

# **GESTÃO DE RISCOS NUM CONTEXTO DE PLANEAMENTO DA CONTINGÊNCIA E RECUPERAÇÃO**

Leonilde Reis  
Instituto Politécnico de Setúbal, Escola Superior de Ciências Empresariais  
Departamento de Sistemas de Informação  
Campus do IPS - Estefanilha  
Setúbal, Portugal  
[lreis@esce.ips.pt](mailto:lreis@esce.ips.pt)

Luís Amaral  
Universidade do Minho, Escola de Engenharia  
Departamento de Sistemas de Informação  
Campus de Azurém  
Guimarães, Portugal  
[amaral@dsi.uminho.pt](mailto:amaral@dsi.uminho.pt)

## **Resumo**

Este artigo pretende dar ênfase a um conjunto de preocupações inerentes à ocorrência de acidentes numa envolvente organizacional. Pretende-se mencionar as vantagens associados à implementação de medidas de contingência e recuperação como suporte ao negócio tendo em vista a dependência da generalidade das organizações quer em função da criticidade da informação que manipulam quer face à envolvente em termos de potenciais acidentes.

Salienta-se a importância do mapeamento dos diferentes riscos a que a organização está exposta, analisando a forma de mapear esses riscos, bem como o impacto da paragem dos Sistemas de Informação no que respeita às aplicações críticas de suporte ao negócio, bem como o papel das auditorias tecnológicas num contexto da gestão de riscos.

A finalizar, mencionam-se as características e vantagens de uma abordagem integradora das actividades de Planeamento de Sistemas de Informação e de Contingência e Recuperação, tecendo considerações acerca das preocupações inerentes à continuidade do negócio.

**Palavras-chave:** tecnologias de informação, sistemas de informação, planeamento de sistemas de informação, planeamento da contingência e recuperação.

## **1 Introdução**

Actualmente, os negócios estão fortemente dependentes dos Sistemas de Informação (SI), devendo essa dependência ser rigorosamente equacionada. Neste sentido, recuperar rápida e eficientemente a actividade depois de um acidente, minimizando os seus efeitos, deverá ser uma preocupação vincada e real dos decisores.

Assim, a ininterrupção dos SI constitui um dos seus requisitos básicos, sendo inevitável a existência do Planeamento da Contingência e Recuperação (PCR) como forma de minimizar os prejuízos decorrentes de eventuais paragens.

O Planeamento de Sistemas de Informação (PSI) é a actividade da organização onde se define o futuro desejado para o seu SI [Amaral 1994], para o modo como este deverá ser suportado pelas TI e para a forma de concretizar esse suporte.

Na actualidade, quando se efectua o PSI não se pensa na contingência, surgindo essa preocupação, na generalidade das vezes, de forma tímida durante o desenvolvimento e, mais assentadamente, aquando da exploração dos SI.

Este planeamento de forma desagregada suscita só por si diversos problemas decorrentes da desagregação das actividades de planeamento, sendo de referir aqueles que se relacionam com a gestão das equipas, do tempo, da afectação dos recursos e da definição das infra-estruturas.

No que respeita às equipas, verifica-se um maior esforço de recursos humanos na medida em que duas equipas em períodos de tempo distintos terão de ser afectas ao desenvolvimento de ambos os tipos de planeamento, implicando uma reanálise de PSI aquando do PCR, o que resulta num maior esforço de desenvolvimento e, em consequência, por um período de tempo globalmente superior. Por outro lado, corre-se o risco de reformulação das soluções implementadas no âmbito do PSI, podendo implicar a reafectação dos recursos materiais e um maior esforço financeiro.

Acresce que durante o desenvolvimento do PCR surge, normalmente, a necessidade de reponderar a infra-estrutura tecnológica em que assentou a implementação do PSI, seja por necessidade de renovação/reactualização, seja por aumento do nível de segurança, donde resulta um maior esforço financeiro e de implementação.

