DAYRON HUSSID FERREIRA

PROPOSTA DE PLANO PARA RECUPERAÇÃO DE DESASTRES EM SISTEMAS CRÍTICOS DE TI QUE UTILIZAM MAINFRAME

Monografia apresentada ao Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo para conclusão de curso MBA.

Área de Concentração:
Tecnologia da Informação

Orientador:
Eduardo Oliveira

São Paulo
2014

FICHA CATALOGRÁFICA

Ferreira, Dayron Hussid

Proposta de plano para recuperação de desastres em sistemas críticos de TI que utilizam Mainframe / D.H. Ferreira. -- São Paulo, 2014.
p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Tecnologia da informação 2.Mainframe I.Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II.t.

AGRADECIMENTOS

Ao meu pai Dalmo, por todo o incentivo dado na busca do conhecimento e por instigar minha paixão pela leitura.

Á minha mãe Brana, pela formação recebida e por me tornar uma pessoa organizada e preparada.

Aos meus irmãos Aron e Dalminho, pela amizade eterna e por todos os momentos agradáveis que tivemos juntos.

Á minha namorada Renata, pelas palavras de apoio e estímulo para vencer os momentos de dificuldades.

RESUMO

Em muitos casos as áreas de negócios das empresas dependem fortemente do processamento de dados para suas atividades e uma paralisação do processamento para o negócio da empresa. Algumas empresas subestimam os riscos de um desastre e não investem em um Plano de Recuperação de Desastres (PRD), o que pode trazer uma paralisação nos negócios da empresa, com perdas significativas caso um desastre aconteça, principalmente se afetar sistemas críticos de TI. Como motivação para esta monografia foram utilizados os dados do *University of Texas Disaster Study* (2002) sobre empresas sem Plano de Recuperação de Desastres. Segundo os dados, 43% das empresas que tiveram uma grande perda de dados de negócios nunca reabriram, 51% fecharam em até dois anos e somente 6% sobreviveram por longo prazo. Como embasamento acadêmico para esta monografia é utilizado a norma ISO/IEC 24762, que foi criada para definir o que as organizações devem oferecer em termo de serviços para a recuperação de desastres em TI. Esta monografia especifica um novo plano de recuperação de desastres baseando-se na ISO/IEC 24762 e no ITIL V3 focado em sistemas críticos de TI que utilizam mainframe.

Palavras-chave: Tecnologia da Informação. Recuperação de Desastres. Sistema crítico. ITIL. Mainframe

ABSTRACT

In many cases the business areas of enterprises rely heavily on data processing for their activities and when the processing stops the company's business also stops. Some companies underestimate the risks of a disaster and do not invest in a Disaster Recovery Plan (DRP), which can bring a business outage, with significant losses if a disaster happens, especially if Critical IT systems are affected. The University of Texas Disaster Study (2002) on firms without the Disaster Recovery Plan was used as motivation for this monograph. According to the data, 43% of companies that had a major loss of business data never reopened, 51% closed within two years and only 6% survived long term. The ISO/IEC 24762 standard will be used as academic foundation for this monograph. ISO/IEC 24762 defines what organizations should offer in terms of services for disaster recovery in IT. This monograph will specify a new plan for disaster recovery basing on the ISO/IEC 24762 and on ITIL V3 focused on critical IT environments that uses mainframe.

Keywords: Information Technology. Disaster and Recovery. Critical System. ITIL. Mainframe

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BCP	Business Continuity Planning
CCTA	Central Computing and Telecommunications Agency
DB2	Data Base 2
DR	Disaster and Recovery
DRP	Disaster and Recovery Plan
GDPS	Geographically Dispersed Parallel Sysplex
I/O	Input/Output
IBM	International Business Machines
IMS	Information Management System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Tecnology infrastructure library
OGC	Office of Government Commerce
PPRC	Peer to peer remote copy
RACI	Responsible, Accountable, Consulted, Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SO	Sistema Operacional
ICT DR	Information and Communications Technology Disaster Recovery
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

1.1 Contexto Inicial

Desastres como falta de energia, inundações e até mesmo invasões hacker afetam os negócios todos os dias. As organizações devem desenvolver um Plano de Recuperação de Desastres para se preparar para tais ocorrências. Um Plano de Recuperação de Desastres é um processo detalhado para a recuperação de informações ou de um sistema de TI em caso de um desastre catastrófico, como um incêndio ou inundação. Os gastos com a recuperação de desastres estão aumentando em todo o mundo entre as instituições financeiras. (BALTZAN; PHILLIPS, 2008, p.239).

Segundo os dados do *University of Texas Disaster Study* (2002), 43% das empresas que tiveram uma grande perda de dados de negócios nunca reabriram, 51% fecharam em até dois anos e somente 6% sobreviveram por longo prazo. Portanto um Plano de Recuperação de Desastres é imprescindível para o funcionamento dos negócios em situações disruptivas (Figura 1).

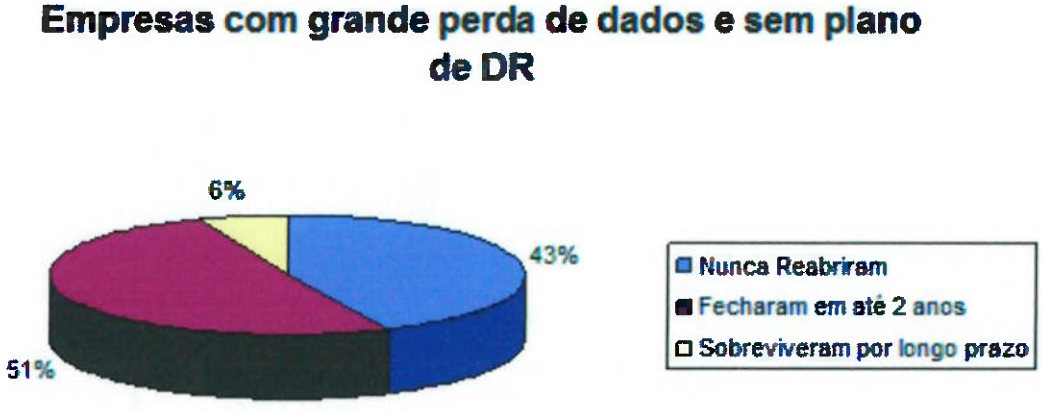

Figura 1 - Empresas sem plano de DR (Fonte: University of Texas)

1.2 Problema

Diversas áreas de negócios dependem fortemente do processamento de dados para suas atividades e uma paralisação de um sistema crítico de TI impacta a capacidade da empresa funcionar. Conforme os dados da *University of Texas* (2002), apenas 6 % das empresas que sofreram grandes perdas de dados de seus sistemas críticos conseguiram sobreviver a longo prazo.

Dependendo da criticidade do sistema, a paralisação pode ser mais impactante que o próprio desastre, pois muitas vezes o desastre afeta uma área específica, já o sistema crítico pode ter abrangência global e a inoperância desse sistema pode resultar em lesões às pessoas, danos aos ambientes e perdas econômicas. Os Mainframes vêm sendo utilizados por diversos sistemas críticos devido a sua alta confiabilidade e desempenho, como exemplo de alguns sistemas críticos que utilizam mainframe, pode-se citar o sistema de tráfego aéreo de algumas empresas ou até mesmo um sistema médico hospitalar interligando vários hospitais.

Algumas empresas subestimam os riscos de um desastre e não investem em um Plano de Recuperação de Desastres (PRD), ou possuem um PRD, mas não seguem um conjunto de boas práticas. Segundo um questionário realizado com milhares de empresas no *"Prove It" disaster readiness consortium* (2002), 75% delas estão na zona de perigo, 21% precisam melhorar e apenas 4% seguem as melhores práticas. Processos de gestão de serviços de TI que não estão bem estruturados nem padronizados, podem fazer com que qualquer paralisação de um sistema crítico possa levar a um tempo de indisponibilidade inadmissível para o negócio, ou até mesmo a uma situação irrecuperável (*UNIVERSITY OF TEXAS*, 2002).

1.3 Objetivo

O objetivo desta monografia é propor um plano de recuperação de desastres para sistemas críticos de TI que utilizam mainframe, utilizando de algumas das boas práticas do modelo ITIL V3 além da norma ISO/IEC 24762. A norma ISO/IEC 24762 foi criada para definir o que as organizações devem oferecer em termo de serviços para a recuperação de desastres em TI. Esta norma é mais genérica e funciona como um framework para diferentes tipos de empresas. Já o modelo ITIL (*IT infrastructure library*) provê um conjunto de boas práticas a serem aplicadas na gestão de serviços de TI.

1.4 Justificativa

Há muitos anos os mainframes vêm sendo usados por diversos sistemas de grande porte devido a sua alta confiabilidade. Portanto sua utilização já está bem consolidada no mundo das grandes corporações principalmente em sistemas de abrangência nacional ou até mesmo global, conforme os dados do *IBM Investor Briefing* (2014):

- 90 % das transações globais de cartão de crédito são processadas em mainframes IBM;
- 21 das 25 maiores companhias de seguro usam mainframe IBM para executar seus negócios;
- 23 dos 25 maiores varejistas norte-americanos executam seus negócios em mainframes IBM;
- 70% dos dados de negócio do mundo são geridos por mainframes.

Segundo os dados, grande parte dos sistemas críticos utilizam mainframe, e atualmente com a crescente necessidade desses sistemas possuírem disponibilidade contínua e continuarem funcionando mesmo em situações de desastres, algumas organizações internacionais criaram normas e padrões para auxiliar as empresas a alcançarem esse objetivo. Uma das últimas normas publicadas e que é utilizada nesta monografia é a ISO/IEC 24762:2008, que foi

escolhida por ter um foco mais detalhado nos problemas tecnológicos que devem ser tratados em uma situação de desastre. No mercado existem outras normas que tratam do assunto de recuperação de desastres, entretanto elas são um framework de alto nível que descrevem algumas atividades de DR que devem ser incluídas no plano de continuidade de negócios. A norma ISO/IEC 24762 especifica:

- Requisitos para implementação, operação, monitoração e manutenção de serviços e instalações para recuperação de desastres em tecnologias de informação e comunicação (ICT DR);
- Capacidades que os prestadores de serviços terceirizados de ICT DR devem possuir e as práticas que devem seguir;
- Orientação para a seleção de local de recuperação;
- Orientação para os prestadores de serviços de ICT DR para melhorar continuamente os seus serviços.

Para a gestão desse serviço de recuperação de desastres as boas práticas fornecidas pelo modelo ITIL V3 serão utilizadas. O ITIL foca na medição contínua e no melhoramento da qualidade dos serviços de TI entregues, tanto na perspectiva do negócio como do cliente. Segue alguns benefícios segundo Cartlidge et al. (2007):

- Aumento da satisfação dos usuários e clientes com os serviços de TI;
- Melhora na disponibilidade, levando diretamente a um aumento no lucro e na receita dos negócios;
- Economia financeira na redução do retrabalho, perda de tempo e na gestão e uso de recursos;
- Melhora no tempo de mercado para novos produtos e serviços;
- Melhora na tomada de decisões e redução dos riscos.

1.5 Metodologia

Para a fundamentação teórica da monografia foram pesquisados diferentes normas e guias relacionados com a recuperação de desastres. A norma ISO/IEC 24762 por ser uma das mais atuais é bastante utilizada na monografia, além de alguns guias para construção do DRP como o fornecido pela universidade de Michigan.

Para a proposta do Plano de Recuperação de Desastres, a metodologia apresentada na norma ISO/IEC 24762 foi interpretada ao contexto de sistemas críticos, de modo a ficar mais específica às necessidades desse tipo de ambiente. Para esta interpretação as boas práticas fornecidas pelo modelo ITIL V3 foram usadas pensando na qualidade do serviço entregue.

Por fim é apresentado um estudo de caso, considerando um ambiente real e aplicando a proposta apresentada nesse trabalho.

