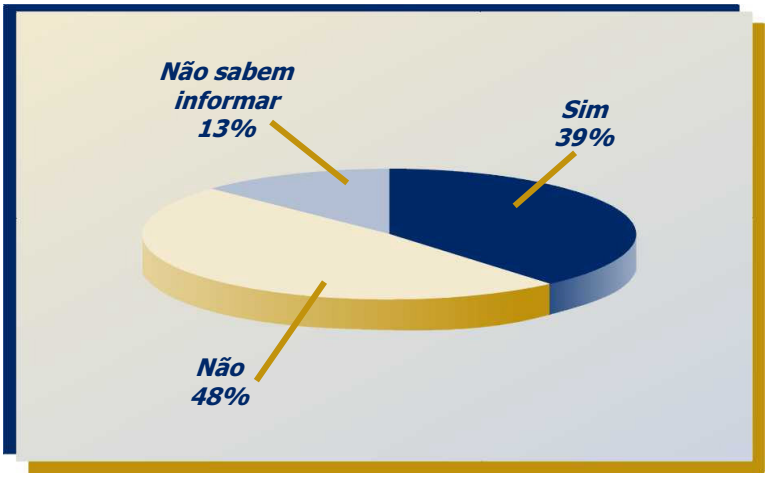
5.6 - Principais Pontos de Invasão

> A maior parte das empresas (60%) indica a Internet como o principal ponto de invasão em seus sistemas.

> Se por um lado aumentou o percentual de invasões via Internet, por outro a pesquisa constata a queda do percentual de invasões via acesso remoto: de 16%, em 2002, para 6%, em 2003.



> Mesmo acreditando no crescimento dos problemas em 2004, 48% das empresas ainda não possuem nenhum plano de ação formalizado para o caso de invasões e ataques.



5.7 - Principais Obstáculos para Implementação da Segurança

> Falta de consciência dos executivos (23%), dificuldade em demonstrar o retorno (18%) e custo de implementação (16%) foram considerados os três principais obstáculos para implementação da segurança nas empresas.

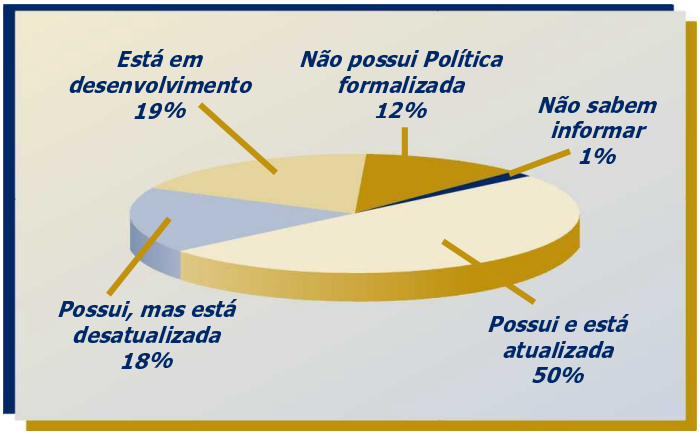
> Em relação ao ano passado, constatam-se duas mudanças significativas: a queda da falta de consciência dos usuários, que passou de 29% para 14%; e o aumento do custo de implementação, que passou de 1% para 16%.

5.8 - Implementação de Segurança da Informação

> 51% dos entrevistados acreditam que os executivos consideram a Segurança da Informação fundamental para a integridade e continuidade de seus negócios, sendo que para 21% é fator vital e para 16% é crítica.

> Apesar dessa visão otimista, a falta de conscientização de executivos ainda é considerada como o principal obstáculo para implementação da Segurança da Informação dentro das organizações.

5.9 - Política de Segurança utilizada



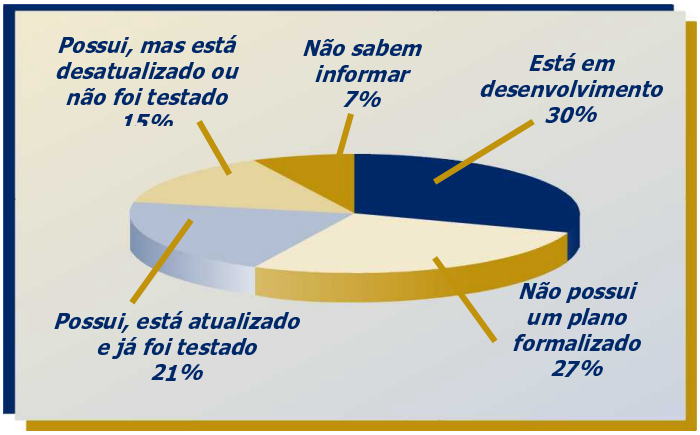
5.10 - Medidas de Segurança já Implementadas

> Pelo terceiro ano consecutivo, antivírus (90%), sistemas de backup (76,5%) e firewall (75,5%) foram apontados como as três principais medidas de segurança mais implementadas.