A solução para estes problemas da actividade de SI passa pela implementação de uma solução integrada para o PSI e o PCR. Nesta procura de uma solução integrada, existe a sensibilidade de que a alteração da metodologia associada à realização da actividade vai causar impacto/interacção dos SI com os recursos humanos a vários níveis, sendo de realçar os efeitos sobre:

- Os colaboradores, na medida em que lhes são apresentadas alterações de procedimentos de trabalho;
- O comportamento e desempenho de grupos, pois é uma nova forma de articular e desenvolver a actividade;

- As organizações, na medida em que obriga à mudança de comportamento, atitudes e até formas de gestão, sendo de realçar que o sucesso deste processo depende intrinsecamente do comprometimento e empenho dos decisores, considerando-se este como o factor crítico de sucesso do mesmo.

Para o desenvolvimento do PCR é importante o conhecimento dos riscos internos e externos a que a organização está ou poderá vir a estar exposta, sendo importante uma análise do nível de risco que a organização pode suportar sem comprometer a continuidade do negócio, por forma a adequar a afectação dos recursos humanos, materiais e financeiros ao esforço necessário.

Neste artigo pretende-se analisar a importância da gestão de riscos num contexto do PCR, tendo presente que o objectivo último do PCR é a preservação da continuidade do negócio em caso de acidente.

## **2 A necessidade do Planeamento da Contingência e Recuperação**

Os autores [Goldberg, Davis e Pegalis 1999] salientam, que a elaboração de um PCR é uma prática para a preservação do negócio, considerando que a atenuação do impacto negativo se verifica não só ao nível do negócio, mas também se estende à confiança dos colaboradores e dos clientes da organização.

O objectivo é o de dispor de um documento, orientador das normas de actuação às quais corresponde um organograma estruturado, por forma a desenvolver - partindo das capacidades, da aptidão e dos meios existentes - acções operacionais eficazes susceptíveis de responder, no mais curto espaço de tempo, a uma situação de acidente, através da sua activação pela entidade competente. O objectivo último será o de repor, no mais curto espaço de tempo, a normalidade nas áreas afectadas, minimizando os efeitos de um acidente, sobre os colaboradores, a economia, o património e o ambiente.

Segundo CPR [CPR 1992], é normal a expectativa de que os colaboradores de uma organização sejam capazes de inovar, de executar tarefas pouco familiares, de trabalharem sob *stress* em períodos de tempo alargados, e de sentirem que fazem parte de um plano. Para que uma operação de recuperação tenha sucesso, é necessário que os colaboradores tenham assimilado a importância da missão da organização e que se identifiquem com ela para que se sintam suficientemente motivados a desenvolver o seu trabalho sob um certo nível de *stress*.

Butler [Butler 1997] advoga que, para a generalidade das organizações de menor dimensão, o foco do PCR deverá incidir na manutenção da continuidade das operações normais de funcionamento.

Para Myers [Myers 1993] os objectivos do PCR caracterizam-se pela prevenção da ocorrência de acidentes. A contenção do impacto dos diversos acidentes, quando da sua ocorrência, possibilita providenciar uma resposta organizada a um acidente e minimizar as disfunções para o *cash flow*, providenciar alternativas para os pedidos de serviço de clientes prevenir uma perda significativa da quota de mercado a longo prazo.

Assim, segundo [Ohlson, 2001], o PCR tem por objectivo por um lado prever antecipadamente um acidente e planear a forma de assegurar as funções críticas do negócio por forma a garantir a sua continuidade e, por outro lado, ter um plano que, perante um acidente, permita reagir e recuperar os sistemas.

Os autores [Moscove, Simhin e Bagranoff 1999] sugerem que o PCR inclua o desenvolvimento de um plano formal de recuperação de acidente. Estes planos são necessários em função da imprevisibilidade dos acidentes que possam tornar o centro de processamento de dados inoperacional.

