4. RESULTADOS

Neste capítulo, são apresentados os resultados da pesquisa. Primeiro, para uma melhor compreensão dos resultados obtidos, são mostrados panoramas da segurança da informação no mundo e no Brasil. Estas informações provenientes de fontes secundárias são fornecidas para auxiliar na contextualização do problema e para melhor entender a discussão que será realizada no próximo capítulo.

Em seguida, são apresentados os resultados sob forma de respostas à seqüência das perguntas do questionário que serviu como ferramenta de coleta de dados, no levantamento tipo survey, incluindo gráficos de distribuição de freqüência das respostas. Por último, são destacados pontos importantes levantados nas entrevistas realizadas.

4.1. SI no mundo

Uma pesquisa divulgada pelo Gartner Group (Gonçalves, 2003) revela que 80% das corporações em todo o mundo não possuem planos de continuidade de negócios. Dentre as que possuem um PCN, somente 28% possuem planos que tratam de ataques físicos e 36% que tratam de uma possível perda completa de seus recursos físicos e locais de trabalho.

Esse quadro é confirmado por diversas outras pesquisas. Uma realizada pela Storage Network Industry Association (Módulo, 2003) revelou que mais da metade dos departamentos de TI de empresas européias não possuem ou atualizam de forma correta um plano de continuidade de negócios. Outra pesquisa da AT&T (King, 2002) com 1057 empresas internacionais médias e grandes mostrou que 25% não possuem um PCN. Das que possuem, 27% não fizeram revisão do plano no último ano e 19% não fizeram nenhum tipo de teste nos últimos 5 anos. A AT&T levantou ainda os motivos pelos quais as empresas não possuem um PCN, ilustrados na Figura 2 (múltiplas respostas foram permitidas). O principal deles, infelizmente, é a baixa prioridade do assunto.

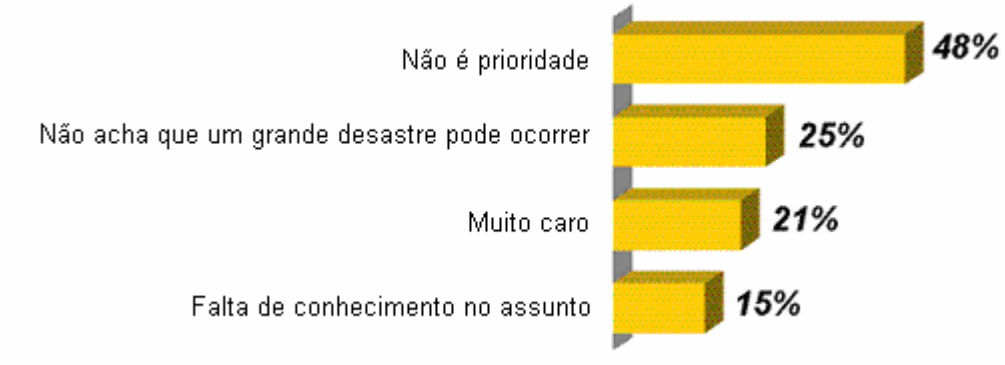

Figura 1: Motivos para não adoção de um PCN (AT&T, 2002)

Apesar do aparente baixo investimento em PCNs, de acordo com um levantamento realizado pela IDC (2001), ilustrado na Figura 3, as receitas mundiais relacionadas a serviços de continuidade de negócios vão crescer de US$2,3 bilhões em 2000 para US$6,3 bilhões em 2006. Esta tendência é confirmada por outro estudo realizado com 883 empresas norte-americanas pela própria IDC (IDG, 2003), que revelou que 38,5% de seus entrevistados aumentaram os investimentos em segurança de 2002 para 2003. Uma outra pesquisa da PricewaterhouseCoopers (2003) também encontrou a mesma tendência, mostrando que, de um total de respostas com 7500 executivos de TI espalhados por 47 países, 62% das empresas disseram que aumentaram seus gastos com segurança em 2003. Essas empresas investem em média 11% de seu orçamento de TI em segurança da informação.

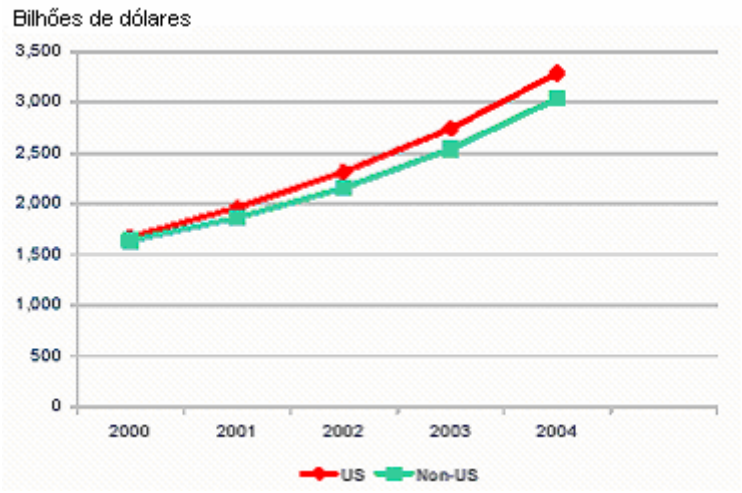

Figura 2: Receitas mundiais relacionadas a serviços de continuidade de negócios (IDC, 2001)

O assunto continuidade de negócios provoca polêmica até dentro da mesma empresa. Segundo um levantamento realizado pela empresa EMC (IDG, 2003) com 274 executivos de grandes organizações dos Estados Unidos, quando o assunto é segurança de dados críticos em casos de desastre, há discrepância entre opinião do executivo de negócios e do diretor de tecnologia da informação. A pesquisa revela que apenas 14% dos líderes de negócios consideram suas informações de negócios muito vulneráveis à perda em caso de desastre. Mas quando a questão é abordada junto dos executivos de TI, esta percepção sobe para 52%.

Outra diferença de percepção diz respeito ao tempo gasto para que operações fossem retomadas se um desastre acontecesse. Somente 9% dos executivos de negócios dizem que seria preciso três ou mais dias para recomeçar. No caso dos CIOs, 23% afirmam que a recuperação se estenderia de três dias para mais de uma semana.

Com relação à certificação em segurança da informação, o número de empresas pelo mundo certificadas pela norma BS 7799 aumentou consideravelmente (Rocha, 2003). Atualmente, tal lista contempla 202 empresas do mundo. O Reino Unido é o país com o maior número de organizações certificadas (86), seguido de Japão (20), Itália (11), Índia (10), Coréia (9), Alemanha (8), Finlândia (8), Singapura (7), Noruega (6), Hong Kong (6) e outros (31). O Brasil está presente com somente duas empresas: a Módulo e a Serasa.

4.2. SI no Brasil

Infelizmente, são poucas as pesquisas realizadas no Brasil em segurança da informação em comparação com as existentes no exterior. Não obstante, foi possível levantar algumas informações importantes.

Segundo levantamento feito pela Symantec (2002) com 240 empresas nacionais de grande porte, 36% não possuem PCN, 13% não souberam responder – o que provavelmente significa não -, 4% não responderam e apenas 47% confirmaram que possuem (veja Figura 4).

À primeira vista, o número de empresas (47%) que possuem PCN parece alto, mas devemos fazer algumas considerações a respeito. Primeiramente, a pesquisa não perguntou se esses planos estão atualizados, o que certamente faria

baixar a porcentagem. Segundo, a pesquisa não averiguou a qualidade desses planos. E terceiro, o público-alvo da pesquisa é constituído por empresas de grande porte, muitas das quais filiais de multinacionais, que podem investir com somas mais altas em SI e que provavelmente já possuem PCN em suas matrizes. Portanto, esse número de 47% das empresas que possuem PCN não é de forma alguma tranqüilizador. Tampouco é uma surpresa, que o maior impedimento para alterar esse quadro está ligado muito mais à conscientização (60%) do que ao orçamento (25%).

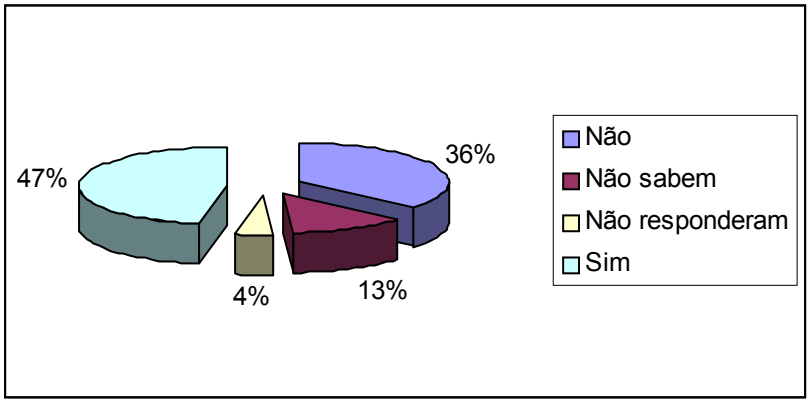

Figura 3: Empresas que possuem um PCN (Symantec, 2002)

A 8ª Pesquisa Nacional de Segurança da Informação realizada pela Módulo (2002) com 547 empresas brasileiras traz um rico panorama do setor. Destacam-se os seguintes dados:

- **a.** 78% das empresas no Brasil reconhecem que tiveram perdas financeiras. Porém, 56% ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança da informação. Em 22% das organizações que conseguiram contabilizar estes valores, o total de perdas registradas foi de R$ 39,7 milhões.
- **b.** Das medidas de segurança adotadas, a análise de riscos teve o maior aumento com relação à pesquisa anterior, passando de 24% em 2001, para 53% em 2002.
- **c.** A segurança da informação passou a ser fator importante para 45% dos executivos, sendo que 16% a consideram crítica e 32% entendem ser vital. Mesmo assim, a falta de conscientização dos executivos

(45%) e dos usuários (38%) foram apontadas como os principais obstáculos para implementação da segurança nas corporações.

d. 77% dos profissionais entrevistados informaram que suas empresas pretendem aumentar os investimentos em segurança em 2003. Este número era de 80% na pesquisa passada.

e. 30% dos entrevistados alocam de 1 a 5% do orçamento total da empresa para a área de tecnologia da informação.

f. 78% das empresas possuem orçamento específico para área de segurança da informação, sendo que 33% alocam recursos entre 1 e 5% do orçamento total de tecnologia, 24% alocam de 5 a 10%.

g. 36% das empresas ainda não possuem um planejamento dedicado à segurança da informação.

h. 98% das empresas pesquisadas possuem pelo menos 1 pessoa dedicada a segurança da informação, sendo que 24% destas possuem mais de 10 pessoas dedicadas.

i. 81% das empresas pretendem investir em capacitação da equipe técnica contra apenas 40% na pesquisa anterior.

j. Apenas 26% das empresas possuem um PCN atualizado (veja Figura 5).

k. Dentre os investimentos prioritários para 2003, o plano de continuidade de negócios passou da posição de 27º na pesquisa anterior para 15º na atual, citado por 50% dos respondentes.

l. As principais medidas adotadas ainda possuem características técnicas e pontuais, como a aquisição de equipamentos e softwares antivírus.

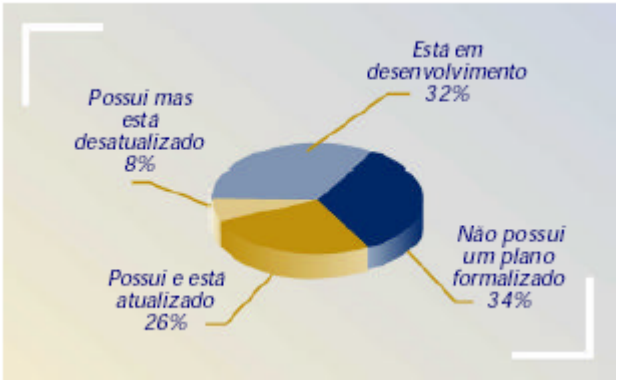

Figura 4: Empresas que possuem um PCN (Módulo, 2002)

Em pesquisa realizada pela empresa de segurança Módulo Security em parceria com a PUC-RJ com 950 pessoas do setor (Campos, 2003), foi possível traçar um perfil dos profissionais que estão atuando nessa área no país. A nova carreira dos CSOs (Chief Security Officer) está emergindo como uma das mais promissoras dentro da disputada área de Tecnologia da Informação.

Os CSOs têm uma grande responsabilidade nas mãos: gerenciar a segurança da informação de empresas, instituições financeiras, universidades e consultorias, entre outras organizações. A maioria está na faixa entre 20 e 30 anos e atua nos grandes centros como Rio de Janeiro, São Paulo e Brasília. Consideram-se profissionais planejadores, racionais, observadores e comunicativos. Além de um bom conhecimento tecnológico, têm como missão o desafio de convencer pessoas a adotarem de fato as normas de segurança que criam. No geral, trabalham com orçamentos enxutos e precisam ainda persuadir a diretoria das organizações de que prevenção é um bom negócio.

Para encerrar esta seção, são apresentados dados fornecidos pelo CAIS (2003) – Centro de Atendimento a Incidentes de Segurança – que podem auxiliar no convencimento da importância da prevenção de incidentes de segurança. Veja o aumento exponencial dos incidentes de segurança da informação ao longo dos últimos anos ilustrados na Figura 6. Vale destacar que a grande maioria dos incidentes não é comunicada, seja por desconhecimento dos serviços prestados pelo CAIS, medo de perda de imagem da empresa ou simplesmente falta de interesse.

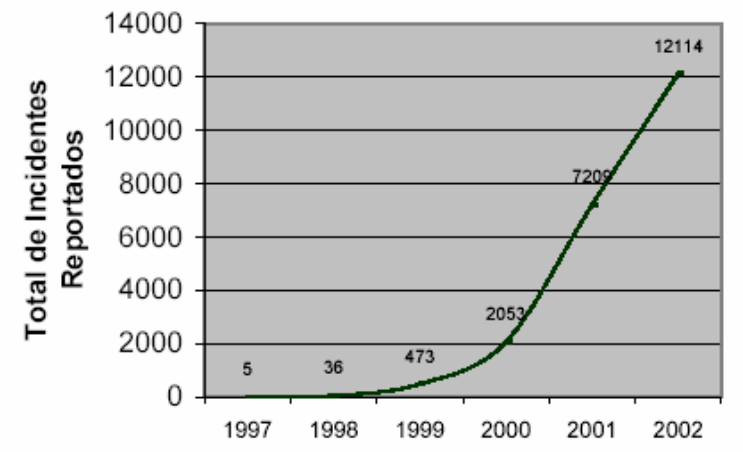

Figura 5: Incidentes reportados ao CAIS (CAIS, 2002)

4.3. Análise dos resultados

Nesta seção são analisados e confrontados os dados obtidos por meio dos documentos averiguados, dos questionários recebidos e das entrevistas realizadas. São também fornecidos gráficos para ilustrar os dados pesquisados.

Planejamento estratégico

No que concerne à variável Planejamento estratégico, buscou-se saber a importância que as empresas pesquisadas estão dando à continuidade dos seus negócios. Vale ressaltar que não necessariamente o discurso de apoio estratégico ao tema se traduz em recursos efetivos para a implementação do PCN. Por esse motivo, a variável procura também identificar se a prática reflete o apoio teórico.

Dentre as empresas pesquisadas, somente 21% declararam que possuem um plano de continuidade de negócios, como ilustrado na Figura 7.

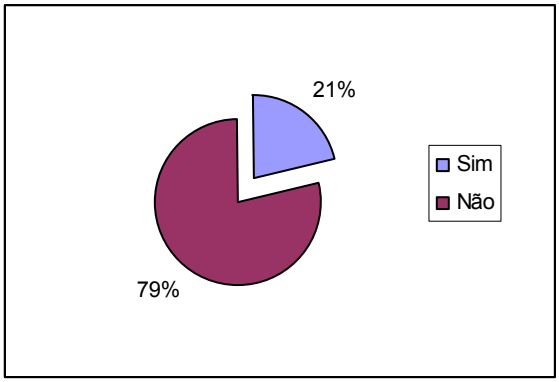

Figura 6: A empresa possui um PCN?

O percentual é significantemente baixo, visto que a pesquisa englobou empresas que são líderes em seus segmentos e teriam, portanto, maior disponibilidade de recursos, bem como maior preocupação em evitar a interrupção de suas atividades operacionais. Dentre os motivos mais citados para a não adoção do PCN estão:

- Desconhecimento do assunto (17 citações)
- Probabilidade de desastres é baixa (9 citações)
- Ferramentas adquiridas fornecem proteção necessária (8 citações)
- Baixa prioridade (6 citações)
- Alto custo de criação e manutenção (3 citações)

A segunda causa mais citada foi à baixa probabilidade de desastres. Como já assinalado no referencial teórico, é provável que a cultura do "jeitinho" brasileiro favoreça a falsa ilusão de que os problemas só acontecem com o vizinho, mas nunca conosco e que sempre é possível "dar um jeitinho" para evitar os incidentes. A falta de conhecimento dos riscos aos quais a empresa está submetida aumenta essa crença. Um dos entrevistados relatou que tem discutido muito com a diretoria sobre o assunto, expondo a necessidade de se contratar um parceiro de confiança para realização da análise de riscos e da criação de uma política de segurança a ser transmitida para toda a empresa. Novamente, entra neste contexto a questão de conscientização das empresas.

A terceira causa mais citada - ferramentas adquiridas fornecem proteção necessária - é de igual forma muito preocupante, pois a empresa está se escondendo atrás da tecnologia. Dois entrevistados também alegaram que suas empresas estão preparadas para enfrentar os incidentes de segurança, porque estão aparelhadas com dispositivos tecnológicos modernos. Embora se reconheça a importância da aquisição dos equipamentos e da sua correta configuração – já que a simples aquisição sem a preocupação em fazer com que o equipamento atenda às reais necessidades da empresa ajuda muito pouco -, não se pode deixar de apontar que o plano de continuidade de negócios está muito mais focalizado na dupla pessoas/procedimentos do que na tecnologia empregada.

A baixa prioridade do assunto foi a quarta causa mais citada. Um dos entrevistados, cuja empresa possui um PCN, explicou que o maior problema que

tiveram para implementar o plano foi a resistência dos funcionários em alterar os seus procedimentos habituais. A resistência encontrada só foi contornada por meio de palestras e muito treinamento. Entraremos em maiores detalhes sobre isso adiante no construto Treinamento.

Ao se confrontar o motivo alegado de baixa prioridade para a falta de investimentos na área com o resultado obtido para a afirmação de que a segurança da informação é considerada importante pela diretoria da empresa, chega-se ao que parece ser uma inconsistência. Conforme ilustra a Figura 8, 66% responderam que concordam ou concordam totalmente com a afirmação. Ou seja, a diretoria apóia verbalmente os investimentos em SI, mas a prioridade de investimentos na área é baixa.

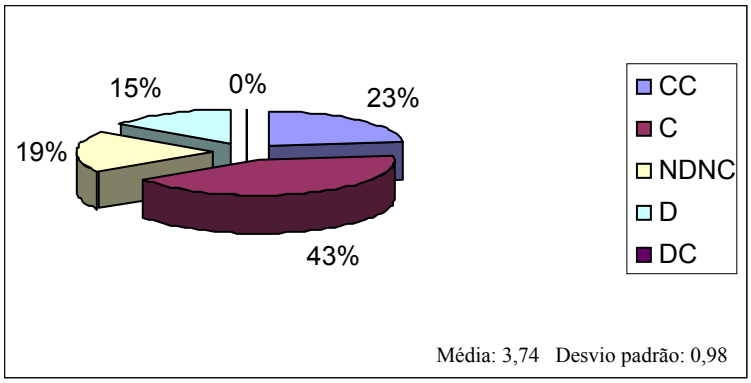

Figura 7: SI é importante para a diretoria da empresa

O mesmo fenômeno ocorre em relação às respostas da afirmação de que PCN é importante para a diretoria da empresa. Neste caso, 41% concordam ou concordam totalmente com a afirmação, apesar de que apenas 21% das empresas possuem um pano de continuidade de negócios.

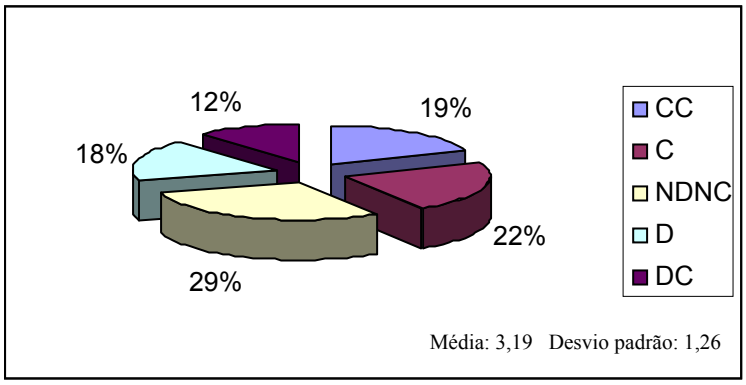

Figura 8: PCN é importante para a diretoria da empresa

A última causa mais citada foi o alto custo de criação e manutenção do plano, que realmente é bastante custosa. Essa questão de orçamento insuficiente será tratada mais à frente pelo construto Financeiro.

Em seguida, é visualizado um quadro que mostra a quantidade de empresas que possuem um PCN por setor. É possível verificar que alguns poucos setores estão mais maduros no tema do que os outros. Dos 12 setores pesquisados, apenas 6 apresentaram empresas que observam um PCN, sendo todos eles tradicionalmente empregadores de tecnologia.

Setor	PCN (qtde)	PCN (%)
Alimentação	0	0%
Construção	0	0%
Eletrônico	3	20%
Energia	4	100%
Farmacêutico	1	14%
Financeiro	6	50%
Hospitalar	0	0%
Telecom	6	100%
Têxtil	0	0%
TI	4	25%
Transporte	0	0%
Varejo	0	0%

Tabela 1: Empresas que possuem PCN por setor

Além do PCN propriamente dito, buscou-se saber se as empresas realizam análise de risco de suas atividades e recursos. Esta análise, como já explicado no referencial teórico, é importante para estabelecer os riscos aos quais os recursos das empresas estão submetidos, de forma que possam se precaver adequadamente para os casos de incidentes. Apenas 23% das empresas já realizaram a análise.

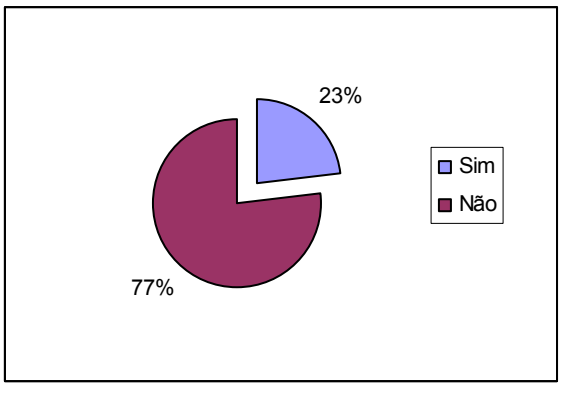

Figura 9: A empresa já realizou uma AR?

Não bastando que o percentual seja pequeno, somente 19% realizaram a análise nos últimos 6 meses. A maior parte, 43%, realizou há mais de um ano. As análises realizadas no período anterior a 12 meses são consideradas ultrapassadas, pois não refletem mais os riscos correntes que afligem as atividades operacionais.

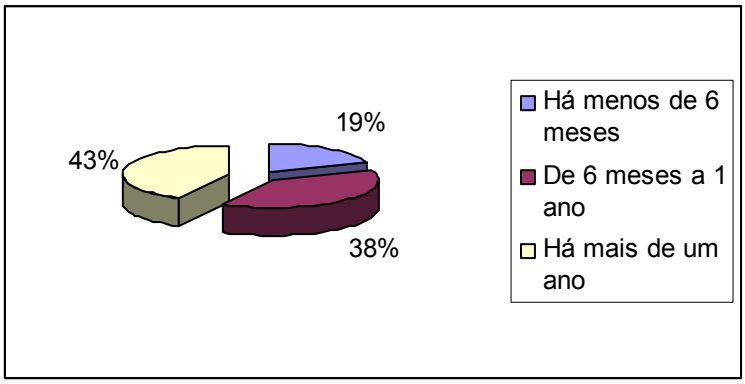

Figura 10: Realização da última AR

Analogamente, buscou-se saber se as empresas realizam análise de impacto em seu negócio. O resultado obtido foi de que tão somente 16% das empresas já realizaram, sendo que apenas 22% delas nos últimos 6 meses. A análise de impacto, bem como a análise de risco, deve ser realizada periodicamente para fazer face à nova realidade vivenciada pela empresa.

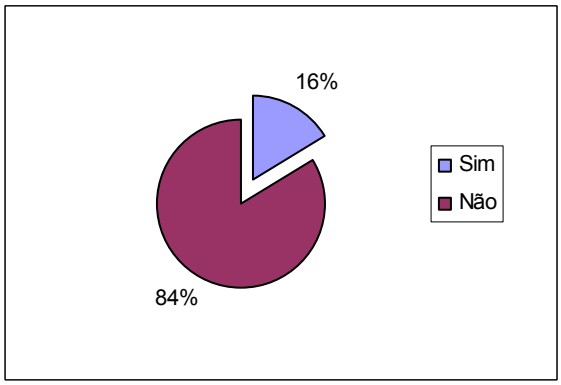

Figura 11: A empresa já realizou uma BIA?

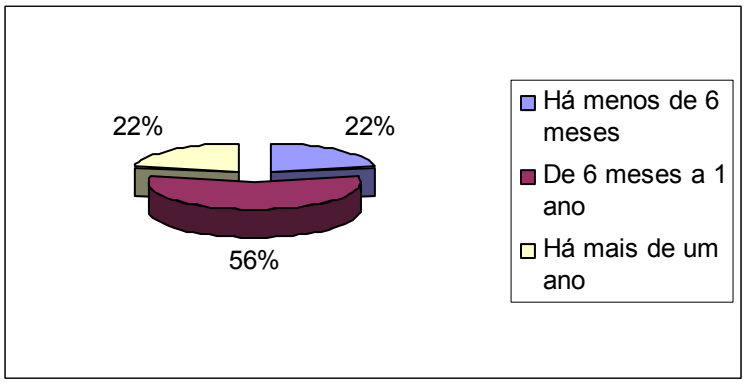

Figura 12: Realização da última BIA

Financeiro

Orçamento insuficiente é sempre um motivo alegado para a falta de investimento em segurança da informação. Sendo um mercado ainda em maturação, os equipamentos ainda são caros e os serviços de continuidade de negócios são muito dispendiosos. Logicamente, se compararmos esses custos com as conseqüências que podem ocorrer em casos de desastres, como perda de imagem para a empresa, perda de mercado e falência, os custos não vão parecer assim tão assustadores. Por esse motivo, o aspecto estratégico deve ter um peso maior do que o aspecto orçamentário.

De qualquer forma, o percentual do orçamento da empresa reservado para SI é menor do que 1% para 67% das empresas e de mais que 2% para apenas 4% delas, conforme ilustrado na Figura 14. O resultado vem a confirmar a reclamação dos entrevistados quanto aos magros recursos financeiros dirigidos à segurança da informação.

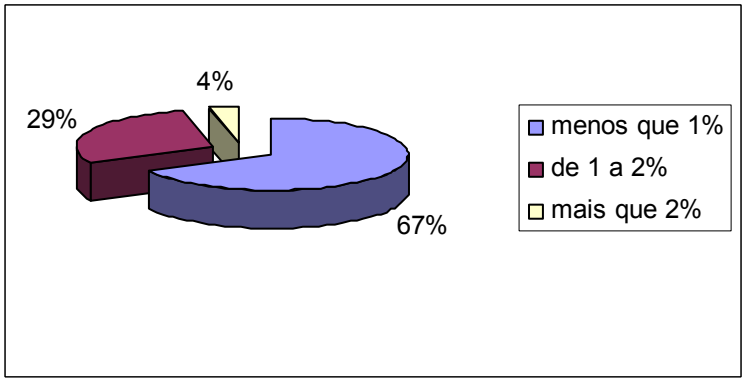

Figura 13: Percentual do orçamento para SI

Um dos entrevistados relatou que quase desistiram da implementação dos procedimentos do PCN pela metade, pois os custos estavam por demais elevados e a diretoria estava colocando diversos obstáculos para liberar mais recursos.

Esse quadro não deve ser alterado tão cedo, como nos informa a Figura 15. Segundo a pesquisa, apenas 21% das empresas pretendem aumentar os recursos. O quadro só não é tão desolador, porque um número restrito de 9% das empresas querem diminuir os recursos.

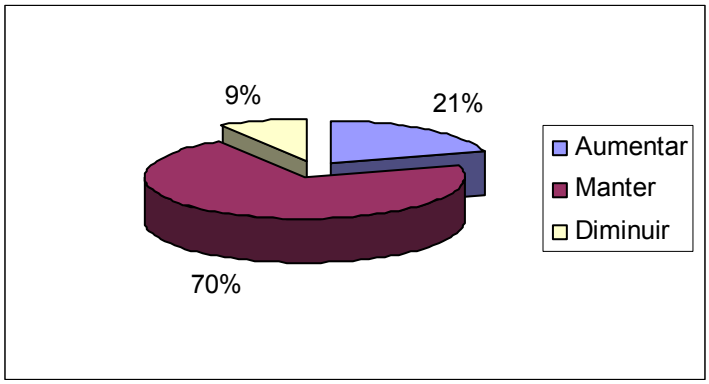

Figura 14: Tendência de variação do orçamento para SI

Os baixos números observados para SI se tornam ainda mais dramáticos para PCN. Nenhuma empresa pesquisada investe mais de 2% de seu orçamento em continuidade de negócios. A maioria absoluta de 87% reserva menos de 1%.

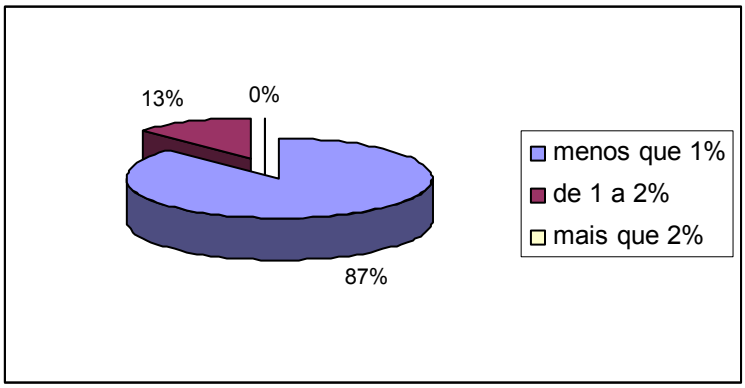

Figura 15: Percentual do orçamento para PCN

Tal qual a tendência quase nula de crescimento de recursos para SI, a tendência de variação do orçamento para PCN de 87% das empresas é de manutenção.

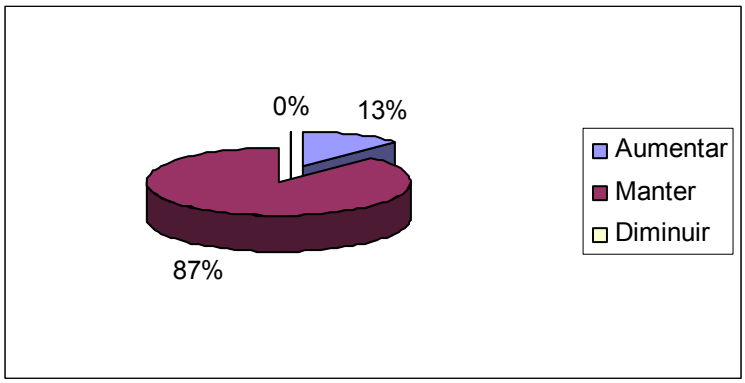

Figura 16: Tendência de variação do orçamento para PCN

Manutenção

A empresa pode ter investido bastante dinheiro para implementar o PCN, mas se ela não faz revisões periódicas, o plano fica desatualizado e a empresa se encontra despreparada para enfrentar os incidentes. Vale ressaltar que um plano desatualizado é apenas um pouco melhor do que plano algum.

A freqüência anual de revisão do PCN é de uma vez ao ano para 75% das empresas, o que mostra que quem resolve investir em continuidade dos negócios, realmente mostra disposição em se manter protegido. Este é o primeiro indicador positivo do estudo.

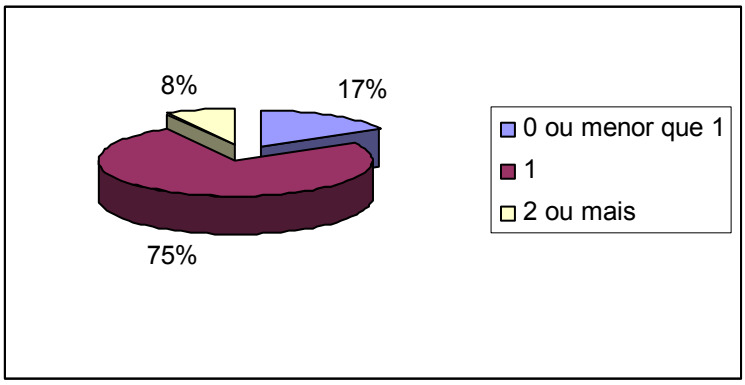

Figura 17: Freqüência de revisão do PCN

Fato análogo ocorre em relação à freqüência de simulação dos procedimentos contidos no PCN. Mais de três quartos (83%) das empresas realizam simulações uma vez por ano. Ou seja, a revisão do PCN costuma ser seguida por simulações dos procedimentos. Este é outro indicador positivo. Entretanto, diferentemente da revisão do PCN, nenhuma empresa possui freqüência igual ou maior do que 2 de simulação, enquanto 8% revisam em freqüência maior do que um.

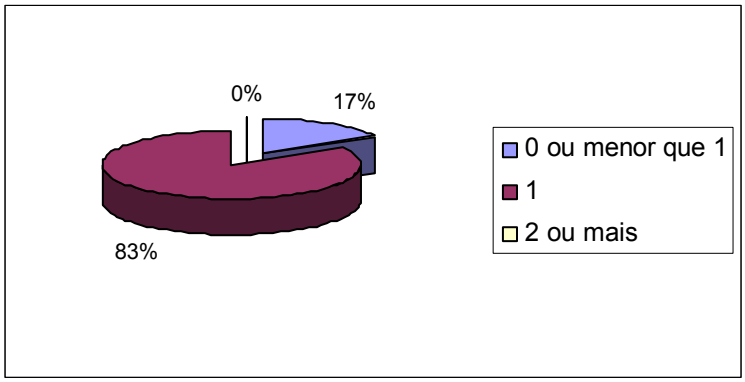

Figura 18: Freqüência de simulação dos procedimentos do PCN

Embora a grande maioria das empresas simule os procedimentos do PCN, a abrangência dos testes está aquém do desejado. Conforme ilustra a Tabela 7, enquanto a equipe de TI está envolvida nas simulações de todas as empresas, os outros participantes tiveram baixos percentuais de participação. Este resultado demonstra que as empresas ainda não estão empregando a prevenção aos incidentes de segurança a todos os elos da sua cadeia. Apesar da plena participação da equipe de TI ser um dado muito positivo, somente 38% das empresas envolveram todos os seus funcionários. Ou seja, ainda há grande despreparo para enfrentar desastres que não são de origem tecnológica, além de permitir que as conseqüências sejam espalhadas para os outros elos da cadeia.

Abrangência	Empresas (qtde)	Empresas (%)
Equipe de TI	24	100%
Todos os funcionários	9	38%
Fornecedores	7	29%
Clientes	3	13%
Serviços públicos	5	21%

Tabela 2: Abrangência das simulações

Treinamento

Treinamento é outro construto muito importante para a pesquisa. O investimento em treinamento é essencial para o sucesso da realização eficiente dos procedimentos contidos no PCN.

Três quartos (74%) das empresas pesquisadas treinam suas equipes de TI em segurança da informação uma ou mais vezes por ano, como a Figura 20 ilustra. Esse número realmente surpreendeu, pois se esperava que fosse menor. Vale enfatizar que não fez parte deste estudo averiguar a qualidade dos treinamentos ministrados. Outra observação importante é que um simples treinamento anual não garante a proteção necessária. É essencial que as empresas possuam um núcleo responsável pela área de segurança, o qual deve se dedicar inteiramente ao assunto. Um dos entrevistados revelou que só após a constituição de um grupo dedicado exclusivamente a SI é que foi possível aumentar a prevenção contra os riscos.

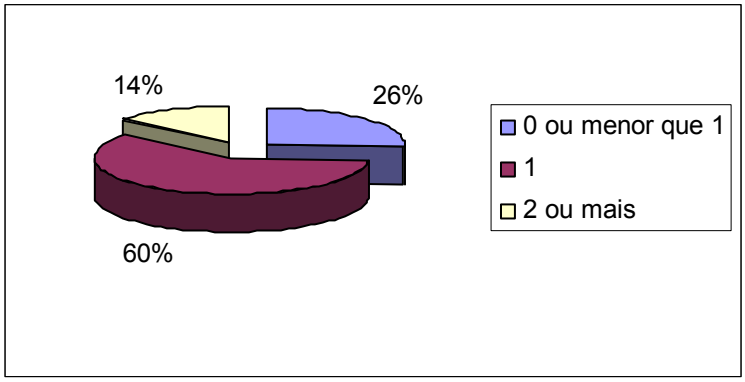

Figura 19: Freqüência de treinamento em SI para a equipe de TI

O quadro se torna diferente quando se trata do treinamento em segurança da informação para todos os funcionários da empresa. 64% das empresas não treinam seus funcionários adequadamente. Novamente, reforçamos nosso alerta em relação à falta de preparo dos funcionários em lidar com os incidentes de segurança.

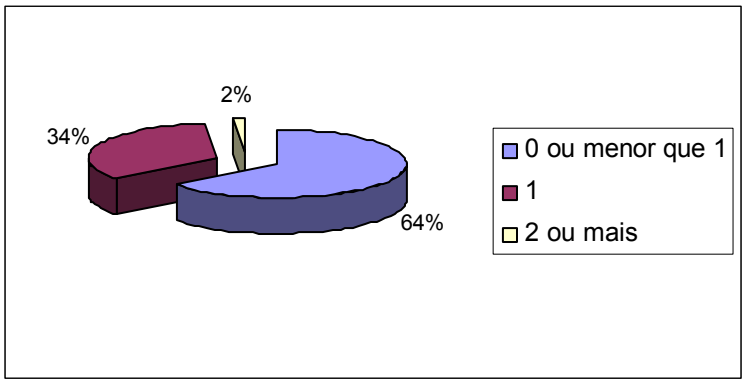

Figura 20: Freqüência de treinamento em SI para todos os funcionários

Do treinamento em SI, vamos passar para o treinamento em PCN. Nossa pesquisa indicou que 83% das empresas que possuem PCN treinam suas equipes de TI em continuidade de negócios. Outra grata surpresa do estudo. Isso mostra mais uma vez que as empresas que investiram em PCN estão bem conscientes da importância da mitigação dos riscos.

