

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
MBA EM ADMINISTRAÇÃO DA TECNOLOGIA DA INFORMAÇÃO

JOSÉ LUIS MARQUES ANDRADE

GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS
UTILIZANDO TÉCNICAS DE VIRTUALIZAÇÃO

Porto Alegre
2010

AGRADECIMENTOS

Ao término de mais uma pequena etapa deste eterno aprender que é a vida, agradeço primeiramente à minha esposa Eliane Rampon pelo carinho, apoio e incentivo, por ser aquela que, mais do que colega de curso, mas como minha companheira de todos os momentos, criou as condições para que eu pudesse concluir este curso.

Agradeço ao meu filho Thomas, fonte de toda a minha força e motivação.

Agradeço a todos os professores que, ao longo deste curso, compartilharam de forma brilhante e dedicada o seu conhecimento e as suas experiências. Destes, agradeço em especial ao meu orientador, o professor Fernando José Karl, pela orientação, pelo incansável apoio, pela extrema boa vontade e compreensão que, sem os quais, este trabalho não teria sido concluído. Ao coordenador do MBA, Prof. Dr. Orcar Rudy Kronmeyer Filho, pela energia, pela alegria de ensinar e pelo suporte e atenção nesta fase final de conclusão do curso.

Finalmente, agradeço ao BANRISUL, na pessoa daqueles colegas (deste curso ou não) que, assim como eu, trabalham sério dentro dos mais elevados padrões de qualidade e princípios de lisura e ética, dedicando suas vidas profissionais ao sucesso desta grande instituição, agradeço também, àqueles, profissionais de todas as áreas, que têm o orgulho de contribuir ou fazer parte da equipe que faz Gestão da Tecnologia da Informação do Banco do Estado do Rio Grande do Sul.

RESUMO

A infraestrutura da Tecnologia da Informação das instituições financeiras no Brasil é geralmente complexa e heterogênea. Várias plataformas computacionais são utilizadas de forma complementar e interdependente para dar suporte aos produtos e serviços da empresa aos seus clientes e parceiros de negócios. Paralelamente, algumas aplicações legadas e soluções integradas – *Hardware, software* e serviços – adquiridas ao longo do tempo não apresentam o nível de resiliência desejados ou regulamentados. Como exemplo de sistemas operacionais mais utilizados pode-se citar o Linux em seus vários sabores, o *Windows* e *z/OS* utilizado na absoluta maioria dos ambientes de processamento de dados de grande porte – Mainframes. Aplicações desenvolvidas utilizando estas plataformas como base tecnológica acabam sendo integradas de forma alinhada ao negócio compondo então uma rede complexa de ativos de TI, interligado e dependente, os quais precisam estar disponíveis 24 horas por dia, todos os dias. Dessa forma, um dos desafios da administração da Tecnologia da Informação é o de manter esta infraestrutura disponível, gerenciável e flexível a ponto de acompanhar as necessidades do negócio em suas flutuações (crescimento ou retração) garantindo a disponibilidade e a conformidade com normas e padrões de entidades regulamentadoras como o Banco Central, por exemplo. Considerando que a maioria destas instituições vem buscando esta conformidade tendo como fator limitante os custos decorrentes da duplicação da infraestrutura de TI, bem como a complexidade da escolha de uma tecnologia que permita um gerenciamento padrão independente das plataformas computacionais adotadas surgem questões como: A virtualização pode ser utilizada para auxiliar o desenvolvimento de um conjunto de planos de continuidade de negócios? Como modificar a base tecnológica da empresa de forma a atender os quesitos de segurança, disponibilidade e desempenho, causando um mínimo de impacto na sua estrutura atual? Sendo assim, a ideia central deste trabalho é realizar um estudo sobre as tecnologias de virtualização e sua aplicação para definir um processo contínuo de gerenciamento de continuidade de negócios em ambientes de missão crítica-heterogêneo e voltado à conformidade e disponibilidade. Este material também poderá ser utilizado como referência para a elaboração de um planejamento estratégico de TI visando o direcionamento tecnológico das aquisições com estes objetivos (conformidade e disponibilidade). O trabalho inicia com uma abordagem sobre o surgimento da virtualização, os principais conceitos envolvidos e sua evolução. A seguir é feita uma análise das vantagens, desvantagens e das justificativas normalmente utilizadas para adoção da virtualização, passando brevemente pelo

retorno do investimento previsto após a sua implementação. Na sequência será feito um estudo de caso único onde será desenhado o cenário de TI de uma grande instituição financeira em relação às tecnologias de virtualização já utilizadas e aquelas em processo de aquisição bem como o seu relacionamento com o planejamento estratégico de Tecnologia da Informação da instituição. Ao final do trabalho, levando-se em conta os projetos já implementados e seus resultados projetados, bem como o seu alinhamento com o COBIT (Auditoria de processos) e ITIL (Gerenciamento dos serviços), será fundamentada a utilização da virtualização com o objetivo de continuidade de negócios.

Palavras-Chave: Virtualização; Servidores; Continuidade de Negócios.

ABSTRACT

The Information Technology infrastructure of financial institutions in Brazil is often complex and heterogeneous. Many computing platforms are used in a complementary and interdependent way to support the company's products and services to its customers and business partners. Alongside some legacy applications and integrated solutions - hardware, software and services - purchased over the time not provide the desired level of resilience or compliance. As examples of operating systems most used we can mention the Linux in its various flavors, Windows and z / OS used in the absolute majority of data processing environments, large - Mainframes. Applications developed using these platforms based on integrated technology ends up being aligned to the business and then composing a complex network of IT assets linked and dependent that needs to be available 24 hours a day, every day. One of the challenges of the information technology administration is to maintain this infrastructure available, manageable and flexible enough to follow the business needs in its fluctuations (growth or shrinkage) ensuring the availability and compliance with standards of regulatory authorities as the Banco Central do Brasil, for example. As the most of these institutions has been pursuing this compliance and considering as a limiting factor the cost of doubling the IT infrastructure and the complexity of choosing a technology that allows a standard management platform-independent we face some questions such as: Virtualization can be used to provide the development of a set of plans for business continuity? How to change the technological base of the company in order to meet the issues of security, availability and performance causing minimal impact on its current structure? Being thus, The central idea of this work is a case study on virtualization technologies and their application to define a continuous process of managing business continuity in heterogeneous mission critical environments focuses in compliance and availability. This material can also be used as a reference for the development of an IT strategic planning providing a direction of technological purchases with these objectives (Compliance and availability). The work begins with a discussion of the virtualization first steps, the main concepts involved and their evolution. The following is an analysis of the advantages, disadvantages and justifications that are usually taken for adoption of virtualization by briefly passing by the expected return of investment after their implementation. Following a unique case study will be made in with a drawn of a large financial institution IT infrastructure scenario. The virtualization technologies already in use and those in the delivering process and its relationship with the strategic planning of the bank Technology information. At the end of the work, considering

the projects results and their alignment with the COBIT (audit procedures) and ITIL (Management Services) will be justified the use of virtualization with the goal of business continuity.

Key-words: Virtualization; Servers; Business Continuity.

SUMÁRIO

1 INTRODUÇÃO	08
1.1 ESTRUTURAÇÃO	08
2 MOTIVAÇÃO	09
3 OBJETIVOS	10
3.1 OBJETIVO GERAL.....	10
3.2 OBJETIVOS ESPECÍFICOS	10
4 METODOLOGIA.....	11
5 BREVE HISTÓRICO DA VIRTUALIZAÇÃO	12
5.1 VIRTUALIZAÇÃO DE SISTEMAS OPERACIONAIS	14
5.1.1 A virtualização total	14
5.1.2 Para-virtualização	15
5.2 VIRTUALIZAÇÃO DE <i>STORAGE</i>	16
5.3 PRINCIPAIS FORNECEDORES	18
6 A JUSTIFICATIVA PARA O GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS.....	21
6.1 CONCEITOS PARA UTILIZAÇÃO DO PCN.	22
6.1.1 A avaliação dos impactos no negócio BIA – <i>Business Impact Analysis</i>	22
6.1.2 Testes dos planos de continuidade.	23
7 ESTUDO DE CASO	25
7.1 CENÁRIO DE TI DA EMPRESA.	25
7.2 AMBIENTE DE GRANDE PORTE- <i>MAINFRAME</i>	26
7.3 DEMAIS PLATAFORMAS.....	27
7.4 O AMBIENTE <i>LINUX</i> CENTRALIZADO	28
7.5 O AMBIENTE WINDOWS	28
7.6 O AMBIENTE <i>UNIX</i>	29
7.7 INFRAESTRUTURA DE <i>HARDWARE</i>	30
7.8 A DEFINIÇÃO DO ESCOPO DE TRABALHO	30
7.8.1 Gestão da Continuidade de Negócios: foco Tecnologia da Informação	31
7.8.2 Metodologia para a GNC adotada pela empresa.....	33
7.9 COLETA DE DADOS	34
7.9.1 A seleção dos servidores de missão crítica e o processo de coleta	35
7.10 AS SIMULAÇÕES OBTIDAS	36
7.10.1 Utilização média dos processadores.....	36
7.10.2 As estimativas de otimização	36
7.10.3 As taxas de virtualização.....	37
7.11 CENÁRIO DE CONTINUIDADE DE NEGÓCIOS ANTES DA IMPLANTAÇÃO DO PROJETO DE VIRTUALIZAÇÃO	37
7.12 O PROJETO	40
7.12.1 Premissas e Requisitos do Projeto.....	40
7.12.2 Objetivos do projeto	40
7.12.3 Requisitos	41
7.12.4 O desenvolvimento do projeto.....	41

7.13 O AMBIENTE DE TI DA EMPRESA COM A CONCLUSÃO DO PROJETO.....	42
8 ANÁLISE DOS RESULTADOS	49
8.1 ANÁLISE FINANCEIRA DOS RESULTADOS	49
8.2 O RETORNO DO INVESTIMENTO	50
9 CONCLUSÃO.....	52
REFERÊNCIAS	53
ANEXO A - Relação de Servidores.....	55
ANEXO B – Log do SRM com evidências de teste do PCN do ambiente <i>Vmware</i> executado com sucesso	56

1 INTRODUÇÃO

As tecnologias de virtualização de servidores, dos “*desktops*”, das aplicações e mais recentemente das plataformas de armazenamento, abrem um conjunto quase ilimitado de possibilidades de otimização, controle e gerenciamento dos atuais ambientes de Tecnologia da Informação. Considerando estas aplicabilidades voltadas a um cenário de continuidade de negócios é possível projetarmos a criação de uma infraestrutura de tecnologia da informação flexível, resiliente e em conformidade com as melhores práticas de mercado (DAWNSON, PHILLIP 2005).

1.1 ESTRUTURAÇÃO

De forma a definir um escopo limitado de abrangência a estrutura deste trabalho apresenta-se da seguinte maneira:

No capítulo 2 consta a motivação do estudo.

Os objetivos são apresentados no capítulo 3.

A metodologia da pesquisa é descrita no capítulo 4.

O capítulo 5 discorre sobre a virtualização, apresentando uma breve passagem sobre sua história e desenvolvimento e os tipos de virtualização e seus principais modelos, além dos principais fornecedores deste tipo de tecnologia no mercado atual.

O capítulo 6 constitui da justificativa da continuidade de negócios, métricas e métodos.

O estudo de caso, feito em instituição financeira com mais de 430 agências e 3.000 pontos de autoatendimento, é apresentado no capítulo 7, abordando o desenvolvimento de um conjunto de projetos voltados à disponibilidade dos serviços de TI, apostando na aplicação de uma solução de continuidade de negócios baseada em técnicas de virtualização desde a escolha da ferramenta até a demonstração do retorno do investimento obtido após sua implantação.

No decorrer do capítulo 8 é feita a análise dos resultados.

No capítulo 9 é apresentada a conclusão do trabalho, seguido das referências bibliográficas utilizadas nesse estudo, assim como os anexos utilizados nessa pesquisa.

2 MOTIVAÇÃO

É quesito fundamental para as instituições financeiras no Brasil o atendimento às normas e regras definidas pelo Banco Central do Brasil. Esta conformidade se traduz em um maior ou menor risco operacional (BACEN - Resolução 3380, 2006) o que implica diretamente no resultado financeiro destas instituições. Por outro lado o funcionamento dos Bancos, seus produtos e serviços são hoje totalmente dependentes da disponibilidade da infraestrutura da Tecnologia da Informação. Conciliar esta disponibilidade necessária com a capacidade desta infraestrutura, levando-se em conta os custos envolvidos, é um grande desafio para os administradores.

As tecnologias de virtualização representam uma alternativa para a solução deste desafio, mas qual delas tem a sua aplicação mais adequada ao cenário das instituições financeiras em termos de custos, segurança e tempo de implementação?

A motivação deste trabalho, que tem origem neste desafio, é validar a proposta de uma solução baseada nas tecnologias de virtualização capazes de atender, de forma adequada, o planejamento de continuidade de negócios. Dessa forma, foi utilizado como referência um estudo de caso que aborda um conjunto de projetos desenvolvidos de forma integrada, contemplando desde a virtualização de estações de trabalho (“*Desktops*”) até a virtualização de soluções de armazenamento.

3 OBJETIVOS

Os objetivos do estudo dividem-se em objetivo geral e específicos.

3.1 OBJETIVO GERAL

Este trabalho tem como objetivo geral a realização de um estudo sobre a validade da aplicação de uma solução de continuidade de negócios baseada em técnicas de virtualização.

3.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos dessa pesquisa se resumem em:

- a) Fazer o levantamento dos riscos e problemas da atual infraestrutura de TI;
- b) Apresentar os benefícios obtidos através de um processo de virtualização; e
- c) Demonstrar o retorno do investimento obtido após sua implantação.

4 METODOLOGIA

A metodologia define quais os meios utilizados para se chegar ao fim pretendido. Na classificação, quanto aos fins da pesquisa, Vergara (2009) comenta que as mesmas podem ser definidas como: exploratória, descritiva, explicativa, metodológica, aplicada e intervencionista.

A pesquisa exploratória tem a função de buscar mais informações sobre o tema por meio de investigação, assume geralmente as formas de pesquisa bibliográfica e estudo de caso.

Dessa forma, quanto aos aspectos metodológicos para a realização do presente estudo, utilizar-se-á a pesquisa bibliográfica com estudo de caso, sendo que, a pesquisa bibliográfica usa como fonte, materiais já publicados, através de livros, artigos científicos, revistas, dissertações, entre outros. Por outro lado, o estudo de caso tem por objetivo analisar um determinado setor de uma empresa, na tentativa de identificar possíveis problemas que o mesmo possa estar enfrentando, ou seja, problemas concretos com a finalidade prática, além de sugerir uma proposta para melhoria desses problemas.

Sendo assim, essa pesquisa tem como objetivo analisar uma única empresa, procurando levantar problemas relacionados ao gerenciamento da continuidade de negócios utilizando técnicas de virtualização, pretendendo-se realizar uma investigação profunda e detalhada, sendo classificada assim como um estudo de caso.