1.6 Estrutura do Trabalho

Este trabalho está estruturado em cinco capítulos básicos, a saber:

1. Introdução: O primeiro capítulo apresenta o contexto inicial a respeito desta monografia, bem como os objetivos que serão atingidos, a justificativa, metodologia e a estrutura do trabalho.
2. Fundamentação teórica: O segundo capítulo apresenta os fundamentos teóricos, que foram utilizados para comparar e analisar a proposta inicial apresentada no capítulo 3.
3. Proposta de Plano para Recuperação de Desastres em sistemas críticos de TI que utilizam mainframe: O terceiro capítulo apresenta a proposta de recuperação de desastres que é um complemento a norma existente, e além disso algumas das melhores práticas do ITIL V3 são utilizadas.

4. Estudo de Caso: O quarto capítulo apresenta um estudo de caso, onde são apresentados dados reais de um sistema crítico que utiliza mainframe.
5. Conclusões: O quinto capítulo apresenta a conclusão e considerações finais a respeito desse trabalho.

2 FUNDAMENTOS TEÓRICOS

2.1 Continuidade de Negócios

A Continuidade de Negócios é definida como a capacidade da organização continuar entregando produtos e serviços em níveis pré-definidos como aceitáveis após um acidente disruptivo (ISO 22301, 2012). Todos os aspectos são considerados, como pessoas, processos, recursos e tecnologias.

Segundo a *Georgetown University* (2012), a base da Continuidade de Negócios é composta por normas, políticas de apoio, orientações e procedimentos necessários para garantir o funcionamento da empresa sem interrupções, independentemente das circunstancias ou eventos adversos. Todo o projeto de sistemas, implementação, suporte e manutenção devem ser baseados nestes fundamentos para se alcançar a Continuidade de Negócios. A Recuperação de Desastres é uma pequena parte da Continuidade de Negócios.

A Continuidade de Negócios conforme o guia de contingência NIST 800-34 (2010) define dois componentes chaves que são utilizados como métricas para a construção de um Plano de Recuperação de Desastres (Figura 2). Esses parâmetros são estabelecidos durante a análise de impacto aos negócios:

- *Recovery Time Objective* (RTO): Define o tempo máximo que um recurso de sistema pode ficar indisponíveis antes que um dano irreparável aconteça à organização.
- *Recovery Point Objective* (RPO): Representa o ponto no tempo antes do desastre, no qual os dados de negócios devem ser recuperados.

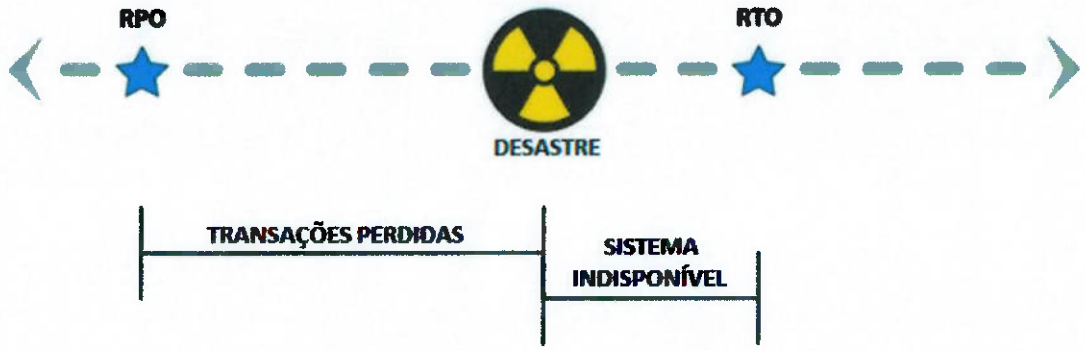

Figura 2 – RPO e RTO (Fonte: bluelock.com – 11/02/15)

2.2 Recuperação de Desastres

Segundo a *Georgetown University* (2012) a Recuperação de Desastres é um componente da Continuidade de Negócios e inclui os processos, políticas e procedimentos relacionados com a preparação para restauração ou manutenção de infra-estrutura tecnológica, que são vitais para uma organização após um desastre natural ou causado pelo homem. No caso de um desastre afetando um site primário, devem existir estratégias e procedimento para a recuperação da infra-estrutura tecnológica em um outro local conforme a figura 3.

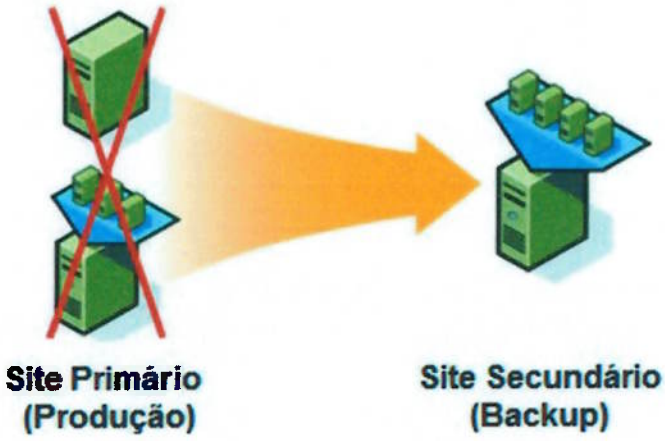

Figura 3 – Situação de desastre (Fonte: WoodITWork.com – 10/09/14)

Conforme a *Georgetown University* (2012) o conceito de Recuperação de Desastres surgiu em meados da década de 70 a partir do momento que as organizações começaram a perceber a dependência nos seus sistemas de computadores. Além disso, os desastres são normalmente classificados em duas categorias:

- Desastres naturais: Inundações, furacões, terremotos, etc.
- Desastres artificiais: Vazamento de materiais perigosos, falha na infra-estrutura, bio-terrorismo, etc.

Enquanto evitar um desastre natural é muito difícil, medidas como um bom planejamento, que inclui medidas de mitigação de problemas, pode ajudar a reduzir ou evitar perdas. Agora no caso de desastres artificiais, a vigilância e planejamento de mitigação são de valor inestimável para evitar ou diminuir as perdas desses tipos de eventos (ROEBUCK, 2011).

Conforme citado anteriormente, o planejamento de Recuperação de Desastres é um componente da Continuidade de Negócios e deve incluir o planejamento para a retomada de aplicações, dados, hardware, comunicações (como redes) e outras infra-estruturas de TI. Um plano de Continuidade de Negócios (BCP) inclui o planejamento para aspectos não relacionados a TI, como o pessoal chave, instalações, comunicação em meio à crise e devem se referir ao plano de Recuperação de Desastres (PRD) para recuperação da infra-estrutura de TI. Alguns controles podem ser utilizados para ajudar a prevenir que eventos desastrosos ocorram (*GEORGETOWN UNIVERSITY*, 2012):

- Medidas preventivas destinadas a evitar que um evento ocorra;
- Medidas de monitoração destinadas a detectar ou descobrir eventos indesejados;
- Medidas corretivas visando a corrigir ou recuperar sistemas após um evento ocorrer.

Quando quaisquer uns desses controles são implementados, eles devem ser sempre documentados e testados regularmente. Os testes regulares garantem que o processo esteja sempre atualizado, e as pessoas envolvidas estejam sempre preparadas e treinadas para que o plano de Recuperação de Desastres seja eficaz.

2.3 Sistemas Críticos de TI

Sommerville (2011) define como sistemas críticos aqueles no qual uma falha do sistema pode resultar em lesões às pessoas, danos ao ambiente ou perdas econômicas extensivas. Esses sistemas podem ser classificados em três tipos:

- Sistema Crítico de Segurança: Esse sistema é desenhado para perder menos de uma vida por bilhões de horas de operação. A falha resulta na perda de vidas, lesão ou dano ao ambiente. Por exemplo, o sistema de proteção de uma fábrica de produtos químicos.
- Sistema Crítico de Missão: É um sistema essencial a sobrevivência do negócio ou da organização. A falha resulta no erro de alguma atividade direcionada a um objetivo. Por exemplo, o sistema de navegação de uma espaçonave.
- Sistema Crítico de Negócio: É um sistema diretamente relacionado ao negócio da empresa. Falha resulta em grandes perdas financeiras. Por exemplo, o sistema de contabilidade do cliente de um banco.

Segundo Sommerville (2011), para os sistemas críticos normalmente a propriedade do sistema mais importante é a confiabilidade. Ela reflete o grau de confiança do usuário, no qual irá operar o sistema como esperado e não irá ocorrer falha no uso normal do sistema. Entretanto existem as situações fora da normalidade como os desastres naturais e artificiais, portanto para esses casos é necessário haver um planejamento de Recuperação de Desastres.

Sommerville (2011) divide a confiabilidade em diferentes propriedades mais básicas:

1. Disponibilidade: É a probabilidade de o sistema estar funcionando e ser capaz de prestar serviços úteis ao usuário a qualquer dado momento.
2. Fiabilidade: É a probabilidade de que a dado período de tempo o sistema irá corretamente entregar os serviços conforme esperado pelo usuário.
3. Integridade: É um julgamento de quão provável o sistema irá causar danos a pessoas ou o ambiente.
4. Segurança: É um julgamento de quão provável o sistema pode resistir a intrusões acidentais ou deliberadas.
5. Reparabilidade: Falhas de sistemas são inevitáveis, entretanto a interrupção causada por uma falha pode ser minimizada se o sistema puder ser corrigido rapidamente. Para que isso aconteça é necessário que seja possível diagnosticar o problema, acessar o componente que falhou e fazer modificações para corrigir o componente.
6. Manutenibilidade: Como os sistemas são usados, novos requerimentos surgem e é importante manter a utilidade do sistema alterando-o para acomodar essas novas exigências.
7. Sobrevivência: É a capacidade de o sistema continuar entregando serviços enquanto sob ataque, e potencialmente enquanto parte do sistema é desativada.
8. Tolerância a erros: O sistema deve ser projetado para que os erros de entrada do usuário sejam evitados e tolerados.

Conforme Sommerville (2011) caso o software não seja muito confiável, é possível obter melhorias significativas a custos relativamente baixos, utilizando uma melhor engenharia de software. No entanto, se as boas práticas já estiverem sendo utilizadas, os custos de melhoria são muito maiores e os benefícios são menores. Com o aumento da confiabilidade do software há cada vez menos falhas, e, por

conseguinte, mais e mais testes são necessários para tentar avaliar quantos problemas permanecem no software. Com o aumento da quantidade e intensidade dos testes, os custos dos sistemas de alta confiabilidade são aumentados drasticamente (figura 4).

Figura 4 – Curva de custo / confiabilidade
(Fonte: Engenharia de Software - Sommerville)

2.4 Mainframes

Há muitos anos os mainframes vêm sendo usados por diversos sistemas críticos devido a sua alta confiabilidade. Segundo Ebbers; O'Brien e Ogden (2006) mainframe é um grande sistema de computador que é usado para hospedar banco de dados, servidores transacionais e aplicações que requerem um alto grau de segurança e disponibilidade. Diferentemente da arquitetura cliente/servidor, a arquitetura do mainframe é centralizada. Os clientes que acessam o mainframe são terminais sem capacidade de processamento ou armazenamento de dados. Todo o poder de processamento do sistema está dentro do próprio mainframe.

Hoje, os mainframes desempenham um papel central nas operações diárias da maioria das grandes corporações do mundo. Enquanto outras formas de computação são utilizadas extensivamente no negócio em várias áreas, o mainframe ocupa hoje um cobiçado lugar nos negócios efetuados por meios eletrônicos (*e-business*). No setor bancário, finanças, saúde, seguros, serviços públicos, governo, e uma infinidade de outras entidades públicas e privadas, o mainframe continua a ser à base do negócio moderno (EBBERS; O'BRIEN E OGDEN, 2006).

