UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

TRABALHO DE LICENCIATURA

Plano de Continuidade de Negócios - sua aplicação nos CFM

AUTOR: **Mahomed Akil Ashraf**
SUPERVISORES: **Prof. Doutora Esselina Macome e Prof. Doutor Emílio Mosse**
DATA : **Fevereiro de 2009**

Dedicatória

A quem devo a vida, meus pais.

Agradecimentos

Em primeiro lugar agradecer aos meus pais, por todo o apoio e amor incondicional, pela mestria e calma com que me criaram e contribuíram para o que sou hoje. Sem esquecer a minha irmã e a minha noiva: foram muitos os sorrisos que vocês "arrancaram" de mim em momentos difíceis e me deram força anímica para continuar sempre caminhando nesta jornada.

Gostaria de agradecer igualmente à Prof. Doutora Esselina Macome e ao Prof. Doutor Emílio Mosse, pela sapiência com que guiaram e acompanharam este trabalho e pela forma como transmitiram um espírito investigador.

Seria injusto não mencionar aqui todos os docentes, colegas e funcionários do DMI, que tornaram os anos nesta instituição, os melhores da minha vida. A todos o meu muito obrigado.

Um agradecimento especial aos amigos Devan, Danilo, Euclides, Nelson, Nélia, Cecília e Anilza pelo apoio na realização deste trabalho e pelo companheirismo demonstrado.

Por fim, mas não menos importante, um obrigado especial aos funcionários do Serviço de Informática dos CFM, pelo valioso tempo dispendido comigo.

Mahomed Akil Ashraf

Declaração de Honra

Declaro por minha honra, que este trabalho é resultado da minha investigação e que não foi submetido para outro grau que não seja o indicado "Licenciatura em Informática", na Universidade Eduardo Mondlane.

Maputo, Fevereiro de 2009

O Estudante

(Mahomed Akil Ashraf)

Resumo

Na actual Sociedade de Informação, o correcto uso das TIC proporciona vantagem competitiva e estratégica às organizações. Dos recursos explorados há que salientar as redes informáticas que permitem a partilha de informação e recursos, e os sistemas de informação que permitem elevar os níveis de gestão fornecendo dados de forma íntegra e consistente.

Os CFM não fogem à regra das organizações que pretendem transitar para a nova Era, estando neste momento num processo acelerado de expansão da rede informática, o que permite aos seus utilizadores a nível nacional o acesso aos serviços de rede tais como *Internet* e *E-mail*.

Por outro lado, a recente aquisição de um sistema de informação, cuja implementação é conduzida pelo Serviço de Informática dos CFM traz novas responsabilidades tais como a garantia de acesso e disponibilização de informação correcta e em tempos aceitáveis.

Estas responsabilidades e as necessidades de garantia de um serviço contínuo invocam o conceito Plano de Continuidade de Negócios, como uma ferramenta que visa preparar as organizações para que em situações adversas não se vejam forçadas a interromper suas actividades nucleares.

Assim, o presente trabalho debruçar-se-á sobre este conceito e sua envolvente tendo como caso de estudo o Serviço de Informática dos CFM.

Siglas

- AIN – Análise de Impacto no Negócio
- BSI – *British Standards Institute*
- CD – *Compact Disc*
- CFM – Caminhos de Ferro de Moçambique
- CPD – Centro de Processamento de Dados
- CSU/DSU – *Channel Service Unit/Data Service Unit*
- DHCP – *Dynamic Host Configuration Protocol*
- DNS – *Domain Name System*
- DVD – *Digital Versatile Disc*
- ERP – *Enterprise Resource Planning*
- IP – *Internet Protocol*
- ISO – *International Organization for Standardization*
- LAN – *Local Area Network*
- NAV – Norton Anti-Virus
- PCN – Plano de Continuidade de Negócios
- RAID – *Redundant Array of Independent Disks*
- RPO – *Recovery Point Objective*
- RTO – *Recovery Time Objective*
- SIGRH – Sistema Informático de Gestão de Recursos Humanos
- STP – *Spanning Tree Protocol*
- TACACS – *Terminal Access Controller Access-Control System*
- TIC – Tecnologias de Informação e Comunicação
- UPS – *Uninterruptible Power Supply*
- WAN – *Wide-Area Network*

Índice de Figuras

Índice de Tabelas

Índice

CAPÍTULO I

1 INTRODUÇÃO E OBJECTIVOS

1.1 Introdução

Nesta Era de Informação, o papel das Tecnologias de Informação e Comunicação (TIC) tornou-se relevante e sua efectiva utilização pelas organizações tem sido considerada crucial para a sobrevivência e para a estratégia competitiva (Oliveira, 2004).