Os autores [Marcela, Sampias e Kincaid 1993] advogam que posteriormente à organização ter decidido por um PCR, existem diversas tarefas a desenvolver no âmbito do projecto. Estas tarefas de desenvolvimento incluem a análise do impacto organizacional, determinando as necessidades mínimas de processamento, identificando o nível de exposição aos riscos e suas implicações e o desenvolvimento de estratégias de recuperação em que se salienta a análise do impacto organizacional.

Segundo [Fontana e Connor, 2001], qualquer plano de continuidade de negócio tem que fazer parte da cultura da organização. Qualquer medida de impacto estratégico nas funções críticas da organização deve conduzir a uma reanálise dos riscos e, conseqüentemente, a uma readequação do PCR, para que em caso de acidente se possa repor o novo modelo funcional da organização.

### **3 Gestão de Riscos**

Os riscos a que uma organização está exposta são em número elevado e será pertinente analisar as preocupações descritas por Myers [Myers 1993] uma vez que salientam a importância da prevenção, preparação e treino, da existência de uma resposta organizada e contenção de prejuízos, da protecção do *cash flow* e utilização de procedimentos alternativos, bem como a existência de um plano de recuperação e reinício das operações normais.

Segundo Hall [Hall 1998], actualmente efectua-se a gestão de riscos como um procedimento genérico para solucionar eventuais riscos que possam comprometer o negócio. A gestão de

riscos consiste em avaliar a qualquer instância quais as consequências que possam ser aceitáveis pela organização.

De acordo com o BCI [BCI, 2001], actualmente não é possível evitar todas as formas de risco organizacional ou os prejuízos potenciais. Um objectivo realista consiste em assegurar a sobrevivência da organização estabelecendo uma cultura organizacional que possibilite a identificação e a gestão daqueles riscos que possam causar maior prejuízo, tais como:

- A impossibilidade de manter activo o serviço ao cliente;
- Danos na imagem, reputação ou marca;
- Incapacidade de proteger os activos – humanos, materiais e financeiros – da organização;
- Falha do controlo do negócio;
- Impossibilidade de cumprir com requisitos regulamentares ou legais.

Definindo como risco aceitável, aquele em que se conseguem gerir as suas consequências, existem basicamente duas actividades no processo de gestão do risco: a primeira designada por avaliação do risco, que compreende a sua definição e a identificação das fontes de risco, bem como a avaliação dos seus efeitos potenciais; a segunda actividade, designada por controlo do risco e que tem como objectivo a sua resolução.

Uma vez identificados os potenciais riscos [Reis, 2001] que podem afectar uma organização, é possível avaliar o seu grau de importância segundo diferentes factores, nomeadamente o grau de exposição ao risco e a frequência em que se prevê que o mesmo possa ocorrer.

Na figura 1 apresenta-se uma matriz de análise dos os riscos a que uma determinada organização se encontra exposta, avaliados segundo aqueles factores.

O Plano Estratégico de uma organização é uma das fontes principais para a identificação e avaliação dos riscos a que uma organização poderá estar exposta, uma vez que partindo da definição da missão e dos objectivos estratégicos da organização se estabelece a estratégia da organização, tendo por base a análise dos seus trunfos/oportunidades e fraquezas/ameaças.