O mainframe deve muito de sua popularidade e longevidade à sua confiabilidade e estabilidade inerentes, resultado dos cuidadosos e constantes avanços tecnológicos que vêm sendo feito desde a introdução do System/360 em 1964. Nenhuma outra arquitetura de computadores pode reivindicar tantas melhorias contínuas e evolutivas, enquanto mantém a compatibilidade com versões anteriores (EBBERS; O'BRIEN E OGDEN, 2006).

Devido a esses pontos fortes do projeto, o mainframe é freqüentemente usado por organizações de TI para hospedar os sistemas mais críticos. Estas aplicações tipicamente incluem o processamento de pedidos de clientes, transações financeiras, produção e controle de estoque, folha de pagamento, bem como muitos outros tipos de serviços (EBBERS; O'BRIEN E OGDEN, 2006).

A IBM foi a empresa responsável por introduzir no mercado o primeiro mainframe na década de 60, e foi também quem desenvolveu os primeiros sistemas operacionais (SO) capazes de executarem nessas máquinas. Atualmente esse SO é chamado de z/OS e oferece diversos atributos dos sistemas operacionais modernos, mas ainda mantêm muitas das funcionalidades originais, permitindo a compatibilidade com programas desenvolvidos décadas atrás. Na década de 90, pensando em alta disponibilidade e recuperação de desastres a IBM introduziu o *Parallel Sysplex* no Mainframe. Que nada mais é que um cluster de mainframes agindo em conjunto como um único sistema operacional. O *Parallel Sysplex* combina computação paralela e compartilhamento de dados com o objetivo de dividir a carga transacional para aumentar a performance e disponibilidade (EBBERS; O'BRIEN E OGDEN, 2006).

Os sistemas críticos precisam manter a confiabilidade mesmo em situações de desastre, ou seja, a perda de dados tem que ser praticamente nula e consequentemente os *Recovery Point Objective (RPO)* e *Recovery Time Objective (RTO)* estão cada vez mais próximos de zero. Com esse objetivo a IBM desenvolveu o *Geographically Dispersed Parallel Sysplex (GDPS)* que segundo Ebbers; O'Brien e Ogden (2006) é uma solução de recuperação de desastres e disponibilidade contínua para ambientes mainframes multi-sites. O GDPS espelha automaticamente os dados críticos e balanceia a carga de trabalho entre os sites. Essa solução utiliza da automação e da tecnologia *Parallel Sysplex* para oferecer disponibilidade contínua, movimento eficiente da carga de trabalho entre os sites, gerenciamento de recursos, e recuperação de dados rápida para sistemas críticos em mainframe. Isto proporciona uma solução síncrona que ajuda a garantir que não haja perda de dados em uma situação de desastre.

2.5 ITIL

Muitas empresas já possuem um Plano de Recuperação de Desastres, entretanto muitos deles não seguem um conjunto de boas práticas. Conforme uma pesquisa realizada no *"Prove It" disaster readiness consortium* (2002) apenas 4% das empresas averiguadas seguiam as melhores práticas. Normalmente, cada empresa constrói internamente um processo de recuperação de desastres, e esse processo usualmente pertence a um conjunto restrito de pessoas e não são bem estruturados nem padronizados. Em uma situação de desastre, se não existem processos padronizados de gestão do ambiente, o tempo de indisponibilidade pode ser maior que o RTO definido, causando danos irreparáveis ao negócio da empresa. Portanto é importante a utilização de boas práticas para a gestão de serviços de TI, e a ITIL promove esse objetivo.

A *"Information Technology Infrastructure Library"* (ITIL) é uma biblioteca de infra-estrutura de TI que reúne as boas práticas para a gestão de serviços de TI. Ela foi desenvolvida inicialmente pela CCTA *(Central Computing and Telecommunications Agency)*, atual OGC *(Office of Government Commerce)*. O

OGC é um órgão do governo britânico que tem como objetivo desenvolver metodologias e criar padrões dentro dos departamentos do governo britânico buscando otimizar e melhorar os processos internos.

Segundo Palma e Meirelles (2008) é importante ressaltar que a ITIL não é uma metodologia. Sua filosofia é prover boas práticas para servirem de inspiração, sugerindo onde e porque chegar. Não é uma Norma como a ISO, não é possível aprovar o seu uso dentro de uma empresa através de um checklist ou comprimento de requisitos. A ITIL não é um objetivo, o objetivo é o Gerenciamento de Serviços de TI, ela deve sofrer adaptações para ser implantada na organização, que pode ser uma empresa de qualquer tamanho. Entre os objetivos da ITIL estão:

- Reduzir Custos
- Aumentar a Disponibilidade
- Ajustar a Capacidade
- Aumentar a Eficiência e Eficácia
- Melhorar a Escalabilidade
- Reduzir Riscos

Em 2007 foi lançada a versão 3 da ITIL e as boas práticas estão reunidas em cinco livros principais:

- *Service Strategy* (Estratégia de Serviço)
- *Service Design* (Desenho de Serviço)
- *Service Transition* (Transição de Serviços)
- *Service Operation* (Operação de Serviços)
- *Continual Service Improvement* (Melhora Contínua de Serviço)

Segundo a ITIL V3 (2007), um serviço é um meio de entregar valor aos clientes, facilitando os resultados que os clientes querem alcançar, sem ter que assumir custos e riscos. Esse serviço nasce, se desenvolve, vai para operação e morre. Portanto a estrutura da ITIL v3 é baseada no ciclo de vida do serviço (figura 5).

Figura 5 – Ciclo de vida do Serviço na ITIL v3 (Fonte: ITIL v3)

Segundo BOM (2006), a ITIL define que o gerenciamento de serviços é um conjunto de habilidades da organização para fornecer valor para o cliente em forma de serviços. Ele é composto de funções e processos com o objetivo de gerenciar os serviços durante o seu ciclo de vida. Um processo é um conjunto de atividade inter-relacionadas com um objetivo específico. Possui entrada de dados, informações e produtos com a função de transformar as entradas de acordo com um objetivo específico. Para que os processos funcionem são necessárias pessoas que executem certos papéis. Segundo a ITIL um papel é um conjunto de responsabilidades, atividades e autoridades definidas em um processo e aplicadas a uma pessoa ou equipe.

A ITIL V3 (2007) criou uma maneira formal de estabelecer os papéis para as pessoas envolvidas em determinados processos, que é a matriz RACI. Nessa matriz são definidos os seguintes papéis:

- *Responsável:* São os responsáveis pela tarefa.
- *Autoridade:* É o proprietário do processo.
- *Consultado:* São os consultados na necessidade de compartilhar informação.
- *Informado:* São os informados durante o progresso.

Com a utilização dessa matriz fica claro quem é o responsável pelo processo e quem são os outros envolvidos.

2.6 Norma ISO/IEC 24762

A norma ISO/IEC 24762 foi criada para definir o que as organizações deveriam estar oferecendo em termos de recuperação de desastres para TI. Ela abrange uma ampla gama de problemas que as empresas devem endereçar para garantir que os serviços oferecidos estejam protegidos. Isto inclui construção de prédios, medidas de segurança, fornecimento de serviços de infraestrutura, como energia, água e telecomunicações, e controles ambientais. (KIRVAN,2008).

Esta norma internacional tem por objetivo auxiliar a operação de um Sistema de Gestão da Segurança da Informação (ISMS), fornecendo orientações nos serviços de recuperação de desastres para tecnologias da informação e comunicação (ICT DR), como parte da gestão de continuidade de negócios. A norma inclui os requisitos para implementação, operação, monitoração e manutenção dos serviços de ICT DR.

A norma é baseada em um framework composto de diferentes elementos com o objetivo de prover serviços para a recuperação de desastres (figura 6).

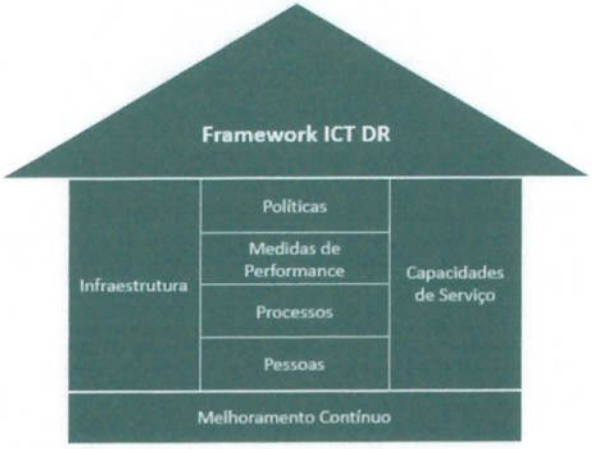

Figura 6 – Framework ICT DR (Fonte: ISO 24762)

As quatro camadas centrais ajudam a definir a infraestrutura e as capacidades de serviço. O melhoramento contínuo destaca práticas que ajudam a melhorar as atividades de recuperação de desastres em áreas específicas (ISO 24762, 2008). Com relação as quatro camadas centrais:

- Políticas: Habilitam os provedores de serviços em ITC DR definir a direção das áreas relacionadas com a recuperação de desastres, e além disso permite a comunicação clara para as partes relevantes sobre os requisitos que podem ser atendidos pela recuperação de desastres.
- Medidas de Performance: Provê a revisão e melhoria dos serviços e ao mesmo tempo garante os meios de mostrar que os serviços estão alcançando os requisitos da organização.
- Processos: Garantem que uma abordagem consistente será adotada nas áreas de serviços de recuperação de desastres, tornando possível a manutenção contínua dos níveis de serviço e facilitando o treinamento do pessoal.
- Pessoas: Refere-se ao conjunto de prestadores de serviço qualificados e experientes. A organização e algumas vezes empresas terceirizadas precisam ajudar a operar e manter as práticas de recuperação de desastres. Além disso a segurança e o bem-estar dos funcionários é mais um aspecto que deve ser cuidado.

Segundo a ISO 24762 (2008), as empresas não devem partir diretamente para a construção de um plano de recuperação de desastres sem antes fazer todo um trabalho de análise. Durante este trabalho é realizada a análise de impacto aos negócios (BIA), que segundo a ISO 24762 é uma avaliação direta e objetiva do impacto financeiro que a organização vai sofrer mediante uma falha da operação dos serviços de TI. Devido a amplitude e complexidade do tema de BIA, ele não é o foco desta monografia e portanto não é abordado em detalhes. Além da análise de impacto aos negócios é necessário identificar as prioridades, e em seguida, a

estratégia correta e mais econômica de continuidade de negócios adequada ao ambiente. Os riscos também devem ser gerenciados para reduzir ainda mais a probabilidade de se declarar um desastre, e reduzir o impacto do desastre ou da falha caso ocorra. A figura 7 mostra a abordagem geral recomendada pela ISO 24762 para a construção de um plano de recuperação de desastres.

