BANCO CENTRAL DO BRASIL

CIRCULAR Nº 2892

Estabelece diretrizes com vistas à implementação de plano destinado a assegurar a continuidade operacional e a integridade das informações das instituições financeiras, demais instituições autorizadas a funcionar pelo Banco Central do Brasil e administradoras de consórcio, ante eventuais situações emergenciais que possam afetar os sistemas eletrônicos de informação automatizados na passagem para o ano 2000.

A Diretoria Colegiada do Banco Central do Brasil, em sessão realizada em 26 de maio de 1999, com base no art. 3º da Resolução nº 2.453, de 18 de dezembro de 1997,

D E C I D I U:

Art. 1º Determinar que as instituições financeiras, demais instituições autorizadas a funcionar pelo Banco Central do Brasil e as administradoras de consórcio, considerando as peculiaridades e complexidade de seus processos operacionais, providenciem a elaboração, validação e implementação, até 30 de setembro de 1999, de plano de continuidade, de modo a assegurar a continuação de suas operações vitais e a integridade das informações processadas em sistemas sob sua responsabilidade e em interfaces com sistemas de terceiros, diante de eventuais situações emergenciais que possam ocorrer na passagem para o ano 2000.

Parágrafo único. O plano de continuidade de que trata este artigo deve ser implementado observando-se, no mínimo, as fases e respectivos detalhamentos contidos no anexo, contemplando:

I - planejamento estratégico de continuidade;
II - análise de riscos potenciais;
III - planos de contingência;
IV - validação/testes;
V - procedimentos complementares.

Art. 2º A instituição deve manter documentação completa de todo o processo relativo à elaboração, validação e implementação do plano de continuidade para eventuais análises por parte do Banco Central do Brasil.

Art. 3º As instituições que já possuam plano de continuidade devem promover as adaptações necessárias para certificarem-se que as diretrizes contidas no anexo estejam nele contempladas.

Art. 4º Esta Circular entra em vigor na data de sua publicação.

Brasília, 26 de maio de 1999.

Sérgio Darcy da Silva Alves — Luiz Carlos Alvarez

Diretor Diretor

ANEXO à Circular 2.892, de 26.05.99

Plano de Continuidade dos Negócios

O objetivo deste anexo é apresentar diretrizes básicas para a elaboração de um plano de continuidade das instituições financeiras, de- mais instituições autorizadas a funcionar pelo Banco Central do Brasil e administradoras de consórcio, de modo a assegurar que eventuais falhas em seus sistemas ou em sistemas de terceiros com quem mantém relacionamento não inviabilizem a continuidade de suas operações em função da passagem para o ano 2000, colocando em risco o negócio da instituição e de seus clientes. A instituição deve, de acordo com as suas características, certificar-se que o seu Plano de Continuidade contemple as recomendações contidas nas fases detalhadas a seguir.

I - Planejamento Estratégico de Continuidade

Consiste no desenvolvimento, em nível estratégico, com a respectiva documentação, de um projeto de continuidade operacional e integridade das informações, de modo a conscientizar os principais executivos da instituição sobre os riscos potenciais de falhas operacionais que podem interromper os seus negócios durante a passagem para o ano 2000, e propor-lhes soluções para enfrentá-las, bem como informá-los sobre o esforço de trabalho e custos estimados para implementação dessas soluções.

Deverão ser contemplados nessa fase os seguintes aspectos:

1.1. Designação de grupo de trabalho, que deverá estar subordinado ao diretor estatutário referido no artigo 4º da Circular 2.803, de 4 de fevereiro de 1998.

1.2. Definição da estratégia para a continuidade dos negócios da instituição.

1.3. Avaliação dos procedimentos utilizados atualmente para continuidade dos negócios em situações emergenciais, para eventual aproveitamento no projeto.

1.4. Estabelecimento de cronograma para o projeto de continuidade supra citado, com detalhamento das atividades, prazos e responsáveis.

1.5. Identificação dos processos operacionais críticos da instituição, com o levantamento das respectivas interdependências, principalmente daqueles nos quais participam fornecedores, empresas subcontratadas e parceiras no desenvolvimento de negócios, entre outros.

1.6. Identificação dos sistemas de processamento de dados que suportam os processos críticos e mapeamento de seus inter-relacionamentos.

1.7. Avaliação do impacto adicional causado pela interrupção no fornecimento de serviços públicos essenciais, tais como, energia elétrica, comunicações, transportes, segurança e nos serviços financeiros de infra-estrutura, tais como, liquidação e compensação.

