Etapas de elaboração de um plano de contingência para a área de tecnologia da informação em âmbito corporativo

Prof. Me. Washington Lopes da Silva – Mestre em Engenharia Elétrica – Concentração em Engenharia da Computação pela Universidade Mackenzie; e Aluno Especial de Doutorado da Escola Politécnica da Universidade de São Paulo; washington.lopes@poli.usp.br

Resumo

Um plano de contingência, de um modo geral, é um plano de ação para um eventual desastre ou emergência que ameace interromper ou destruir a continuidade das atividades normais de uma organização.

Com o crescimento vertiginoso do uso da Tecnologia da Informação (TI), as organizações deverão se preocupar cada vez mais com a continuidade de seus processos operacionais críticos que dependem da TI. Neste ponto, este artigo pretende servir como um material de apoio na decisão e elaboração de um plano de contingência para a área de TI.

Apresentamos um conjunto de etapas estruturadas para a elaboração de um plano de contingência para a área de TI. Desta forma, inicialmente damos uma visão geral do aspecto de conscientização que todos os envolvidos nos processos decisórios de uma organização deveriam ter a respeito dos riscos e ameaças que cercam todo o ambiente de TI. Em seguida, propomos de uma forma ordenada seqüencialmente as etapas para se elaborar um plano de contingência para a área de TI.

As quatro etapas de elaboração de um plano de contingência para a área de TI propostas no artigo: Conscientização; Avaliação dos Riscos e Vulnerabilidades; Desenvolvimento; e Teste e Manutenção; permite-nos demonstrar que o plano de contingência para a área de TI está acima de procedimentos isolados como, por exemplo, os procedimentos de gravação de cópias de segurança, adotados por algumas organizações para tentar suportar a paralisação de sua área de TI por algum tempo.

Palavras chaves: Contingência; conscientização; riscos; desenvolvimento; teste.

Introdução

É impossível escrever sobre plano de contingência para a área de Tecnologia da Informação (TI), sem antes termos a definição de plano de continuidade dos negócios. Conforme Austin, G. e Colaboradores (2000), podemos definir continuidade dos negócios como a capacidade de sobreviver e continuar as operações da organização, mesmo que haja um eventual desastre [1]. O plano deve ser rigoroso e ter o compromisso com os recursos necessários para se adequar à situação. O plano de continuidade dos negócios é primeiramente de responsabilidade da alta administração, pois ela é a principal encarregada em manter a salvaguarda dos ativos e a sobrevivência da organização.

O plano de continuidade dos negócios vem suportar um dos postulados importantes das Ciências Contábeis, o Postulado da Continuidade das Entidades (organizações). De acordo com Iudícibus S. e Colaboradores (2003), para a Contabilidade, a Entidade é um organismo vivo que irá viver (operar) por um longo período de tempo (indeterminado) até que surjam fortes evidências em contrário [2].

Uma forte evidência que poderia levar à descontinuidade de uma organização é a paralisação de sua área de TI e uma outra forte evidência que poderia evitar a morte da organização, neste caso específico, é a formalização de um plano de contingência para a área de TI.

Sabemos que as organizações estão a cada dia se informatizando, sejam elas de grande, médio ou pequeno porte. Se tivermos como exemplo as instituições financeiras, as seguradoras, as montadoras de automóveis, etc, observaremos que elas são totalmente dependentes da TI em seus processos diários. Mas não podemos menosprezar as médias e pequenas organizações que realizam muitos de seus processos com auxílio do computador: contabilidade, informações sobre vendas e fornecedores, folha de pagamento, relatórios gerenciais, etc.

Segundo Boehm, B. W. (1998), a interrupção dos serviços de um CPD pode drasticamente afetar a capacidade de funcionamento da organização e afetar seus clientes. A perda pode ser maior do que as perdas de hardware e/ou software. Em casos extremos pode causar perdas em longo prazo, talvez até levar a organização à falência [3].