5 BREVE HISTÓRICO DA VIRTUALIZAÇÃO

Nos anos 60 a *International Business Machines* (IBM), com o objetivo de disponibilizar um ambiente multiusuário aos seus clientes, proporcionando um uso melhor dos recursos de processamento, desenvolveu em sua plataforma computacional de grande porte, o S/360-67, uma funcionalidade que se baseava no conceito de simulação da realidade. Este conceito consistia em simular um conjunto de recursos maior do que o existente particionando os recursos de *hardware*. Antes disso os computadores sequer tinham a capacidade de executar mais de um programa concorrentemente. O conceito de multiusuário chamado na época de “*Time Sharing*” onde mais de um serviço podia ser executado concorrentemente (ainda não simultaneamente) representava uma inovação sendo este uma das bases das futuras tecnologias de virtualização (JOHN MCCARTHY, 1983).

Como marcos históricos do desenvolvimento desta tecnologia pode-se citar:

- **1959** - O professor da Universidade de Oxford, Christopher Strachey publicou um estudo intitulado "*Time Sharing in Large Fast Computers*". Sua intenção era a de utilizar os recursos de processamento enquanto esperava pelos periféricos (o tempo de acesso a discos e fitas e mesmo a memória é muitas vezes maior que a velocidade de processamento). Basicamente seu objetivo era o de que isso acontecesse enquanto um programador estivesse analisando (*debugg*) seu programa na console do sistema;
- **1961** - *Compatible Time-sharing System* (CTSS). Ativado no MIT pela primeira vez neste ano e sobreviveu até 1973. Permitiu que múltiplos usuários utilizassem um *Mainframe* IBM 7094 a partir de terminais remotos. O CTSS foi originalmente apresentado em um documento no “*1962 Spring Joint Computer Conference*”, mesmo ainda não estando totalmente funcional (CORBATÓ, 1962). Não é muito divulgado, mas o e-mail como conhecemos hoje teve sua origem neste sistema operacional (TOM VAN VLECK);
- **1974** – Neste ano um cientista da computação americano, Robert P. Goldberg, lançou a base teórica da arquitetura para sistemas computacionais virtuais em sua dissertação na universidade de *Harvard*. No mesmo ano a IBM lançou um *mainframe* capaz de executar simultaneamente diferentes sistemas operacionais sob a supervisão de um programa de controle – *hypervisor*. O sistema 370 da IBM foi o primeiro computador comercial

inteiramente projetado para virtualização, que, com o sistema operacional CP/CMS, permitia executar múltiplas instâncias simultaneamente. A partir daí, a IBM construiu os supercomputadores da família 360 e o MIT desenvolveu o projeto MAC um acrônimo para *Multiple Access Computer*, projeto este que ficou famoso pelas inovações na pesquisa nas áreas de sistemas operacionais, inteligência artificial e teoria da computação. Um dos maiores focos do projeto MAC foi o de desenvolver um sucessor para o CTSS, o *Multics*, o qual foi o primeiro sistema operacional de alta disponibilidade, desenvolvido como parte do consórcio que incluía a GE General Electric e o Bell *Laboratories*.

De forma, independente, a IBM continuou a desenvolver sistemas de máquinas virtuais como CP-40 (desenvolvido a partir de uma modificação da versão do IBM 360/40), o CP-67, VM/370 e muitos outros. Tipicamente, máquinas virtuais IBM eram cópias idênticas do *hardware* adjacente, onde um componente chamado *virtual machine monitor* (VMM) roda diretamente no *hardware* real. Múltiplas máquinas virtuais podem então ser criadas por meio do VMM e cada instância pode rodar seu próprio sistema operacional.

Mais tarde, os *mainframes* incorporaram o conceito de LPAR (*Logical Partition*) como um padrão. Esta funcionalidade representava a possibilidade de particionamento lógico e físico do *hardware* com o compartilhamento de canais e outros recursos. Anos depois o sistema operacional do *mainframe* IBM (MVS) passaria a rodar obrigatoriamente em uma LPAR.

Nos anos 80 e 90, a virtualização ficou restrita quase que exclusivamente ao ambiente *Mainframe*. Nesta época o surgimento dos PCs (x86) trazia ao mercado um ambiente da baixa plataforma onde o modelo cliente-servidor era o padrão. Nem todas as empresas tinham a necessidade de adquirir ou manter um ambiente de grande porte, pois os custos desta plataforma (*Mainframe*) sempre foram altos. Nesta época, as empresas passaram a adquirir servidores de plataforma x86 possibilitando o crescimento horizontal da capacidade de processamento, processo este chamado de *low-end* (várias máquinas pequenas fazendo o trabalho de um grande servidor).

Neste cenário, ao invés de ter um alto custo inicial com a aquisição de um mainframe, optava-se por adquirir servidores menores ao longo do tempo de acordo com a necessidade. O impacto dessa nova estratégia foi que, para garantir uma boa margem de folga contra problemas de dimensionamento de *hardware*, grande parte destes servidores eram utilizados para uma única aplicação ou sistema. Os servidores eram superdimensionados para a aplicação que iriam executar, e por consequência, acabavam por sofrer do mesmo problema

dos mainframes da década de 60, isto é, não se aproveitava toda sua capacidade computacional.

Em 1999, a *Vmware Inc.* introduziu o conceito de virtualização na plataforma x86 como uma maneira mais eficiente para utilizar os equipamentos desta plataforma, aproveitando servidores x86 para fornecer uma estrutura computacional que possibilitasse o total aproveitamento dos recursos computacionais.

A partir de 2005, fabricantes de processadores como Intel e AMD passaram a dar mais atenção à necessidade de melhorar o suporte via *hardware* em seus produtos. A Intel com sua tecnologia Intel VT e a AMD com a AMD-V. Estes *hardwares* contêm funcionalidades explícitas que permitem que “*hypervisores*” melhorados sejam utilizados com a técnica de virtualização completa (*full virtualization*), que tornam mais fácil a implementação e potencializam a melhora de desempenho.

5.1 VIRTUALIZAÇÃO DE SISTEMAS OPERACIONAIS

Essa etapa aborda as duas formas principais de implementação dos monitores de máquina virtual: a virtualização total e a para-virtualização.

5.1.1 A virtualização total

Entrega ao sistema operacional uma imagem do *hardware* no qual executa. Nesta modalidade o sistema operacional executa sem quaisquer modificações sobre uma camada que executa a virtualização propriamente dita, normalmente chamada de monitor de máquina virtual (VMM – *Virtual Machine Monitor*). Esta implementação tem alguns problemas como, por exemplo, o número de dispositivos a serem suportados pelo VMM que tem de ser muito grande. Assim o uso de *drivers* de dispositivos genéricos que funcionam bem para a maioria dos dispositivos disponíveis, mas não garantem o uso da totalidade de sua capacidade, torna-se uma necessidade. Problemas de desempenho também são comuns, pois, como o sistema operacional não tem conhecimento de que está sendo executado sobre o VMM, as instruções executadas por ele devem ser testadas pelo VMM para que depois sejam executadas diretamente no *hardware*, ou executadas pelo próprio VMM e simulada a execução para o sistema visitante. As atividades de paginação da memória virtual são um exemplo desse último inconveniente, pois há a disputa de recursos entre diversas instâncias de sistemas operacionais.



Figura 1 – Virtualização Total
Fonte: o autor

5.1.2 Para-virtualização

Representando uma alternativa a virtualização total nesse modelo de virtualização, o sistema operacional é modificado para chamar o VMM, sempre que for executar uma instrução sensível que possa alterar o estado do sistema. Com isso o VMM não precisa testar todas as instruções aumentando o desempenho do conjunto *hardware*-virtualizador-sistema operacional em muito. Além disso, neste modelo de virtualização não é necessário o uso de *drivers* genéricos, pois os dispositivos de *hardware* são acessados por *drivers* da própria máquina virtual permitindo o uso total das funcionalidades dos mesmos.



Figura 2- Para-virtualização
Fonte: o autor

Esta aparente vantagem de performance entre a virtualização total e a para virtualização têm sido superada devido ao desenvolvimento pelos fabricantes de hardware de instruções específicas voltadas a virtualização nos processadores Intel e AMD. A AMD utiliza a AMD-V (*AMD – Virtualization*) de codinome *Pacífica* e a Intel usa o IVT (*Intel Virtualization Technology*) chamado de *Vanderpool* ponto desfavorável a paravirtualização é o fato de que os sistemas operacionais devem sofrer modificações para acessar as *APIs* (*Application Program Interface*) providas pela camada de virtualização.

5.2 VIRTUALIZAÇÃO DE *STORAGE*

Uma característica comum à maioria das grandes empresas do segmento financeiro é o volume crescente de dados armazenados em *storages* externos. Nas instituições financeiras a necessidade de se manterem arquivos históricos é uma constante. Trilhas de auditoria, relatórios de movimentações financeiras e outros tantos precisam ser armazenados mantidos para efeitos de conformidade. O rápido o crescimento vegetativo deste volume de dados geralmente acarreta, ao longo do tempo, a aquisição de mais e mais equipamentos de armazenamento. Depois da aquisição de vários *storages*, geralmente de fabricantes e capacidades diferentes, a administração da grande massa de dados torna-se uma tarefa complicada e de difícil planejamento para sua recuperação em caso de desastres.

Assim como na virtualização de servidores a virtualização de “*storages*” surgiu no ambiente *mainframe* para otimizar o uso dos equipamentos de armazenamento. Um dos problemas encontrados era o número cada vez maior de fitas que armazenavam estes dados corporativos e históricos, cada um delas com utilização parcial de sua capacidade. Em 1997 a IBM lançou no mercado sua solução de virtualização de fitas, o VTS (*Virtual Tape Server*). Este equipamento era composto de uma *tape library* (equipamento de montagem automática de fitas composto de *drives* de leitura, *slots* de armazenamento de fitas e um mecanismo de montagem robotizado), um conjunto de discos e um servidor rodando um *software de backup* modificado. O equipamento se apresentava ao sistema operacional como se fossem 64 unidades de fita transferindo e recebendo os dados simultaneamente e de forma mais rápida, pois os dados eram lidos e gravados em disco. A utilização total da capacidade de armazenamento das fitas fica garantida pela divisão das fitas em espaços menores de armazenamento correspondentes as “*fitas virtuais*”.

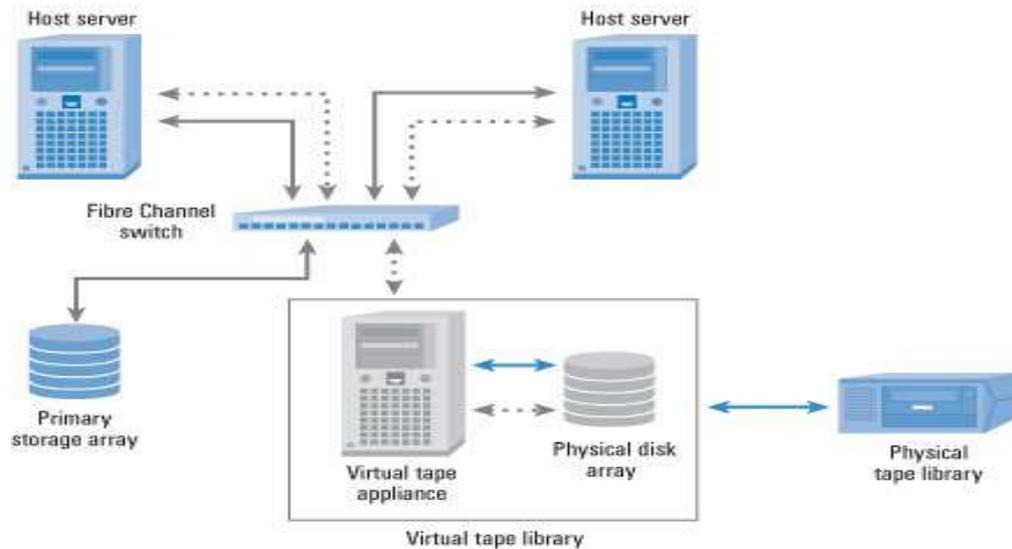


Figura 3 – Virtualização de *Storage – Tape Library Virtual*
 Fonte: DELL Power Solutions – *Examining Virtual Tape Librarys*

Atualmente, para as plataformas de menor porte, diferentemente da virtualização dos servidores, a virtualização do *storage* ainda não é tão popular, uma vez que tem sua aplicação mais específica em organizações que possuem sistemas de armazenamento heterogêneos o que é comum em grandes empresas. A virtualização do *storage* permite simplificar a administração, reduzir o custo de gerenciamento do sistema de *storage* como um todo preservando os investimentos anteriores. O conceito é simples: Todos os sistemas de *storage* passariam a funcionar como um sistema único do ponto de vista do administrador. Os recursos disponíveis então poderiam ser melhores aproveitados, independente da plataforma (Windows, Linux, Unix, etc.).

A virtualização pode acontecer no nível *LUN* (*Logical Unit Number*) ou no nível do sistema de arquivos (*File System*). No caso da virtualização no nível *LUN*, o *storage* virtual se apresenta para os servidores na forma de discos virtuais. O conceito de virtualização do *storage* pode incluir discos, blocos, unidades de fita, sistemas de arquivos e até mesmo os arquivos. A virtualização pode ocorrer nos *hosts*, no *storage*, ou na rede via *switches* inteligentes ou *appliances*. A virtualização do *storage* requer automação das rotinas e deve também ser baseada em políticas para reduzir a intervenção manual.

Appliances de Virtualização: A virtualização utilizando *appliances* é a mais comum, pois propicia independência do *host* e do *storage*, conforme Figura 2. O termo *appliance* refere-se a um sistema encapsulado de *hardware* e *software* em um único equipamento. Os *appliances*

existentes propiciam interconexão com diferentes sistemas operacionais, plataformas de *hosts* e *storage* de diferentes fornecedores podendo suportar protocolos FC (*Fibre Chanel*) e iSCSI (*Internet Small Computer System Interface*) para acesso dos *hosts*. (CLARK E WESLEY, 2005)

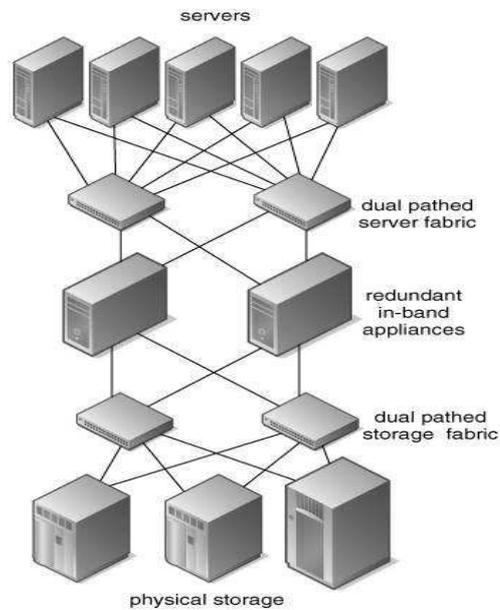


Figura 4 – *Appliances de Virtualização de Storage - Providing high availability for in-band virtualization requires deployment of redundant fabric switches, appliances, and paths.*

Fonte: Tom Clark, 2005 - *Storage Virtualization: Technologies for Simplifying Data Storage and Management.*

5.3 PRINCIPAIS FORNECEDORES

O mercado de soluções de virtualização é bastante variado. Neste trabalho são abordados, brevemente, as três maiores soluções em termos de mercado fabricadas pela Vmware, Microsoft e Citrix, conforme o Gartner no eu estudo publicado em maio de 2010.