> Em 2003, dois novos itens figuram na lista Top 10: segurança física na sala de servidores (63%) e criptografia (57%).

> Apesar de não constarem na lista Top 10, certificados digitais (52%) e autoridades certificadoras (45%) também foram medidas amplamente adotadas pelas empresas.

5.11 - Plano de Continuidade de Negócios



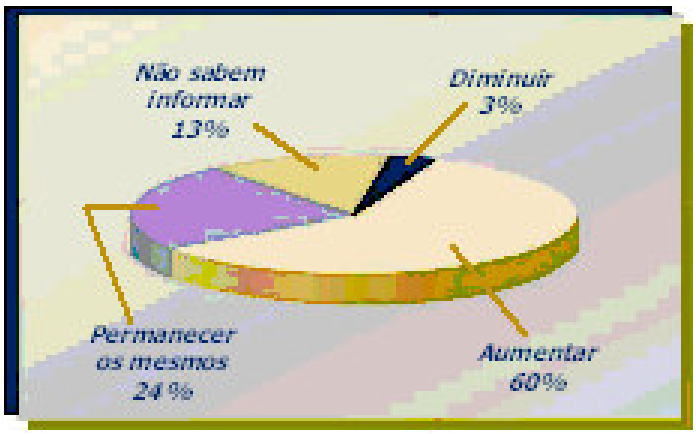
5.12 - Medidas de Segurança mais Implementadas das Empresas pesquisadas

5.13 - Responsáveis pela Segurança da Informação nas Empresas

5.14 - Número de Profissionais Dedicados

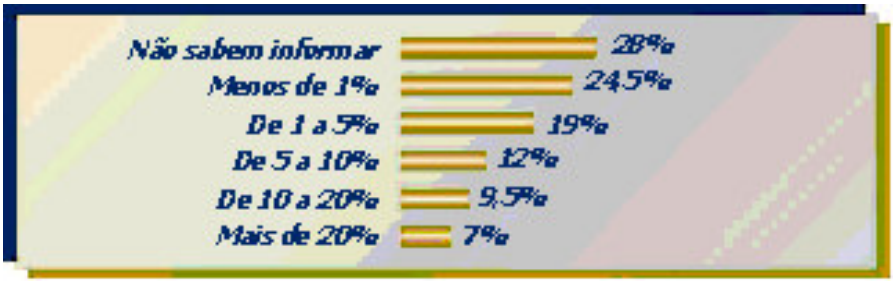
5.15 - Investimentos em Segurança da Informação

> Para 78% dos entrevistados, as ameaças, os riscos e os ataques deverão aumentar em 2004.
> Diante desse quadro, 60% afirmam que os investimentos em segurança vão aumentar no próximo ano.



5.16 - Orçamento destinado à Segurança da Informação

> 73% das empresas possuem orçamento específico para área de Tecnologia da Informação.
> Deste total, 24,5% alocam menos de 1% em recursos de segurança, 19% entre 1% e 5%, 12% de 5% a 10%, 9,5% entre 10 a 20% e 7% destinam mais de 20% do orçamento total de TI para área de Segurança da Informação.



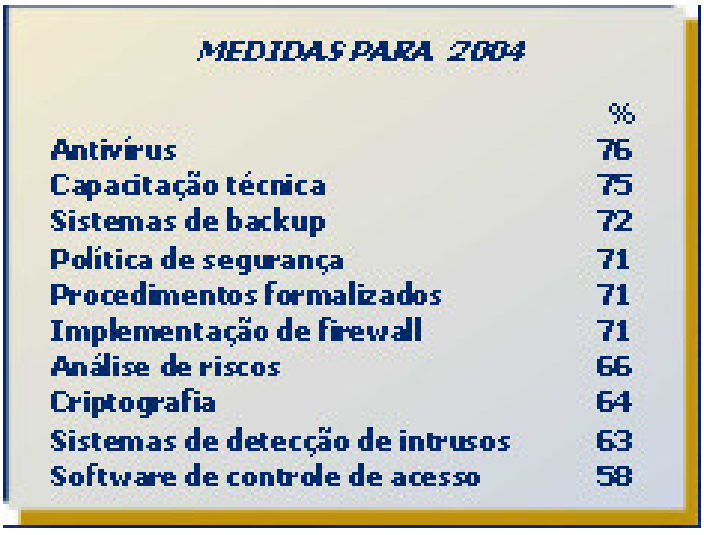
5.17 - Top 10 medidas de Segurança para 2004

> Em 2003, as empresas tiveram imensas dificuldades com a disseminação em massa de diversas pragas virtuais, como o Slammer, Blaster, Sobig, entre outros. Esse cenário pode explicar a primeira colocação de antivírus como a principal medida de segurança a ser implementada em 2004.

