

Plano de Continuidade – Um estudo da Circular BACEN 2.892

**Cassiano G. de Moraes, Elias Paulo B. de Araújo, Joaquim Silveira
Mello e Rubens M. Faro Pompeu**

Orientador: Prof. Ly Freitas

Resumo

Com a possibilidade de ocorrências de falhas nos sistemas eletrônicos de informação automatizados, devido à passagem do ano 2000, o Banco Central do Brasil determinou, através da Circular BACEN 2.892 de 26 de maio de 1.999, que as instituições financeiras, demais instituições autorizadas a funcionar por ele e administradoras de consórcios, elaborem um plano de continuidade. Para implementação do plano, as instituições devem desenvolver, em nível estratégico, 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. Deverá ser feita uma análise dos riscos, visando estimar a probabilidade de falhas e o impacto das mesmas nos processos operacionais críticos. Esta análise será utilizada para compor os diversos planos de contingência que depois de testados e validados deverão ser documentados, aprovados e assinados pelo diretor estatutário.

Palavras-Chave

Plano de Continuidade; Contingência; Integridade; Desastre; Processos operacionais críticos.

Abstract

With the possibility of problems occurrences in automatized electronic information systems, due to the passage of year 2000, the Central Bank of Brazil determined, through Circular BACEN 2.892 of May 26th of 1999, that the financial institutions, others institutions authorized to work by them, and administrators of trusts, elaborate a continuity plan. To implement this plan, the institutions must develop, in strategical level, a project that contemplate operational continuity and information integrity, in order to show the main executives of the institution about potential risks of operational imperfections that can interrupt its businesses. An analysis of the risks will have to be made, aiming the probability of imperfections and the impact of them in the critical operational processes. This analysis will be used to compose the several contingency plans that after tested and validated will have to be documented, approved and signed by the statutory director.

Keywords

Continuity Plan; Contingency; Integrity; Disaster; Critical Operational Processes.

1. Introdução

O presente artigo traz um estudo sobre a Circular BACEN 2.892 de 26 de maio de 1.999 e seu anexo que estabelece diretrizes com vistas a 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 consórcios.

Diante das ameaças e riscos associados à continuidade dos sistemas eletrônicos de informação na passagem para o ano 2000, somados à necessidade de adequação de segurança, torna-se fundamental a elaboração de um plano de continuidade, a fim de mapear novas falhas e riscos que irão orientar ações corretivas de emergências posteriores.

A elaboração do plano de continuidade deve contemplar as seguintes fases: planejamento estratégico de continuidade; análise de riscos potenciais; planos de contingências; validação/teste e procedimentos complementares. A instituição deve, de acordo com as suas características, certificar-se que o seu Plano de Continuidade contemple as recomendações contidas nas fases acima.

2. Detalhamento das Fases do Plano de Continuidade

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 o Banco Central do Brasil exige que seja, elaborado, validado e implementado, planos que contingenciem a infra-estrutura, a tecnologia e os processos críticos, seguindo as seguintes fases:

2.1 Planejamento Estratégico de Continuidade

Em uma organização, 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 e necessitam de um planejamento bem elaborado que garanta a continuidade dos serviços. [SÊMOLA,1999]

O planejamento estratégico 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 e propor-lhes soluções para enfrentá-las, bem como informá-los sobre o esforço de trabalho e custos estimados para implementação dessas soluções.

2.2 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. [BACEN,1999]

Deve-se levantar todos os processos críticos da organização e o impacto provocado pela interrupção dos mesmos, com isso propondo soluções alternativas minimizando ao máximo os possíveis prejuízos.

2.3 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.

Dar a providência imediata invocando os procedimentos de recuperação do sistemas corporativos, considerando o tempo de espera previsto para restabelecimento da atividade, definido pelos Gestores das informações. Para cada sistema corporativo, hierarquicamente definido segundo o grau de criticidade e processado nos CPD's, são previstos o tempo de paralisação possível e ações subsequentes para seu restabelecimento. [SYMANTEC,2002]

Para a elaboração do Plano de Contingência é necessário que seja levantado os seguintes itens básicos:

Quais são os sistemas críticos que garantem a continuidade do negócio da empresa?