Segundo Austin, G. e Colaboradores (2000) e Myers, K. N. (1999), a continuidade dos negócios é um processo evolutivo, contínuo, que nasce na área de TI, com a idealização de um plano de contingência e se expande para as demais áreas de negócios das organizações [1, 4].

Sendo assim, este artigo estará sendo enfocado para uma parte significativa da continuidade dos negócios das organizações, que é o plano de contingência para a área de TI.

1. Metodologia

Formaram a base metodológica deste trabalho os estudos bibliográficos dos componentes de um plano de contingência para a área de TI. Partiu-se da conscientização que toda organização deveria ter sobre os riscos de não se ter um plano de contingência para essa área. Criou-se posteriormente uma proposta das etapas julgadas necessárias para se compor um plano de contingência para a área de TI.

2. Resultados

Como resultado do nosso estudo, foi proposta, de forma estruturada e metodológica as etapas de elaboração de um plano de contingência para a área de TI. As etapas foram divididas em quatro partes conforme ilustrado na figura abaixo:

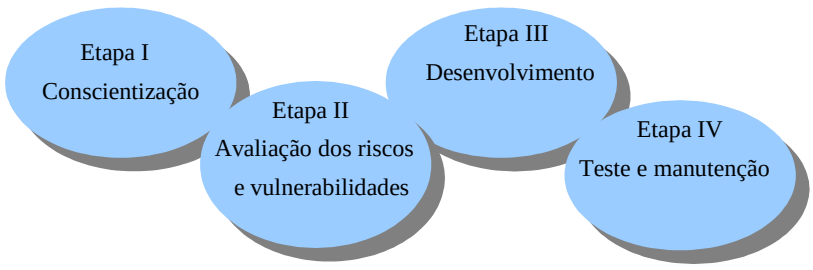

Figura 1 - Etapas de elaboração de um plano de contingência para a área de TI

2.1 Primeira etapa - conscientização

De acordo com Myers, K. N. (1999) e KPMG-BCP (1998), para que qualquer plano de contingência funcione bem é necessário que todos os membros da organização estejam conscientes de sua importância [4, 5].

Programas de conscientização dentro da organização deverão ser periódicos e deverão abranger, no mínimo, todos os departamentos usuários da TI. O programa de conscientização deverá abordar o objetivo do plano, explicar suas terminologias e deixar claras as responsabilidades de cada pessoa incluída no plano.

Recomendar algumas técnicas e estratégias que poderão auxiliar o plano de contingência também é válido como, por exemplo, a implantação de uma política de segurança da informação, contendo algumas metodologias de como evitar possíveis perdas de dados importantíssimos para a organização.

A política de segurança da informação poderá ajudar na prevenção de contingências, dando soluções para o controle de acesso lógico, evitando possíveis sabotagens de funcionários mal intencionados, alertando para os controles ambientais, como extintores de incêndio, ar condicionado e controle de acesso físico ao CPD. Porém a política de segurança da informação apenas minimiza as ameaças de acontecer um evento, mas o risco de continuidade dos negócios, caso aconteçam às ameaças, continuarão existindo para organização. Desta forma, a política de segurança da informação não descarta a importância de um plano de contingência para a área de TI.

Para se fazer um programa de conscientização, a alta administração deverá ser a primeira a ter consciência do problema. Desta forma deverá ser formado um comitê executivo com os representantes da alta administração, que patrocinará todo o plano. Os objetivos do plano, suas premissas básicas e a formação de uma equipe operacional mantenedora do plano deverão ser aprovados pelo comitê executivo, partindo-se assim de um programa de conscientização com uma visão “top-down” (de cima para baixo), da alta administração até o nível hierárquico, usuário da TI, mais baixo dentro da organização.

O programa de conscientização do plano de contingência será algo que deverá ser abordado no início do projeto e continuar em paralelo durante a fase de teste e manutenção do plano.