A *Safe in the Knowledge Limited* [1] apresenta, em um artigo disponibilizado na sua página de Internet, uma pesquisa efectuada em 2005 no mercado Inglês, na qual as estatísticas indicavam que por ano, 20% das organizações sofrem uma interrupção de vulto. O factor de sobrevivência das organizações reside no seu estado de preparação para fazer face a estas interrupções de modo a que estas durem o mínimo possível. Uma interrupção prolongada pode gerar inúmeras perdas, não só financeiras, como também de reputação junto a clientes, parceiros e fornecedores, verificando-se em alguns casos o fim de uma organização.

Canton (2005) aponta os desastres, quer sejam naturais, tecnológicos ou humanos, voluntários ou involuntários como origens destas interrupções nos serviços das TIC e por outro lado, Fagundes (2004) afirma que nestas circunstâncias, as organizações tornam-se muitas vezes forçadas a operar manualmente durante um período significativo. A Gestão da Informação normalmente automatizada passa agora a ser processada manualmente o que requer um esforço laboral extra e consequentemente uma diminuição da eficiência do negócio, trazendo prejuízos à organização.

Todas as organizações procuram o sucesso no negócio, contudo poucas são as que se preparam para as devastadoras consequências de um desastre, e estar preparado pode ser a ferramenta mais eficiente a aplicar para garantir que a organização sobreviva (Sikich, 2003).

[1] Líder na área de continuidade de negócios no mercado Inglês

Questiona-se assim se devemos ficar impávidos a estas situações e apenas aguardar para que elas não aconteçam ou que tenham o mínimo impacto possível? Ou devemos manifestar-nos e movimentar-nos de forma a precaver ou minimizar os danos causados por tais incidentes e desastres?

Doughty (2004) responde a estas questões indicando como objectivo primário de qualquer organização, o fornecimento dos seus produtos e/ou serviços sem interrupção incentivando assim a prevenção contra os incidentes.

Assim, ao se prevenir deve-se ter uma visão mais abrangente que consiste em manter a organização activa através da manutenção dos seus processos nucleares. A esta prevenção denomina-se Plano de Continuidade de Negócios (PCN).

O PCN é definido por Elliot *et al* (2002) como sendo um guia de acções a serem tomadas, numa sequência determinada, no evento de uma interrupção nas operações de uma organização.

Doswell (2000) cita o ciclo a ser percorrido durante a implementação de um PCN, de forma a tornar o processo devidamente estruturado e mais económico. Este ciclo é composto pelas seguintes fases:

- Análise de Riscos no Negócio;
- Definição da estratégia organizacional para lidar com os riscos identificados na fase anterior bem como implementação de medidas preventivas e desenvolvimento do plano;
- Testes à (s) equipa (s) envolvida (s) e ao plano, de forma a avaliar a real capacidade de resposta e posterior manutenção do plano.

Neste âmbito, o presente trabalho propõe-se a abordar o Plano de Continuidade de Negócios, tomando os Caminhos de Ferro de Moçambique (CFM) como caso de estudo, dada a sua disponibilidade para participar do mesmo. Como complemento, foi também efectuado um inquérito a empresas seleccionadas a partir do relatório das 100 maiores empresas moçambicanas realizado em 2006 pela KPMG[2].

[2] Multinacional e um dos líderes mundiais na área de Auditoria

De seguida apresenta-se a definição do problema que se debruça sobre os principais constrangimentos das organizações em geral, e das moçambicanas em particular, na sua vertente de Continuidade de Negócios.

1.2 Definição do problema

Segundo Oliveira (2004), a efectiva utilização das TIC pelas organizações tem sido considerada crucial para a sobrevivência e estratégia competitiva das mesmas. De acordo com a KDDI[3], algumas das causas de interrupções que podem prejudicar sensivelmente a estrutura de uma empresa, enquadram-se na categoria de causas naturais tais como inundações, tornados, terramotos, incêndios, explosões vulcânicas e outras.