- Análise de Impacto nos Negócios;
- Análise de Riscos para os principais Negócios;
- Homologação dos sistemas críticos por parte dos Executivos da Empresa.

De que recursos de hardware, software e infraestrutura tais sistemas dependem?

- Software
 - Configuração
 - Versão/Release
 - Nível de atualizações
 - Customizações
 - Fornecedores
- Hardware
 - Configuração
 - Up-Grade
 - Espaço em disco para o S.O. e Sistemas críticos
 - MIPS utilizado
 - Memória
 - CPU

- Controladora de Discos
- Controladora de Mídia Magnética
- Mídias Magnética
- Fornecedores

- Infraestrutura
 - robôs/cilos/estantes
 - Rede/Teleprocessamentos
 - MUX
 - Porta de Controladora de Linha
 - Circuito de Comunicação
 - Multiplexadores
 - Concentradores
 - Circuitos
 - CCU
 - Roteadores
 - Switch
 - Hubs
 - Bridge
 - Satélite
 - Concessionárias

- Ambiência
 - Definição de carga de refrigeração
 - Temperatura
 - Umidade
 - Alimentação de energia elétrica
 - No-Break
 - Gerador de energia
 - Bateria de energia
 - PABX e telefonia em geral
 - Prédios inteligentes e elevadores

Levantamento e atualização da documentação dos sistemas críticos

- Objetivos do sistema
- Analistas responsáveis
- Usuários Gestores e usuários Finais
- Backup diário, semanal, mensal, semestral e anual - Retenção de arquivos
- Fases do sistema e sua descrição
- Relação de programas utilizados - Batch - Código e descrição
- Relação de programas utilizados - On line - Código e descrição
- Interfaces
 - Interna - Arquivos de entrada
 - Interna - Arquivos de saída
 - Externa- Arquivos de entrada
 - Externa- Arquivos de saída
 - Identificação dos serviços críticos dentro dos sistemas prioritários - programas e tabelas

- O que deve ser retido no período de contingência para recuperação dos sistemas não críticos
- Serviços que devem ser considerados críticos já que são essenciais para recuperação de sistemas não críticos
- Quais são os componentes críticos dos sistemas críticos
- Backup
 - Tamanho em Bytes dos dados necessários para funcionamento dos sistemas críticos
 - Volume de mídias magnéticas que fazem atualmente o Backup externo dos sistemas críticos
 - Espaço físico, estimado, para guarda do Backup externo dos sistemas críticos
 - Forma de criação dos backup externo (link específico / transporte)
 - Relação dos backup dos sistemas críticos
 - Hierarquia a ordem cronológica de baixa dos backup
 - Definição do backup-site
 - Definição do Modelo de Backup_Site (espelhamento, transmissão remota...)
 - Cold-Site próprio
 - Cold-Site de Terceiros
 - Hot-Site próprio
 - Hot-Site de terceiros
 - Hot-Site próprio compartilhado
- Decisões Pós-Desastre para a Recuperação
 - Evitar novos danos, executando os procedimentos de emergência
 - Identificar hardware e material que pode ser salvo
 - Auxiliar a equipe de logística na movimentação de recursos salvos
 - Informar as equipes de telecomunicação e de hardware do andamento dos trabalhos de salvamento
 - Avaliação do desastre no aspecto de estrutura física
 - Laudo e estimativa de recuperação da estrutura física
 - Avaliação do desastre no aspecto de parque computacional
 - Laudo e estimativa de substituição do parque computacional
 - Decisão quanto a localidade e formas de processamento pós-desastre dos sistemas crítico
 - Decisão quanto a localização e forma de processamento pós-desastre dos demais sistemas
- Plano de Retorno
 - Definição de datas e procedimentos para retorno às atividades normais.
 - Retorno do CPD e estrutura básica
 - Definição de estrutura de apoio
 - Definição das datas de retorno
 - Criação de relatórios históricos

2.4 Validação e 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. [BACEN,1999]

Os testes e validações são de grande importância pois a partir deles se pode rever o plano de contingência, corrigindo e melhorando se necessário, garantindo assim que quando for preciso utilizá-lo funcione como previsto.

2.5 Procedimentos Complementares

Deve se prever um plano de recuperação e retorno. 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.

Os planos de contingência e respectivos testes de validação devem ser documentados, aprovados e assinados pelo um diretor estatutário.