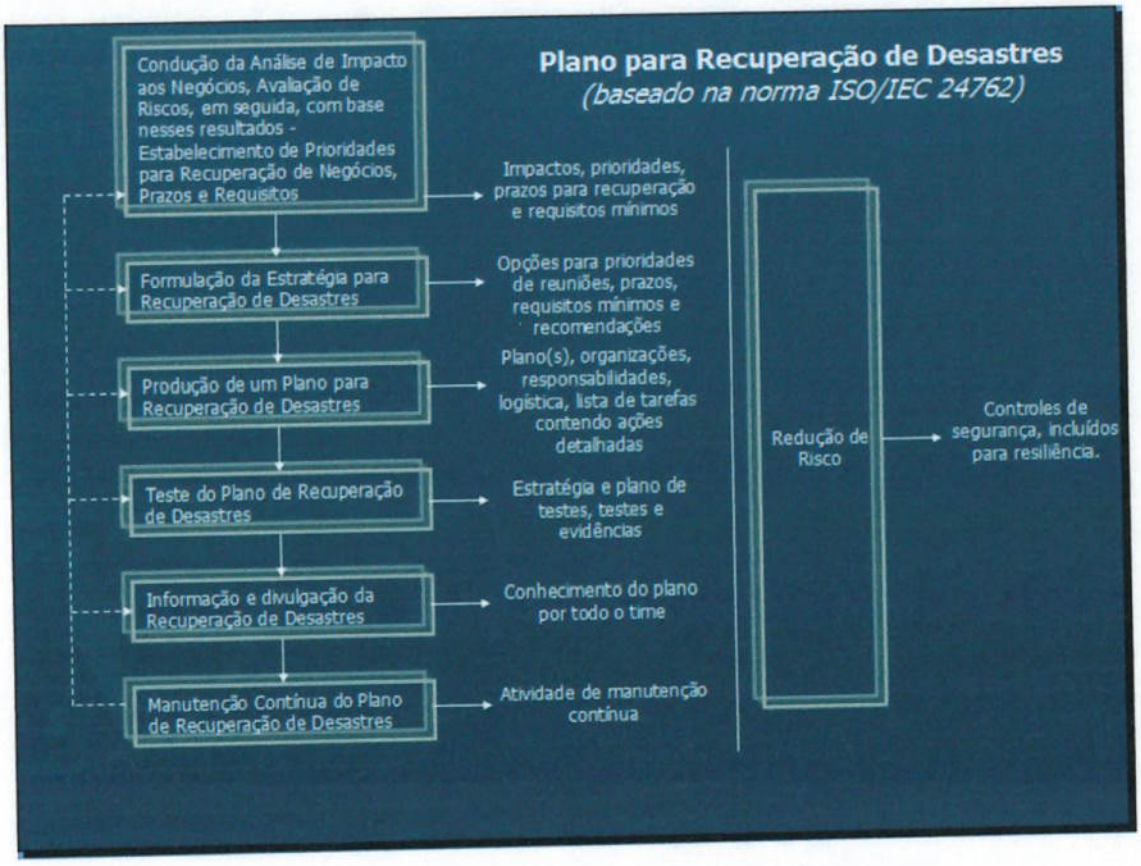

Figura 7 – Abordagem recomendada para construção PRD
(Fonte: ISO 24762)

A ISO 24762 (2008) determina que os estágios de condução da análise de impacto, avaliação de riscos, formulação da estratégia de DR, produção do plano, teste e divulgação são consecutivos, e quando o plano for produzido e testado o estágio de manutenção acontece periodicamente ou após uma mudança significativa que possa afetar a validade do plano. O estágio da redução de risco acontece em paralelo com os outros estágios.

Segundo a norma ISO 24762, cada organização em particular deve identificar um recurso que é responsável pelo plano. Inicialmente esse recurso auxiliará na análise de impacto aos negócios e avaliação de riscos, para posteriormente formular

a estratégia de recuperação de desastres. A norma também especifica que os sites secundários não devem estar localizados em áreas expostas a riscos naturais, como vulcões, terremotos, furacões e caso estejam os riscos devem ser mitigados ou aceitos. Além disso, o site secundário deve estar localizado em uma área de boa acessibilidade, permitindo que os times envolvidos sejam transportados de maneira eficiente.

Na fase de produção do PRD, a norma ISO 24762 especifica que os planos devem ser construídos contendo ações detalhadas, responsabilidades e lista de tarefas. Entretanto a norma ISO 24762 não descreve como a gestão da segurança da informação deve acontecer, nem como os processos e procedimentos devem ser documentados e controlados. Com esse objetivo a ISO/IEC 27002 foi criada e ela procura estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. A norma ISO 27002 especifica uma estrutura para gerenciar a segurança da informação, além de procedimentos de controle e revisão, com o objetivo de manter os documentos como o PRD atualizados e precisos (ISO 27002, 2013).

Com relação a fase de testes, a norma ISO 24762 especifica que testes devem ser realizados e documentados pelo menos uma vez ao ano. Eles também devem ser conduzidos quando ocorrer alguma mudança significativa na organização. Todos os testes devem ser planejados e agendados, de modo a serem executados dentro dos períodos combinados.

Por fim, na fase de manutenção a ISO 24762 especifica que revisões e auditorias são mandatórias no caso de mudanças significativas nos processos.

2.7 Considerações para sistemas críticos que utilizam mainframe

Diferentemente da arquitetura cliente/servidor, a arquitetura mainframe é centralizada. Os clientes que acessam o mainframe são terminais sem capacidade

de processamento e armazenamento de dados, todo o poder de processamento está no mainframe (NIST 800-34, 2010).

No mainframe a disponibilidade e backup dos dados são críticos devido a arquitetura centralizada. O *National Institute of Standards and Tecnology* (2010) sugere algumas medidas importantes que devem ser tomadas antes que um desastre aconteça afetando um sistema crítico que utiliza mainframe:

- As mídias de backup devem ser armazenadas fora do site primário: É considerado como site primário aquele onde os sistemas de missão crítica executam, já o site secundário é um local alternativo no qual os sistemas de missão crítica possam executar no caso de um desastre. A mídia de backup deve ser rotulada, registrada e armazenado externamente em uma instalação segura, com ambiente controlado. O site secundário deve estar localizado suficientemente longe do local original para reduzir a probabilidade de que ambos os sites sejam afetados pelo mesmo evento. Além disso, criptografia de dados pode ser necessária para proteger as mídias de backup, minimizando o risco no caso da mídia de backup ser perdido ou roubado. Atualmente já existem soluções síncronas, que garantem uma cópia do dado no site secundário de maneira quase instantânea.
- As configurações dos sistemas e dados de fornecedores devem ser documentadas: Manter registros detalhados das configurações dos sistemas melhora as capacidades de recuperação. Além disso, os fornecedores que proveem hardware, software e outros componentes essenciais devem ser identificadas no plano de recuperação de desastres.
- A política de segurança de redes e o controle de segurança do sistema devem ser coordenados: A solução de recuperação de desastres em mainframe deve incluir a duplicação de interfaces e infraestrutura de telecomunicações, bem como as políticas de segurança de redes, tais como rigorosos controles de acesso.

O *National Institute of Standards and Tecnology* (2010) especifica que componentes de sistema redundantes são críticos para assegurar que a falha de um componente do sistema, tal como uma fonte de alimentação, não provoque uma falha total no sistema. Como mainframes são centralizados e normalmente processam grandes sistemas críticos, pode ser necessário uma solução de backup de energia de longo prazo. Um gerador a gás ou diesel pode garantir que o processamento do mainframe não seja interrompido por falta de energia, mitigando assim certas situações que poderiam provocar uma situação de desastre.

No mercado existem diferentes soluções de redundância para discos, que são extremamente importantes para a recuperações de desastres minimizando o RPO e RTO. Devido a arquitetura centralizada do mainframe, existem algumas estratégias de contingência que mantêm um sistema de backup disponível e funcional no site secundário. Segundo o PAS 77 (2006), existem os seguintes modelos para a definição do site secundário:

- Ativo/Contingência (*"Cold Site"*): provê o espaço mas não fornece a infraestrutura necessária para retornar a operação rapidamente.
- Ativo/Backup (*"Warm Site"*): duas estruturas separadas são mantidas, mas a produção só é executada no site primário, o site secundário somente é ativado quando ocorre um grave incidente.
- Ativo/Alternativo *("Hot Site")*: a produção opera em um site com uma cópia espelhada, em *standby*, no site secundário.
- Ativo/Ativo ("*Hot Site*"): no funcionamento normal ambos os sites operam no modelo de balanceamento de cargas entre os sistemas.
- Multi-site/Híbridos: modelo utilizado por algumas organizações, necessitam de mais de dois sites.

3 PLANO DE RECUPERAÇÃO DE DESASTRES

3.1 Proposta

A norma ISO 24762 é genérica, não contemplando as características particulares dos sistemas críticos, nem as tecnologias envolvidas. A norma tem o foco na especificação da infraestrutura do site secundário, levando em consideração questões como o controle de acesso, telecomunicações e energia. Em contrapartida, a análise de impacto aos negócios e avaliação de riscos não são tratadas e nenhum plano de documentação específico é recomendado para a implementação de um PRD.

Interpretando a norma ISO 24762 ao contexto de recuperação de desastres em sistemas críticos, esta monografia propõe tópicos que devem ser considerados para a construção de um plano de recuperação de desastres. Analisando a estratégia de continuidade de negócios como um meio de entregar valor aos clientes, garantindo alta disponibilidade e minimizando o risco de uma situação de desastre afetar os negócios da empresa, esta monografia define a recuperação de desastres como um serviço, e esse serviço apresenta um ciclo de vida. Essa visão do ciclo de vida é embasada no ITIL V3, entretanto é adaptada para mostrar a recuperação de desastres como um serviço, conforme pode ser visualizada na figura 8:

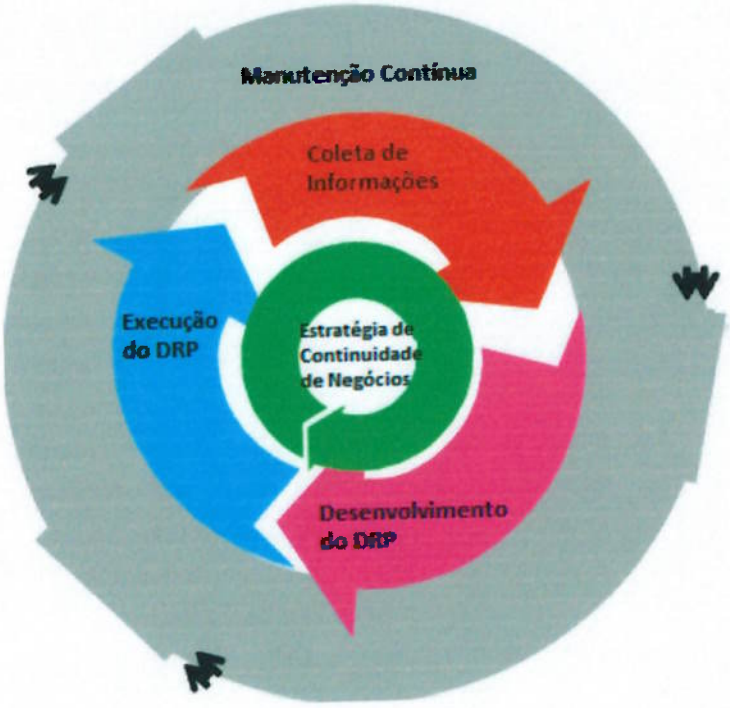

Figura 8 – Proposta para a construção e manutenção de um PRD
(Fonte: O Autor, 2014)

A figura 8 propõe uma interpretação da norma ISO 24762 ao contexto de recuperação de desastres em sistemas críticos. Conforme descrito no capítulo 2, a ISO propõe uma abordagem linear e consecutiva, onde é possível modificar uma fase somente durante a revisão periódica. Já a abordagem proposta nesta monografia foi construída visando as aplicações críticas que dependem de um dinamismo maior, já que em situações de falha é necessária uma atuação assertiva e direta para resolver o problema o mais rápido possível.

Nesta monografia a visão linear foi substituída por uma cíclica, onde o processo está em contínua mudança. Logo após a execução de um teste de DR, informações sobre a execução já são coletadas, os riscos e prioridades são modificados e consequentemente o plano é atualizado para a próxima execução. Além disso a estratégia pode ser modificada a qualquer momento, e o processo tem que se adaptar à nova estratégia.

3.1.1 Estratégia de Continuidade de Negócios

Na abordagem da norma ISO 24762, o primeiro ponto do planejamento do PRD é a análise impacto aos negócios e avaliação de riscos. Já a proposta desta monografia considera como primordial iniciar o planejamento pela determinação da estratégia de continuidade de negócios. Ambientes e sistemas distintos, precisam de estratégias específicas, pois cada sistema e cliente suporta um determinado período de indisponibilidade. Dependendo das estratégias adotadas, os riscos e prioridades serão diferentes afetando a análise de impacto e avaliação de riscos.