> A capacitação técnica (75%) continua fazendo parte das principais medidas a serem implementadas pelas organizações.

> Termo de responsabilidade (58%), análise de ataque real-time (57,5%) e certificação digital (50%) não entraram na lista Top 10 2004, mas também fazem parte da lista de investimentos.

> Outra medida bem cotada é a certificação BS 7799, almejada por 16% das empresas.



5.18 - Outsourcing dos Serviços de Segurança da Informação

> 67% das empresas são favoráveis a algum tipo de outsourcing.

> 22% consideram ser possível gerenciar a segurança por conta própria.

> Para 51% dos entrevistados, o outsourcing dos serviços de Segurança da Informação é importante, uma vez que é uma atividade que necessita ter o apoio de especialistas.

5.19 - Serviços remotos de Gerenciamento de Segurança

> 71% das organizações são favoráveis aos serviços remotos de gerenciamento.

> 18% consideram ser possível gerenciar sozinha a segurança.

> Para 52% dos profissionais entrevistados, os serviços remotos de gerenciamento são importantes, pois têm uma boa relação de custo/benefício.

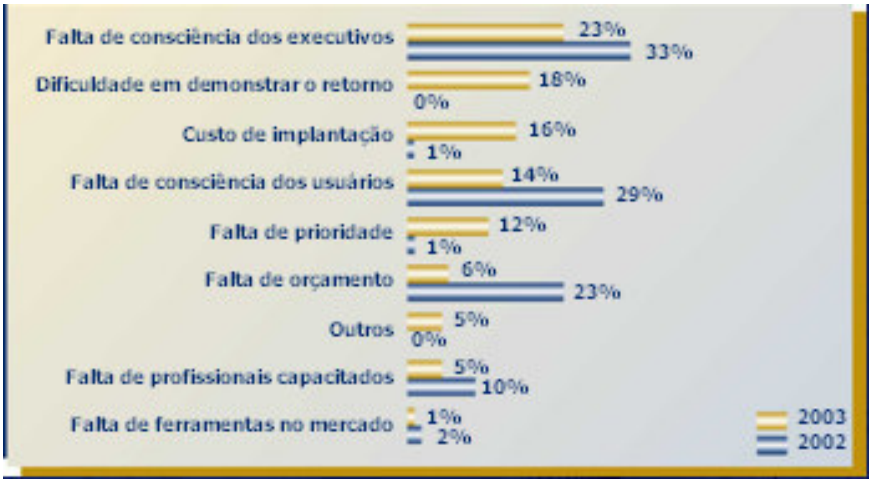
CAPÍTULO VI

ANÁLISE COMPARATIVA

6.1 - Obstáculos para Implementação da Segurança da Informação

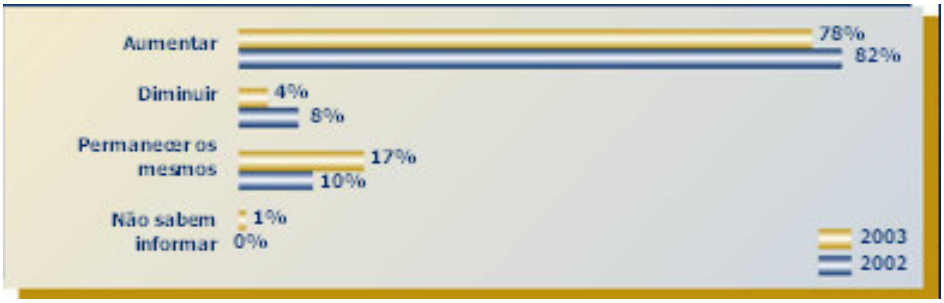
> Comparando os resultados de 2003 com os obtidos em 2002, constatam-se mudanças significativas: a falta de consciência dos usuários era o segundo item mais apontado em 2002. Nesse ano, a dificuldade de demonstrar o retorno e o custo de implantação aparecem nas primeiras colocações.

> No entanto, como em 2002, a falta de consciência dos executivos continua sendo apontada como o principal obstáculo, apesar de uma queda de 10 pontos percentuais.