Um auditor independente deverá emitir parecer sobre a adequação dos planos de contingência e os resultados obtidos nos testes de validação.

3. Conclusão

Toda empresa com potencial de gerar uma ocorrência anormal, cujas conseqüências possam provocar sérios danos a pessoas, ao meio ambiente e a bens patrimoniais, inclusive de terceiros, devem ter, como atitude preventiva, um Plano de Continuidade (ou Emergência).

O Plano de Continuidade é um documento onde estão definidas as responsabilidades, estabelecidas em uma organização para atender a uma emergência, e contém informações detalhadas sobre as características da área envolvida. É um documento desenvolvido com o intuito de treinar, organizar, orientar, facilitar, agilizar e uniformizar as ações necessárias às respostas de controle e combate às ocorrências anormais.

A prevenção deve possuir um corpo técnico altamente qualificado para desenvolver e auditar qualquer Plano de Continuidade e sempre de forma a atender as necessidades e condições da organização.

A aplicação dos conceitos de contingência e redundância oferece maior segurança e confiabilidade para a rede de computadores através das soluções para a proteção das informações e aplicativos, equipamentos, espaço físico e demais funções críticas.

A redundância é um fator que pode contribuir para a disponibilidade de uma rede de computadores. Entretanto, apenas a redundância é insuficiente, visto que um sistema pode apresentar diferentes vulnerabilidades. Uma rede de alta disponibilidade, por exemplo, requer que cada sistema “backup” ofereça funcionalidades equivalentes, porém com implementação diferenciada. Esta variação afasta tentativas de comprometer tanto o sistema primário quanto o sistema de “backup” a partir de uma única estratégia de atendimento.

Já um plano de contingência requer procedimentos inteligíveis e objetivos, simulações de possíveis ocorrências futuras e soluções simples, imaginando situações possíveis, mesmo que pouco prováveis. Induz a elaboração de procedimentos operacionais diretos que permitam, em uma ocorrência indesejada, tomarem-se ações que reparem ou minimizem os efeitos da falha. As idéias são tratadas e as hipóteses classificadas segundo a chance, o custo e a segurança envolvida.

Embora redundância e planos de contingência sobrecarreguem o funcionamento e o gerenciamento de uma rede, ambos são necessários para evitar problemas futuros. A decisão sobre o grau de redundância ou contingência que se deve adotar pode ser balizada por vários fatores, entre eles: ambiente de funcionamento da rede, protocolos e sistemas utilizados e importância da rede para o negócio da empresa.

Apesar de realmente fazerem parte fundamental dos planos de recuperação de Desastres e Continuidade, a contingência de componentes não garante continuidade. Apenas garante que encontraremos os meios necessários para planejá-la, de acordo com nossas necessidades e limitações.

Referências Bibliográficas

[BACEN,1999] BANCO CENTRAL DO BRASIL – BCB Home Page: “Circular 2.892”,

http://www5.bcb.gov.br/pgIFrame.asp?idPai=NORMABUSCA&urlPg=/ixpress/correio/correio/DETALHAMENTOCORREIO.DML?N=099111333&C=2892&ASS=CIRCULAR+2.892, consulta em 17/06/05.

[BRODERICK,2002] BRODERICK, Stuart, PhD - Symantec Securit Services - A Definitive Introduction to Information Security Policies, Standards and Procedures – julho, 16, 2002

[INGRAN,2002] INGRAN, Danny - Symantec Securit Services - Plan to Save - The Importance of Proper Security Planning – maio, 7, 2002

[PINHEIRO,2004] PINHEIRO, José Maurício Santos – Conceitos de redundância e contingências, 06 de dezembro de 2004

[RIBEIRO,1988] RIBEIRO, Alexandre Menezes – Como criar um plano de contingência, 27 de junho de 1988

[SÊMOLA,1999] SÊMOLA,M. – Módulo Home Page: “2892: quatro algarismos e pouco tempo”,*http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=59&pagecounter=0&idiom=0, consulta em 17/06/05.*

[SYMANTEC,2002] Symantec Corporation Home Page: “Guia para o planejamento de Contingência”,*http://www.symantec.com/region/br/enterprisecurity/content/framework/BR_573.html, consulta em 17/06/05.*