A norma ISO 24762 não especifica nenhum fator a ser considerado na estratégia de continuidade de negócios, entretanto, sob essa ótica a proposta desta monografia considera alguns fatores do guia de contingência NIST 800-34 (2010) que são significativos para a definição da estratégia em sistemas críticos. São fatores que variam de acordo com as características e necessidades de negócios das empresas:

- Disponibilidade: Cada organização tem a sua suscetibilidade a indisponibilidade. O custo envolvido com a indisponibilidade varia de acordo com o negócio, e portanto o tempo de indisponibilidade permitido também é variável.
- Custo: Cada organização está disposta a investir até certo valor para manter baixa a indisponibilidade, e consequentemente obter um impacto menor.

Segundo Hiles (2007), quanto menor a perda de dados maior o custo necessário para manter a infraestrutura de uma replicação em tempo real. Na figura 9 é possível verificar que caso o tempo máximo aceitável para a recuperação seja pequeno, o custo da solução de recuperação de desastres é mais alto. E no caso contrário, quanto maior o tempo de recuperação, maiores são os impactos e custos para os negócios da corporação.

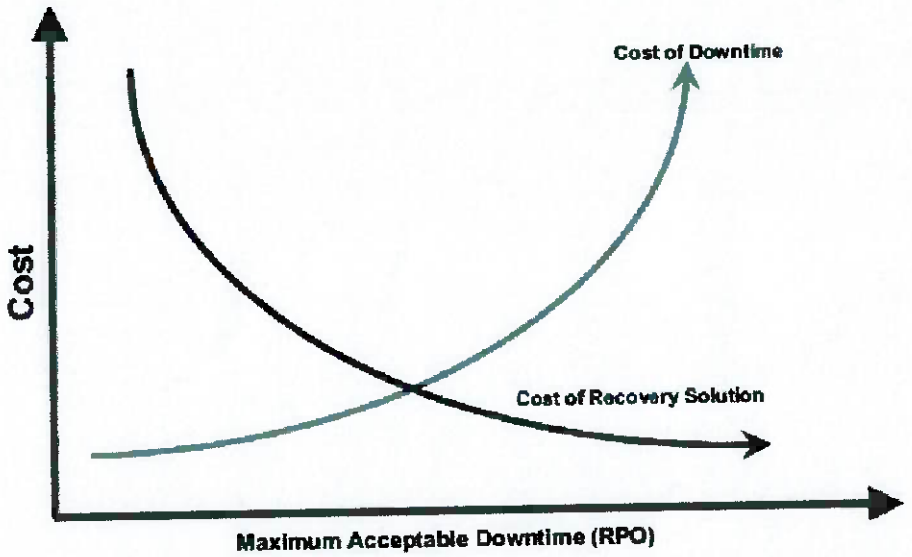

Figura 9 - Custo x Benefício para recuperação de desastre. (Fonte: Hiles, 2007)

Outra característica que deve ser analisada, é o modelo de site secundário adotado. Conforme descrito no capítulo 2, o modelo escolhido influencia de maneira crucial no tempo de indisponibilidade. Considerando os sistemas críticos em mainframe, a estratégia utilizada não pode tolerar perda de dados e em certos casos também não pode tolerar interrupção no funcionamento do sistema. Para os casos no qual interrupção não é tolerada, o modelo recomendado é o de Ativo/Ativo ou Ativo/Passivo, onde existe um mainframe ativo e funcional que é uma réplica do ambiente primário (produção), e no caso de desastre o ambiente secundário assume a carga de maneira imediata não havendo perda de dados nem impacto significativo ao funcionamento normal do sistema.

Por fim, o último ponto a ser analisado na estratégia de continuidade de negócios é a escolha do site secundário. Nesse ponto, a recomendação da norma ISO 24762 sobre a localização do site secundário deve ser seguida com o objetivo de minimizar e mitigar riscos. Entretanto, no caso de aplicações críticas alguns cuidados especiais devem ser tomados, como a distância entre os sites primário e secundário pode ser impactante para o funcionamento da aplicação. Caso seja utilizado alguma tecnologia de replicação síncrona, o dado somente é considerado gravado quando for gravado nos dois sites. Portanto, quanto maior a distância entre sites, maior o tempo de gravação do dado e consequentemente a aplicação demora

mais tempo para executar. Esse aumento de tempo de execução pode ser impactante, impossibilitando o funcionamento da aplicação.

3.1.2 Coleta de Informações

Após as decisões da estratégia de continuidade de negócios, o próximo ponto a ser analisado e discutido para a construção do PRD é a coleta de informações. É nessa fase que a avaliação de impacto e riscos acontecerão, diferentemente da norma ISO 24762, essa fase acontece após a escolha da estratégia de continuidade de negócios e durante a coleta de informações alguns conceitos do ITIL são utilizados. Algumas das boas práticas do ITIL como a matriz RACI, o ciclo de vida de um serviço e controle de documentação são utilizadas na proposta desta monografia com o objetivo de aumentar a eficiência e eficácia do processo de DR, além de reduzir os riscos com o uso de uma documentação padronizada.

Nessa fase um coordenador de DR deve ser escolhido para auxiliar na construção e manutenção do plano de recuperação de desastres. Esse coordenador deve apresentar experiência na gestão de pessoas, capacidade de lidar com diferentes grupos dentro da empresa além de ter um conhecimento técnico, mesmo que básico do ambiente e das aplicações críticas do cliente.

É responsabilidade do coordenador de DR, fazer reuniões com os diversos times envolvidos na recuperação dos sistemas e coletar dados e procedimentos técnicos sobre o funcionamento dos sistemas. Nesse ponto, começa a ser construída a tabela de contatos com todos envolvidos na recuperação de desastres. Baseando-se nas boas práticas do ITIL, uma matriz RACI deve ser construída, para a atribuição de responsabilidades intrínsecas ao PRD. Essa matriz contribui para a divisão clara das tarefas entre as pessoas envolvidas no DR. No caso de diversas aplicações críticas, essa matriz facilita a identificações dos donos das aplicações e das pessoas responsáveis por atuar em situações de problemas.

Durante a fase de coleta de informações, uma análise de impacto aos negócios (BIA) e avaliação de riscos devem ser feitas. A norma ISO 24762 cita os dois processos, mas não especifica sobre a aplicação dos mesmos, além disso, devido a magnitude e complexidade do tema de BIA, ele não é o foco desta monografia e portanto não é abordado em detalhes.

Na análise de impacto aos negócios, o coordenador de DR juntamente com um recurso que conheça o negócio da empresa determina o que necessita ser recuperado e em quanto tempo. As aplicações críticas devem ser priorizadas, devido à importância e repercussão ao negócio do cliente. O resultado dessa análise é o relatório de avaliação de impacto.

O relatório de avaliação de impacto gerado durante o BIA deve conter todos os sistemas / aplicações envolvidas com o negócio do cliente, suas funções e informações de contatos dos responsáveis. Essas aplicações devem ser classificadas de acordo com a sua criticidade e impacto no caso de indisponibilidade. Os impactos devem ser classificados como impacto ao cliente, financeiro e regulamentar. Por fim o tempo máximo de indisponibilidade aceito para aquele sistema deve ser especificado, entretanto essa informação é proveniente do BIA e não é o alvo desta monografia não sendo abordada em detalhes. Baseado nos dados levantados durante a análise de impacto aos negócios é possível a definição dos seguintes parâmetros (NIST 800-34, 2010):

- *Recovery Time Objective* (RTO): Representa o tempo de indisponibilidade, quanto maior esse tempo maior o impacto aos negócios.
- *Recovery Point Objective* (RPO): Representa o quanto dos dados serão perdidos. Para algumas aplicações críticas esse valor tem que ser igual a zero, para não causar danos irreparáveis ao negócio.

Com relação a avaliação de risco, todos os possíveis eventos disruptivos que possam impactar negativamente a capacidade da empresa funcionar devem ser identificados. Segundo a norma ISO 24762 esses eventos disruptivos podem ser desde:

- Desastres ambientais como fogo, enchentes, terremotos, etc.
- Indisponibilidade deliberada como ato terrorista, guerras, roubos, etc.
- Falha de sistemas que inclui falha elétrica, falha no equipamento ou até mesmo bug no software.
- Falta de pessoal capacitado, com conhecimento nas ferramentas de TI utilizadas.

O resultado desse levantamento, é o relatório de riscos. Todos os eventos identificados serão classificados de acordo com a probabilidade de acontecerem e o impacto utilizando-se uma escala entre zero e um (sendo "zero" possibilidade/impacto nulo e "um" o inverso). Deve-se tomar um especial cuidado com os sistemas críticos, para determinar a probabilidade do mesmo se tornar indisponível e documentar a aceitabilidade desses riscos pela organização. Além disso, no caso dos mainframes onde a replicação síncrona é utilizada, a distância entre os sites pode ser um risco e deve ser calculado, pois distâncias muito grandes podem impactar o funcionamento normal dos sistemas. O dado somente é considerado gravado, quando for gravado nos dois sites, portanto, quanto maior a distância entre sites, maior o tempo de gravação do dado e consequentemente a aplicação demora mais tempo para executar.

Ao fim dessa etapa, o coordenador de DR já tem construído a lista de contatos e a matriz RACI com as devidas responsabilidades. Além disso, os relatórios de avaliação de impacto e riscos auxiliam no desenvolvimento do PRD, determinando quais aplicações devem ser recuperadas e qual prioridade.

3.1.3 Desenvolvimento do PRD

A construção do plano de recuperação de desastres é responsabilidade do coordenador de DR que foi determinado na fase de coleta de informações. O coordenador de DR trabalha em conjunto com diferentes times de TI considerando

as responsabilidades definidas na matriz RACI e os dados da tabela de contatos. No âmbito de uma empresa com sistemas críticos, esse coordenador deve identificar especialistas em hardware, software e processos para auxiliá-lo. De acordo com a norma ISO 27002 com relação a documentação, é necessário definir uma estrutura hierárquica para a organização de documentos. Os documentos relacionados a recuperação de desastres são classificados em políticas, normas, procedimentos e controles / métricas, estabelecendo um ciclo de melhoria contínua do serviço. Ademais, os documentos devem ter um controle de revisão, identificando os documentos e responsáveis, e classificando-os como ativos ou revogados. Conforme as boas práticas da norma ISO 27002, é recomendado que os documentos sejam revisados pelo menos uma vez ao ano.

Conforme especificado no capítulo 2, a norma ISO 24762 não detalha como o plano de recuperação de desastres deve ser construído. Esta monografia se baseou no guia da Universidade de Michigan para propor o PRD. O guia da Universidade de Michigan (2014) foi construído especificamente para tratar de sistemas universitários não críticos, nesta monografia esse guia foi utilizado devido a sua divisão do PRD em fases bem definidas e práticas, porém, levando em consideração os sistemas críticos em mainframe. Portanto, considerando os sistemas críticos é recomendado que o plano de recuperação de desastres contenha as seguintes seções:

- Controle do documento: Nessa seção é importante definir os donos do processo (documento), incluindo nome, e-mail, função e telefone. Também devem ser identificados os aprovadores do documento. Por fim, deve conter uma tabela com um controle de versão contendo o nome de quem realizou a revisão, a data e o objetivo da revisão.
- Objetivo e escopo: Nesta seção os objetivos primários e secundários serão especificados. Conforme os dados do relatório de avaliação de impacto, é necessário classificar quais aplicações e banco de dados estão incluídos e excluídos da recuperação, além de especificar se somente aplicações críticas serão recuperadas. É recomendado a inclusão de uma tabela contendo os objetivos e quais os critérios para completá-los com sucesso, além de outra

tabela contendo quais os sistemas, aplicações e banco de dados estão no escopo do DR. Nessa tabela de escopo, é interessante a identificação da categoria dos sistemas, como produção, teste ou desenvolvimento.