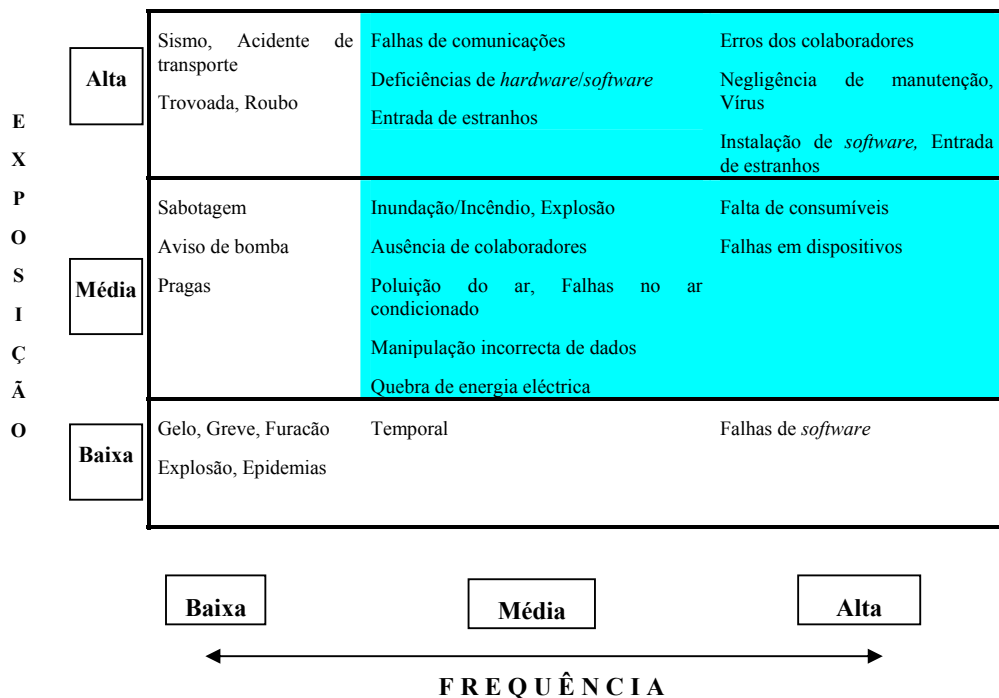


Figura 1 Matriz de riscos

O Plano Estratégico de uma organização é uma das fontes principais para a identificação e avaliação dos riscos a que uma organização poderá estar exposta, uma vez que partindo da definição da missão e dos objectivos estratégicos da organização se estabelece a estratégia da organização, tendo por base a análise dos seus trunfos/oportunidades e fraquezas/ameaças.

Após a caracterização dos riscos (fraquezas/ameaças) a que a organização pode estar exposta, é importante definir a probabilidade de acontecimento, definindo-se muitas vezes essa probabilidade em termos de sensibilidade de ocorrência, tal como acontece na matriz acima.

De referir que esta matriz deve ser dinâmica, construída e actualizada com base no historial da organização, a probabilidade da frequência de ocorrência dos fenómenos no tempo, o conhecimento do meio envolvente, as literaturas no domínio e a experiência de outras organizações similares.

Na área sombreada da matriz identificam-se os riscos em relação aos quais a organização deverá tomar medidas de controlo por forma a garantir a continuidade do negócio.

Na avaliação de riscos, as áreas de negócio/funções de negócio bem como as aplicações inerentes devem ser caracterizadas de acordo com os pressupostos dos domínios de recuperação,

devendo estes serem tipificados de forma adequada à especificidade da organização em causa, tal como por exemplo: (0), se a aplicação deve ser recuperada em menos de 2 horas; (1), se a aplicação deve ser recuperada em menos de 8 horas; (2), se a aplicação deve ser recuperada num período inferior a 1 dia; (3), se a aplicação deve ser recuperada num período superior a 1 dia.

Concluída a avaliação dos riscos torna-se importante definir os mecanismos necessários ao seu controlo, desempenhando o PCR um papel primordial para a sua efectivação, uma vez que tal como se referiu anteriormente o PCR deverá estabelecer os procedimentos a adoptar no caso de ocorrência de uma acidente, por forma a garantir o normal desenvolvimento dos processos críticos do negócio.

O desenvolvimento do PCR deve ter por base a identificação dos processos e funções críticos para a missão da organização, em vez de assentar numa análise específica e global. Desta forma, adequa-se o PCR às funções críticas da organização e optimiza-se a afectação de recursos e de tempo quer na fase de desenvolvimento do PCR quer nas fases de implementação e de manutenção do mesmo.