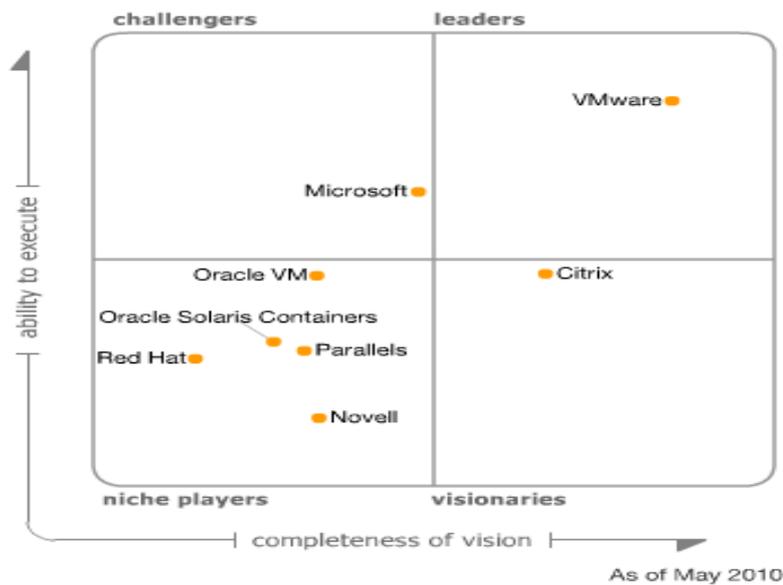


Figura 5 – *Magic Quadrant for Virtualization Technologies and Vendors*

Fonte: Gartner® 2010, - *Magic Quadrant for Virtualization Technologies and Vendors*

a) VMWARE

Líder de mercado de virtualização e pioneira nesta tecnologia, as soluções deste fabricante têm sido consolidadas ao longo do tempo e oferecem, além das funcionalidades básicas muitas opções no contexto de disponibilidade. O SRM – *Site Recovery Manager*, por exemplo, integra o *VSphere Center* e é uma ferramenta que simplifica o processo de recuperação de desastres. Ela se propõe a eliminar as causas comuns de falha durante a recuperação de desastres além de tornar possível testar os planos de recuperação. Ao automatizar a recuperação, o SRM elimina os erros possíveis nas várias etapas manuais comuns a um processo de recuperação de desastres e garante que os procedimentos sejam sempre executados conforme o esperado.

b) Microsoft – Hyper V

É um produto fornecido gratuitamente com o *Windows Server 2008* para uso em até 4 instâncias do mesmo. Conforme o site da Microsoft:

“O *Microsoft® Hyper-V™ Server 2008 R2* é um produto independente que apresenta uma solução de virtualização segura e otimizada, permitindo que as organizações façam melhor uso dos servidores e eliminem custos. Como o *Hyper-V Server* é um produto especializado independente, que contém apenas o *Windows Hypervisor*, o modelo de *driver* do *Windows Server* e os componentes de

virtualização, ele consome poucos recursos e requer o mínimo de custos. Ele se integra com facilidade aos ambientes de TI, aproveitando suas ferramentas de suporte, correções, provisionamento, gerenciamento, processos e especialização. Entre os recursos disponíveis no *Microsoft Hyper-V Server 2008 R2* destacam-se a *Live Migration*, suporte a volumes de cluster compartilhados e o suporte estendido a processadores e memória para sistemas host.”

O *Hyper-V* tem uma diferença básica a seu favor que é o fato de ser desenvolvido pela mesma empresa que desenvolve o sistema onde rodará, no caso, o *Windows Server 2008*. Diferentemente de soluções como o *VMware* que fornece um sistema de virtualização baseado em um processo comum executado no *host* (ESX), onde esse processo emula uma CPU virtual, memória e dispositivos, entregando-os para as máquinas virtuais o *Hyper-V* é basicamente um "hypervisor" (uma camada abstrata rodando sob o *hardware* real) e utiliza o próprio *hardware* nativo para a execução de parte das tarefas solicitadas pelos sistemas convidados (*guests*).

c) CITRIX XEN

Citrix® *XenServer*® é uma de servidor de virtualização construída um *hypervisor* chamado *Xen*®. É uma versão comercial da ferramenta de código aberto *Xen* que é reconhecida como uma alternativa de virtualização rápida e segura. O *XenServer* é projetado para uma gestão dos servidores *Windows*® e *Linux*® .

Como requisito de *Hardware* é necessário um processador com as funcionalidades INTEL –VT ou AMD-V.

6 A JUSTIFICATIVA PARA O GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS

A globalização dos serviços financeiros e a sofisticação da tecnologia bancária no mercado Brasileiro contribuíram para o aumento da complexidade dos riscos envolvendo a Tecnologia da Informação. O sistema financeiro, por ser fortemente dependente da automação e dos elementos de TI que lhe dão suporte, está muito vulnerável a falhas operacionais e às consequências que estas podem trazer, por exemplo:

- Fraudes internas ou externas (roubo ou alteração de informações, *hacking*);
- Práticas ilegais (lavagem de dinheiro, violação de sigilo bancário);
- Dano a ativos físicos (vandalismo, terrorismo, incêndio, inundação);
- Falhas de sistemas/equipamentos e consequente descontinuidade; e
- Falhas no gerenciamento dos processos (execução e entrega de produtos ou serviços).

Por outro lado, as instituições financeiras têm a necessidade de estarem alinhadas as regulamentações vigentes, atendendo, por exemplo, a resolução 3380 emitida pelo BACEN, que reflete especificações apresentadas na Basiléia II tratando do risco operacional. O Risco operacional é a ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas ou de eventos externos.

Resumindo, o GCN – Gestão de Continuidade de Negócios, é o processo de melhoria contínua que tem por objetivo garantir a Continuidade dos Negócios frente a eventos que possam ocorrer, através da identificação dos impactos, possibilitando que ações mitigadoras sejam planejadas, previamente, e mantidas de acordo com as necessidades da organização. O PCN – Plano de Continuidade de Negócios é um conjunto de planos que são elaborados para que a empresa esteja preparada para atuar nos casos de exceção.

- Plano de Gerenciamento de Incidentes;
- Plano de Continuidade Operacional;
- Plano de Recuperação de Desastres; e
- Plano de Administração de Crises.

6.1 CONCEITOS PARA UTILIZAÇÃO DO PCN

PCN implementa um conjunto de planos que objetivam prover orientação em momentos de anormalidade, entretanto é necessário conhecer alguns conceitos.

- a) **Incidente:** Um incidente é uma situação de indisponibilidade que, se não tratada em tempo hábil, pode levar a um desastre ou mesmo provocar uma crise. O plano que trata incidente é o PGI – Plano de Gerenciamento de incidentes;
- b) **Desastre:** Um desastre é um evento súbito que ocasiona perda ou dano de um ativo, implicando em uma descontinuidade no processo de negócio. O plano que trata desastres é o PRD – Plano de Recuperação de Desastres; e
- c) **Crise:** Uma crise é um evento crítico, que se não for gerenciado apropriadamente, impacta negativamente no negócio da organização, podendo ter consequências operacionais, financeiras ou mesmo de reputação. O plano que trata Crises é o PAC – Plano de Administração de Crises.

Além destes, temos ainda dois tipos de plano: PCO – Plano de Continuidade Operacional e o PTV – Plano de Testes e Validação.

6.1.1 A avaliação dos impactos no negócio BIA – *Business Impact Analysis*

A análise do impacto nos Negócios (BIA) é imprescindível para o PCN. Os quatro principais objetivos definidos num processo de BIA são:

- Determinar o potencial impacto para a organização em caso de uma falha;
- Identificar serviços críticos / processos e seus máximos períodos de indisponibilidade tolerável (*Maximum Tolerable Period of Disruption*), Objetivo de tempo para recuperação (*Recovery Time Objective*) e o Objetivo de Ponto de Recuperação (*Recovery Point Objective*);
- Determinar a sequência de recuperação de negócios funções e dados em caso e uma interrupção; e

- Identificar estratégias de recuperação, os recursos mínimos, e registros vitais que são necessários para o negócio continuidade.

Para dar a dimensão adequada em relação à importância das funções e processos do negócio o BIA deve ser executado sempre no pior caso de análise (Rama). Neste contexto as instituições financeiras têm os menores objetivos em termos de tempo, principalmente no que diz respeito ao RPO.

6.1.2 Testes dos planos de continuidade

A validação periódica é uma atividade indispensável no ciclo da GCN. O Banco Central, através da resolução 3.380, de 29/06/2006, exige a existência de um plano de contingência “para limitar graves perdas decorrentes de risco operacional”, o qual é auditado por esta instituição. Então, a validação dos planos, além de ser um requisito de segurança, vem atender à regulamentação existente, apontando evidências e problemas que ainda restam ser corrigidos nos procedimentos de continuidade.

A escala e a complexidade dos testes devem ser apropriadas aos objetivos de recuperação definidos. Os testes devem ser realistas, bem planejados e acordados com as partes interessadas (recursos humanos, fornecedores, terceiros, órgãos de defesa civil, etc.), de modo que haja um risco mínimo de interrupção dos processos de negócio. Um exercício precisa minimizar as chances de que ocorra um incidente como seu resultado direto. Todo teste deve ter objetivos claramente definidos. Uma análise deve ser realizada após o teste, e devem ser gerados relatórios que demonstrem se os seus objetivos foram alcançados. O Relatório de Testes e Validação tem por objetivo garantir a eficiência dos planos e identificar a necessidade de atualização dos mesmos, além de documentar as evidências da execução dos testes.

Tipos de testes:

- a) **Teste de Mesa** Executar os procedimentos dos Planos, sem colocá-los em prática, buscando encontrar incoerência dos mesmos;
- b) **Simulação Parcial** Provocação prática, com o objetivo de obter o teste parcial do Plano;

- c) **Simulação Total** Provocação prática, com o objetivo de obter o teste total do Plano;
- d) **Exercício Parcial** Ocorrências que afetaram o cotidiano, e comprovam a validade parcial do plano; e
- e) **Exercício Total** Ocorrências que afetaram o cotidiano, e comprovam a validade total do plano.

7 ESTUDO DE CASO

7.1 CENÁRIO DE TI DA EMPRESA

A instituição financeira analisada tem foco principal de negócios na região sul do país. Com 10.000 funcionários, 423 agências e mais de 3.000 pontos de autoatendimento, onde são processadas mensalmente mais de 1,32 bilhões de transações por mês.



Figura 6 – Infraestrutura de TI
Fonte: o autor

Todo o suporte técnico bem como a administração e o gerenciamento destes ambientes estão concentrados em uma divisão da TI da empresa, aqui chamada de gerência de suporte técnico. Composta por mais de 90 técnicos esta gerência tem como responsabilidades:

- A garantia da disponibilidade;
- A prospecção de tecnologias; e
- O gerenciamento da capacidade e desempenho dos ativos de TI, excetuando-se os de rede LAN e WAN.

Neste estudo de caso único abordar-se-á as duas principais plataformas de processamento que são o ambiente de grande porte (*Mainframes*) e as demais plataformas RISC e x86 (Unix, Linux e Windows).

7.2 AMBIENTE DE GRANDE PORTE – *MAINFRAME*

O ambiente de grande porte é composto por dois *mainframes* com capacidade de processamento de 11.000 MIPS (Milhões de instruções por segundo). São equipamentos IBM da linha *z10 Enterprise Class (EC)* com processadores diversificados e especializados (ibm.com/systems/z/hardware/):

- **CP** - *Central Processor* - O processador que implementa a arquitetura *CISC z/Architecture* possuindo 4 *cores*;
- **IFL** - *Integrates Facility for Linux* – É um CP dedicado à execução de Linux, com ou sem camada de virtualização por software (zVM);
- **ICF** - *Internal Coupling Facility* – É um processador dedicado a serviços de compartilhamento de dados e estruturas de memória;
- **zAAP** - *z Application Assist Processor* – É um processador dedicado à execução de cargas específicas JAVA e XML sob o sistema operacional z/OS; e
- **zIIP** - *z Integrated Information Processor* – É um processador especializado para o uso do banco de dados DB2.

Este ambiente central de processamento, caracterizado como sendo de missão crítica da instituição, utiliza o sistema operacional z/OS versão 1.10 disposto em 6 partições lógicas (LPARs – *Logical Partitions*) para produção, homologação, desenvolvimento e testes.

A infraestrutura de armazenamentos é composta por discos e fitas totalmente replicados e dispostos nos dois *sites* da empresa (CPD I e CPD II). A empresa utiliza uma solução virtualizada com duas *tape libraris*, também replicadas que usam tecnologias de virtualização (VTS – *Virtual Tape Servers*) com capacidade de armazenamento de mais de 264 *Petabytes*. Os discos são de modelo DMX2-M2 fabricados pela EMC e tem capacidade de armazenamento de 16 *Terabytes*, também replicados. Estes equipamentos estão configurados em RAID 1 e são replicados sincronamente de forma que em cada um dos dois *sites* da empresa existe uma cópia, duplicada pelo uso do RAID1 dentro do mesmo *site*.

Nesta plataforma, ainda são executados todos os serviços de criptografia e certificação digital, utilizados pela empresa.

Como a maioria dos ambientes das grandes instituições financeiras, a infraestrutura de TI de grande porte desta instituição, tem os serviços e aplicações totalmente contingenciados, com planos de continuidade de negócios estabelecidos, gerenciados e controlados. Cada um dos *Mainframes* é capaz de suportar a carga total de processamento da empresa sendo que os dados corporativos armazenados em discos e fitas são replicados sincronicamente entre os *sites*. Esta plataforma não será objeto de análise deste trabalho pelo fato de já atender aos quesitos de conformidade, disponibilidade e contingenciamento sob todas as regulamentações existentes no mercado, conforme estudos realizados semestralmente pelas várias empresas de auditoria especializadas, contratadas pela instituição.

7.3 DEMAIS PLATAFORMAS

Os sistemas operacionais dos servidores utilizam basicamente duas plataformas computacionais (Intel x86 e RISC) onde executam os três principais sistemas operacionais: RISC com o *Unix* (HP-UX) e x86 com um variado ambiente *Linux* (Várias distribuições e versões) e *Windows* também em várias versões. Este conjunto de equipamentos das demais plataformas é composto por 22 Servidores *Unix*, 285 servidores *Windows* e 75 Servidores *Linux*, distribuídos equivalentemente entre os dois *sites* ou virtualizados.

Neste ambiente são executados vários serviços passando desde os mais básicos (DNS, DHCP, Controladores de domínio, *Active Directory*, *Proxy Servers*, LDAP, etc.), bancos de dados (*ORACLE*, *Microsoft SQL Servers*, *PostGree*, e outros) até os sistemas de operação da empresa (empréstimos, cadastro, etc.), considerados também como sendo de missão crítica. O desenvolvimento das aplicações nestas plataformas foi baseado, em sua grande maioria, em uma arquitetura SOA (*Service Oriented Architecture*).