- Premissas: As premissas feitas durante a criação do documento devem ser escritas na forma de lista. Uma das premissas a serem consideradas, é o critério para a declaração de uma situação de desastre. A detecção de um evento que pode resultar em desastre é responsabilidade do time de segurança / time técnico alocado localmente no ambiente de TI da empresa. Assim que o time de segurança / técnico descobrir a situação de emergência ou receber informação sobre a mesma, devem entrar em contato com o coordenador de DR, que avalia a situação e tem a responsabilidade de invocar uma situação de Recuperação de Desastres, seguindo as informações do PRD.
- Dependências: Devido à complexidade dos sistemas críticos, é necessário a existência de uma seção no PRD, apresentando as dependências entre os diferentes sistemas, máquinas e times envolvidos. Essa seção deve conter diferentes tabelas e diagramas, mostrando a dependência na execução dos diferentes procedimentos de restauração.
- Papéis e responsabilidades: Para essa seção é necessário a criação de uma tabela classificada de acordo com os sistemas, contendo os papéis e responsabilidades, além dos contatos primários e secundários.
- Procedimentos técnicos de recuperação: Esta é a seção mais importante do plano, que são os procedimentos para recuperar os sistemas após um desastre. Devem-se ter procedimentos para inicializar o hardware e softwares no ambiente secundário. Além disso, os sistemas de middleware, banco de dados, redes e por fim as aplicações também devem ser recuperadas. Estes procedimentos devem ser técnicos e bem descritos de modo que uma pessoa que não conheça detalhadamente o sistema do cliente, possa seguir com sucesso os procedimentos. Além dos

procedimentos de recuperação separados por área, é recomendado a inclusão de uma tabela resumida contendo os principais passos na recuperação dos sistemas, e a ordem de execução desses passos. Esta tabela deve conter também um campo com o tempo estimado da execução daquele passo, além de outro campo com o tempo real da finalização da execução daquele passo.

- Procedimentos pós-desastre: Nessa seção são estabelecidos os critérios e procedimentos para que os sistemas produtivos retornem do site secundário ao primário, após a situação de desastre se normalizar. Em muitos casos, os procedimentos serão semelhantes aos definidos nos procedimentos técnicos de recuperação.
- Apêndice: A última parte do plano é um apêndice contendo diferentes formulários como uma lista de contatos, contendo as informações de todas as pessoas envolvidas no PRD. Tambem deve ser incluído ao apêndice uma tabela contendo as mudanças recomendadas ao plano e por fim um registro dos problemas encontrados na execução do PRD.

Após a finalização do desenvolvimento do PRD, em concordância com as melhores práticas do ITIL e as recomendações relacionadas ao controle de documentação proposto pela ISO 27002, o PRD deve ser aprovado. Como a ISO 24762 não contempla detalhadamente a criação do PRD, nessa fase de desenvolvimento ela não foi utilizada diretamente. A aprovação do documento deve ser feita por alguém com responsabilidade e autoridade conforme a tabela RACI, construída durante a fase de coleta de informações.

3.1.4 Execução do PRD

Após o plano já estar construído e aprovado é necessário a execução de um primeiro teste para a validação do plano. Este teste é importante para determinar a efetividade do PRD e identificar os tempos reais para a recuperação dos diferentes sistemas.

Após a implementação do plano de recuperação de desastres na empresa, é responsabilidade do coordenador de DR realizar testes periódicos. Conforme a norma ISO 24762, estes testes devem ser pelo menos anuais e deverão incluir diferentes times desde suporte técnico ao time do aplicativo. Tratando-se de sistemas críticos em mainframe existe a possibilidade dos testes de recuperação de desastres durarem mais de um dia devido à complexidade dos sistemas, nessas situações é importante sempre ter definido um contato secundário para que possa substituir as pessoas chaves devido ao cansaço. Além disso, esta monografia propõe o uso de meios visuais para diferenciar os ambientes de teste dos de produção. No caso da arquitetura mainframe, onde o acesso ao sistema é centralizado e os terminais de acesso 32x70 são muito parecidos, existe a possibilidade de que comandos sejam dados erroneamente em produção podendo causar uma verdadeira situação de desastre. É possível alterar as telas de *logon* dos sistemas mainframe, de modo a exibir mensagens em destaque diferenciando os sistemas de teste dos de produção. Além disso, nos procedimentos técnicos de recuperação descritos no PRD, deve existir um *checklist* para verificação se realmente é um ambiente de teste que está sendo utilizado.

Com a execução dos testes periódicos, o ambiente e os times envolvidos devem estar preparados para a execução do PRD em uma situação real caso ela venha a acontecer, após a declaração de uma situação de desastre pelo coordenador de DR.

3.1.5 Manutenção Contínua

Esta monografia propõe que o coordenador de DR seja responsável por rever as mudanças no ambiente, na tecnologia e nos procedimentos e deve incluí-las ao plano. No caso do mainframe, existem diferentes subsistemas executando aplicações críticas e diferentes áreas são afetadas, portanto é crucial que o coordenador de DR tenha um papel de mediador entre as diferentes áreas, e coordene os impactos das mudanças de versão e funcionalidades dos softwares,

além de atualizações de hardwares que possam afetar o PRD. Essa manutenção deve ser periódica, e complementando a norma ISO 24762 esta monografia propõe a execução dessa revisão um pouco antes dos testes periódicos.

Durante a revisão o coordenador de DR executa um conjunto de reuniões com todas as pessoas envolvidas no processo de recuperação de desastres. Nessas reuniões todos os procedimentos de recuperação são revistos, a tabela de contatos é atualizada e a análise de impacto é modificada caso a prioridade de alguma aplicação tenha sido alterada. Todas as alterações no PRD são documentadas seguindo as melhores práticas conforme descrito na fase de desenvolvimento do PRD.

A norma ISO 24762 estabelece como parte da manutenção contínua a execução de auditorias periódicas, que podem ser internas ou externas, com o objetivo de verificar como o plano está funcionando, e principalmente a eficácia e qualidade da recuperação das aplicações críticas em uma situação de desastre. Essa recomendação deve ser seguida prezando em garantir a qualidade do PRD.

4 ESTUDO DE CASO

4.1 Configuração do sistema crítico

Desde a década de 60 com o lançamento do system/360 da IBM, as instituições financeiras vêm utilizando os mainframes para a execução de operações de *back-office*. Com o advento do *internet banking,* o processamento de dados das instituições financeiras passaram a ter que estar disponíveis por 24 horas no dia e 7 dias na semana (24x7). Para garantir este nível de disponibilidade os bancos investem em soluções e tecnologias focando na continuidade de negócios.

Este capítulo tem a finalidade de apresentar um estudo de caso mostrando a aplicação da proposta de PRD apresentada nesta monografia, para um sistema crítico bancário que utiliza mainframe. Os dados aqui apresentados se referem a um banco americano, cujo nome é omitido, além disso certas características e nomes de aplicações são alterados por questão de confidencialidade.

O sistema crítico aqui apresentado é o de conta corrente, que é responsável por manter todos os dados e status da conta corrente de todos os clientes do banco. Todos os dados de negócio desse sistema estão armazenados no DB2 para z/OS que é um banco de dados relacional desenvolvido pela IBM. Existem diferentes transações que acessam esses dados, e todas essas transações rodam via IMS (Information Management System) que é um gerenciador de transações também desenvolvido pela IBM (Figura 10). Todos esses subsistemas estão executando em um mainframe z196 com 13 processadores quad-core de 5.2 GHz e por volta de 400 GB de memória. Essa máquina pode chegar a executar 25000 Mips, que são milhões de instruções por segundo.

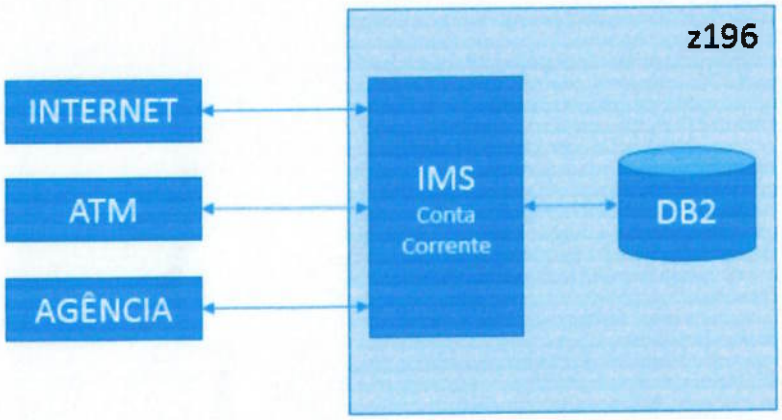

Figura 10 – Sistema Crítico de Conta Corrente executando no Mainframe

A aplicação de conta corrente é acessada por um conjunto de transações que em horários de pico podem chegar a mais de 1000 transações por segundo. O tempo de resposta varia de acordo com a transação e sua complexidade.

Antes da aplicação da proposta o cliente já possuía um site secundário configurado e preparado para situações de desastre localizado a 10 Km do site primário. Esse site era um "*Warm Site*" no modelo Ativo / Backup, onde todos os dados eram copiados de maneira assíncrona a cada 30 minutos. Esta configuração garantia um RPO que poderia chegar a 30 minutos e um RTO de até 2 horas.

O plano de recuperação de desastres utilizado pelo cliente, não seguia as melhores práticas. Eram apenas vários procedimentos técnicos operacionais anexados em conjunto. Não existia padronização desses documentos, nem controle de versão, e muitas das informações de contatos estavam desatualizadas. Testes eram realizados anualmente, entretanto no último teste conseguiram restaurar o sistema de conta corrente, mas fora do prazo estipulado.

4.2 Aplicação da proposta

No estudo de caso apresentado nesse capítulo, foi implementado uma solução síncrona utilizando o GDPS, garantindo que todos os dados da aplicação estariam replicados no site secundário. Entretanto, os subsistemas que garantem a execução das aplicações ainda executariam no site primário, e no caso de uma situação de desastre eles deveriam ser reinicializados no site secundário.

O plano de recuperação de desastre que o cliente utilizava anteriormente, foi aprimorado de acordo com a proposta apresentada nesta monografia, de modo a se adequar a solução síncrona e seguir algumas das melhores práticas propostas.

4.2.1 Estratégia de continuidade de negócios

Devido a criticidade do sistema de conta corrente, a nova solução de recuperação de desastres procurou garantir um RPO igual a zero, não permitindo inconsistência nos dados, nem perda de dados. Com relação ao RTO, seria aceitável pelo cliente a indisponibilidade de até uma hora que seria o tempo de reiniciar os sistemas, entretanto quanto menor a indisponibilidade menor o impacto ao cliente.

A nova solução confinuaria utilizando o site secundário localizado a 10 Km, entretanto ele passaria a ser um "Hot Site" no modelo Ativo/Passivo, onde os dados seriam copiados de maneira síncrona, contudo os sistemas não estariam ativos no site secundário (Figura 11). Essa cópia seria feita utilizando o protocolo PPRC (Peer to peer remote copy), no qual os volumes contendo os dados de sistema e de negócios seriam replicados no site remoto de maneira síncrona. Cada gravação no volume do site primário seria também executada no secundário, e o I/O somente seria considerado completo quando ambas as gravações fossem realizadas.