1.8. Identificação de datas críticas nas quais os sistemas poderão apresentar interrupções ou falhas, de modo a possibilitar a definição de estratégia de distribuição das operações e de compromissos, com vistas a evitar-se sobrecarga dos sistemas naquelas datas.

1.9. Elaboração de planos de revisão para análise e validação dos procedimentos desenvolvidos.

1.10. Indicação, para cada processo crítico, das pessoas envolvidas e respectivos substitutos, e definição de esquema de convocação, em caso de sobrevir uma situação crítica.

II - Análise de Riscos Potenciais

O objetivo dessa fase é estimar, com a pertinente documentação, a probabilidade de que os sistemas de processamento de dados sofram interrupção ou mau funcionamento, quer devido a maior susceptibilidade às alterações nos campos de data, quer devido a maior dependência ou influência de outros sistemas, e avaliar o impacto dessas eventuais falhas em seus processos operacionais críticos.

Deverão ser contemplados nessa fase os seguintes aspectos:

2.1. Levantamento e documentação de informações a respeito dos processos operacionais críticos, necessárias à posterior análise e utilização no desenvolvimento do plano de continuidade dos negócios, contendo:

a) esquemas de funcionamento;
b) interdependências;
c) riscos existentes;
d) alternativas que poderiam ser implementadas em situações de contingência.

2.2. Comprovação da existência de planos de contingência documentados e de soluções alternativas para o atendimento aos clientes mantidos pelos provedores de serviços.

2.3. Avaliação das conseqüências para os negócios da instituição caso ocorra uma situação extrema, provocada pela interrupção de todos os sistemas que suportam os processos críticos e de todos os serviços essenciais. Adicionalmente, considerar a possibilidade de que um provedor de serviços afete várias instituições simultaneamente.

2.4. Análise quanto à forma de ocorrência de eventuais falhas, considerando que:

a) o sistema poderá ser capaz de processar apenas informação não sensível a datas;
b) o sistema poderá produzir resultados incorretos;
c) o sistema poderá produzir resultados imprevisíveis;
d) ocorra falha completa do sistema.

2.5. Análise e estimativa do nível de impacto (alto, médio, baixo) que a interrupção dos processos críticos causados por falhas em seu ambiente computacional (hardware, software, infra-estrutura, etc.) poderá causar aos negócios e a terceiros, visando o estabelecimento de prioridades e a alocação de recursos humanos e materiais para o desenvolvimento dos diversos planos de contingência que irão compor o plano de continuidade.

2.6. Construção de uma matriz "impacto versus probabilidade" que permita definir prioridades para as ações corretivas que se fizerem necessárias em cada um desses sistemas e nos processos críticos de negócios.

2.7. Estabelecimento de níveis de abrangência e desempenho para os planos de contingência a serem desenvolvidos (serviços a serem oferecidos, padrão de qualidade desses serviços, tempo máximo para disponibilização do sistema após a ocorrência de falhas, etc.).

III - Planos de Contingência

Com base no levantamento obtido na fase anterior, na presente fase deve ser procedida a identificação, o desenvolvimento e a documentação dos planos de contingência, a definição dos respectivos procedimentos de ativação, o estabelecimento de prazos para a implementação dos mesmos e a designação das equipes que ficarão responsáveis pela operacionalização dos referidos planos.

Deverão ser contemplados nessa fase os seguintes aspectos:

3.1. Análise e seleção, dentre as alternativas de plano de contingência levantadas na fase anterior, daquelas que apresentarem as melhores relações de custo/benefício.

3.2. Definição da estratégia de continuidade adequada e subseqüente retomada da operação para cada processo crítico, considerando:

a) hipóteses de continuidade de processos críticos, entre outras: substituição total de sistemas por outros equivalentes, já adaptados e testados; alteração dos programas, em caráter de emergência; aquisição de programas aplicativos que permitam a continuidade dos processos em nível operacional mínimo, para o caso de atraso na modificação de sistemas críticos; contratação e treinamento de pessoal que possa emular os processos críticos automatizados, atendendo o nível operacional mínimo;

b) tempo total para implementação da alternativa e para retomada da operação ao nível adequado;

c) capacidade de suprir todas as funções necessárias para atingir o nível operacional mínimo;

d) custo da alternativa, considerando aquisição de produtos e serviços, treinamento de pessoal e teste;

e) perdas estimadas para os negócios e para a reputação da instituição, devidas à interrupção total ou parcial desses processos críticos e o tempo para retomada das operações ao nível normal.