Com 460 agências espalhadas, principalmente pelo interior do estado do Rio Grande do Sul, a empresa utiliza um modelo descentralizado de processamento para as filiais. Com um servidor próprio para cada filial é garantida a disponibilidade da maioria dos serviços de cada uma das agências aos seus clientes. Estes servidores utilizam o sistema operacional *Linux* (CENT/OS) e estão conectados em rede com os demais equipamentos que são os *desktops*, impressoras, terminais de caixa, terminais de autoatendimento (*Cash Dispensers*) e dispensadores de cheques. Estes servidores *Linux* rodam basicamente um sistema de

automação bancária que disponibiliza à rede da agência os serviços básicos de DNS, DHCP, Servidor de Impressão, compartilhamento de arquivos, *Proxy* e HTTP.

Cada servidor tem sua imagem, com os dados individuais da agência na qual estão localizados, transferida ao longo das operações diárias para o ambiente centralizado da instituição. Em caso de perda total ou parcial de algum destes equipamentos a recuperação é padronizada e tem um RTO definido que varia conforme a região de localização da agência. Como este conjunto de servidores tem seu plano de continuidade definido e implementado, ele também não será abordado neste trabalho que tem seu foco no processamento centralizado da instituição.

7.4 O AMBIENTE *LINUX* CENTRALIZADO

Inicialmente desenvolvido com uma distribuição *Linux-Conectiva* este ambiente cresceu e hoje conta com 75 servidores em produção e mais de 30 em ambientes de desenvolvimento e laboratório. Atualmente este ambiente é padronizado na distribuição CENT/OS para servidores de aplicação e *ORACLE Linux* utilizado nos servidores de banco de dados ORACLE. Em alguns poucos servidores ainda são mantidas as distribuições Conectiva Linux 10 e o Red Hat 9.

Com a descontinuidade do ambiente Unix a empresa tem investido cada vez mais nesta plataforma, para onde foram direcionados os serviços de bancos de dados *ORACLE*, em cluster ou não. Serviços básicos como os de *firewall*, NTP (*Time servers*) e monitoração da rede são prestados por esta plataforma.

A empresa foi uma das pioneiras no uso de *Linux* para os seus terminais de autoatendimento, nos quais ainda são executadas versões especializadas formatadas exclusivamente para esta finalidade pela equipe técnica da empresa.

No Anexo A é possível encontrar uma relação que exemplifica os servidores *Linux* da empresa.

7.5 O AMBIENTE WINDOWS

O Ambiente *Windows* é composto por 285 servidores divididos entre os dois sites (CPD I e CPD II). Nestes servidores os sistemas operacionais utilizados são o *Windows* 2000, o *Windows* 2003 e o *Windows* 2008 em suas versões em 32 e 64 bits. Alguns servidores *Windows* estão dispostos em uma configuração de *farm e são* balanceados por um serviço de

web switch (distribuição de carga entre servidores que executam as mesmas aplicações e serviços) disponibilizado pela infraestrutura de rede local corporativa. Nem todos os servidores tinham contingenciamento, mas os serviços básicos de infraestrutura (DHCP, DNS, ISA-Proxy, controladores de domínio) são contingenciados e ou replicados.

Ao longo do tempo este ambiente, assim como o *Linux*, foi crescendo e absorvendo uma boa parte das novas cargas de trabalho que antes eram desenvolvidas exclusivamente no ambiente de grande porte. Esta movimentação das aplicações e serviços criou a necessidade de uma padronização do ambiente bem como uma definição de novos processos de controle, gerenciamento e operação.

As linguagens de programação utilizadas são o “.net”, o ASP e ainda o VB6 da *Microsoft*. O suporte deste ambiente é prestado pela equipe técnica da empresa em conjunto com a equipe da *Microsoft*. Novos projetos e implementações desta plataforma são desenvolvidos em conjunto com o fabricante. Durante o período de análise estava sendo desenvolvido um trabalho verificação de nível de maturidade em relação ao ITIL pelas métricas da *Microsoft*, o MOF. “O *Microsoft Operations Framework* (MOF) que é uma estrutura de melhores práticas formada por guias, princípios e atividades que ajudam a planejar, entregar, operar, gerenciar e melhorar serviços e soluções de TI, de forma confiável e padronizada.” (MICROSOFT, 2010)

No Anexo A encontra-se a relação que exemplifica o conjunto dos servidores *Windows* virtualizados ou não.

7.6 O AMBIENTE UNIX

O ambiente UNIX da empresa já foi bem maior do que hoje. Buscando simplificar a estrutura de TI e seu gerenciamento bem como reduzir os custos operacionais da manutenção de várias equipes de suporte nas várias plataformas usadas pela empresa foi feita, já há algum tempo, a opção de não mais investir neste ambiente. Atualmente o ambiente *UNIX* da empresa é padronizado em equipamentos HP e utiliza-se o HP-UX.

Alguns sistemas e serviços de missão crítica ainda executam neste ambiente. As bases de dados *ORACLE* foram migradas recentemente para a plataforma x86 em *Linux*, mas os servidores de aplicação ainda permanecem. A linguagem de programação utilizada neste cenário é o *Microfocus COBOL*.

Este ambiente ainda recebe a funcionalidade de backup corporativo para toda a plataforma não *mainframe* da empresa. Os backups são feitos com o *software* EMC

Networker primeiramente em disco e depois são migrados para fitas compartilhando as duas *tape libraries* com o *mainframe*.

A estratégia de descontinuidade deste ambiente adotada pela empresa foi acelerada devido a uma medida do fabricante em descontinuar o seu processador PA-RISC passando a fornecer seus servidores de médio e grande porte na plataforma Intel – *Itanium*. A o planejamento da empresa é de migrar os serviços para as plataformas Intel x86 com *Linux* e *z/Linux* no ambiente *mainframe* o qual já possui um planejamento de continuidade estabelecido. Por este motivo este conjunto de servidores também não será abordado neste trabalho.

7.7 INFRAESTRUTURA DE HARDWARE

A falta de padronização dos servidores nas plataformas não *mainframe* ocorreu pelos diversos processos de aquisição ao longo do tempo. Esta tendência vem sendo modificada uma vez que há 7 anos atrás a empresa alterou suas especificações técnicas nas RFPs (*Request For Price*). Isso trouxe uma diminuição na variedade de fabricantes e também quanto ao formato dos equipamentos. A maioria dos servidores é para uso em *RACKs* sendo os em formato de lâminas (*Blade Servers*) os mais recentes.

Para hospedar o ambiente virtualizado foram adquiridos 4 equipamentos do tipo “*blade servers*” (*Enclosures* HP C7000) com 56 lâminas (*Blades*) modelo BL460C os quais estão em processo de instalação e deverão receber todo o ambiente virtualizado da empresa. O *hardware* utilizado para armazenamento dos dados dos servidores é composto por cinco *storages* dos fabricantes HP (EVA-8000) em número de três e EMC (CX4-960) em número de dois. Juntos, estes *storages* disponibilizam um espaço para armazenamento de mais de 200 TB. Os equipamentos da linha EMC-CX são, a exemplo do ambiente *mainframe*, replicados sincronamente entre os dois *sites* da empresa. Esta replicação é uma funcionalidade básica para os processos de recuperação de desastres analisados a seguir e foram adquiridos recentemente. As bases de dados em Oracle são responsáveis pela maior parte dos dados armazenados nos *storages*.

7.8 A DEFINIÇÃO DO ESCOPO DE TRABALHO

Numa grande empresa com um ambiente tão heterogêneo e complexo como esta os processos de continuidade de negócios são igualmente complexos e trabalhosos. Este

planejamento envolve uma equipe de técnicos dedicada e multidisciplinar, além da participação efetiva de representantes de todas as áreas de suporte da empresa.

Os processos de GCN têm uma abrangência total na organização. Este trabalho tem a sua abordagem focada especificamente na área da infraestrutura de TI em relação ao uso das tecnologias de virtualização e como elas podem proporcionar uma redução na complexidade a própria infraestrutura de TI e conseqüentemente do gerenciamento da continuidade trazendo também uma redução nos investimentos necessários.

7.8.1 Gestão da Continuidade de Negócios: foco Tecnologia da Informação

A Gestão da Continuidade de Negócios (GCN) consiste em uma atividade cíclica que tem por finalidade garantir a continuidade dos negócios da empresa em situações de adversidade. Além disso, a GCN busca incentivar uma cultura de preparação da empresa para evitar ou mitigar os riscos trazidos por uma situação de crise. A NBR 15999 1 e 2, baseadas na BS25999:2006 foram utilizadas como base do trabalho realizado na empresa

“Esta Norma foi desenvolvida por especialistas da comunidade de continuidade de negócios, tendo como base suas experiências acadêmicas, técnicas e práticas da gestão de continuidade de negócios. Seu propósito é servir como um único ponto de referência para a maior parte das situações em que a gestão da continuidade de negócios é praticada e ser usada por organizações de grande, médio e pequeno porte, nos setores comerciais, públicos e de caráter voluntário” (NBR 15999-1:2007).

Na empresa analisada, a Gestão da Continuidade de Negócios se concretiza através da elaboração de Planos de Continuidade de Negócios (PCN), que descrevem em detalhes os ativos e processos de TI críticos a disponibilidade do negócio, seu funcionamento, procedimentos operacionais, gestores responsáveis, grupos de pessoas envolvidas, procedimentos de recuperação e tempo de resposta esperado no caso de uma contingência.

Esta metodologia acarreta na realização de um conjunto de ações preventivas, previamente planejadas, focadas na manutenção das atividades de TI que afetem de alguma forma o negócio e que sofram o risco de serem interrompidas, fazendo todo o possível para efetivamente evitar uma contingência. Além disso, a GCN contribui para proteger juridicamente a organização, atender a regulamentações e à legislação, conquistar a maior confiança do mercado e manter a disponibilidade do ambiente de TI que suporta a totalidade dos produtos e serviços de negócio da empresa.



Figura 7 – Gestão de Continuidade de Negócios
Fonte: o autor

Em 2006, dando cumprimento às recomendações do acordo da Basileia II, o Banco Central do Brasil, através da Resolução 3.380, determinou que as instituições financeiras implementassem uma estrutura de gerenciamento de risco operacional. Parte desta Resolução, em vigor desde 31/12/2007, determina que os bancos mantenham “planos de contingência contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco operacional”. Neste contexto a Tecnologia da Informação tem um papel fundamental.

Até 2007, não havia no Brasil uma norma técnica que tratasse de continuidade de negócios. A referência internacionalmente usada como código de melhores práticas ainda é a norma britânica BS 25999, que é composta de 2 partes:

- BS 25999-1:2006 (Código de Prática); e
- BS 25999-2:2007 (Guia de Certificação).

Atualmente, a ABNT já publicou:

- NBR 15999-1:2007 (Código de Prática); e
- NBR 15999-2:2008 (Requisitos).

7.8.2 Metodologia para a GNC adotada pela empresa

A metodologia adotada na Gestão da Continuidade dos Negócios é baseada nas melhores práticas propostas pela norma BS25999, partindo do princípio de que a GCN é um processo cíclico de melhoria contínua, baseado no PDCA. Este processo envolve:

- Identificação das necessidades (*Plan*)
- Planejamento das estratégias (*Plan*)
- Aplicação das estratégias (*Do*)
- Implementação de novos planos (*Do*)

- Revisão dos planos existentes (*Check*)
- Testes e Validações (*Check*)

- Manutenção dos planos (*Act*)
- Implementação de melhorias (*Act*)

No entendimento da empresa, a maturidade da GCN acontece na medida em que este ciclo for sendo executado, por isso é um processo contínuo e gradual, onde naturalmente a cada ciclo concluído, a GCN incorpora-se nas atividades cotidianas

Atualmente na empresa, cada ciclo é realizado num período de seis meses, as atividades deste ciclo ocorrem paralelamente nas unidades de TI envolvidas, ou seja, são realizadas ações de elaboração de planos, atualização, testes, refinamento dos procedimentos e demais ações necessárias para a melhoria do processo a cada “girada” de ciclo.

Na distribuição dos planos por áreas de aplicação o escopo deste trabalho aborda apenas os 17% do conjunto dos PCNs relativos à Tecnologia da Informação e, dentro destes, aqueles voltados a infraestrutura de TI que podem ser estruturados e desenvolvidos com a utilização de tecnologias de virtualização.

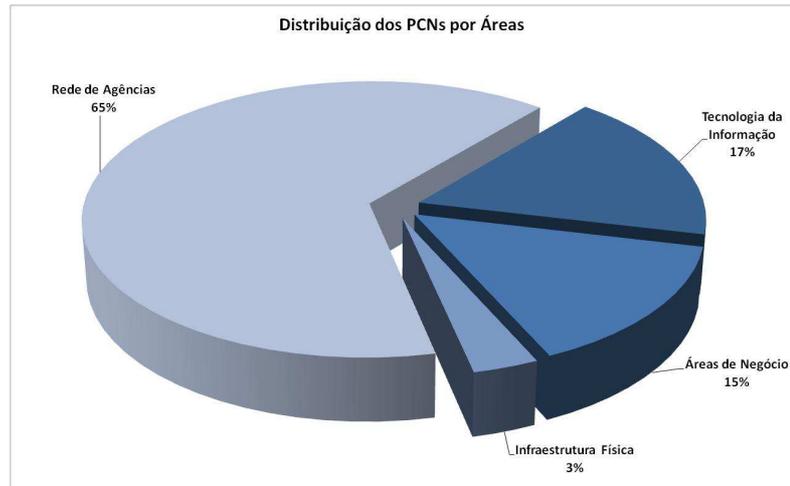


Figura 8: Distribuição dos PCNs por área
Fonte: o autor

7.9 COLETA DE DADOS

Tendo em mente as questões iniciais:

- A virtualização pode ser utilizada para auxiliar o desenvolvimento de um conjunto de planos de continuidade de negócios?
- Como modificar a base tecnológica da empresa de forma a atender os quesitos de segurança, disponibilidade e desempenho causando um mínimo de impacto na sua estrutura atual?

Não é trivial a definição de um conjunto de projetos que enderecem de forma eficiente estas questões. Tampouco é simples a tarefa de justificar os investimentos necessários. Para que tenhamos, ao fim deste trabalho, fundamentado que as tecnologias de virtualização são a resposta a estas questões é necessário o estabelecimento de uma métrica que justifique os investimentos e ateste a estratégia adotada. Neste trabalho foi utilizado um estudo comparativo entre as hipóteses de duplicação da infraestrutura de TI no que diz respeito aos serviços de missão crítica e a virtualização, tendo como base o retorno do investimento dentro de um prazo de 36 meses.

A coleta de dados, base da análise comparativa, foi realizada em períodos intercalados de 15 dias em datas representativas das principais cargas de processamento de transações.

Estes dados, coletados antes e depois da implementação dos projetos, representam o

resultado obtido na prática pela empresa, sem inferências ou simulações considerando apenas modelos reais de análise.