A equipe operacional mantenedora do plano poderá ser a responsável pela centralização das alterações do plano, pelo cronograma dos testes periódicos e pelo programa de conscientização. No início do projeto, bem como na fase de teste e manutenção do plano, a participação dos usuários da TI será imprescindível, desta forma, a equipe operacional mantenedora do plano deverá, por meio de reuniões interativas com os usuários:

- Demonstrar os aspectos gerais do plano de contingência;
- Conceituar riscos, ameaças e desastres;
- Demonstrar, com exemplos fictícios, mas prováveis, os riscos e ameaças que cercam a organização; e
- Acima de tudo, conscientizar da responsabilidade que cada usuário da TI tem pela operacionalidade do plano.

Para que o pior não aconteça, é importante que a organização tenha consciência de suas ameaças e dos riscos relacionados a ela. Com certeza isso exigirá que alguém, ou um grupo de pessoas dentro da organização conduza essa análise e encoraja a alta administração a visualizar, antecipadamente, os problemas que uma contingência trará.

2.2 Segunda etapa - avaliação de riscos e vulnerabilidades

De acordo com Boehm, B. W. (1998), exposição do risco (RE – "Risk Exposure") algumas vezes é chamada de impacto do risco, sendo definida pela seguinte relação:

RE = Prob(UO) * Loss (UO)

Onde Prob(UO) é a probabilidade de um resultado insatisfatório e Loss(UO) é a perda das partes afetadas, caso o resultado seja insatisfatório [3].

O principal trabalho desta etapa é identificar os riscos internos e externos relacionados ao negócio da organização. Cada risco possui um relacionamento com determinadas atividades dentro da organização que dependendo do grau de exposição ao risco, poderá levar os processos operacionais vitais da organização à descontinuidade.

Conforme Myers, K. N. (1999), KPMG-BCP (1998), KPMG-CSS (1999), Price Waterhouse-DCP (1992) e Burtles, J. e Yates, S. (1998), esta etapa é denominada de BIA (Business Impact Analysis – Análise de Impacto nos Negócios) [4, 5, 6, 7, 8].

De acordo com Meredith, B. (1998), a análise de impacto nos negócios é uma análise que identifica os impactos no caso de perdas de recursos disponíveis da organização [9].

As atividades desta etapa podem se resumir em:

- Identificar os controles da área de TI, incluindo segurança física, controles ambientais, procedimentos de emergência, existência de procedimentos de recuperação de backups, ameaças externas e recursos críticos;
- Analisar e levantar os processos operacionais da organização;
- Analisar e classificar os riscos em cada atividade de cada processo operacional, considerando os sistemas de processamento eletrônico de dados; e
- Relatório final demonstrando:
  1) funcionamento de cada processo operacional;
  2) os riscos relacionados aos processos;
  3) a avaliação e classificação dos riscos por impacto nos negócios em baixo, moderado ou alto; e
  4) a identificação dos processos operacionais críticos.

2.3 Terceira etapa – desenvolvimento

Ao se chegar nesta etapa, a equipe responsável pelo desenvolvimento do plano estará de posse do relatório de análise de impacto nos negócios. Este relatório servirá de suporte para definir a estratégia global do plano, detalhando seus objetivos e premissas básicas. A partir do relatório de análise de impacto nos negócios poderemos identificar quais serão as atividades de cada processo operacional que deverá ser contingenciado. Geralmente estas atividades são as que apresentaram riscos altos e moderados durante a segunda etapa do processo, ou então são as atividades que embora não apresentaram riscos altos ou moderados elas suportam outras atividades de outros processos operacionais consideradas críticas para o negócio.

Durante o desenvolvimento do plano deverão ser identificadas todas as possíveis alternativas de recuperação de uma atividade crítica, juntamente com os recursos necessários para retornar à atividade no caso de uma contingência. A escolha da melhor alternativa que fará parte integrante do plano deverá ser escolhida, por meio de um consenso entre a equipe responsável pelo projeto e pelo gestor da atividade, com aval do comitê executivo responsável pelo plano.

