06 – Julho de 1999

2892: quatro algarismos e pouco tempo

O segmento financeiro anda mesmo em ebulição. A chama foi acessa pela Resolução 2554 - emitida pelo Conselho Monetário Nacional CMN – que estabelece a necessidade de controles internos e que comentei em artigo anterior. Agora é a vez do Banco Central do Brasil, com a Circular 2892 – que define diretrizes para implementação de plano destinado a assegurar a continuidade operacional e a integridade das informações, ou se preferir, plano de contingência – e passa a ser a mais nova exigência do BACEN às instituições financeiras ligadas à ele.

Analisando rapidamente o assunto, trata-se da elaboração, validação e implementação de planos que contingenciem a infra-estrutura, a tecnologia e os processos críticos para garantir a continuidade das operações vitais e a integridade das informações processadas em sistemas sob sua responsabilidade e em interfaces com sistemas de terceiros, ou seja, deve-se garantir a operação do negócio em caso de desastres, eventualmente provocados pela possível pane nos sistemas de computador ou em equipamentos "inteligentes" em virtude da virada do ano 2000.

Mas o que é exatamente Plano de Contingência? Em uma corporação, existem produtos finais, que utilizam recursos e serviços de fornecedores, baseados em processos, que fazem uso de redes, computadores, programas e que são por sua vez, suportados pela infra-estrutura básica e serviços essenciais. Fica evidente a interdependência de cada um desses elementos, como em uma cadeia de valor agregado. E como em toda atividade, existem processos críticos ou processos que são os alicerces da instituição. Os planos contendo procedimentos alternativos para a continuidade desses processos em tempo de desastre, são conhecidos como Planos de Contingência.

Tudo começa com a definição das estratégias, onde o que deve ser contingenciado é identificado (processos essenciais) e seu grau de criticidade é apurado, para só então, elaborar os procedimentos que irão fazer parte do plano. As demais etapas do escopo da circular, são a identificação dos riscos iminentes, análise de vulnerabilidade dos ambientes informatizados, os planos de contingência propriamente ditos, testes e simulações.

É bom esclarecer e separar o plano de contingência dos planos de retorno e recuperação. São na verdade, procedimentos complementares. O plano de recuperação se encarrega de solucionar o desastre, seja restaurando uma cópia de segurança, repondo um equipamento ou disponibilizando outro local para a operação da atividade. Já o plano de retorno, é responsável por restabelecer a operação normal da atividade, nas mesmas condições iniciais.

Em termos práticos, se sua empresa está em situação confortável por já ter preparado seus sistemas pensando na virada do ano e no bug do milênio, surge uma nova e emergencial preocupação com os planos de contingência. O assunto foi discutido recentemente no Congresso Internacional de Automação Bancária - CIAB e recebeu muita atenção. Algumas

soluções interessantes já foram apresentadas, à exemplo da Módulo, que desenvolveu uma metodologia específica para Plano de Contingência de instituições financeiras que buscam a conformidade com a 2892 e um plantão técnico de especialistas para assegurar a continuidade das operações vitais na passagem para o ano 2000.

.

Ah! Justificando o título, ao falar do tempo... a circular determina que tais planos de contingência sejam implementados até 30 de setembro de 1999. Não precisa dizer mais nada, não é?!

Marcos Sêmola *é MBA em Tecnologia Aplicada e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br