7.9.1 A seleção dos servidores de missão crítica e o processo de coleta

A empresa já havia, em um dos ciclos do GCN, definido quais os sistemas vitais a continuidade dos negócios e quais os seus respectivos ativos base de TI. O método escolhido foi o BIA (*Business Impact Analysis*), que tem como produto principal a identificação dos serviços críticos, tendo como referência as perdas potenciais que a paralisação destes serviços/processos pode acarretar. Esta combinação “Serviços X perdas potenciais” é fundamental para a tomada de decisão à seleção de futuros investimentos em continuidade dos negócios.

Com base nesta definição, não detalhada neste trabalho por motivos de confidencialidade, o levantamento dos dados foi estabelecido. A representatividade dos perfis de carga ao longo dos dias e meses do ano foi identificada de forma a certificar o processo de coleta conforme o gráfico a seguir:

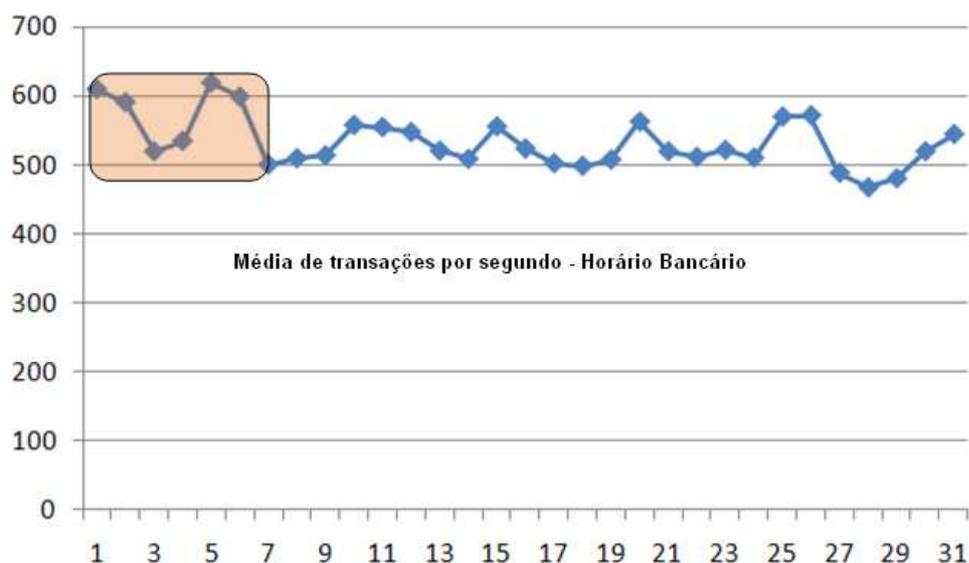


Figura 9 – Gráfico Período de coleta das informações

Fonte: o autor

O método de coleta das informações foi baseado na ferramenta chamada *VMware Capacity Planner Data Manager*. A partir da sua instalação em um servidor específico são coletados de forma automática os dados de todos os servidores *Linux e Windows*, sem a

necessidade de instalação de clientes. Com o período de coleta fechado os dados são enviados a *VMWare* criptografados e com os identificadores principais (nome do servidor, endereço IP, etc.) descaracterizados, por questões de segurança. No caso da empresa analisada foi realizado um *Capacity Assessment (CA)* que consiste em uma análise profunda do ambiente de TI escolhido como amostra entregando um mapa detalhado.

7.10 AS SIMULAÇÕES OBTIDAS

7.10.1 – Utilização média dos processadores

Um dos indicadores básicos para a tomada de decisão em relação ao processo de virtualização é a média de utilização dos processadores. A média de uso dos processadores da empresa é de 8,82%. Se compararmos com os valores médios do mercado mundial ponderados pelo Gartner que variam entre 10 e 15%, poderemos verificar o nível de subutilização dos mesmos.

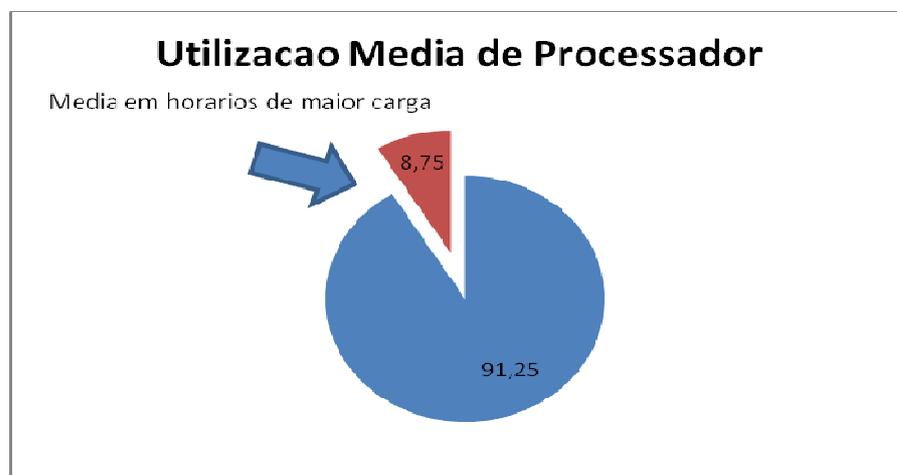


Figura 10 – Utilização Média de Processador
Fonte: o autor

7.10.2 As estimativas de otimização

Geralmente os projetos de virtualização de servidores têm sua justificativa no retorno do investimento. Isso se consegue pela redução da infraestrutura física (*hardware*, energia, espaço físico, etc.). *Forrester Consulting, 2009 – The Business Value of Virtualization.*

Embora no caso da empresa analisada a motivação seja baseada na conformidade e na continuidade de negócios a seguir são relacionados os benefícios estimados:

	Processadores	Memória	Disco	Rede	Consumo de recursos			
	GHZ	GB	TB	GB/Segundo	Rack	Peso Kg	Energia KW	BTU/Hora
Atual	1.074,81	657,5	58,92	400,40	150	1.467	73,63	20,95
Projetado	358,17	530,48	35,96	102,20	70	641	37,43	14,35
Redução	716,64	127,02	22,96	298,20	80	826	36,20	6,60

7.10.3 As taxas de virtualização

A estimativa em relação aos 165 servidores virtualizados foi calculada em 12 para 1. Isto é, a cada 12 servidores virtualizados apenas um *hardware* será necessário. O hardware projetado é baseado em um equipamento padrão IBM Blade Center HS22 (Linha *Blade Center H*) com dois processadores Intel Xeon *QuadCore* com 96 Gb de memória, quatro placas de rede (NICs – *Network Interface Cards*) e dois HBAs (*Host Bus Adapters*) de 8 GBpor canal.No entanto o processo de aquisição acabou resultando em um equipamento diferente (OS HP C7000 com laminas BL460C) com capacidade de processamento superior ao hardware originalmente projetado.

7.11 CENÁRIO DE CONTINUIDADE DE NEGÓCIOS ANTES DA IMPLANTAÇÃO DO PROJETO DE VIRTUALIZAÇÃO.

Como característica histórica da plataforma baixa da empresa, os servidores foram sendo adquiridos ao longo do tempo sem uma padronização mínima quanto ao seu formato (Torre, Rack, etc.) nem quanto as suas funcionalidades. Além disso, a alocação dos mesmos para os diversos sistemas da empresa nunca foi planejada e os servidores foram sendo utilizados conforme mais e mais aplicações foram sendo desenvolvidas ou adquiridas.

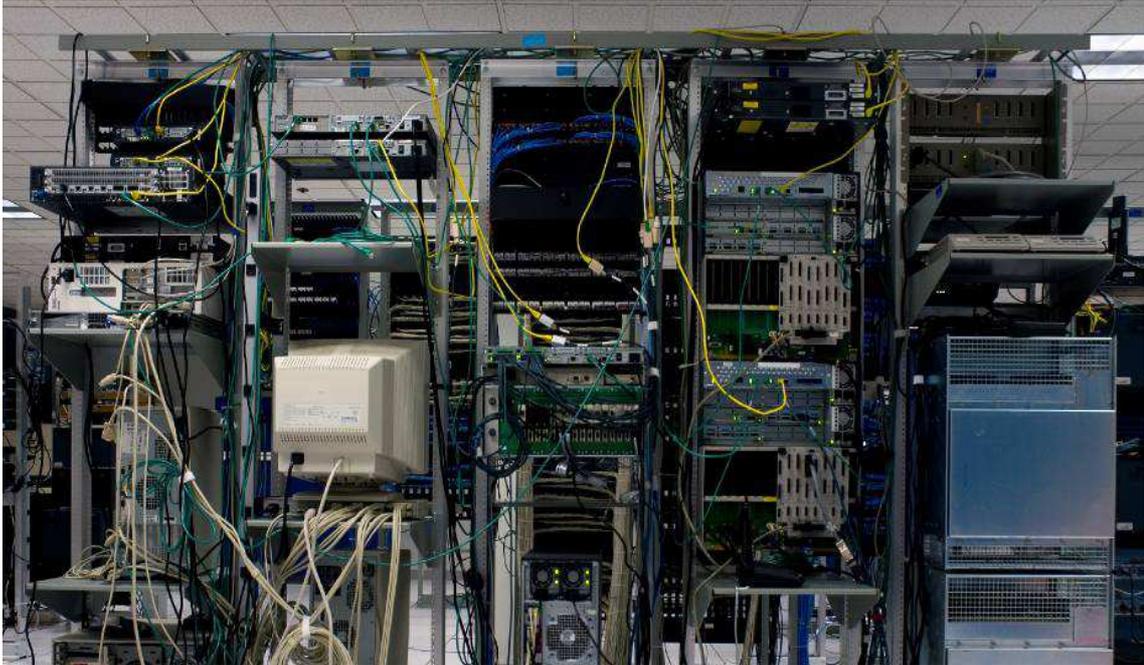


Figura 11 – Sala de Servidores sem padronização de equipamentos
Fonte: o autor

A metodologia de desenvolvimento de sistemas utilizada pela empresa baseia-se no modelo SOA – *Service Oriented Architecture* onde componentes básicos são desenvolvidos e acoplados a um “*Enterprise Service bus*” gerando um reaproveitamento de código, o que dinamiza o desenvolvimento das aplicações.

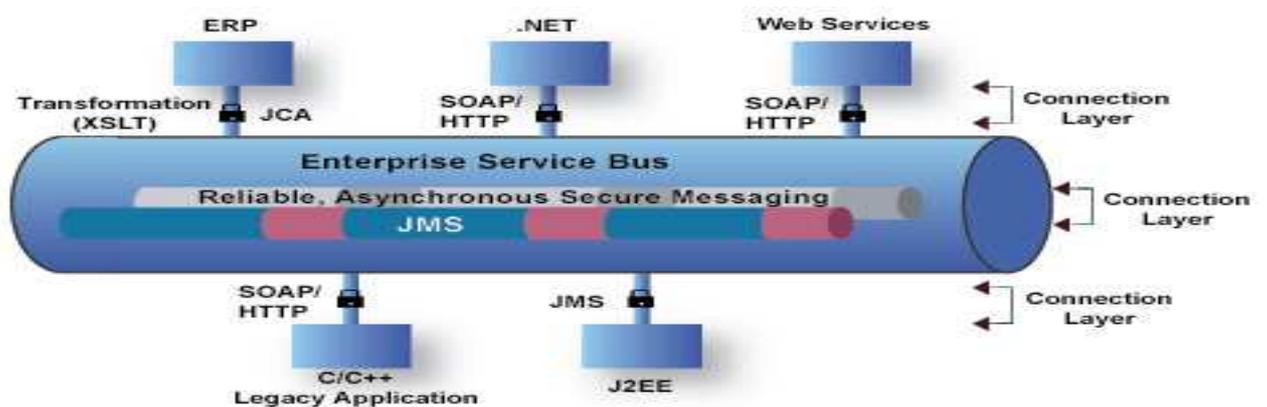


Figura 12: Arquitetura SOA
Fonte: SOA – *American Developers Institute*

Esta distribuição de servidores de forma desordenada aliada as peculiaridades da metodologia de desenvolvimento cria um cenário de dependência entre os servidores. Por exemplo: Um sistema executa em um servidor, mas, para o seu funcionamento, é necessário que outros serviços sejam executados em diferentes servidores criando uma cadeia não mapeada de dependências. Neste cenário, manter um conjunto de PCNs 100% atualizado

para estes servidores é uma tarefa quase impossível, pois, a cada modificação ou criação de um novo componente as relações de dependência podem se alterar modificando totalmente o PCN de um determinado ativo de TI ou mesmo de um grupo deles.

Desta forma, embora os servidores de missão crítica sejam contingenciados (por duplicação, por *clusterização* ou pelo estabelecimento de *farms* de servidores) não há uma garantia de que, entre um ciclo e outro de atualização do PCN, não tenha ocorrido alguma mudança. Até o processo de reativação (*Boot*) dos servidores em caso de falha é problemático, pois, dependendo da ordem de ativação dos servidores, alguns serviços com relação de dependência mais fechada são inicializados inadequadamente.

Outro ponto crítico do ambiente de TI da empresa diz respeito aos processos de restauração da normalidade em caso de falhas em algum servidor. O processo de recuperação é baseado na restauração de imagens de *backup* que são realizados semanalmente (*full backup*) e diários (Incrementais). Como os tempos de restauração são diferentes entre os servidores e se alteram conforme um grande número de variáveis (uso da rede, carga dos equipamentos de fitas, capacidade do servidor, desempenho do equipamento de armazenamento, entre outros), não é possível medir ou inferir os tempos de retorno individuais para o estabelecimento de um RTO (*Recovery Time Objective*) a ser perseguido. A falta de padronização dificulta ainda o processo de replicação de dados, pois muitos dos servidores utilizam áreas de armazenamento internas baseadas em discos internos ligados diretamente ao servidor (*DAS – Direct Attached Storage*)

Os servidores de arquivos (*File Servers*) também representam um risco. A empresa utiliza uma estrutura de *file servers* baseada em 17 servidores Windows (*Windows Server 2003*) onde são armazenados os dados dos mais de 10.000 usuários. A recuperação de arquivos nestes servidores é demorada e a falha de algum deles causa transtornos operacionais graves. Embora exista um forte controle onde 3 servidores de software antivírus (*McAfee EPO – ePolicy Orchestrator*) distribuam e gerenciem os clientes e o conjunto de vacinas a utilização do Windows como *file server* facilita o processo de infecção.

O último ponto de atenção identificado na infraestrutura de TI da empresa analisada foi a ausência de um processo de gerenciamento da capacidade e desempenho para a baixa plataforma. Os servidores vão sendo substituídos (Crescimento vertical) ou novos servidores são agregados (Crescimento horizontal) à medida que recursos de processamento, memória ou armazenamento vão sendo utilizados. Isso ocorre de forma reativa ocasionando problemas de desempenho durante o período de justificativa, aquisição e instalação. Este tipo de abordagem

não deixa alternativas para a redistribuição de recursos entre os servidores criando ilhas onde por vezes sobram recursos em um lado e faltam em outro.

7.12 O PROJETO

O projeto consiste na aquisição de uma solução de *software VMWare* para virtualização com gerenciamento de recuperação de desastres (*Site Recovery Manager*), *hardware (Blades)* para hospedar as máquinas virtualizadas, e também serviços de treinamento, migração e implementação.