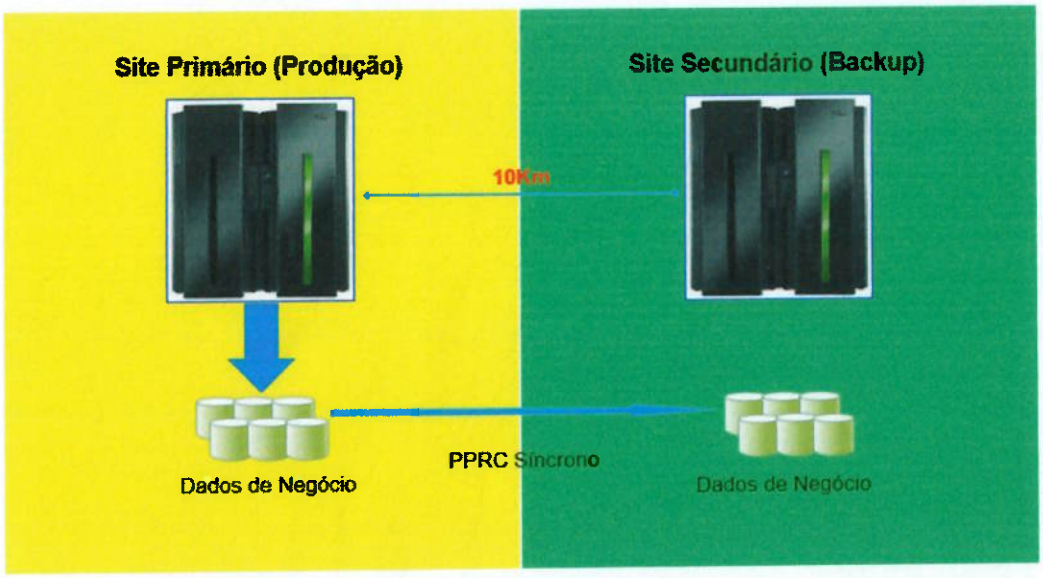

Figura 11 – Sistema Crítico de Conta Corrente executando no Mainframe

No caso de uma falha nos discos de produção contendo os dados de negócio da conta corrente, uma automação detectaria a situação de erro e em questão de segundos a aplicação executando no site primário passaria a acessar os dados do site secundário, conforme a figura 12.

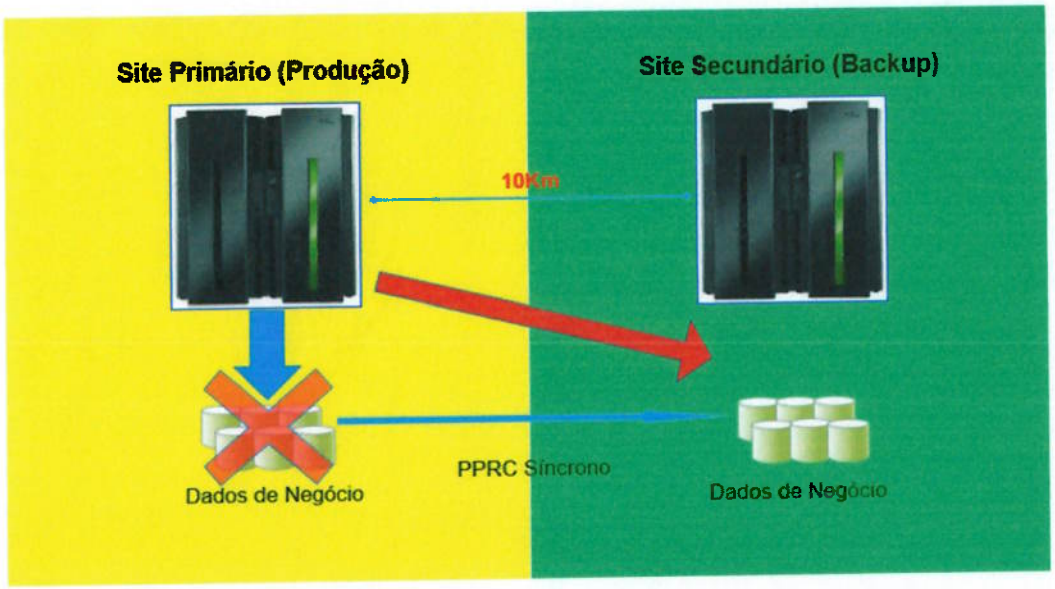

Figura 12 – Falha nos volumes contendo dados de conta corrente

No caso de uma situação de desastre onde todo o site primário fosse afetado, os dados de negócio já se encontrariam no site secundário garantindo um RPO igual

a zero, entretanto seria necessário reiniciar os sistemas nesse site. Esse tempo de reinicialização que poderia ser por volta de minutos garantiria também um RTO em torno de minutos (Figura 13).

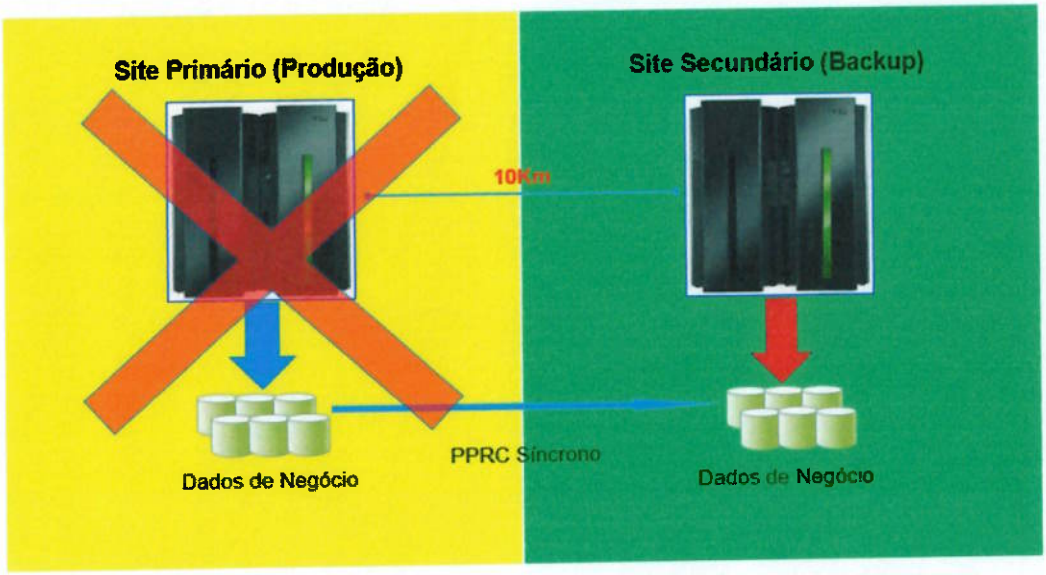

Figura 13 – Situação de desastre no site primário

4.2.2 Coleta de Informações

O coordenador de DR escolhido possui experiência em gestão, lidando com diferentes grupos de pessoas, além de conhecimento no ambiente e suas aplicações críticas.

Antes da implementação da proposta, o cliente já possuía uma tabela contendo os dados de todas as pessoas responsáveis pela recuperação e restauração do sistema de conta corrente no site secundário. Entretanto essa tabela foi revista e modificada contemplando os seguintes dados dos contatos primários e secundários: nome, telefone, e-mail, papel e responsabilidades.

Além disso, ainda baseado na proposta desta monografia foi criado uma matriz RACI, definindo os papéis e responsabilidades. Esta matriz foi construída definindo os papéis de dono da atividade (A), de responsável pela execução (R), de

consultado (C) e de informado (I). Segue uma tabela resumida, focando no caso da recuperação do sistema crítico de conta corrente (tabela 4.1):

Atividade	Coordenador de DR	Time Mainframe	Time da Aplicação	Cliente
Construção do PRD	RA	R	R	CI
Declaração de situação de desastre	RA	C	C	I
Monitoração e acompanhamento do sincronismo entre sites	I	RA	-	-
Restauração de subsistemas no site secundário	I	RA	I	I
Recuperação da aplicação de conta corrente	I	I	RA	I
Garantir que os acordos de SLA sejam alcançados	RA	R	R	CI
Documentar e anotar todos os tempos e problemas encontrados na execução do PRD	RA	R	R	I

Tabela 4.1 – Matriz RACI

Ainda considerando o sistema de conta corrente, foi necessário a construção de um relatório contemplando a análise de impacto aos negócios (tabela 4.2), com o objetivo de priorizar a inicialização das aplicações e determinando o tempo máximo de indisponibilidade que impacta a determinação do RTO e RPO. Antes da implementação da proposta, o cliente não possuía um relatório específico para o sistema em questão. Segue uma tabela resumida contemplando o sistema de conta corrente:

Aplicação	**Conta Corrente**
Função	Responsável pelo controle da conta corrente dos

	clientes do banco. Contém o controle de saldo, saques, débitos e transferências. É acessado por diversas outras aplicações.
Contato	Nome, Telefone, E-mail
Classificação da função	Crítica
Impacto ao cliente	Alto
Impacto financeiro	Alto
Impacto regulamentar	Médio
Tempo máximo de indisponibilidade	1 hora para funções críticas
Caso a função não seja recuperada	Impacto financeiro - Transações bancárias não serão executadas Impacto ao cliente – Resultados decrescente na reputação do banco Impacto regulamentar – Possibilidade de pagar multa devido a indisponibilidade

Tabela 4.2 – Análise de impacto aos negócios

Por fim, segundo a proposta desta monografia o último relatório construído foi o de riscos. Segue uma tabela resumida contemplando algumas estimativas de risco do sistema de conta corrente (tabela 4.3):

Evento	Probabilidade de acontecer	Impacto	Fator de risco (Prob X Impa)
Falha de sistemas afetando o conta corrente	0,4	0,9	0,36
Deadlocks afetando o banco de dados da aplicação conta corrente	0,7	0,4	0,28
Degradação dos links síncronos entre o site primário e secundário	0,6	0,6	0,36
Lentidão no conta corrente devido a distância entre sites	0,7	0,5	0,35

Tabela 4.3 – Análise de riscos

4.2.3 Desenvolvimento do PRD

De acordo com as tabelas e documentos gerados na fase de coleta de informações, o plano de recuperação de desastres foi construído. Neste caso de uso, é apresentado uma descrição do PRD que foi gerado embasado na proposta dessa monografia.

A primeira seção do documento gerado foi a de controle, no qual o coordenador de DR foi identificado como dono do processo, e todos os seus dados foram definidos. Também foram identificadas pessoas do cliente responsáveis pela aprovação do documento. Por fim, o histórico de revisões foi incluído ao documento (tabela 4.4).

Revisão	Data	Responsável	Objetivo da revisão
1	XX/XX/XXXX	Coordenador de DR	Criação do PRD

Tabela 4.4 – Histórico de revisões

Na próxima seção os objetivos foram definidos, além dos sistemas e bancos de dados. O objetivo primário definido é a restauração do sistema crítico de conta correntes, tanto os ambientes de produção como homologação poderão ser recuperados pelo plano. Como se trata apenas de um sistema crítico, o relatório de análise de impacto não foi utilizado para dar prioridades às recuperações, entretanto ele foi utilizado para dar prioridade à recuperação dos subsistemas necessário para a execução da aplicação de conta corrente. Nessa seção também foi definido a tabela de escopo (tabela 4.5):

	Dentro do escopo da recuperação	Fora do escopo da recuperação
Plataformas envolvidas	Produção e homologação	Desenvolvimento e teste
Máquinas envolvidas	Mainframe 1	Mainframe 2 e 3
Subsistemas envolvidos	IMS 1	IMS 2 e IMS 3
Banco de dados envolvidos	DB2 1	DB2 2 e DB2 3
Aplicações envolvidas	Conta corrente	Outras aplicações (Seguro, financiamento, etc)

Tabela 4.5 – Tabela de escopo

A próxima seção conforme descrita nessa monografia é a de premissas. Nos tópicos abaixo está um breve resumo das premissas, de maneira genérica:

1. No site primário existem funcionários de segurança monitorando a infraestrutura por situações de desastre, além de técnicos monitorando por qualquer situação anormal dos sistemas.
2. Em situações de emergência, ou funcionamento anormal dos sistemas o coordenador de DR é informado e avalia se uma situação de desastre deve ser declarada.
3. O coordenador de DR e times envolvidos estão disponíveis para realizar as atividades definidas no PRD.
4. Todos os envolvidos podem ser notificados e localizados na situação de desastre.
5. O PRD está atualizado, considerando as definições de todos os softwares e hardwares.
6. Com relação aos procedimentos técnicos de recuperação é assumido que os times técnicos tenham *skill* e acesso a todos os sistemas.
7. O PRD é construído assumindo o ambiente de produção para o caso de uma verdadeira situação de desastre. Atividades relativas somente a ambientes de teste são identificadas no PRD.