6.2 - Expectativas em Relação aos Problemas

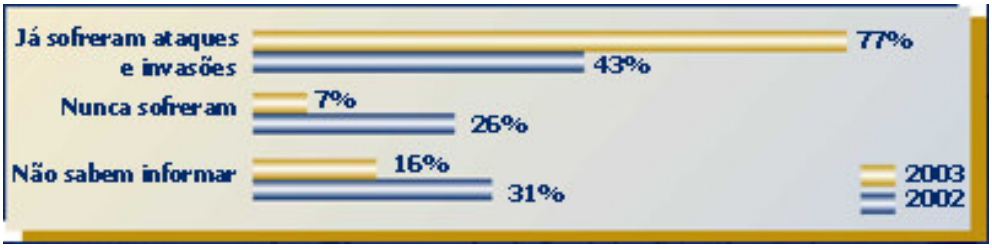
> Em relação às expectativas em relação aos problemas com segurança, o estudo registrou uma pequena variação: passou de 82% para 78%, índice que continua alto.



6.3 - Ocorrência de Ataques e Invasões

> O percentual de empresas que afirmam ter sofrido ataques e invasões subiu de 43%, em 2002, para 77%, em 2003.

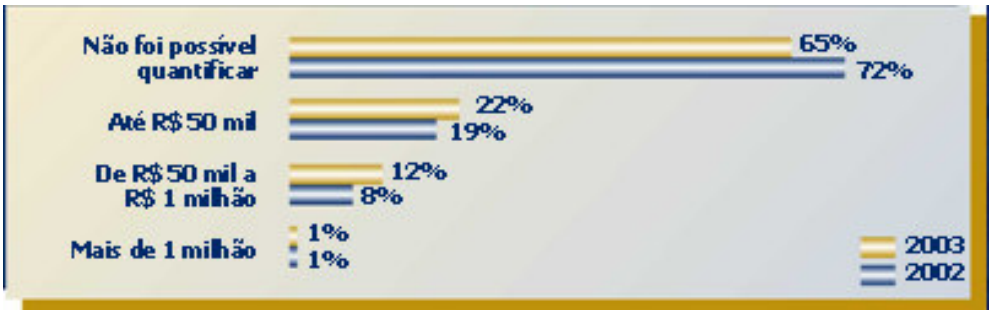
> Outro resultado expressivo foi a queda do percentual de empresas que não sabem informar se sofreram algum tipo de ataque ou invasão: de 31%, em 2002, para 16%, em 2003.



6.4 - Prejuízos Registrados

> O percentual de empresas que não conseguiram quantificar as perdas diminuiu de 2002 para 2003.

> Além disso, foi registrado um aumento de quatro pontos percentuais em relação às empresas que quantificaram seus prejuízos na faixa entre R$ 50 mil a R$ 1 milhão.



6.5 - Principais medidas de Segurança adotadas pelas Empresas

> Pelo terceiro ano consecutivo, antivírus, sistemas de backup e firewall foram apontados como as principais medidas de segurança implementadas.

> No Top 5, as mudanças aparecem na quarta e quinta posições. Se em 2002 essas posições foram ocupadas, respectivamente, por capacitação técnica e intrusion detection, neste ano os lugares são de política de segurança e capacitação técnica, respectivamente.

> O crescimento do item Política de Segurança reflete o aumento da adoção da norma NBR ISO/IEC 17799 nas empresas.

Ranking	2003	%	Ranking	2002	%
1	Antivírus	90	1	Antivírus	77
2	Sistemas de backup	76,5	2	Firewall	76
3	Firewall	75,5	3	Sistema de backup	69
4	Política de segurança	72,5	4	Capacitação técnica	63
5	Capacitação técnica	70	5	Intrusion detection	61
6	Software de controle de acesso	64	6	Política de segurança	60
7	Segurança física na sala de servidores	63	7	Proxy Server	58
8	Proxy Server	62	8	Monitoração de log	55
9	Criptografia	57	9	Análise de riscos	53
10	Análise de riscos	56	10	Software de controle de acesso	52

CAPÍTULO VII

CONCLUSÕES SOBRE A 9º PESQUISA NACIONAL DE INFORMAÇÕES NAS EMPRESAS

> Em relação ao Top 10 de Medidas de Segurança Adotadas, a lista apresenta duas novidades em relação à pesquisa de 2002: criptografia e segurança física na sala de servidores.

> Software de controle de acesso foi o item que apresentou o aumento mais significativo: passou da 10º, com 52%, para 6º, com 64%.

> A Segurança da Informação tornou-se fator prioritário na tomada de decisões e nos investimentos das organizações no país. Essa afirmação é uma das principais conclusões apontadas pelos índices obtidos pela 9ª Pesquisa Nacional de Segurança da Informação.