Isto é, a análise e gestão de riscos possibilita à organização avaliar quais os riscos que podem ser geridos e assim dimensionar o PCR ao encargo financeiro que pode suportar bem como o prazo de derrogação desses encargos.

#### **4 Exercício, manutenção e auditoria do PCR**

Uma vez concluído o PCR é importante efectuar o teste do mesmo, que segundo o BCI [BCI, 2001] deverá ter um objectivo duplo: verificar a adequação do Plano às necessidades de controlo dos riscos potenciais identificados e familiarizar todos os colaboradores envolvidos com a operacionalização do Plano.

Os resultados deste exercício são extremamente importantes para se poder concluir se o PCR desenvolvido permite à organização defender-se dos riscos identificados bem como se o tempo de reposição dos SI/TI é o adequado para a continuidade do negócio.

A dinâmica da envolvente das organizações conduz a alterações nos seus recursos humanos, nos processos, nos riscos a que está exposta e, nalguns casos, até da missão do negócio, devendo as mesmas ser reflectidas no PCR. Assim, é importante a definição de um esquema de manutenção e actualização do PCR, com a identificação do(s) responsável(eis), após o que se deverão realizar os respectivos testes.

Segundo o BCI [BCI, 2001], para que o PCR se mantenha actualizado e aderente com a realidade e objectivos da organização, é importante o estabelecimento de um processo de auditoria, que não deve ser circunscrito apenas ao Plano.

Considerando a importância estratégica da gestão das TI e da inovação para a competitividade e o sucesso das organizações, Marques [Marques 1997] defende que as auditorias tecnológicas podem desempenhar um papel relevante nesta matéria, apoiando as organizações, quer através da criação de mecanismos para a detecção de insuficiências nos SI, quer avaliando os riscos e propondo medidas correctivas

O processo de auditoria dentro de um departamento, [Fantinatti 1988] principalmente na área do processamento de dados, é de vital importância, pois é através dela que os decisores poderão ditar os rumos da organização.

Segundo o Instituto de Informática [II 1994], a auditoria tecnológica tem por objectivo controlar a observância das medidas de segurança informática aprovadas e a sua caracterização passa por criar operações periódicas de controlo das medidas de segurança em vigor. O controlo deve incidir com frequência sobre as áreas críticas do negócio, podendo esta função ser assumida por auditores internos ou externos.

Consequentemente, a realização de fracos investimentos corresponde a propiciar directamente ameaças aos negócios. Preservar o negócio é ter que protegê-lo e essa protecção passa por assegurar formas de segurança para os SI. No entanto em Portugal, a auditoria tecnológica implica verbas difíceis de suportar pela generalidade das organizações.

É desejável que o processo de auditoria do PCR se baseie em processos estabelecidos para o sector de actividade em que a organização se insere por forma a facilitar o *benchmarking*, a avaliar da adequação do Plano face aos riscos a que está exposta e a melhor garantir a continuidade do negócio.

## **5 Conclusões**

A consciencialização das organizações de que estão cada vez mais a correr mais e maiores riscos, leva a que, gradualmente, as políticas de segurança sejam mais rígidas e encaradas com maior rigor e seriedade. A definição do nível de segurança pretendido para o SI deverá aumentar definindo as necessárias políticas de segurança, dada a divulgação e a consciencialização dos perigos e a dependência das organizações dos SI.

A implementação planeada das medidas de segurança implica a sua gestão, cujos objectivos se centram na definição dos objectivos de segurança, na avaliação dos riscos, no estabelecimento



de medidas de segurança, na afectação de responsabilidades, no teste à segurança do sistema e na avaliação dos níveis de segurança implementados.

Actualmente, a informação é um dos factores estratégicos das organizações. Nesse sentido será crucial identificar a informação estrategicamente importante, bem como as fontes de informação relevantes, assegurando assim que os colaboradores recebem essa informação, aumentando a eficiência e a eficácia do processamento da informação com vista à optimização do negócio.