A seção seguinte proposta por esta monografia e aplicada foi a de dependências. No caso do conta corrente, foram consideradas as dependências entre a aplicação e subsistemas. Atividades com o mesmo número de sequência podem ser executadas em paralelo (tabela 4.6):

Sequencia	Atividade	Time	Contato
1	Ativação do mainframe	Time Mainframe (Hardware)	xxx
2	Ativação do z/OS	Time Mainframe (Software Básico)	xxx
3	Ativação do IMS	Time Mainframe (IMS)	xxx
3	Ativação do DB2	Time Mainframe (DB2)	xxx
4	Ativação do Conta Corrente	Time Aplicação	xxx

Tabela 4.6 – Dependências

As próximas seções conforme a proposta desta monografia são:

- Papéis e responsabilidades
- Procedimentos técnicos de recuperação
- Procedimentos pós-desastre

No plano de recuperação de desastres do cliente antes da implementação da proposta desta monografia, ele possuía uma planilha contendo os papéis e responsabilidades, além disso, cada time técnico possuía seus respectivos documentos técnicos contendo os procedimentos de recuperações e pós-desastre. Todos os documentos foram agrupados e reescritos dentro do padrão proposto nesta monografia, que está de acordo com as melhores práticas de documentação. Por questão de confidencialidade, os procedimentos técnicos não serão descritos neste estudo de caso.

4.2.4 Execução do PRD

Após a conclusão do desenvolvimento do PRD, o próximo passo é a execução. Nas soluções de recuperação de desastres que utilizam sincronismo, é necessário considerar a distância entre os sites e as tecnologias envolvidas, pois ambos impactam a performance do sistema. Por um lado está sendo garantido um RPO igual a zero, entretanto o desempenho da aplicação não pode ser muito impactado.

No caso da aplicação de conta correntes, antes da implementação da solução de recuperação de desastres, o tempo que o disco levava para fazer um I/O, ou seja gravar / ler um dado era em torno 0,3 ms. Após a implementação do sincronismo esse valor passou para 0,7 ms. Esse valor pode ser explicado da seguinte maneira:

0,3 – tempo de gravação no site primário
0,3 – tempo de gravação no site secundário (discos iguais da produção)
0,1 – tempo para transmitir o dado entre sites (10 Km)

Entretanto deve-se também levar em consideração o impacto para a aplicação, se houve um aumento no tempo de execução das transações. A tabela abaixo tem o tempo médio de execução das 5 transações mais executadas do conta corrente (tabela 4.7):

TRANSAÇÃO TEMPO MÉDIO	ANTES DA SOLUÇÃO (ms)	DEPOIS DA SOLUÇÃO (ms)	DIFERENÇA
TRANSAÇÃO 1	4,33	6,97	37,9%
TRANSAÇÃO 2	7,96	10,43	23,7%
TRANSAÇÃO 3	7,09	9,48	25,2%
TRANSAÇÃO 4	16,58	18,03	8,0%

TRANSAÇÃO 5	5,49	8,26	33,5%
MÉDIA	8,29	10,63	25,66%

Tabela 4.7 – Transações mais executadas (Conta Corrente)

Pela tabela acima, é possível analisar que o uso da solução síncrona de PRD provocou um aumento médio de 25,66% no tempo de execução da aplicação de conta corrente. Entretanto essa aplicação é composta de transações bem rápidas, que executam em torno de 10 ms, e esse aumento para o usuário final foi transparente.

Após a aplicação da solução descrita nesta monografia, o cliente chegou a realizar testes de recuperação de desastres. Foram realizadas simulações, envolvendo os times de z/OS, IMS, DB2, Operações e Aplicação. Inicialmente os times de z/OS com Operações atuaram utilizando alguns utilitários do GDPS para quebrar a cópia síncrona no site secundário. Após a quebra da cópia, os times de sistema operacional e subsistemas passaram a atuar remotamente seguindo o PRD, e inicializando todos os subsistemas envolvidos com o Conta Correntes no site secundário. Por fim, o time de Aplicação realizou testes verificando o funcionamento do Conta Correntes no site secundário, confirmando o sucesso da recuperação de desastres.

Segue os resultados dos testes obtidos pelo cliente:

Situação 1 - Falha nos volumes contendo dados de conta corrente (Figura 12)

Nesse teste os discos do site primário contendo os dados da aplicação conta corrente foram desativados, em questão de segundos a automação detectou a situação e a aplicação que estava rodando no site primário passou a acessar os dados no site secundário. Esse processo levou 45 s e não houve perda de dados, portanto, obteve-se um RPO = 0 e um RTO = 45 s.

Situação 2 - Situação de desastre no site primário (Figura 13)

Nesse teste foi simulado uma situação no qual o site primário se tornou inoperante, devido a um desastre. Portanto os sistemas deveriam ser reiniciados no site secundário após a declaração da situação de desastre seguindo o PRD. O cliente seguiu o plano de recuperação de desastres construído baseado na proposta desta monografia e conseguiu restaurar o sistema após 53 minutos. Nesse teste obteve-se um RPO = 0 e o RTO = 53 min, que já mostra uma melhora após a aplicação da proposta. Como foi realizado apenas um teste com a nova proposta, ainda existe possibilidade para diminuir o valor do RTO, diminuindo o tempo de indisponibilidade e consequentemente reduzindo o impacto financeiro.

4.2.5 Manutenção Contínua

Por fim, foi definido uma manutenção periódica que é realizada dois meses antes da execução dos testes de recuperação de desastres. Os testes acontecem anualmente e no caso de falha nos testes, eles podem acontecer com mais frequência até que os objetivos sejam alcançados. Também foram definidas auditorias internas anuais, e externas também podem acontecer entretanto não foi definido periodicidade.

5 CONCLUSÃO

5.1 Contribuições do Trabalho

Esta monografia procurou conciliar os conceitos de continuidade de negócios e ITIL, desenvolvendo uma proposta de plano para recuperação de desastres em sistemas críticos de TI. A proposta foi embasada na norma ISO 24762, entretanto não é o intuito substituir a norma, e sim complementá-la.

Após uma análise das normas de recuperação de desastres disponíveis no mercado, conclui-se que muitas são genéricas não trabalhando com as características particulares dos sistemas críticos, como os mainframes. Portanto, com esta monografia, foi pretendido mostrar de maneira mais prática como desenvolver o PRD, utilizando conceitos de ITIL como a matriz RACI, o ciclo de vida de um serviço e as melhores práticas na padronização e controle de documentação.

A proposta desta monografia foi construída para ambientes críticos em mainframe, entretanto ela também pode ser aplicada em diferentes situações e ambientes, desde que pequenas adaptações sejam feitas.

A proposta de plano para recuperação de desastres especificado por esta monografia foi aplicada em um caso real do mundo corporativo. Essa situação é mostrada em um estudo de caso, no qual um banco que possui aplicações críticas em mainframe implementa uma nova solução de continuidade de negócios. Essa implementação foi facilitada por ser focada em apenas um sistema crítico e pela existência prévia de um PRD, mesmo que ele ainda não contemplasse as melhores práticas. A maior dificuldade da implementação foi a tecnologia síncrona em si, pois foi preciso garantir que não existisse nenhum link degradado (fibra óptica com eficiência comprometida) conectando o site primário ao secundário afetando a performance da aplicação.

É possível concluir que um bom PRD construído seguindo algumas das melhores práticas do ITIL afeta de maneira significativa os tempos de recuperação dos sistemas de TI. Na atualidade como as empresas estão cada vez mais dependentes dos sistemas de TI para manter o seu negócio funcionando, consequentemente também se tornam cada vez mais dependentes do PRD.

Em certas situações, infere-se que a implementação de um novo PRD e a utilização de uma nova tecnologia para a replicação de dados, permitem uma redução no *Recovery Time Objective* e no *Recovery Point Objective* para os clientes, tornando-os melhor preparados para atuar em uma situação real de desastre, diminuindo o impacto ao negócio.

5.2 Trabalhos Futuros

Esta monografia procurou propor todas as fases para a construção de um plano de recuperação de desastres em sistemas críticos. Entretanto alguns pontos não foram abordados em detalhes e carecem de trabalhos futuros para aprofundamento. Este é o caso das análises de impacto e risco, existem diversos métodos disponíveis no mercado que podem ser adaptados e melhorados para os sistemas críticos e não foram considerados nesta monografia.

REFERÊNCIAS BIBLIOGRÁFICAS

INTERNATIONAL STANDARDS ORGANIZATION AND INTERNATIONAL ELECTRO TECHNICAL COMISSION. **US ISO/IEC 24762:** Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services. Suíça, 2008.

PALMA, F. F.; MEIRELLES, E. F. **Gerenciamento de serviços de TI com base na ITIL V3.** Implantando boas práticas na IPRAJ e na GDK – dois estudos de caso reais. 2008. 125 p. Monografia (Bacharelado) – Universidade Salvador, Salvador, 2008.

NATIONAL INSTITUTE OF STANDARDS AND TECNOLOGY. **NIST Special Publication 800-34 Rev. 1:** Contingency Planning Guide for Federal Information Systems. Gaithersburg, 2010.

EBBERS, M.; O'BRIEN, W.; OGDEN, B. **Introduction to the New Mainframe: z/OS Basics.** Estados Unidos: IBM Corp, 2006. 710 p

BALTZAN, P.; PHILLIPS, A. **Introduction Business Driven Information Systems.** New York: McGraw-Hill/Irwin, 2008. 990 p

SOMMERVILLE, I. **Software Engineering.** 9thed. Boston: Addison-Wesley, 2011. 790 p

BOM, J. V. **Foundations of IT Service Management base on ITIL V3**. Estados Unidos: Van Haren, 2007

CARTLIDGE, A. et al. **An Introductory Overview of ITIL® V3**. Londres, Best Management Practice Editora, 2007.

ROEBUCK, K. **Business Continuity and Disaster Recovery: High-impact Technology**. Estados Unidos, Emereo Pty Limited, 2011. 446 p

HILES, A. **The Definitive Handbook of Business Continuity Management**. [s.l.]: John Wiley & Sons, 2007

B S I STANDARDS. **PAS 77:** It service continuity management code of practice. [s.l.], 2006.

INTERNATIONAL STANDARDS ORGANIZATION AND INTERNATIONAL ELECTRO TECHNICAL COMISSION. **US ISO/IEC 27002:** Information technology — Security techniques — Code of practice for information security controls. Suíça, 2013.

INTERNATIONAL STANDARDS ORGANIZATION. **ISO 22301:** Societal security -- Business continuity management systems --- Requirements. Suíça, 2012.

TEXAS UNIVERSITY. **University of Texas disaster study**. 2002
Disponível em:
<http://www.oceanedgeconsulting.com/consulting/disaster_management.html>.
Acesso em: 01 setembro 2014.

DISASTER READINESS CONSORTIUM. **Prove IT**. 2002
Disponível em:
<http://contingencynow.com/resources/BusinessContinuityStatistics.pdf>.
Acesso em: 01 setembro 2014.

MICHIGAN STATE UNIVERSITY. **DRP Plan.** Disponível em:<
http://drp.msu.edu/index.htm>. Acesso em: 12 julho 2014.

GEORGETOWN UNIVERSITY. **Systems and Operations Continuity.**
Disponível em: <http://continuity.georgetown.edu/dr/>. Acesso em: 01 setembro 2014.

INTERNATIONAL BUSINESS MACHINES. **IBM Investor Briefing.** 2014
Disponível em: <http://
www.ibm.com/investor/att/pdf/Evolving_IBMsCore_Franchises_Overview.pdf>.
Acesso em: 01 setembro 2014.

BUSINESS CONTINUITY INSTITUTE'S. **SearchDisasterRecovery - Paul Kirvan.**
Disponível em: < http://searchdisasterrecovery.techtarget.com>. Acesso em: 16 outubro 2014.