> Esses dados ficam evidentes quando observamos que 73% das empresas destinam orçamento específico para área de TI e que, deste total, 28,5% alocam mais de 5% para área de Segurança. Além disso, 60% dos entrevistados acreditam que os investimentos de suas empresas para 2004 vão aumentar.

> A pesquisa traz ainda importantes avanços relacionados com os três principais aspectos dentro de um projeto de Segurança: Tecnologia (recursos físicos e lógicos), Pessoas (cultura, capacitação e conscientização) e Processos (metodologia, normas e procedimentos).

> Em termos de Tecnologia, constata-se a consolidação das soluções técnicas e pontuais (antivírus e firewall, por exemplo) como as principais medidas de segurança implementadas. Além disso, os profissionais apontaram como satisfatória a oferta dessas ferramentas e soluções no mercado.

> Em relação a Processos, é preciso ressaltar que as novas exigências legais (como o Novo Código Civil, a regulamentação Sarbanes e Oxley, Publicações do Conselho Federal de Medicina, entre outros) tornaram a Segurança da Informação prioridade entre os requisitos de negócios de executivos e empresas.

> Ainda nessa área, a 9ª Pesquisa revela o fortalecimento da NBR ISO/IEC 17799 como a principal norma para implementação da Gestão em Segurança da Informação, complementando outras normas, legislações e regulamentações que já vinham sendo utilizadas pelas organizações.

> Se analisarmos as principais ameaças (vírus, divulgação de senhas e vazamento de informações) e obstáculos para implementação da Segurança da Informação (falta de consciência de executivos e usuários) apontados neste ano, verifica-se a necessidade de um contínuo investimento em programas de formação, capacitação e conscientização.

> O fator positivo é que as organizações já enxergam a necessidade de reverter esse cenário: Política de Segurança e Capacitação Técnica estão entre as cinco principais medidas de Segurança a serem implementadas em 2004.

CONCLUSÃO

A Segurança de Informações é o elemento chave dentro da organização, deixando de estar ligada apenas à Tecnologia e passando a ser compreendida como ferramenta estratégica para a Gestão de negócios, pois envolve aspectos técnicos, humanos e organizacionais, sendo fundamental a definição e existência de uma Política para efetiva proteção das informações.

Cada vez mais conectadas as Empresas compartilham informações, explorando crescentemente as possibilidades oferecidas pela tecnologia. Contudo, a concorrência no mercado, em que qualquer informação estratégica representa o diferencial competitivo da Empresa, passando a fazer parte da Gestão do próprio negócio.

A implementação das principais práticas de Segurança da Informação na Gestão estratégica é uma responsabilidade de todos e, como tal, deve ser de conhecimento de cada profissional da Empresa o cumprimento e conscientização de medidas de proteção dos recursos da informação, pois se trata de questão de alta prioridade estratégica.

BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBRISO/IEC17799: Tecnologia da informação - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

9ª PESQUISA nacional sobre segurança da informação. 2003. Disponível em: <http://www.modulo.com.br>. Acesso em: 20 abr. 2004.

COLTRO, Renata. Segurança: prioridade coorporativa. Computerworld, São Paulo, p. 26, 13 mar 2002.

CONCEITOS de segurança – TI. 2000. Disponível em: <http://www.ti.petrobras.com.br/gcom/seguranca/>. Acesso em: 25 jul. 2002.

MÓDULO Security Solutions S/A. 2004. Disponível em: <http://www.modulo.com.br>. Acesso em: 13 maio. 2004.

MOREIRA, Stringasci Nilton. Segurança mínima: uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

A FUGA Involuntária das Informações Estratégias nas Empresas: Fragilidade nas Redes. Disponível em: < http://www.brasiliano.com.br/artigo_102.htm>. Acesso em: 10 maio 2004.

O PENSAMENTO Competitivo e a Segurança de Informações. 2002. Disponível em: < http://www.brasiliano.com.br/artigo_20021028_a6.htm>. Acesso em: 06 abr 2004.

POLÍTICAS e diretrizes. 2002. Disponível em: < http://www.serinf.petrobras.com.br/politicas/politica.htm>. Acesso em: 03 maio. 2004.

SEGURANÇA da tecnologia. 2001. Disponível em: <http://www.modulo.com.br>. Acesso em: 10 maio. 2004.

ÍNDICE

FOLHA DE AVALIAÇÃO

Nome da Instituição:

Título da Monografia:

Autor:

Data da entrega:

Avaliado por: **Conceito:**
Avaliado por: **Conceito:**
Avaliado por: **Conceito:**

Conceito Final: