2. REFERENCIAL TEÓRICO

Foi iniciada uma revisão da literatura, a fim de conhecer os trabalhos mais recentes sobre o tema e contribuir para a elaboração do arcabouço teórico do estudo. Como já era de se esperar, considerando o ineditismo do assunto, não foi possível encontrar nenhum artigo científico sobre plano de continuidade de negócios até o presente momento.

Estendendo um pouco o escopo da revisão, foi possível encontrar vários artigos e dissertações sobre segurança da informação, embora grande parte deles se restrinja a abordar o assunto sob o ponto de vista tecnológico.

Embora a falta de material científico tenha se constituído em um sério obstáculo a ser superado, a literatura especializada possui diversos artigos e livros que foram utilizados para a construção do referencial teórico do presente estudo, o qual, pelos motivos expostos, possui um forte componente exploratório.

Apesar da frustração sentida, num primeiro momento, ao se deparar com a escassez de bibliografia pertinente, continuou-se no firme propósito de pesquisar sobre PCNs, a fim de contribuir para um melhor entendimento do tema e para um melhor preparo das organizações em lidar com os problemas de continuidade dos seus negócios.

A revisão da literatura está dividida em duas grandes seções. A primeira oferece referencial sobre segurança da informação, fornecendo subsídios para a compreensão da segunda que, por sua vez, discorre sobre plano de continuidade de negócios propriamente dito. Dentro de cada seção, são abordados diversos tópicos considerados importantes para a constituição do arcabouço teórico.

2.1. Segurança da informação

Alguns autores classificam segurança da informação como proteção dos dados digitais armazenados ou transmitidos (Goldberg, 2000; Webopedia, 2002).

McDaniel (1994, p. 53) propõe um conceito mais amplo da área, definindo segurança da informação da seguinte forma:

> *Os conceitos, técnicas e medidas técnicas e administrativas utilizadas para proteger recursos de informação contra aquisição, estrago, divulgação, manipulação, modificação, perda ou uso de forma premeditada ou negligente.*[1]

O Institute for Telecommunication Sciences – ITS (1996) possui uma definição bem similar na norma FS-1037C, enquanto o departamento INFOSEC da TAMU[2] estende um pouco a definição do termo, incluindo *hardware*, *software*, políticas e preparação para desastres como forma de proteger os sistemas de informação.

Já a NBR ISO/IEC 17799 (ABNT, 2001) se preocupa mais com a interrupção dos negócios ao afirmar que a segurança da informação, além de proteger a informação de diversos tipos de ameaças, garante a continuidade das atividades, minimiza danos aos negócios e maximiza o retorno dos investimentos. Esta definição foi adotada na elaboração da presente pesquisa por ser mais pertinente ao tema específico de PCN.

Faz-se apenas uma ressalva quanto à última parte da definição que concerne à maximização do retorno dos investimentos. Não é objetivo primário da SI oferecer lucro contábil nem algum outro tipo de retorno financeiro, mas, sim, servir de seguro contra as ameaças de segurança. Embora possa vir a cortar custos ao otimizar o acesso aos recursos de informação de uma organização, na maior parte das vezes, ela impõe altos custos cujos benefícios associados somente serão avaliados em caso de desastres.

Outra definição relevante é a da expressão incidente de segurança. A norma N3017 (ISO, 2002) define o termo como sendo uma real, tentativa ou suspeita de violação de segurança, causada por erro humano, mau funcionamento ou forças da natureza.

A segurança da informação instituiu ainda quatro outros conceitos importantes que devem ser rigorosamente observados: confidencialidade, integridade, disponibilidade e irretratabilidade.

---

[1] Tradução livre do autor. No original: "Information Security.. the concepts, techniques, technical measures and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss or use."

[2] As abreviaturas utilizadas ao longo do texto estão explicadas na seção Lista de Abreviaturas.

De acordo com a norma NBR ISO/IEC 17799 (ABNT, 2001), confidencialidade é a garantia de que a informação seja acessível somente às pessoas autorizadas. Integridade é a garantia de que as informações e os métodos de processamento somente sejam alterados por meio de ações planejadas e autorizadas. Disponibilidade é a garantia de que os usuários autorizados tenham acesso à informação sempre quando desejarem. Irretratabilidade – também conhecida como não repúdio – é a garantia de que é impossível se negar a autoria de um documento.

Normas de segurança

A norma supracitada, NBR ISO/IEC 17799, é um documento muito importante para todas as pessoas e empresas que desejam conhecer o tema em questão a fundo e se guiar por meio de práticas reconhecidas internacionalmente como as melhores para a gestão da segurança da informação. Ela é equivalente à norma ISO 17799 que, por sua vez, é oriunda da BS 7799.

A BS 7799 é uma norma britânica criada em 1995 que foi o primeiro documento a ser reconhecido internacionalmente como guia completo de práticas de SI. Normas criadas em diversos países e organizações posteriormente se basearam nela.[3]

As normas reduziram um dos maiores obstáculos à adoção da segurança da informação nas empresas que era a falta de padrões com relação à metodologia de implementação das soluções (COBB, 2001). Isso permitiu uma melhor proteção dos sistemas das organizações, principalmente quando estas passaram a atuar no âmbito da internet.

Terminada a parte dedicada às definições, trata-se na seção seguinte de um tópico muito comentado atualmente que é a segurança na internet.

Segurança na internet

Somos bombardeados o tempo todo por notícias de vírus que se espalham pelo mundo inteiro, números de cartão de crédito que são roubados, contas bancárias que são invadidas e vários outros incidentes similares.

[3] Veja um pequeno histórico das normas de segurança da informação em Gonçalves (2003).

Esse tipo de ação é de certo modo facilitado, uma vez que a segurança na internet é, por sua natureza, muito interdependente (CERT, 2002). Cada sistema exposto a ataques depende, além do seu próprio nível de segurança, do nível de todos os outros sistemas também presentes na rede. Conseqüentemente, a fraqueza de um compromete a proteção de todos.

Dessa forma, considerando também os avanços na técnica dos ataques, a interconectividade permite que um invasor possa empregar um grande número de sistemas para atacar um dado alvo.

O grande paradoxo presente no melhor rendimento obtido nos ataques realizados nos últimos tempos – explorados exaustivamente pela mídia – é que a mesma tecnologia que permite maior agilidade e redução de custos de operação também contribui para o desenvolvimento das técnicas de invasão (Chapman, 1995). Contudo, faz-se uma ressalva de que a internet é apenas um meio que, por sua vez, pode ser utilizada para fins lícitos e ilícitos.

Os fins ilícitos são decorrentes de diversos tipos de ameaça para pessoas e empresas que dependem de recursos de informação para entretenimento, pesquisa e negócios. Elas devem estar cientes do perigo que correm, pois a conscientização é o primeiro passo para se criar uma cultura de segurança. A seguir elabora-se a respeito dessas ameaças.

Ameaças

Os profissionais atuantes na área de segurança da informação possuem uma máxima que diz que não existe segurança absoluta (Sêmola, 2003). Uma empresa pode se sentir segura se desconectar todos os computadores da rede, não trocar informações eletrônicas com o mundo exterior e vigiar continuamente todos os seus funcionários o tempo todo. Como isso não é possível, a empresa deve saber lidar com as ameaças que podem atingi-la.

Uma vez que a empresa tenha necessidade de interagir eletronicamente com o mundo exterior, é importante lembrar que a segurança se faz em pedaços, porém todos eles interligados, como os elos de uma corrente (Sêmola, 2003). Esse conceito de corrente originou um importante axioma da segurança da informação: uma corrente não é mais forte do que o seu elo mais fraco (Goldani, 2001).

Exemplificando, não adianta a empresa ter os equipamentos[4] mais seguros que existem, se as senhas dos funcionários estão disponíveis em cima das respectivas mesas[5]. Por esse motivo, a gestão da segurança da informação deve abranger a empresa como um todo.

Uma grande fonte de preocupação para as organizações em geral são os *hackers*. De acordo com Lopes (2000), os *hackers* – piratas do século XXI – são motivados pelo desafio de se mostrarem melhores do que os projetistas dos sistemas de segurança. Essa disputa moderna entre "o bem e o mal" envolve cifras milionárias no desenvolvimento e compra de softwares mais seguros.

Vale ressaltar que, diferentemente do que foi sempre informado pela mídia, os *hackers* não necessariamente causam danos aos sistemas que invadem. Muitas vezes, eles avisam aos respectivos proprietários dos riscos que estão correndo. Por outro lado, os *crackers* são extremamente perigosos, pois destroem arquivos, roubam informações e podem paralisar os sistemas de uma empresa.

A força dos *crackers* pode ser ilustrada no ocorrido de 22 de outubro de 2002, quando a maior parte dos servidores-raiz da internet, responsáveis pelo sistema de domínios da rede (DNS – Domain Name Server) foi paralisada devido a diversos ataques perpetrados simultaneamente.

A ameaça quase mitológica dos invasores de computadores é real, mas não é nem o maior nem o mais iminente perigo para a segurança das empresas (Goldani, 2001).

As ameaças de segurança da informação podem ser oriundas de situações, como:

a. Catástrofes: incêndio, alagamento, vazamento, explosão, desabamento, relâmpago.

b. Problemas ambientais: variações térmicas, umidade, poeira, radiação, ruído, vapores, gases, fumaça, magnetismo, trepidação, falta de energia elétrica.

c. Comportamento anti-social: paralisação, greve, piquete, invasão, alcoolismo, drogas, sabotagem, omissão, inveja, rixa entre funcionários,

[4] Segundo Souza Machado (2002), a maioria dos autores (Nilles, 1997; Chen, 2000; Hirsch, 2000; Purcel 2000; Reid, 2000; Cartwright, 2001) recomenda somente o uso de ferramentas técnicas e equipamentos como forma de reduzir os riscos de segurança.

[5] Veja no Apêndice B como é possível oferecer melhor proteção aos dados de uma organização.

ação criminosa, furtos, fraudes, terrorismo, seqüestro, espionagem industrial.

d. Eletrônica: pane nos equipamentos, pane na rede, falhas nos sistemas operacionais, parada de sistema.

e. Procedimentos: supressão de serviços, erros de usuários, erros de backup, uso inadequado de sistemas, manipulação errada de arquivos, dados incompletos ou inconsistentes, violação de confidencialidade, treinamento insuficiente, ausência e demissão de funcionários, sobrecarga de trabalho.

Cada uma dessas situações expõe as empresas a riscos que devem ser avaliados cuidadosamente. Merecem também meticulosa análise os impactos associados a esses riscos. No processo de análise é possível identificar ações a serem tomadas imediatamente para minimizar as ameaças e as ações que devem ser tomadas para recompor a atividade operacional prejudicada. Maiores detalhes serão fornecidos na seção 2.2.

Para encerrar este tópico sobre ameaças, destaca-se a citação de Tzu (2001) que ilustra bem o nível de conhecimento que se deve ter internamente da organização a ser protegida e das ameaças que a afligem:

> *Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá um derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.*

É importante lembrar que a proteção contra ameaças gera benefícios para as organizações, recrudescendo a segurança de tudo que ela abrange, seja material, financeiro ou humano. Entretanto, isso tudo tem um custo que deve ser devidamente ponderado com os benefícios proporcionados.

Benefícios e custos

O melhor nível de segurança para uma determinada empresa não é a garantia de ser igualmente bom para outra. De acordo com Sêmola (2003), cada negócio tem suas características e especificidades próprias que devem ser consideradas para formulação de uma política de segurança da informação.

Gil (1995) apontou corretamente que as empresas devem ter suas necessidades estudadas dentro do trinômio bem/ameaça/medida de segurança, analisando sempre a relação custo/benefício de cada ação. Caso contrário, o orçamento para a área será por demais oneroso. O próprio Gil acrescenta que não basta elaborar um orçamento para a área de segurança, sendo necessário provar o retorno financeiro das atividades envolvidas.

É imprescindível frisar que qualquer que seja o nível de segurança aplicado em uma empresa, ele deve ser compatível com os valores essenciais de uma sociedade democrática, incluindo a liberdade de expressão, o fluxo livre de informações e o legítimo interesse de terceiros (OECD, 2002).

2.2. Plano de continuidade de negócios

Muitas vezes a expressão plano de continuidade de negócios é lembrada somente como o restabelecimento das operações em caso de desastre (Hiles, 1999), quando esta definição é mais correta a ser utilizada para plano de recuperação de desastres (PRD).

Segundo definição da SANS (2002), enquanto o PRD focaliza na recuperação dos recursos de informação que foram paralisados, o PCN descreve os processos e procedimentos que uma organização deve implantar para assegurar que funções essenciais continuarão a operar durante um desastre.

A literatura disponível não é unânime em relação ao PCN incluir o PRD (Bradashcia, 2002; Moore, 2000; Whatis.com, 2002) ou se são planos separados (Fagundes, 2003; IDC, 2001; KPMG, 2002; SANS, 2002). Para esta pesquisa, será utilizada a definição mais abrangente que inclui as ações de recuperação. Portanto, o PCN visa a assegurar a continuidade das atividades críticas de uma organização durante um desastre, procurando restabelecer a normalidade de todas as operações no menor espaço de tempo possível.

Ao longo desta seção, serão fornecidas informações detalhadas sobre a elaboração de um plano de continuidade de negócios etapa por etapa e os benefícios que ele proporciona.

Prevenção

A mídia sempre explora com muito destaque os desastres de grandes proporções ao exemplificar a importância dos PCNs. Embora eventos de grande magnitude ocorram, resultando quase sempre em perdas imensas, são os pequenos eventos, por possuírem maior freqüência, que causam danos contínuos às empresas.

De qualquer forma, as organizações devem estar preparadas para todos os tipos de ameaças, sejam externas ou internas, antigas ou novas. Ameaças em potencial devem ser foco de constante monitoramento, a fim de que não causem problemas no futuro.

A chave para o sucesso de qualquer programa de segurança da informação reside exatamente em tomar uma posição preventiva contra as ameaças e riscos de segurança, reduzindo os pontos vulneráveis (ABNT, 2001; Correia, 2002).

É importante enfatizar que o PCN não deve ser preocupação somente do setor de TI das organizações, mas, sim, adotado por toda a organização (Figueirêdo, 2002).

A norma NBR ISO/IEC 17799 (ABNT, 2001) acrescenta ainda que a gestão da continuidade do negócio deve incluir controles para a identificação e redução de riscos, limitação dos danos e garantia de recuperação tempestiva das operações vitais.

De acordo com a norma, os elementos-chave da gestão da continuidade do negócio são:

a. Conhecimento dos riscos a que a organização está exposta, incluindo probabilidade de ocorrência e impacto.

b. Conhecimento do impacto que as interrupções provavelmente causarão sobre os negócios.

c. Estabelecimento dos objetivos do negócio relacionados com os recursos de informação.

d. Consideração da possibilidade de contratação de seguro compatível com os riscos identificados.

e. Definição de estratégia de continuidade consistente com os objetivos estabelecidos para o negócio e os requisitos de segurança da empresa.

f. Detalhamento e documentação de plano de continuidade alinhados com a estratégia definida.

g. Execução de testes e simulações do plano elaborado.

h. Revisões periódicas do plano, possibilitando imediata atualização do mesmo, de acordo com a nova realidade apresentada.

i. Garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização.

A DRI (2002) adiciona um outro elemento-chave que é a identificação das funções críticas da organização – funções de negócios, suporte e interdependências –, de modo que se possa conhecer melhor os incidentes aos quais elas podem estar expostas.

Fites (1989) identifica os seguintes passos para elaborar um plano de segurança para um *site* que pode servir de ponto de partida para ser aplicado em uma empresa:

a. Identificar o que se está querendo proteger.

b. Determinar do que se está protegendo.

c. Determinar de forma mais detalhada possível como as ameaças são.

d. Implementar medidas que protegerão os recursos da empresa.

e. Revisar o processo continuadamente, realizando as devidas alterações quando alguma falha for detectada.

A norma NBR ISO/IEC 17799 (ABNT, 2001) é mais específica na estruturação de um plano para a continuidade do negócio que abrangeria os seguintes itens:

a. Condições e procedimentos para ativação dos planos, explicitando como avaliar a situação e quem deve ser acionado.

b. Procedimentos de emergência que descrevam as ações a serem tomadas após a ocorrência de um incidente de segurança, incluindo a

preservação de vidas humanas e das operações do negócio e o rápido contato com as autoridades competentes, tais como, polícia, bombeiros e governo.

c. Procedimentos de recuperação das atividades essenciais do negócio e reativação dos serviços no prazo necessário.

d. Procedimentos de recuperação com as ações a serem tomadas quando do restabelecimento das operações.

e. Programação especificando quando e como o plano deverá ser testado e a forma de se proceder à sua própria manutenção.

f. Desenvolvimento de atividades educativas e de conscientização que visem o entendimento do processo de continuidade e garantam a efetividade do mesmo.

g. Designação das responsabilidades individuais, descrevendo quem é responsável pela execução de que item do plano, incluindo possíveis suplentes.

Atividades terceirizadas e serviços públicos também devem ser contemplados no plano. É comum o esquecimento da inclusão de processos realizados por terceiros, mas que muitas vezes são essenciais para a empresa, como, por exemplo, o fornecimento de energia elétrica e água.

Os responsáveis pelos serviços terceirizados devem estar envolvidos na elaboração do plano e participando dos procedimentos de teste, revisão e atualização do mesmo.

Da mesma forma, os serviços públicos, como bombeiro, polícia e hospital precisam estar igualmente contemplados nos procedimentos de continuidade.

É essencial que as organizações identifiquem os seus respectivos requisitos de segurança, a fim de poderem prover uma melhor segurança para si mesmas. Os requisitos apontam o que se está querendo proteger, fornecendo material crucial para a definição do PCN.

A ISO 17799 (ABNT, 2001) afirma que são três as principais fontes para o estabelecimento dos requisitos. A primeira é obtida por meio da análise de risco dos ativos de informação. A segunda é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que as organizações, seus parceiros e

contratados e prestadores de serviços têm que atender. A terceira é o conjunto particular de princípios, objetivos e requisitos para o processamento da informação decorrente das atividades de cada organização.

Análise de riscos

É sempre importante frisar que segurança absoluta não existe (Goldani, 2001). Podem-se identificar vários exemplos de situações que fogem totalmente ao nosso controle, como: ataques nucleares, epidemias, guerras ou mesmo uma simples indigestão. Entretanto, existem inúmeros riscos que podem e devem ser analisados para prevenir a empresa de possíveis estragos.

A análise de riscos (AR) provê subsídios necessários para que seja possível conhecer os fatores que podem influenciar negativamente as operações da empresa (GAO, 1999), bem como estabelecer controles para redução dos riscos identificados (NIST, 1996).

Outra importante contribuição da análise é justificar investimentos em segurança da informação (DRI, 2002), uma vez que ficam evidentes os perigos aos quais a empresa está submetida. Esse ponto é muito importante, conforme observa Figueirêdo (2002), já que o plano de continuidade de negócios não visa a obter maiores lucros, o que pode causar dificuldades para aprovação de orçamento para esse fim.

Vale frisar que não necessariamente os riscos podem ser eliminados completamente. Sempre existirão riscos residuais que devem ser de pleno conhecimento do alto escalão das empresas, a fim de que fique claro o que pôde ser eliminado e o que ainda persiste.

De acordo com a OECD (2002), a análise de riscos deve ser dinâmica, englobando todos os níveis das atividades dos funcionários e todos os aspectos de suas operações. Uma AR bem feita deve iniciar com a identificação do que se deseja proteger. Uma sugestão de lista é fornecida por Pereira (2000):

a. Hardware: computadores, servidores, impressoras, equipamentos de rede.

b. Software: programas fonte, utilitários, sistemas operacionais.

c. Dados: bases de dados, backups, logs, dados em transferência.

d. Pessoas: pessoas-chave na organização.

e. Documentação: planilhas, gráficos, procedimentos, arquivos em geral.

f. Suprimentos: papéis, formulários, mídias magnéticas.

O segundo passo é identificar as ameaças as quais a empresa está sujeita. Diversas situações de ameaças já foram apontadas anteriormente, mas vale destacar suas fontes (DRI, 2002):

a. Natural, humana, tecnológica ou política

b. Acidental versus intencional

c. Interna versus externa

d. Risco controlável versus risco não controlável

e. Eventos com alertas prévios versus eventos sem alertas

Em seguida, deve-se proceder com a classificação dos riscos. Existem diversas técnicas de AR descritas na literatura. Vejamos a matriz de riscos adotada por GAO (1999):

Nível de Severidade	Probabilidade de ocorrência				
	(A) Frequente	(B) Provável	(C) Ocasional	(D) Remota	(E) Improvável
I - Alto					
II					
III					
IV - Baixo					

= Risco 1 (indesejável; requer ação corretiva imediata)
= Risco 2 (indesejável; requer ação corretiva, mas permite gerenciamento discreto)
= Risco 3 (aceitável; requer revisão)
= Risco 4 (aceitável sem revisão)

Tabela 1: Matriz de riscos (GAO, 1999)

GAO (1999) estabelece quatro níveis de severidade e cinco de probabilidade de ocorrência para fatores que são ameaças para as organizações. Com base na matriz, é possível classificar os riscos:

1. Não desejáveis. Devem ser eliminados imediatamente.
2. Não desejáveis. Devem ser eliminados, mas permitem uma revisão mais longa.
3. Aceitáveis, mas devem sofrer revisão.
4. Aceitáveis. Nenhuma ação é necessária.

Outra técnica de AR é a análise preliminar de riscos (APR) que foi desenvolvida com base na norma militar inglesa MIL-STD-882 (Souza Machado, 2002).

	Tipo de Severidade			
Faixa de Probabilidade	**Catastrófica**	**Crítica**	**Marginal**	**Desprezível**
Freqüente	T4	T4	T3	T2
Provável	T4	T3	T3	T2
Ocasional	T3	T3	T2	T1
Remota	T3	T2	T2	T1
Improvável	T2	T2	T1	T1

Tabela 2: Análise preliminar de riscos (Souza Machado, 2002)

A APR classifica os fatores críticos em relação à severidade e à probabilidade de ocorrência. O tipo de severidade é dividido em:

a. Desprezível: não degrada o sistema ou seu funcionamento

b. Marginal: degradação moderada com danos menores, compensáveis ou controláveis.

c. Crítica: degradação com danos substanciais que colocam o sistema em risco, necessitando ações corretivas imediatas para a sua continuidade.

d. Catastrófica: séria degradação ou perda do sistema.

A análise de riscos, por si só, já é um avanço, porém as organizações não podem se acomodar nesse ponto. A AR dever ser complementada com a análise de impacto nos negócios que determina a severidade do impacto que os incidentes acarretam no negócio da empresa.

Análise de impacto no negócio

Segundo Fernando Marinho (Coutto, 2003), CIO da Storm Security, a análise de impacto no negócio (BIA – Business Impact Analysis) serve para indicar o valor do custo financeiro de parada de um processo de negócio ou componente que os suporte, indicando a ordem de restauração ou reposição.

De acordo com Bradaschia (2002), nessa análise deve-se identificar as aplicações mais criticas para o negócio e o tempo de recuperação necessário para cada um delas.

O MIT (2002) classificou suas funções em quatro tipos:

a. Críticas: não podem ser suspensas.

b. Essenciais: devem ser restauradas o mais breve possível.

c. Necessárias: podem ser desativadas até se completar o processo de restauração, mas os dados que as alimentam devem ser preservados para futuro processamento.

d. Desejáveis: podem ser totalmente desativadas.

Vale ressaltar que cada serviço interrompido possui um determinado tempo de restabelecimento adequado. A organização deve analisar o tempo de recuperação ideal para cada uma de suas atividades e contemplar os recursos necessários – sejam humanos, físicos, tecnológicos ou financeiros –, a fim de implementar os processos que assegurarão que os prazos sejam cumpridos (DRI, 2002).

Uma empresa pode decidir que é suficiente que o departamento de marketing opere com 20% de sua capacidade após um desastre. Entretanto, foi determinado que o departamento de logística deve operar com no mínimo 60% de sua capacidade plena. O cuidado que se deve ter é que quanto maior o nível de atividade que se queira, maiores serão os custos envolvidos para a empresa estar preparada para cumprir esse requisito.

O Banco Bradesco, em exemplo descrito por Gonçalves (2003), possui dois centros de processamento de dados semelhantes distantes um do outro, o primeiro em Osasco e o backup em Barueri. Seu PCN prevê que, em caso de desastre, seus processos críticos voltem a funcionar em no máximo duas horas.

Harger (2003) identifica os seguintes tipos de impacto no negócio a curto, médio e longo prazo, como mostrados na Tabela 3.

Curto Prazo	**Médio e Longo Prazos**
Paralisação das atividades	Perda de mercado
Perda de equipamentos	Perda de imagem
Destruição de instalações	Quebra de confiança
Perda de faturamento	Desânimo
Multas	Descrédito
Aluguel de instalações alternativas	Perda de empregados
	Ações judiciais

Tabela 3: Impactos de um desastre (Harger, 2003)

Harger (2003) também explora a evolução dos prejuízos no tempo em caso de sinistro, como ilustrado na Figura 1.

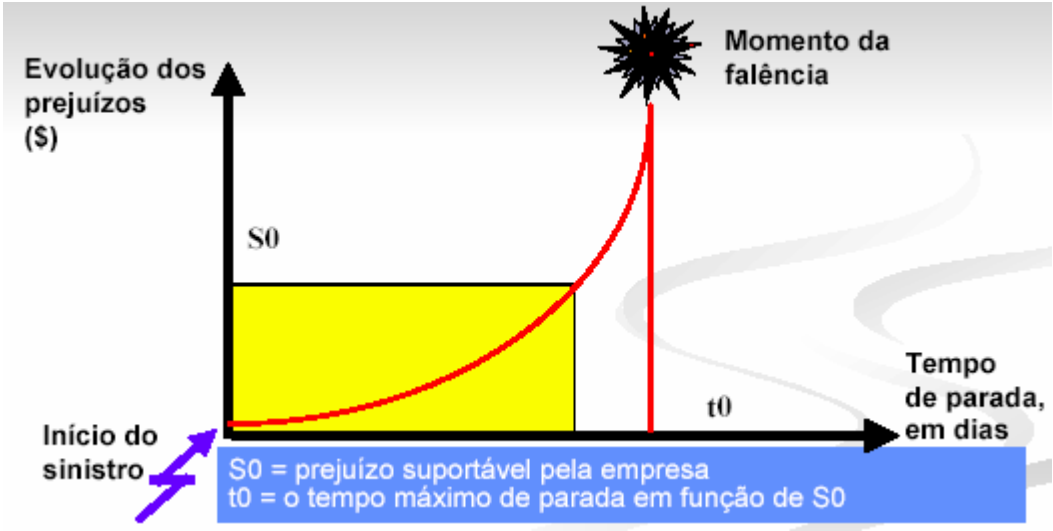

Figura 1: Evolução dos prejuízos (Harger, 2003)

Por meio da BIA, também é possível determinar as necessidades de cobertura de seguros para os diferentes ativos da instituição (MIT, 2002).

Elaboração do PCN

Com base na análise de riscos e na análise de impacto no negócio realizadas e nos elemento-chave anteriormente descritos, é possível descrever as ações necessárias para prevenir ou reduzir sensivelmente os efeitos das possíveis perdas, as cruciais para manter as atividades mais críticas em funcionamento em caso de incidentes e as requeridas para a restauração dos serviços prejudicados. As ações podem conter: controles, procedimentos, equipamentos, treinamentos, orientações, alertas, sistemas e localizações físicas.

As ações preventivas devem ser postas em prática o mais rapidamente possível, enquanto as mantenedoras e as restauradoras devem ser incorporadas ao PCN.

As ações que têm como objetivo manter as atividades críticas interrompidas devem ser definidas de modo a fornecer resposta rápida e efetiva aos incidentes de segurança. Para que isso seja possível, todos os envolvidos devem agir de maneira cooperativa para prevenir, detectar e responder aos incidentes (OECD, 2002).

Por esse motivo, o PCN deve detalhar as funções que cada funcionário deve desempenhar, a fim de que as conseqüências dos eventos de interrupção de serviços sejam minimizadas. O plano de continuidade de negócios do Massachusetts Institute of Technology (MIT, 2002), por exemplo, descreve as responsabilidades de sua equipe de continuidade, bem como lista de telefones, e-mails e endereços para contatar os membros do grupo. Além disso, todas as pessoas presentes na instituição são orientadas a informar à equipe de continuidade qualquer situação de emergência.

As causas dos incidentes devem ser identificadas e analisadas detalhadamente, a fim de que se possa prevenir a recorrência da mesma. Tampouco se pode esquecer que a integridade dos sistemas afetados deve ser validada sem demora.

Como é possível perceber, o recurso humano é essencial para a rápida identificação dos incidentes. Portanto, o treinamento de pessoal é vital para o sucesso do PCN.

Treinamento de pessoal

Segundo Coltro (2000), a orientação dos funcionários sobre as políticas de segurança e o treinamento constante são essenciais para a manutenção da boa saúde das empresas.

De nada adianta elaborar um PCN completo, se os funcionários não recebem treinamento adequado para saberem lidar com as situações previstas no plano. A conscientização dos funcionários sobre riscos e prevenções é a primeira linha de defesa da segurança da informação (OECD, 2002).

Esse ponto pode ser observado em uma pesquisa realizada pelo Computer Security Institute que revela que 71% dos incidentes de segurança são causados pelo pessoal interno, sejam intencionalmente ou não (Correia, 2002). Outro estudo em que é possível chegar à mesma conclusão foi realizado pela empresa CompuTIA (2002), baseado em questionário respondido por 638 profissionais de SI. Destacam-se os seguintes dados:

a. 63% das vulnerabilidades relatadas pelos entrevistados tinham relação com erro humano e apenas 8%, com tecnologia.

b. 80% responderam que os erros humanos que resultaram em incidentes de segurança foram causados por falta de conhecimento em segurança da informação.

Os usuários dos serviços de informação devem ser instruídos para registrar e notificar qualquer falha ou ameaça, ocorrida ou suspeita na segurança de sistemas e serviços. Entretanto, não devem tentar verificar a falha, pois podem corromper possíveis evidências, além de serem suspeitos de participação no episódio (ABNT, 2001).

Segundo Bruce Schneier (Rocha, 2002), especialista na área de SI, as pessoas sempre serão o elo mais fraco em um sistema de segurança.

Dentro da nova cultura de segurança proposta pela OECD (2002), cada participante possui um papel importante e, por isso, deve estar ciente dos riscos e medidas preventivas que envolvem o assunto. Todos devem se sentir igualmente responsáveis pela segurança da informação da empresa (ISO, 2001).

Com bastante razão, Lopes (2000) afirma que a responsabilidade pela implantação de um programa educacional de segurança deve ser sempre dos mais altos escalões das empresas. O apoio da direção das instituições é fundamental para a disseminação das diretrizes do PCN (Ferreira, 2002).

Além disso, deve sempre ser fornecida uma explicação de que as medidas de segurança não são um ônus imposto sem motivo, mas, sim, parte integrante e natural no dia-a-dia de trabalho.

Manutenção do plano

A elaboração de um PCN possui começo, meio, mas não tem fim (Bradaschia, 2002), pois ele deve ser freqüentemente reavaliado e testado (GAO, 1999), de modo a determinar sua eficiência à luz de uma nova realidade que se apresenta para a instituição.

Atualizações do plano podem ser demandas por alterações:

a. Nas pessoas envolvidas.

b. Nos endereços ou telefones.

c. Na estratégia de negócios.

d. Na localização, instalações e recursos.

e. Na legislação vigente.

f. Nos prestadores de serviços, fornecedores e clientes-chave.

g. Nos processos (inclusões e exclusões)

h. No risco (operacional e financeiro)

Os testes somente serão completos se as simulações forem reais e todos os envolvidos forem acionados. As organizações devem instituir um grupo permanente de reavaliação e atualização dos procedimentos de segurança adotados no plano.

O MIT (2002), por exemplo, revisa seu PCN quadrimestralmente, sendo que ele passa por uma reavaliação completa anualmente. Testes para exercitar as ações do plano são realizados também uma vez por ano. Já o Grupo Pão de Açúcar realiza uma única revisão anual dos processos contidos no PCN (Gonçalves, 2003).

A NBR ISO/IEC 17799 identifica algumas técnicas que visam a garantir a confiabilidade do plano:

a. Testes de mesa simulando diferentes cenários.

b. Simulações de situações reais.

c. Testes de recuperação do ambiente técnico.

d. Testes de recuperação em um ambiente alternativo.

e. Testes dos recursos, serviços e instalações de fornecedores.

f. Ensaio geral.

A maioria das técnicas é indicada para ser aplicada em cada elemento do plano em separado. O ensaio geral tem por objetivo testar o conjunto completo de procedimentos que compõem o plano, envolvendo todos os participantes.

Soluções para continuidade

Diversas soluções foram propostas por autores e empresas para facilitar a vida dos profissionais que atuam na área de continuidade de negócios. Felizmente, o futuro se mostra ainda mais promissor, pois novas soluções são disponibilizadas a todo o momento.

Uma forma de trabalho que pode servir muito bem, caso a continuidade das atividades na empresa seja impraticável, é o teletrabalho. Os funcionários podem ser deslocados para hotéis, restaurantes ou até mesmo ficar em suas casas e, mesmo assim, continuar a desempenhar suas funções. As tecnologias de comunicação remota têm evoluído muito ao longo dos últimos anos, tornando esta opção bastante viável e atraente.

Gonçalves (2003) cita um exemplo no qual o jornal The Wall Street Journal utilizou o teletrabalho para que os seus jornalistas e redatores pudessem fechar uma edição na noite da tragédia do dia 11 de setembro.

Empresas que podem comprometer maior volume de recursos têm como opção manter uma estrutura de trabalho independente, mas similar à original (*hot site*) e distante desta (Neverfail Group, 2002). Como já exemplificado, o Bradesco se utiliza desse recurso, a fim de estar preparado para uma eventual interrupção das atividades na sua sede.

Não são muitas empresas que podem se dar ao luxo de ter esse nível de redundância, mas muitas podem contratar um serviço de continuidade de negócio que forneça toda a infra-estrutura de informática e comunicações necessárias, quando é acionada. A infra-estrutura é levada para um outro prédio da empresa (*cold site*) que esteja em condições plenas de operação (Neverfail Group, 2002). Já existem alguns fornecedores que provêm esse serviço, disponibilizando hardware e software previamente acordados. Assim, o custo desse serviço se torna uma espécie de seguro contra desastres.[6]

2.3. Indicadores

Uma das partes mais difíceis deste estudo – senão a mais - foi escolher os indicadores que serviram como base para a operacionalização da pesquisa. A dificuldade em termos de captura e interpretação dos dados pertinentes à obtenção de subsídios para atingir o objetivo principal da pesquisa se apresentou por não ter sido possível encontrar nenhum estudo anterior que já tivesse proposto tais indicadores.

Procurou-se, então, propor, com base na revisão da literatura realizada, os construtos e indicadores a serem utilizados na pesquisa, os quais são apresentados na Tabela 4.

[6] Para maiores informações sobre este tipo de serviço, ver referência Neverfail Group (2002).

Construtos	Indicadores
Planejamento Estratégico	▪ Período da realização da última análise de riscos ▪ Período da realização da última análise de impacto no negócio
Financeiro	▪ Percentual do orçamento da empresa reservado para SI ▪ Percentual do orçamento da empresa reservado para PCN ▪ Tendência de variação do orçamento da empresa reservado para segurança da informação (diminuir, manter, aumentar) ▪ Tendência de variação do orçamento da empresa reservado para continuidade do negócio (diminuir, manter, aumentar)
Manutenção	▪ Freqüência anual de revisão do PCN ▪ Freqüência anual de simulação dos procedimentos do PCN ▪ Abrangência das simulações (equipe de TI, todos os funcionários, fornecedores, clientes, serviços públicos)
Treinamento	▪ Freqüência de treinamento anual em SI para os funcionários da empresa ▪ Freqüência de treinamento anual em SI para a equipe de TI ▪ Freqüência de treinamento anual em PCN para os funcionários da empresa ▪ Freqüência de treinamento anual em PCN para a equipe de TI

Tabela 4: Construtos e indicadores