Foi projetado, de forma conservadora, a virtualização de 168 servidores em 14 novos servidores (*Blade Servers*) dispostos em ambos os *sites* da empresa gerando uma redução média projetada de 40% da necessidade de armazenamento em disco, energia, espaço físico, peso, número de processadores, climatização e outros. Os demais servidores desta plataforma que não apresentam as condições de virtualização serão futuramente também consolidados neste tipo de equipamento (*Blades*).

7.12.1 Premissas e Requisitos do Projeto

A definição do projeto de virtualização e sua aplicação, focando os processos de continuidade de negócios da empresa, teve como premissas:

- A simplificação da infraestrutura de TI e do seu gerenciamento;
- Assegurar a continuidade de negócios, segurança e durabilidade dos dados; e
- O gerenciamento eficiente da informação durante o seu ciclo de vida.

7.12.2 Objetivos do projeto

Garantir a disponibilidade dos produtos da empresa a sua rede e clientes pela replicação de sua estrutura de dados e contingenciamento de servidores em dois *sites* – CPD I e CPD II.

7.12.3 Requisitos

- Utilizar uma tecnologia padrão de hardware e virtualização para sistemas operacionais da plataforma Open (Linux e Windows);
- Estabelecer um ponto único de gerenciamento da estrutura computacional visando simplificar a operação;
- Diminuir os investimentos necessários com a aquisição de novos servidores para o atendimento a novos sistemas e atualização do parque de equipamentos com o reaproveitamento de equipamentos e a eliminação dos que estiverem fora do padrão;
- Utilizar de forma otimizada os recursos de *hardware* (Servidores);
- Reduzir custos fixos: Manutenção, energia elétrica, climatização, entre outros;
- Aumentar a disponibilidade dos serviços de TI;
- Tornar a infraestrutura de TI da empresa flexível de forma a aumentar e diminuir a capacidade de processamento conforme as necessidades do negócio;
- Preservar os investimentos já realizados nesta plataforma; e
- Conclusão dos projetos de reestruturação do ambiente de rede LAN (Novo *Core* de rede) e aquisição de solução de armazenamento de dados com replicação síncrona.

7.12.4 O desenvolvimento do Projeto

Após o processo de aquisição do software de virtualização, subscrição e serviços de instalação, treinamento e suporte foi estabelecida a dinâmica de desenvolvimento do projeto. A metodologia utilizada foi baseada no PMBOK (*Project Management Body of Knowledge*) que é um conjunto de melhores práticas em gerenciamento de projetos publicado pelo PMI (*Project Management Institute*).

Foi então estabelecido o grupo de trabalho composto por técnicos da gerência de suporte da empresa e definidas reuniões semanais de acompanhamento e planejamento das quais era revisado o *Status Report* semanal (Figura 8). Durante os 4 meses nos quais o projeto foi executado todas as atividades e relacionamentos foram priorizados. Havia uma margem muito pequena de prazo e a empresa precisava dos resultados para que fossem geradas as evidências necessárias aos processos de auditoria interna e externa.

Id	%		Nome da tarefa	Duração	Início Prev.	Término Prev.	Início	Término	Pre
1	90%		Projeto de Virtualização e alta disponibilidade Banrisul 17/06/2010	110 dias	Seg 5/4/10	Ter 29/6/10	Seg 5/4/10	Sex 3/9/10	
2	100%	✓	Reunião inicial	1 dia	Seg 5/4/10	Seg 5/4/10	Seg 5/4/10	Seg 5/4/10	
3	100%	✓	PLANO	10 dias	Ter 6/4/10	Seg 19/4/10	Ter 6/4/10	Seg 19/4/10	
5	98%		INSTALAÇÃO E CONFIGURAÇÃO	54 dias	Ter 6/4/10	Seg 31/5/10	Ter 6/4/10	Sex 18/6/10	
6	100%	✓	Instalação e configuração do Vmware ESXI	2 dias	Ter 6/4/10	Qua 7/4/10	Ter 6/4/10	Qua 7/4/10	2
7	100%	✓	Funções de alta disponibilidade	3 dias	Qui 8/4/10	Seg 12/4/10	Qui 8/4/10	Seg 12/4/10	6
12	100%	✓	Configuração das VLANs de Gerenciamento	2 dias	Ter 13/4/10	Qua 14/4/10	Ter 13/4/10	Qua 14/4/10	7
13	100%	✓	Configuração das VLANs de Produção	2 dias	Qui 15/4/10	Sex 16/4/10	Qui 15/4/10	Sex 16/4/10	12
15	100%	✓	Update Manager	2 dias	Seg 19/4/10	Ter 20/4/10	Seg 19/4/10	Ter 20/4/10	13
16	100%	✓	Atualização do Ambiente	4 dias	Qua 21/4/10	Seg 26/4/10	Qua 21/4/10	Seg 26/4/10	15
19	100%	✓	Instalação e configuração do servidor vCenter	3 dias	Ter 27/4/10	Qui 29/4/10	Ter 27/4/10	Qui 29/4/10	18
20	100%	✓	Migração Storage HP EVA para EMC CX480	22 dias	Sex 30/4/10	Seg 31/5/10	Sex 30/4/10	Seg 31/5/10	19
21	95%		Instalação e Configuração do Nexus 1000v	36 dias	Sex 30/4/10	Seg 31/5/10	Sex 30/4/10	Sex 18/6/10	19
23	100%	✓	Implementação Vmware Heartbeat	5 dias	Sex 30/4/10	Qui 6/5/10	Sex 30/4/10	Qui 6/5/10	19
25	100%	✓	Configuração Vmware Linked Mode (não será usado)	2 dias	Qua 21/4/10	Qui 22/4/10	Qua 21/4/10	Qui 22/4/10	15
26	92%		VIRTUALIZAÇÃO E RECUPERAÇÃO DE DESASTRES	63 dias	Seg 5/4/10	Qui 24/6/10	Seg 5/4/10	Qua 30/6/10	
27	94%		Virtualização de Servidores	45 dias	Seg 5/4/10	Sex 4/6/10	Seg 5/4/10	Sex 4/6/10	
29	94%	📄	Instalação do Vmware Tools	45 dias	Seg 5/4/10	Sex 4/6/10	Seg 5/4/10	Sex 4/6/10	
31	100%	✓	Instalação do Vmware Data Recovery Manager	45 dias	Seg 5/4/10	Sex 4/6/10	Seg 5/4/10	Sex 4/6/10	
33	100%	✓	Criação dos Resource Pools	1 dia	Ter 13/4/10	Ter 13/4/10	Ter 13/4/10	Ter 13/4/10	
34	100%	✓	Validação da Infraestrutura vSphere e testes	26 dias	Sex 7/5/10	Qua 12/5/10	Sex 7/5/10	Sex 11/6/10	23
36	0%		Instalação do Power Path EMC no ambiente ESX	5 dias	Qui 13/5/10	Qua 19/5/10	Qui 17/6/10	Qua 23/6/10	37
37	100%	✓	VMware Site Recovery Manager - Validação da Infraestrutura	3 dias	Qui 13/5/10	Seg 17/5/10	Seg 14/6/10	Qua 16/6/10	34
39	69%		VMware Site Recovery Manager	13 dias	Seg 7/6/10	Qui 24/6/10	Seg 14/6/10	Qua 30/6/10	34
44	0%		Relatórios	3 dias	Sex 25/6/10	Ter 29/6/10	Qui 1/7/10	Seg 5/7/10	39
45	0%	📄	Treinamento Formal	5 dias	NA	NA	Seg 30/8/10	Sex 3/9/10	
46	0%	📄	Treinamento Customizado	5 dias	NA	NA	Seg 12/7/10	Sex 16/7/10	

Figura 13 – Cronograma de Macroatividades do projeto

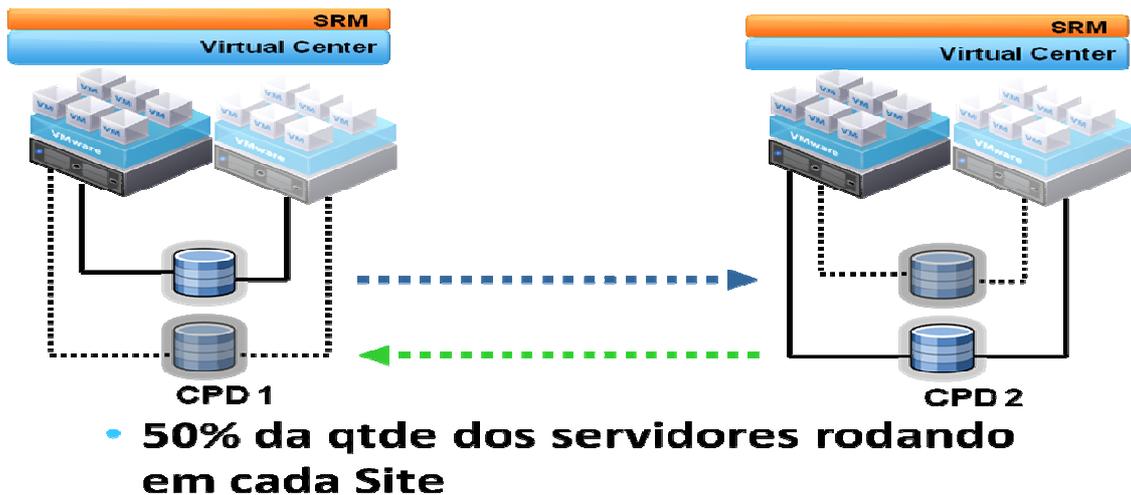
Fonte: o autor

7.13 O AMBIENTE DE TI DA EMPRESA COM A CONCLUSÃO DO PROJETO

Após o término do projeto, ocorrido dentro do prazo estabelecido, os resultados obtidos foram:

a) Melhor uso do Hardware

Criação de um conjunto de recursos de processamento e memória chamados Cluster_CPD I e Cluster CPD II composto inicialmente por 12 servidores DELL modelo R900 nos quais foram distribuídas as 165 Máquinas Virtuais correspondentes aos serviços de missão crítica da empresa. O ambiente foi configurado de forma que os *clusters* de cada um dos dois *sites* da empresa tenham capacidade suportar a carga total de processamento da empresa.



\Figura 14: - Distribuição dos *Clusters* entre os dois *sites*
Fonte: o autor

Neste novo cenário a carga de cada um dos *pools* ficou em menos de 25% possibilitando o crescimento da infraestrutura até um limite seguro de 40% de utilização

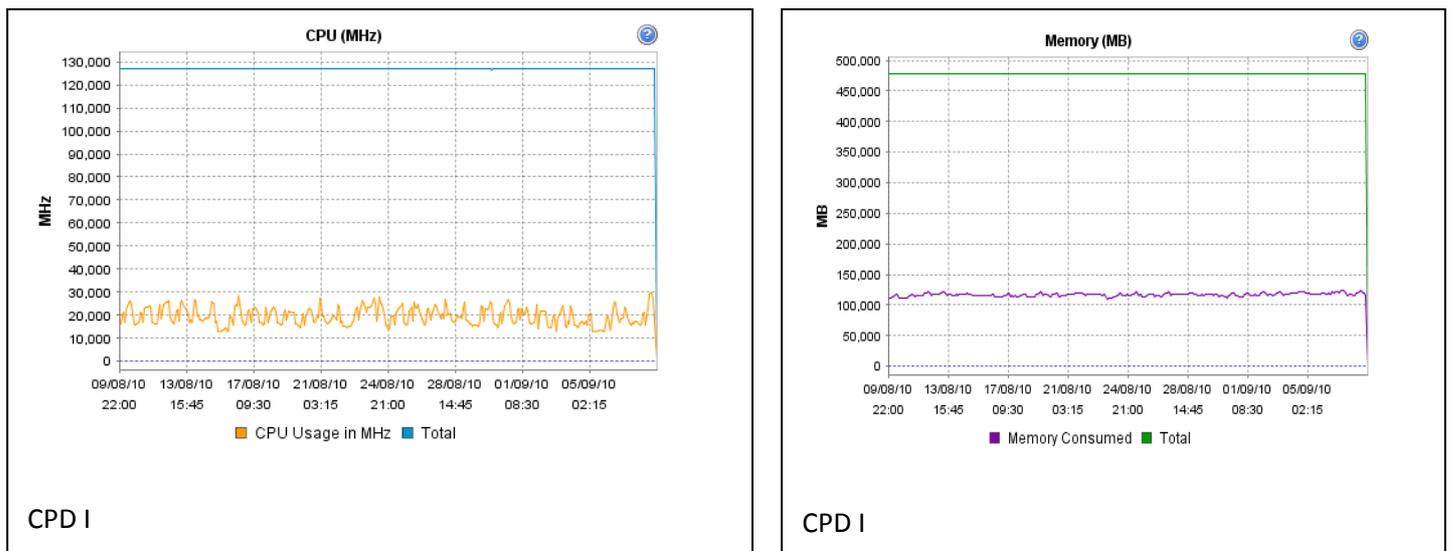


Figura 15 – *Vmware – Vcenter Performance Clusters – CPD cvzxcvzxcvzxcvzxcv*
Fonte: o autor

A Figura 16 ilustra a situação em que duas das máquinas do *pool* do CPD II foram desativadas temporariamente a partir do dia 21/08/2010 diminuindo este conjunto de recursos. Esta distribuição das VMs agora permite a possibilidade de realocação dos recursos dentro de um mesmo *pool* de forma dinâmica e não disruptiva para as VMs criando a possibilidade de se aumentar ou diminuir uma VM conforme a necessidade. Com a utilização do DRS (Distributed Resource Scheduling) foi possível automatizar esta realocação conforme os perfis de carga ao longo dos dias e dos meses.