O PCR consiste num conjunto de políticas definidas pela organização tendo em vista a diminuição, ou até mesmo a eliminação dos riscos que ameaçam a continuidade do negócio da organização, através da manutenção da integridade, confidencialidade e disponibilização da informação que suportam a tomada de decisão dos responsáveis pela gestão da organização. Por outras palavras, são objectivos do PCR garantir o cumprimento da missão e reduzir os efeitos negativos, operacionais e/ou financeiros para o negócio resultantes de uma paragem dos SI.

Para o desenvolvimento do PCR a organização tem que ter um conhecimento completo do negócio e da sua envolvente a fim de poder determinar qual o impacto para o negócio resultante da paragem dos SI, bem como efectuar uma gestão de risco. A fim de que o PCR da organização não inviabilize o equilíbrio financeiro da organização esta deverá definir qual o âmbito do PCR isto é, o risco em que se consegue gerir as suas eventuais consequências. Para tal é importante que a organização proceda à avaliação de risco, a partir da identificação das fontes de risco e avaliação dos seus efeitos potenciais, bem como ao controlo do risco a fim de poder eliminar/diminuir o impacto em caso de acidente.

Uma vez desenvolvido o PCR é importante que se proceda aos testes e se defina um esquema de manutenção do Plano e um responsável pela sua concretização. O estabelecimento de processos de auditoria tecnológica possibilita que o PCR se mantenha aderente à realidade e objectivos da organização, bem como as evoluções e alterações desta aí aparecem reflectidas, por forma a que em caso de acidente o PCR cumpra o seu objectivo de manter a continuidade do negócio.

## **6 Referências**

- Amaral, L. A. M., PRAXIS Um Referencial para o Planeamento de Sistemas de Informação, Tese de Doutoramento, Universidade do Minho, 1994.
- BCI, Business Guide to Continuity Management, The BCI, LPC and Guardian iT, Business Continuity Institute, 2001.
- Butler, J. G., *Contingency Planning and Disaster Recovery: Protecting your Organization's Resources*, Computer Technology Research, 1997.

- CPR, *Contingency Planning Strategies/90tm*, The Research Source for Developing a Disaster Recovery Plan, Contingency Planning Research, inc., 4th Ed., 1992.
- Fantinatti, J. M., *Auditoria em Informática Metodologia e Prática*, Editora McGraw-Hill, 1988.
- Fontana, J. e Connor, D., *Disaster Recovery then and now, Disaster Recovery & Business Continuity*, Special Report, Network World Editors, 2001.
- Goldberg, S. H., S. C. Davis e A. M. Pegalis, *Y2K Risk Management - Contingency Planning, Business Continuity, and Avoiding Litigation*, Wiley Computer Publishing, 1999.
- Hall, E. M.; *Managing Risk – Methods for Software Systems Development*, SEI Series in Software Engineering, Addison-Wesley, 1998.
- II, *Planeamento Estratégico do Sistema de Informação - Guião de Estudo de Âmbito*, Instituto de Informática, 1994.
- Marcela, A. J., W. J. Sampias e J. K. Kincaid, *Disaster Contingency Planning*, Institute of Internal Auditor, 1993.
- Marques, M., *Auditoria e Gestão*, Editorial Presença, 1997.
- Moscove, S. A., M. G. Simhin e N. A. Bagranoff, *Core Concepts of Accounting Information Systems*, John Wiley & Sons, 6th Ed., 1999.
- Myers, K. N. *Total Contingency Planning for Disasters: Managing Risk, Minimizing Loss, Ensuring Business, Continuity*, John Wiley & Sons, 1993.
- Ohlson, K., *Planning for the worst: bring in the best, Disaster Recovery & Business Continuity*, Special Report, Network World Editors, 2001.
- Reis, M. L., *Planeamento de Sistemas de Informação e da Contingência e Recuperação*, Tese de Doutoramento, Universidade do Minho, 2001.