Todas as alternativas de recuperação deverão ser documentadas de forma detalhada, visando fornecer um roteiro dos procedimentos, passo a passo, de como agir durante uma situação de contingência. A distribuição da documentação para as equipes responsáveis deverá

ser feita de preferência durante a fase de testes e manutenção, onde todas as pessoas envolvidas no plano receberão um treinamento de como proceder durante um desastre.

Quando pensamos em plano de contingência para a área de TI temos que nos conscientizarmos que teremos três recursos básicos necessários para o desenvolvimento do plano:

Pessoas;
Hardwares; e
Softwares.

2.4 Quarta etapa – teste e manutenção

Ao entrarmos nesta etapa, significa que nosso plano de contingência está com suas estratégias de recuperação dos processos críticos definidas e detalhadas. Os testes serão os elementos responsáveis para certificar que, realmente, nossos procedimentos de contingência funcionam e estão atendendo as necessidades de continuidade da organização. Os resultados dos testes poderão trazer novas visões com relação ao funcionamento do plano e a partir daí surgirão as manutenções para manter o plano em funcionamento. As manutenções também deverão ser periódicas, pois as organizações estão em constantes mudanças para se adaptarem às suas variáveis internas e externas. Desta forma, nosso plano de contingência também deverá se adaptar aos moldes de sua organização.

De acordo com Austin, G. e Colaboradores (2000), o teste deve cumprir os seguintes objetivos [1]:

- Verificar se o plano foi elaborado de forma completa e precisa;
- Avaliar o desempenho e conscientização do pessoal envolvido nos testes;
- Avaliar a coordenação entre as equipes que compõe o plano e os fornecedores e/ou terceiros;
- Mensurar a habilidade e capacidade do site alternativo referente ao seu desempenho de Processamento;
- Avaliar a capacidade de restauração das cópias de segurança;
- Avaliar o estado e a quantidade de equipamentos e fornecedores que têm sido alocados para a recuperação das operações; e
- Mensurar todo o desempenho operacional e de processamento relacionados à manutenção dos negócios da organização.

Existem alguns mitos sobre os testes de plano de contingência que devem ser esclarecidos, de acordo com Toigo, J. W. (2002) [10].

O primeiro mito diz respeito à funcionalidade dos testes. Neste caso um teste que vier expor erros será um teste falho;

Esclarecimento do primeiro mito: Não existem testes falhos. Um teste deve ser feito para, entre outros objetivos, se identificar falhas;

O segundo mito é do realismo. Para alguns profissionais um teste tem que reproduzir o mais fielmente o ambiente de um desastre e para isto deve se chegar ao ponto de se interromper todas as atividades do dia a dia para executá-lo.

Esclarecimento do segundo mito: Tal procedimento é desnecessário e contraria a essência do plano de contingência que é garantir a continuidade das operações vitais.

O terceiro mito é o da totalidade. Este mito diz que um teste só é válido se todo o plano for testado.

Esclarecimento do terceiro mito: A construção ideal de um plano é por módulos e assim sendo ele poderá ser testado por módulos. Esta estratégia é mais factível, viabilizando que mais

testes sejam realizados. A realização de testes completos é válida, quando possível, mas isto não inviabiliza a realização de testes modulares.

O quarto e último mito é o da capacitação. A capacidade técnica das equipes e a qualidade do plano garantirão, totalmente, seu sucesso.

Esclarecimento do quarto mito: Uma organização jamais estará suficientemente consciente das ações básicas necessárias para enfrentar um desastre eventual. O sucesso da continuidade de suas operações está baseado em um conjunto de fatores que ultrapassam aos que podem ser obtidos pelos treinamentos. Fatores como intuição, dedicação, efetiva participação dos fornecedores, alta capacidade de gerência e acima de tudo sorte se somam à capacidade técnica das equipes e da qualidade do plano.

3. Discussão e Conclusões

Este artigo apresentou como principal contribuição uma proposta de forma estruturada de se elaborar e manter um plano de contingência para a área de TI.