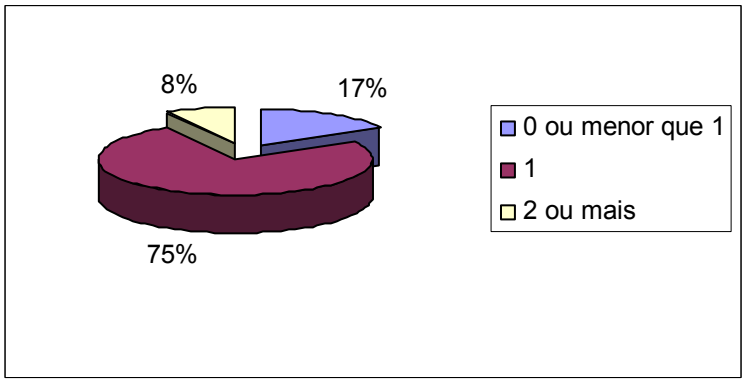

Figura 21: Freqüência de treinamento em PCN para a equipe de TI

Apesar do aparente sucesso no treinamento da equipe de TI, os responsáveis pela área consideram que eles ainda não estão bem preparados para agir em casos de incidentes de segurança. Como pode ser observado na Figura 23, apenas 22% consideram suas equipes preparadas adequadamente. Um dos entrevistados contou que os treinamentos se mostraram inadequados quando os incidentes ocorreram na prática. Portanto, estavam avaliando novos e diferentes tipos de treinamento.

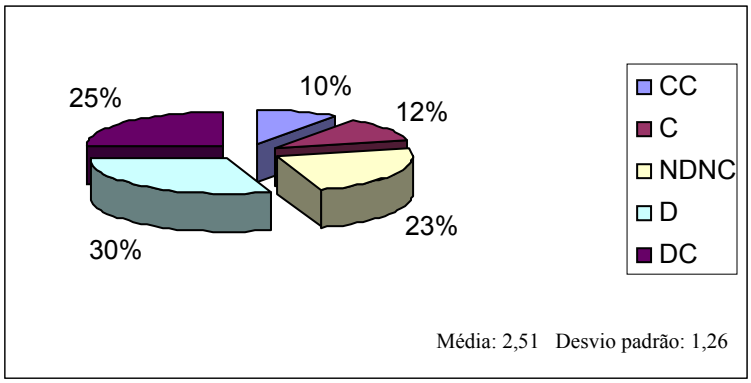

Figura 22: A equipe de TI está bem preparada para agir em incidentes

Infelizmente, o mesmo não se pode dizer da freqüência anual de treinamento em continuidade de negócios para todos os funcionários das empresas. Apenas 37% delas treinam seus funcionários uma ou mais vezes por ano.

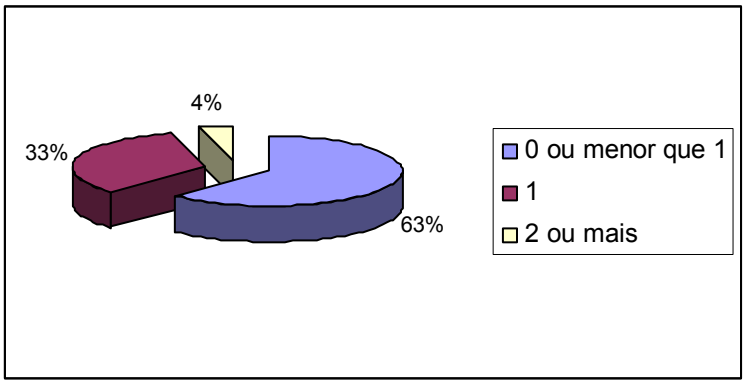

Figura 23: Freqüência de treinamento em PCN para todos os funcionários

A conseqüência da falta de treinamento dos funcionários da empresa é também percebida pelos respondentes, quando indagados se eles estavam bem preparados para agir em casos de incidentes. Somente 10% concordaram ou concordaram totalmente com a afirmação. Isso mostra que ainda há muito que se fazer em relação a treinamento em segurança da informação de maneira geral.

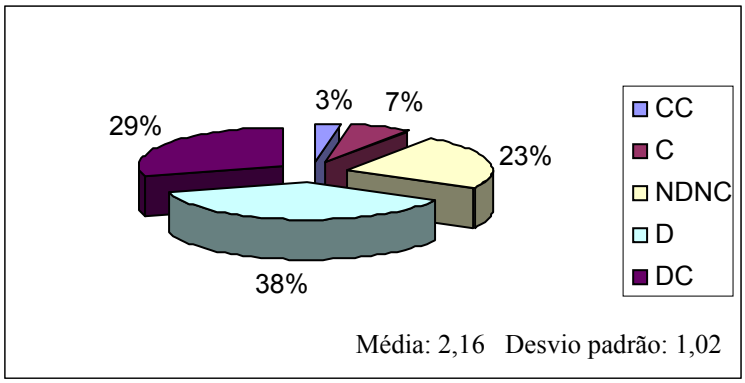

Figura 24: Todos os funcionários estão bem preparados para agir em incidentes