3.3. Designação das equipes de trabalho responsáveis pela implementação de cada um dos planos de contingência.

3.4 Elaboração, com a respectiva documentação, dos planos de contingência para atender cada alternativa, conforme o processo crítico de negócios, contendo:

a) procedimentos a serem adotados e as responsabilidades do pessoal envolvido, na condução do plano de contingência;

b) recursos necessários para implementação da alternativa e para o retorno das atividades ao nível normal de operação e, em especial, nos dias próximos ao dia 31 de dezembro de 1999;

c) requisitos técnicos, funcionais, organizacionais e de infraestrutura que serão necessários para suportar a continuidade de processos críticos de negócios;

d) cronograma que contemple aquisição, teste e implementação da alternativa, a recuperação dos sistemas que suportam os processos críticos e o retorno das atividades ao nível de operação normal;

e) datas-limites para conclusão de cada tarefa, que permitam atribuir percentuais de evolução para implementação da solução alternativa;

f) eventos e condições para acionamento do plano de contingência.

3.5. Para os processos operacionais que envolvam arquivos que necessitem ser recuperados, deverão ser previstos:

a) Cópias de segurança (backups) periódicos de todos os arquivos mestres (cadastros) utilizados;

b) Logs (imagens) anteriores e posteriores de todos os registros atualizados nos arquivos acessados pelas transações englobadas por esses processos;

c) Disponibilização de procedimentos operacionais para rápida recuperação dos arquivos eventualmente afetados por falhas no ambiente computacional;

d) Manutenção de lista atualizada de endereços e telefones para contato com todos os parceiros, clientes e fornecedores, que troquem dados e participem dos procedimentos integrados de recuperação com a instituição.

3.6. Avaliação da necessidade de revisão de contratos com terceiros.

3.7. Previsão de revisões mensais do plano até janeiro de 2000, ou conforme determinado pelos testes de certificação, alterando, se necessário, sistemas, programas aplicativos, procedimentos e recursos previstos originalmente.

3.8. Planejamento para implantação de central de informações durante o período de retomada de negócios, até atingir o nível de operação normal.

IV - Validação/Testes

O objetivo dos testes no processo de desenvolvimento do Plano de Continuidade dos Negócios é avaliar se os diversos planos de contingência desenvolvidos para constituí-lo são capazes de suportar de modo satisfatório os processos operacionais críticos de negócios da instituição e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se tais planos podem ser ativados tempestivamente.

Deverão ser contemplados nessa fase os seguintes aspectos:

4.1. Elaboração de um plano para certificação dos planos de contingência, que inclua:

a) descrição de equipamento, pessoal, cronograma e procedimentos para cada fase;
b) definição de parâmetros para validação do plano de continuidade;
c) desenvolvimento e documentação dos procedimentos de teste dos planos de contingência;
d) designação e treinamento das equipes responsáveis pela condução dos testes;
e) programação de treinamento simulado para todas as equipes responsáveis pela operacionalização dos planos de contingência;
f) ensaios de situações de emergência com o pessoal designado no plano de contingência;
g) validação dos resultados obtidos, considerando-se os aspectos de funcionalidade, performance e segurança;
h) atualização do plano de continuidade em função das observações levantadas durante os testes dos planos de contingência;
i) atualização dos planos e procedimentos para recuperação de falhas.

4.2. Os testes devem ser efetuados, preferencialmente, por equipes diversas das envolvidas nos processos de desenvolvimento dos referidos planos.

4.3. O processo de validação deverá contar com a participação e avaliação da auditoria independente e da auditoria interna.

V - Procedimentos Complementares

5.1. Os planos de contingência e respectivos testes de validação devem ser documentados, aprovados e assinados pelo diretor estatutário referido no artigo 4º da Circular nº 2.803, de 1998.

5.2. O auditor independente deverá emitir parecer sobre a adequação dos planos de contingência e os resultados obtidos nos testes de validação, conforme determinado pela Resolução nº 2.453, de 18 dezembro de 1997.

5.3. A instituição deve criar e manter, por 180 dias, arquivos de recuperação com registros dos dados anteriores à passagem para o ano 2000. Adicionalmente, deve gerar uma segunda cópia dos arquivos de segurança, a ser armazenada em local diverso da primeira.

5.4. A instituição deve evitar, tanto quanto possível, que as datas de vencimento ou renovação de contratos ocorram no período compreendido entre 31 de dezembro de 1999 e 7 de janeiro de 2000.