As quatro etapas de elaboração de um plano de contingência para a área de TI descritas anteriormente: Conscientização, Avaliação dos Riscos e Vulnerabilidades, Desenvolvimento e Teste e Manutenção, nos permitiu demonstrar que o plano de contingência para a área de TI está acima de procedimentos isolados como, por exemplo, os procedimentos de gravação de cópias de segurança, adotados por algumas organizações para tentar suportar a paralisação de sua área de TI por algum tempo.

Demonstramos na Primeira etapa – conscientização, que um plano de contingência para a área de TI deve nascer da conscientização dos membros da organização, principalmente da alta administração que detém o controle de todas as áreas críticas da organização e que esta conscientização deve ser mantida durante a existência do plano de contingência.

Na Segunda etapa – avaliação de riscos e vulnerabilidades, vimos que os riscos relacionados às atividades de cada processo operacional devem ser classificados, de acordo com o grau de exposição de seus riscos inerentes. Isto nos leva a concluir que para se elaborar um plano de contingência para a área de TI é necessário o conhecimento de todos os processos operacionais dependentes da TI, enfim é necessário o conhecimento detalhado das operações da organização.

Na Terceira etapa – desenvolvimento, observamos que as alternativas de recuperação estão atreladas ao conhecimento das atividades de cada processo operacional crítico pelos membros da organização, pois eles serão os principais responsáveis por elaborar, manter e ativar o plano no caso de uma contingência.

Na Quarta etapa – teste e manutenção, vimos que não basta somente termos uma documentação formal do plano de contingência, distribuída entre os membros da organização, faz-se necessário testar o plano periodicamente para se certificar de seu funcionamento e posteriormente atualizá-lo, adequando-o, de acordo com as mudanças que podem acontecer durante a continuidade das atividades da organização.

Com o crescimento vertiginoso do uso da TI, as organizações deverão se preocupar cada vez mais com a continuidade de seus processos operacionais críticos que dependem da TI. Neste ponto, este artigo pretende contribuir como um material de apoio na decisão e elaboração de um plano de contingência para a área de TI em âmbito corporativo.

4. Referências

[1] Austin, G. e Colaboradores (2000). Certified Information System Auditor Review Technical Information Manual. Rolling Meadows, Illinois. Information Systems Audit and Control Association, Inc.

[2] Iudícibus S. e Colaboradores (2003). Manual de Contabilidade das Sociedades por Ações. São Paulo. Atlas.

[3] Boehm, B. W. (1998). Software Risk Management. Los Alamitos, California. IEEE.

[4] Myers, K. N. (1999). Manager's Guide to Contingency Planning for Disaster – New York John Wiley & Sons, Inc.

[5] KPMG-BCP (1998). Business Continuity Planning Methodology. KPMG Peat Marwick.

[6] KPMG-CSS (1999). Contingency Strategy Service Methodology. KPMG Peat Marwick.

[7] Price Waterhouse-DCP (1992). System Management Methodology Disaster Contingency Planning. Price Waterhouse.

[8] Burtles, J. e Yates, S. (1998). The Journal of Business Continuity. London. The Business Continuity Information Centre.

[9] Meredith, B. (1998). The Journal of Business Continuity. London. The Business Continuity Information Centre.

[10] Toigo, J. W. (2002). Strategies for Protecting Critical Information. New York. John Wiley & Sons, Inc.

5. Contato

Autor: Professor Mestre Washington Lopes da Silva – Mestre em Engenharia Elétrica – Concentração em Engenharia da Computação pela Universidade Mackenzie; e Aluno Especial de Doutorado da Escola Politécnica da Universidade de São Paulo; washington.lopes@poli.usp.br

Dados Profissionais: Superintendente de Auditoria de TI – Unibanco S/A – Professor para o curso MBA em Auditoria Interna – FIPECAFI

Fone comercial: (11) 3789-7547