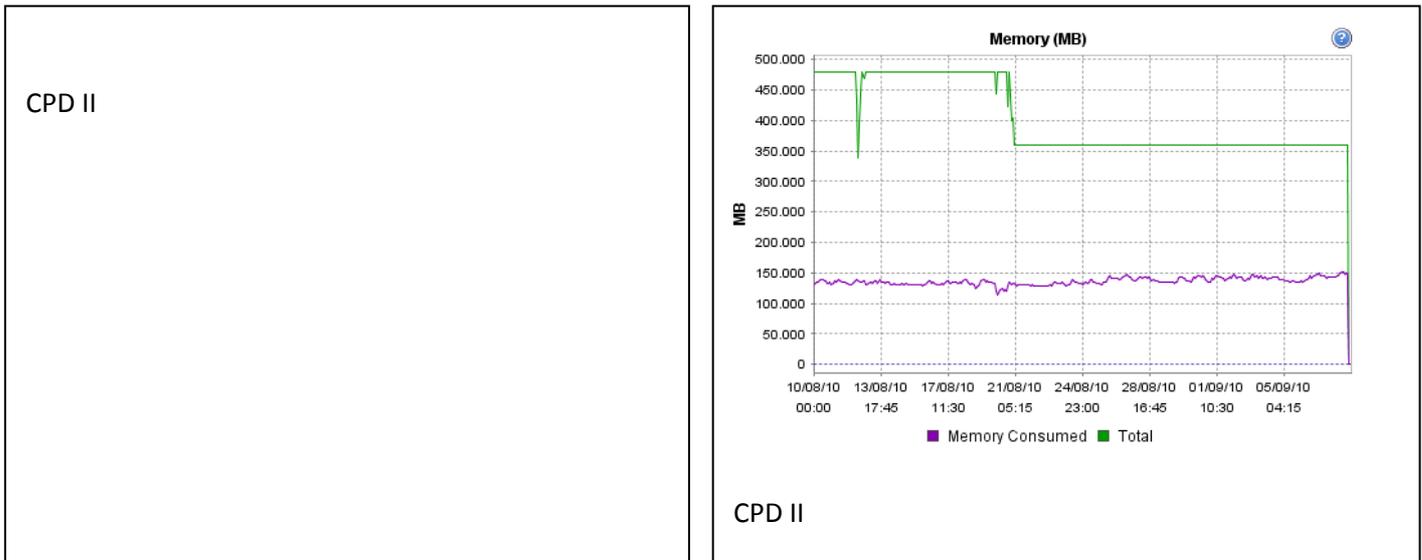


Figura 16 – *Vmware – Vcenter Performance Clusters – CPD*
 Fonte: o autor

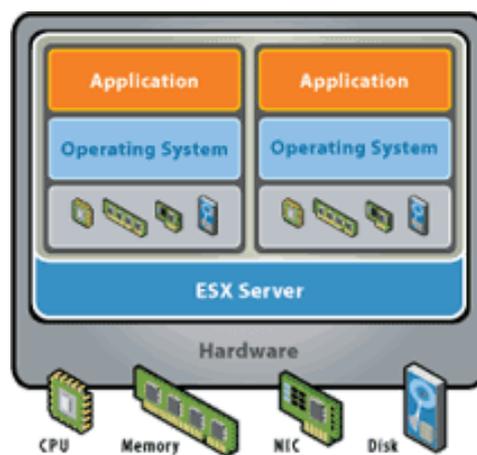


Figura: 17 – *pool* de recursos
 Fonte: *Vmware*

b) Disciplinas de capacidade e performance

A virtualização criou as condições para o desenvolvimento de um processo contínuo de gerenciamento da capacidade e da performance de todo o ambiente virtualizado. Isso significa um planejamento do crescimento horizontal desta infraestrutura de forma não reativa. Para que estes processos fossem estabelecidos e também visando controlar a criação de novas Máquinas Virtuais de forma organizada e planejada a empresa criou uma área responsável por este ambiente.

c) GCN Automatizado e rapidez na recuperação de falhas

O processo de GCN foi endereçado com o uso de duas funcionalidades do VMWare: o HA (*High Availability*) e o SRM (*Site Recovery Manager*):

- O HA permite que ocorra a reativação automática das VMs dentro de um mesmo *pool*. Isso ocorre sempre que alguma VM for interrompida por algum erro de *hardware* ou de *software*. Em testes realizados nos quais foram desligadas determinadas máquinas físicas de um dos *pools* a reativação de todas as máquinas Virtuais que executavam no *hardware* desligado ocorreu em menos de 3 minutos;

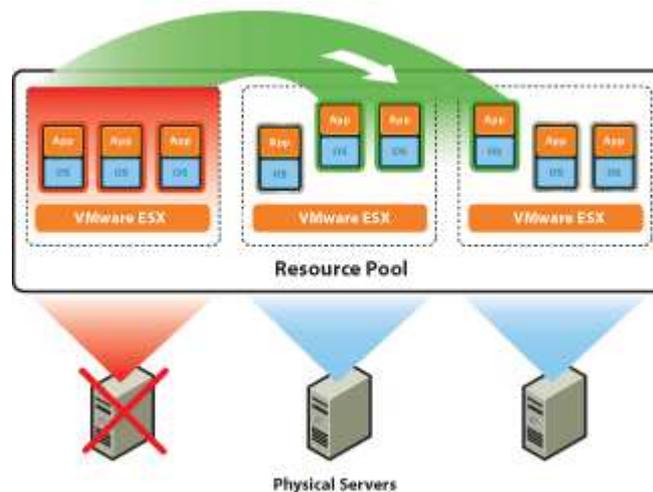


Figura 18: VMware High Availability
Fonte: VMware

- O SRM criou as condições para que fosse escrito um plano de recuperação de desastres para todas as Máquinas Virtuais de um *pool*. Isso ocorre pela definição, no *pool* de um dos sites (*site backup*), de um plano de reativação das Máquinas Virtuais do outro site. Neste plano é descrita a ordem de ativação das Máquinas Virtuais e também o encadeamento entre estas ativações. O SRM é capaz de ativar automaticamente as cópias das Luns no site backup de forma que, quando uma determinada Máquina Virtual seja ativada no site backup os seus dados estejam disponíveis (desde que as Luns sejam replicadas sincronamente entre os sites). Além disso o SRM cria, de forma automatizada e planejada, uma simulação da execução deste plano de ativação das Máquinas Virtuais. Uma terceira cópia dos dados das

Máquinas Virtuais é criada (*Snap Mirror*) para cada uma das Luns. A partir disso cria-se uma “bolha” com os recursos de rede e então as VMs são ali ativadas.

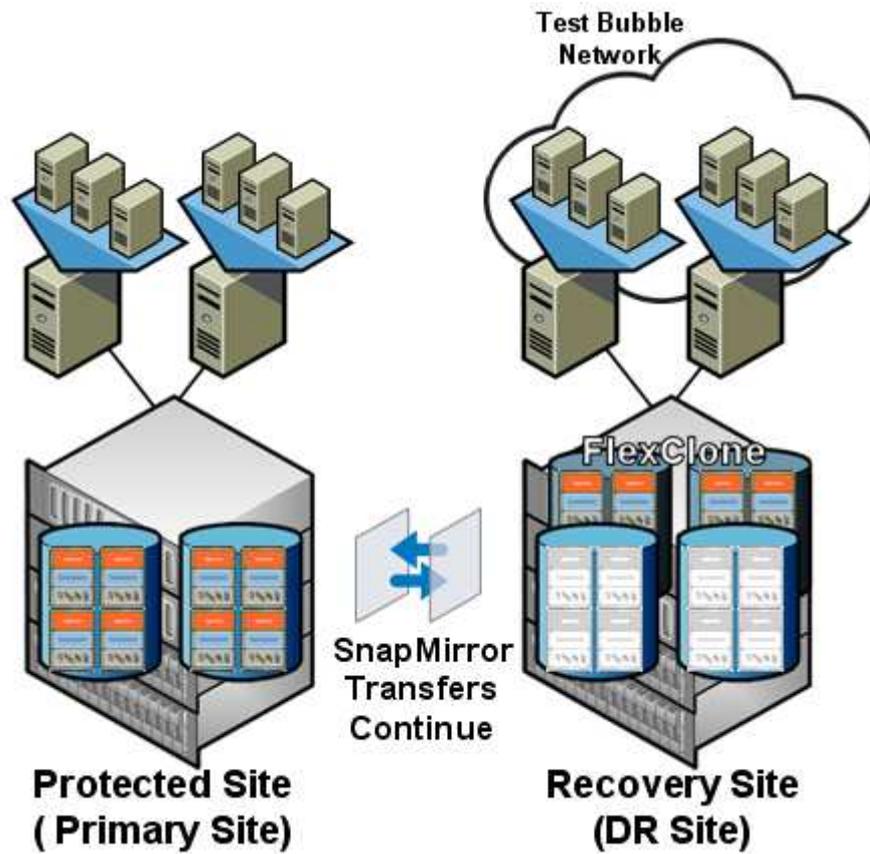


Figura 19 – Site Recovery Manager
Fonte: VMware

Todos os planos de continuidade individuais de cada um dos servidores virtualizados foram padronizados em apenas um plano para a plataforma virtualizada como um todo. Agora apenas os serviços disponibilizados pelos servidores virtualizados tem seus planos estabelecidos, facilitando em muito o controle e a atualização dos planos.

Recovery Step	Status	Task Started	Task Completed	Mode
1. Shutdown Protected Virtual Machines at Prot...	Success	9/23/2009 12:51:35 PM	9/23/2009 12:51:47 PM	Recovery only
1. Shutdown Low Priority Protected Virtual...	Success	9/23/2009 12:51:35 PM	9/23/2009 12:51:35 PM	Recovery only
2. Shutdown Normal Priority Protected Virt...	Success	9/23/2009 12:51:35 PM	9/23/2009 12:51:47 PM	Recovery only
1. Shutdown Protected Site VM "site1-...	Success	9/23/2009 12:51:35 PM	9/23/2009 12:51:47 PM	Recovery only
3. Shutdown High Priority Protected Virtual...	Success	9/23/2009 12:51:47 PM	9/23/2009 12:51:47 PM	Recovery only
2. Prepare Storage	Success	9/23/2009 12:51:47 PM	9/23/2009 12:53:12 PM	
3. Suspend Non-critical Virtual Machines	Success	9/23/2009 12:53:12 PM	9/23/2009 12:53:12 PM	
4. Recover High Priority Virtual Machines	Success	9/23/2009 12:53:12 PM	9/23/2009 12:53:12 PM	
5. Recover Normal Priority Virtual Machines	Running	9/23/2009 12:53:12 PM	60%	
1. Recover VM "site1-vm5"	Running	9/23/2009 12:53:15 PM	60%	
1. Change Network Settings	Success	9/23/2009 12:53:16 PM	9/23/2009 12:53:20 PM	
2. Pre-Power On	Success	9/23/2009 12:53:20 PM	9/23/2009 12:53:20 PM	
3. Power On	Success: Host '192.168.92...	9/23/2009 12:53:20 PM	9/23/2009 12:54:01 PM	
4. Wait for OS Heartbeat	Running	9/23/2009 12:54:01 PM	1%	
5. Post Power On				
6. Recover Low Priority Virtual Machines				
7. Recover No Power On Virtual Machines				
8. Message: Test recovery complete. Please ver...	Inactive			Test only
9. Cleanup Virtual Machines Post Test:	Inactive			Test only
10. Resume Non-critical Virtual Machines	Inactive			Test only
11. Reset Storage Post Test:	Inactive			Test only

Figura 20: Exemplo de plano desenvolvido no SRM
Fonte: VMware

Com isso foram geradas evidências do PCN de todos os servidores virtualizados em um processo que pode ser testado ciclicamente. No anexo G pode ser encontrado um exemplo deste tipo de teste de PCN com as evidências para um grupo de 3 servidores.

d) Padronização e agilidade na criação de servidores

Com a criação de “golden images” usadas como base (*templates*) para criação de novas VMs foi possível reduzir drasticamente os tempos e o trabalho envolvidos no atendimento a demandas por novos servidores. Isso favorece a manutenção dos níveis de correção (*patches* ou *service packs*) em todos os servidores criando um ambiente padrão para as plataformas Windows e Linux.

No caso da empresa analisada, considerando os problemas que esta agilidade pode trazer, houve ainda a preocupação com a criação de um processo para a criação de novos servidores que garante que as questões de capacidade, continuidade/contingenciamento e padronização sejam sempre levadas em consideração.

e) Contingenciamento de servidores não virtualizáveis

Nem todos os servidores das plataformas *Linux e Windows* foram virtualizados. Os servidores que disponibilizam serviços básicos como DHCP (Associa endereços IP sob demanda), DNS (Servidor de nomes), controladores de domínio, servidores de banco de dados e outros foram excluídos do processo de virtualização. Isso ocorreu devido ao perfil de uso e carga dos mesmos não ser adequado às características de virtualização ou simplesmente por questões de segurança. Com a liberação de vários equipamentos foi possível a duplicação, apenas com custos de licenciamento, da infraestrutura destes serviços.

Grupos de servidores foram criados para que a falha de algum deles não interfira na disponibilidade dos serviços atendidos pelo grupo. Desta forma os planos individuais de continuidade dos servidores foram também agrupados.

f) Espaço físico e consumo de energia

Estes são benefícios inerentes a um processo de virtualização. No caso da empresa analisada não foi diferente. Embora a redução esperada, que era de 50% para o consumo de energia e 30% para refrigeração não tenha sido atingidos devido ao reaproveitamento de vários equipamentos para contingenciamento e novos projetos foi obtido uma redução média de 22% em energia e de 14% em refrigeração. O espaço físico reduzido foi proporcional ao número de servidores desativados ficando em torno de 40%.

Foi possível a desativação de 4 racks de 42 “Us” (Cada “U” corresponde a uma unidade de espaço dentro de um rack padrão de 19 polegadas.) e 3 bancadas onde ficavam os servidores tipo Torre ou DeskTop.

g) Padronização do parque de servidores

Todos os servidores com mais de 7 anos de uso, com formato torre ou *desktop* e abaixo de um limite mínimo de capacidade de processamento e memória foram descartados. Para os equipamentos restantes foi estabelecido um processo de manutenção corretiva e preventiva com um SLA definido de acordo com o nível de criticidade do equipamento.

Esta padronização viabilizou um processo de inventário atualizando a base de dados de ativos de TI utilizada pela empresa (*CMDB – Configuration Management Database*)

8 ANÁLISE DOS RESULTADOS

8.1 ANALISE FINANCEIRA DOS RESULTADOS

A análise foi baseada na alternativa de duplicação, que seria outra forma de obter o resultado esperado em relação ao processo de continuidade de negócios mas sem atingir nenhum dos benefícios citados no capítulo 7. Foi constatado que apenas os custos de licenciamento da plataforma *Windows* quase seriam suficientes para justificar o projeto de virtualização no que diz respeito as licenças de VMWare.

Os valores relativos ao licenciamento de 93 instâncias de *Windows Server 2008 Enterprise*, dos servidores *Windows* virtualizados, mesmo considerando a modalidade de licenciamento do tipo “DataCenter” comercializada pela Microsoft (baseada em número de processadores e não em servidores) representam 34% do valor total investido no projeto de virtualização.

Já o investimento em *hardware* para esta análise foi estimado foi apurado levando-se em conta apenas o valor médio de um servidor básico configurado em:

- Dois processadores de quatro cores, 16Gb de memória, duas placas de rede (NICs) e duas placas para acesso a rede de fibra do *storage* (HBAs).

Não foi considerado o conjunto de investimentos decorrentes em rede LAN, SAN, *Storage*, espaço físico, consumo de energia e dissipação de calor.

Custo de pessoal da empresa analisada foi calculado tendo como referência o salário médio dos participantes do projeto transformado em valor/hora alocados conforme abaixo:

- Tempo integral:
 - 1 coordenador;
 - 2 técnicos plataforma *Windows*;
 - 2 técnicos plataforma *Linux*;
 - 2 técnicos *VMWare*;
 - Tempo parcial (80 horas mês);
 - 1 Gerente de projeto;
 - 2 técnicos de rede LAN;
 - 2 Técnicos de infraestrutura física;
 - 1 engenheiro elétricista; e

- 1 técnico de operações.
- Participação eventual (80 horas no total):
 - 5 técnicos plataforma *Windows*;
 - 3 técnicos de rede SAN;
 - 2 técnicos de Banco de Dados;
 - 1 técnico de monitoração; e
 - 2 técnicos de planejamento e controle.

Estimando, de forma conservadora, o mesmo custo de pessoal para ambos os projetos (duplicação da infraestrutura e virtualização) objeto desta análise, chegamos as seguintes proporções financeiras:

	Duplicação da infraestrutura	Virtualização
Custo dos Servidores (hardware)	162%	100%
Custos de Licenciamento Windows	34%	0%
Custos de pessoal	23%	23%
Diferença de investimentos entre os dois projetos	96%	

No cenário analisado a diferença de investimentos, ainda que calculada de forma limitada, entre os dois projetos representa um custo 96% maior se a opção fosse a de duplicação da infraestrutura. Esta diferença fica ainda mais acentuada se considerarmos considerarmos os custos operacionais reduzidos pelos benefícios alcançados pela implementação do projeto de virtualização relacionaados no capítulo 5 deste trabalho.

8.2 – O RETORNO DO INVESTIMENTO

Utilizando as mesmas bases de cálculo, para a apuração dos custos totais do projeto de virtualização, anteriormente citadas, foram relacionados os benefícios tangíveis (que podem ser, incontestavelmente, transformados em valores financeiros) que são:

- Consumo de energia reduzido em 22%;
- Dissipação de calor reduzida em 14%;
- Investimento em hardware para a duplicação dos servidores de infraestrutura (DNS, DHCP, Controladores de domínio, *Firewall*, IPS e IDS, Servidores de autenticação e serviços de diretório) em numero de 16; e
- Encerramento de contratos de manutenção de 149 servidores.

O estudo de retorno do investimento foi baseado num período de 36 meses que é o mesmo considerado para os seguintes componentes do projeto de virtualização:

- *Hosts (Hardware)* e manutenção os 12 equipamentos;
- Licenciamento, subscrição e suporte do VMWare;
- Valor dos serviços de consultoria, suporte e desenvolvimento do projeto (terceirizados);
- Custos de pessoal da empresa analisada para o gerenciamento do ambiente virtual; e
- Custos de infraestrutura (Energia, dissipação de calor, espaço físico).

Fazendo um alinhamento de tempo em relações aos investimentos pelo cálculo do valor presente líquido utilizando o mesmo período (36 meses) e contrapondo as reduções de custo obtidas verificamos que o retorno do investimento acontece a partir do 29º mês demonstrando uma relação financeira favorável.

Neste trabalho foi utilizada uma ferramenta de apoio para cálculo de ROI para as cargas virtualizadas desenvolvida pela Microsoft em conjunto com a Alinean, uma consultoria independente formada por ex-profissionais do Gartner (microsoft.com/virtualization/roitool/default.aspx).

9 CONCLUSÃO

Este trabalho teve como objetivo principal o estudo de caso único de um projeto para o desenvolvimento de uma solução de continuidade de negócios baseada em técnicas de virtualização. Sem entrar nos detalhes dos projetos anteriores desde a escolha da ferramenta de virtualização, da reestruturação da infraestrutura de rede LAN e de *storage* foram abordados todos os pontos chave do projeto de virtualização.

Considerando os resultados obtidos em um projeto de curto prazo com três meses de tempo de implementação, e ainda a análise financeira fica comprovada a aderência da aplicação deste tipo de tecnologia ao contexto de continuidade de negócios.

O uso da virtualização cria as condições para o “*hardening*” da infraestrutura de TI, que é o processo de dar robustez e resiliência ao ambiente de TI e seus ativos. Proporciona a redução de custos operacionais com os processos de GCN automatizando os procedimentos de recuperação e continuidade.

Dessa forma, já é possível a definição pela empresa de um tempo estimado de retorno a normalidade RTO (*Recovery Time Objective*) que é de duas horas. A garantia de funcionamento dos planos de continuidade deste ambiente é obtida pelo teste de simulação com o SRM gerando evidências de funcionamento e material de análise com os eventuais erros ocorridos.

Por fim resta comprovada a eficiência das tecnologias de virtualização no contexto continuidade de negócios, pela viabilização de um ambiente de TI (para as plataformas Windows e LINUX) controlado e gerenciável. Isso ocorre dentro de um cenário financeiro adequado e coerente com a indústria financeira.

REFERÊNCIAS BIBLIOGRÁFICAS

BACEN. **Resolução 3380 – Risco Operacional.** Disponível em <https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=106196825>. Acessado em 01 de Set de 2010.

BASILEIA II. Disponível em <http://www.bcb.gov.br/?BASILEIA2>. Acessado em 01 de Set de 2010.

BURTLES, Jim. **Principles and Practice of Business Continuity: Tools and Techniques** (Paperback).

CLARK, Tom. **Storage Virtualization: Technologies for Simplifying Data Storage and Management.**

CORBATÓ, Fernando J.; DAGGETT, Marjorie Merwin; DALEY, Robert C. **An experimental time-sharing system.** Disponível em: <http://larch-www.lcs.mit.edu:8001/~corbato/sjcc62/>. Acessado em 28 de Jul de 2010.

DATA CENTER. Disponível em http://www.ieee802.org/3/hssg/public/nov06/diminico_01_1106.pdf. Acessado em 28 de Jul de 2010.

GEORGE MASON UNIVERSITY / **The Core of Information Technology.** Disponível em <http://cs.gmu.edu/cne/itcore/virtualmemory/vmhistory.html>. Acessado em 28 de Jul de 2010.

GRAHAM, Julia; KAYE, David; ROTHSTEIN, Philip Jan. **A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance.**

INSTITUTO GARTNER. **Key Issues for IT Operations Management, 2009. Disaster Recovery Plans and Systems Are Essential and Business Continuity Management Key Initiative Overview** . Disponível em <http://www.gartner.com>. Acessado em 02 de Set de 2010.

MARINHO, Fernando. **Como proteger e manter seus negócios**. Campus Elsevier, São Paulo-SP.

MCCARTHY, John. **Reminiscences on the history of time sharing**. Stanford University, 1983 Disponível em <http://www-formal.stanford.edu/jmc/history/timesharing/timesharing.html>. Acessado em 01 de Set de 2010.

NBR 15999-2 – Requisitos. Primeira edição 10/12/2008.

NORMAS NBR 15999-1 – **Código de Prática**. Versão corrigida 01/02/2008.

MICROSOFT. Disponível em: [http://technet.microsoft.com/en-us/library/cc262936\(office.12\).aspx](http://technet.microsoft.com/en-us/library/cc262936(office.12).aspx). In this article: **Licensing requirements. Organizational requirements. Availability and service-level agreements e Performance and scalability** . Acessado em 01 de Set. de 2010.

Storage Virtualization for IT Flexibility. Disponível em: <http://www.sun.com/storage/virtualization/StgVirtWP.pdf>. Acessado em 01 de Set. de 2010.

Storage Virtualization. Disponível em: http://www.snia.org/education/storage_networking_primer/stor_virt/sniavirt.pdf. Acessado em 02 de set de 2010.

VLECK, Tom Van. **The History of Electronic Mail** . Disponível em <http://www.multicians.org/thvv/mail-history.html>. Acessado em 28 de Jul de 2010.

YIN, Robert. **Case Study Research** (Fourth Edition), SAGE 2009.

ANEXO A - Relação de Servidores

Exemplificação do controle de servidores Windows e LINUX distribuídos entre os dois sites da empresa
Levantamento de Setembro/2010

WINDOWS

NOME	UTILIZAÇÃO	SISTEMA OPERACIONAL	HARDWARE
WServer1	Backup Storage Node	Microsoft(R) Windows(R) Server 2003, Standard Edition	HP Storage Server / StorageWorks 1200s
WServer2	Transferencia de Arquivos EDI	Microsoft Windows 2003 Storage Edition	HP Storage Server / StorageWorks 1200s
WServer3	Gerenciamento	Windows XP	N/D
WServer4	Controlador SAN	Microsoft Windows 2003 Storage Edition	HP ProLiant Storage Server DL380 G5
WServer5	Controle de Acesso Físico	Windows XP	Infoway Business Torre/Horizontal
WServer6	Controle de Acesso Físico	Windows XP	Infoway Business Torre/Horizontal
WServer7	Controle de Acesso Físico	Windows XP	Infoway Business Torre/Horizontal
WServer8	Controle de Acesso Físico	Windows XP	Infoway Business Torre/Horizontal
WServer9	DSN, WNS	Microsoft Windows 2000 Server	Infoserver 3040hu h8fr / 8BT/
WServer10	Controlador de Domínio	Microsoft Windows 2000 Server	Dell PowerEdge 2850
WServer11	Server Intranet IIS 6.1	Microsoft(R) Windows(R) Server 2003, Standard Edition	Dell PowerEdge 2850
WServer12	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003 R2 Enterprise x64	Dell PowerEdge 2850
WServer13	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003 Enterprise x64 Edition	Dell PowerEdge 2850
WServer14	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003, Standard Edition	Dell PowerEdge 2850
WServer15	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003, Standard Edition	IBM System x3650 -[7979PBM]-
WServer16	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003, Standard Edition	IBM System x3650 -[7979PBM]-
WServer17	Server Intranet IIS 6.0	Microsoft(R) Windows(R) Server 2003, Standard Edition	IBM System x3650 -[7979PBM]-
WServer18	Em substituição	n/a	Dell PowerEdge 2850
WServer19	Gerenciamento Storage	W2003 Standard	IBM E-Server (L x A x P 49 x 22 x 78 cm)
WServer20	Gerenciamento Storage	Microsoft(R) Windows(R) Server 2003, Standard Edition	N/D
WServer21	Transferencia de Arquivos EDI	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	IBM System x3650 -[7979PBM]-
WServer22	Transferencia de Arquivos EDI	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	IBM System x3650 -[7979PBM]-
WServer23	Lotus Domino Server	Microsoft(R) Windows(R) Server 2003, Enterprise Edition	N/D

Exemplificação do controle de servidores Windows e LINUX distribuídos entre os dois sites da empresa

Levantamento de Setembro/2010

LINUX

NAME	PROVISIONED SPACE	NOTES
LNX001	10,25 GB	Prod – Crédito Rural -Hipotecas
LNX002	35,29 GB	Hom - Servidor de agencia
LNX003	24,05 GB	Prod - Gateway de agências e roteadores
LNX004	57,00 GB	Prod - Web Server
LNX005	44,10 GB	Prod - Contingencia
LNX006	33,03 GB	Des - Build Host e Geracao de Imagens Red Hat
LNX007	128,03 GB	Prod - IDS/logs (Servidores Agencias e DG)
LNX008	36,03 GB	Prod - Time server DG e Agências + OpenLdap Slave
LNX009	27,03 GB	Prod - Logs dos Roteadores do core
LNX010	21,95 GB	Prod - Longo Prazo
LNX011	137,00 GB	Des - Automacao Bancaria, migracao do servidor fisico
LNX012	153,87 GB	Prod - Oracle GRID e RMAN
LNX013	103,79 GB	Hom - CAIXA RS
LNX014	12,03 GB	Prod - smtp suporte HP
LNX015	28,25 GB	Des - Cent OS para automação bancária
LNX016	48,00 GB	Des – Mobile Banking
LNX017	83,95 GB	Prod - Base TerraView
LNX018	82,00 GB	Des - Novas imagens para os servidores das agências.
LNX019	30,50 GB	Produção - Servidor WIKI
LNX020	55,97 GB	Des – Software Monitoração 64 bits
LNX021	14,03 GB	Prod – Sistema de Roteamento
LNX022	18,93 GB	Des – Terminal Eletronico Financeiro

ANEXO B – Log do SRM com evidencias de teste do PCN do ambiente Vmware executado com sucesso.

RP-Group-G04-S2

Description

Start Time: 30/06/2010 07:12:59

Finish Time: 30/06/2010 07:21:14

Total Execution Time: 00:08:14

Mode: Test

Overall Result: Success

Recovery Step	Result	Execution Time
1. Shutdown Protected Virtual Machines at Protected Site "Site Recovery for Empresa Analisada"		
1.1. Shutdown Low Priority Protected Virtual Machines		
1.2. Shutdown Normal Priority Protected Virtual Machines		
1.2.1. Shutdown Protected Site VM "Wserver01"		
1.2.1.1. Shutdown Guest OS for Remote VM "Wserver01"		
1.2.1.2. Wait for Guest OS Shutdown		
1.2.1.3. Power off VM "Wserver01"		
1.2.2. Shutdown Protected Site VM "WSERVER02"		
1.2.2.1. Shutdown Guest OS for Remote VM "WSERVER02"		
1.2.2.2. Wait for Guest OS Shutdown		
1.2.2.3. Power off VM "WSERVER02"		
1.2.3. Shutdown Protected Site VM "WSERVER03"		
1.2.3.1. Shutdown Guest OS for Remote VM "WSERVER03"		
1.2.3.2. Wait for Guest OS Shutdown		
1.2.3.3. Power off VM "WSERVER03"		
1.3. Shutdown High Priority Protected Virtual Machines		
2. Prepare Storage	Success	00:02:24
2.1. Attach Disks for Protection Group "Protection_Group_G04_S2"	Success	00:02:24
3. Suspend Non-critical Virtual Machines	Success	00:00:00
4. Recover High Priority Virtual Machines	Success	00:00:00
5. Recover Normal Priority Virtual Machines	Success	00:03:23
5.1. Recover VM "WSERVER01"	Success: Host	00:03:00
5.1.1. Change Network Settings	Success	00:00:50
5.1.2. Pre-Power On	Success	00:00:00

5.1.3. Power On	Success: Host	00:00:14
5.1.4. Wait for OS Heartbeat	Success	00:01:54
5.1.5. Post Power On	Success	00:00:00
5.2. Recover VM "WSERVER02"	Success: Host	00:03:21
5.2.1. Change Network Settings	Success	00:00:50
5.2.2. Pre-Power On	Success	00:00:00
5.2.3. Power On	Success: Host	00:00:14
5.2.4. Wait for OS Heartbeat	Success	00:02:14
5.2.5. Post Power On	Success	00:00:00
5.3. Recover VM "WSERVER03"	Success: Host	00:02:26
5.3.1. Change Network Settings	Success	00:00:16
5.3.2. Pre-Power On	Success	00:00:00
5.3.3. Power On	Success: Host	00:00:09
5.3.4. Wait for OS Heartbeat	Success	00:01:22
5.3.5. Post Power On	Success	00:00:00
6. Recover Low Priority Virtual Machines	Success	00:00:00
7. Recover No Power On Virtual Machines	Success	00:00:00
8. Message: Test recovery complete. Please verify the success of the test. When done, click Continue to clean up the test and return to a ready state.	Success	00:00:04
9. Cleanup Virtual Machines Post Test	Success	00:00:37
9.1. Remove Test VM "WSERVER01"	Success	00:00:08
9.1.1. PowerOff VM "WSERVER01"	Success	00:00:08
9.2. Remove Test VM "WSERVER02"	Success	00:00:12
9.2.1. PowerOff VM "WSERVER02"	Success	00:00:12
9.3. Remove Test VM "WSERVER03"	Success	00:00:07
9.3.1. PowerOff VM "WSERVER03"	Success	00:00:07
10. Resume Non-critical Virtual Machines	Success	00:00:00
11. Reset Storage Post Test	Success	00:01:43
11.1. Reset Disks for Protection Group "Protection_Group_G04_S2"	Success	00:01:43