O Portal do Governo de Moçambique identifica ainda alguns factores que tornam o país propenso à ocorrência cíclica de calamidades com efeitos socioeconómicos negativos. Tais factores são:

- A localização geográfica e as condições agro-climatéricas que se traduzem em inundações que podem danificar infra-estruturas afectando desta forma as TIC e posteriormente a Gestão da Informação. De forma a exemplificar este tipo de situações pode-se tomar como base as cheias ocorridas no início de 2008, no vale do Rio Zambeze.
- A localização de paióis e repositórios de armamento, situados em centros urbanos e zonas habitacionais, como se verificou aquando das explosões registadas nos paióis das cidades de Maputo e Beira, que levaram à projecção de diversos artefactos militares causando danos humanos e materiais avultados.

Segundo Elliot *et al* (2002), as consequências de alguns eventos podem ainda ser agravadas por factores humanos, mencionando o autor como exemplo o caso das cheias de 2000 em Moçambique, sublinhando que o seu grande impacto negativo foi composto, de entre outros, pela falta de recursos e pela decisão dos países vizinhos de efectuar descargas das suas centrais hidroeléctricas de forma a conter o risco de inundações nos seus territórios, consequentemente transferindo este risco para Moçambique.

A 4ª edição do informe da Estratégia Internacional de Redução de Desastres das Nações Unidas (NU/EIRD) para África, indica cidades situadas na costa oriental de África, tais como a cidade de Beira, como sendo altamente vulneráveis aos danos resultantes de terramotos originados ao longo das

[3] Multinacional operadora de comunicações globais e integradora de soluções de origem Japonesa

ramificações orientais do Grande Sistema de Falhas da África Oriental (EARS), com o problema adicional de ocorrerem possíveis efeitos de ondas do mar provocadas pela sismicidade (*tsunami*). De salientar ainda que Moçambique foi atingido no dia 23 de Fevereiro de 2006 por um terramoto que durou aproximadamente 1 minuto, com uma magnitude de 7.5 graus na escala de Richter, facto corroborado por um Comunicado do Conselho de Ministros, no mesmo dia e disponibilizado no Portal do Governo Moçambicano.

A página de *Internet* da Comissão para a Política de Informática do Governo Moçambicano faz referência a taxa de analfabetismo do país estimada acima dos 50% em 2004 e ao índice de teledensidade do país que é um dos mais baixos do continente. Estas situações contribuem para a falta de conhecimento e experiência nas áreas tecnológicas e consequente incremento da probabilidade de ocorrência de interrupções derivadas de falhas humanas e/ou técnicas, que afectam directamente a integridade e a Gestão da Informação.

Fagundes (2004) retrata ainda a paralisação do serviço de *e-mail* do provedor de *Internet* brasileiro Terra, em Abril de 2003 como um exemplo de interrupção de um sistema por razões técnicas. O provedor teve que abonar dois dias da mensalidade dos seus 800 mil assinantes com um prejuízo de mais de R$ 400.000,00 (quatrocentos mil reais brasileiros), equivalentes a cerca de 5.000.000,00 MT.

O Portal do Governo de Moçambique menciona ainda a grande perda de informação em consequência do incêndio registado a 25 de Maio de 2007 no Ministério da Agricultura, na cidade de Maputo. Este desastre organizacional verificou-se devido ao facto de o referido Ministério não possuir cópias de segurança do sistema informático, tendo como solução a reconstituição com base em informações de outras instituições o que pode deturpa-las. Este é um risco ao qual os CFM se encontram sujeitos, tal como qualquer outra organização.

Os factores acima mencionados são também sublinhados por Doughty (2004), que aponta ainda outros aspectos que são um risco para a continuidade operacional, tais como:

- A pouca formação ou de má qualidade;
- Os riscos de origem técnica tais como a adopção ou mudança de sistema informático, quebra ou falhas de comunicações, falhas de *hardware* entre outros. Este factor está inserido na realidade

dos CFM que atravessa uma fase de transição de sistemas e informatização de diversos processos trazendo à tona questões relacionadas com o *hardware* e comunicações.

Todos estes aspectos têm influência directa sobre a continuidade operacional visto representarem uma ameaça à Informação, a qual em caso de perda e segundo uma estatística realizada pelo Ministério de Trabalho dos Estados Unidos em 2003, traduz-se em 93% de probabilidade de falência de organizações sujeitas a tal prejuízo. Esta situação deixa evidente a vulnerabilidade a que uma grande parte das organizações está sujeita, incluindo os CFM.

Considerando os constrangimentos acima verificados, o presente estudo propõe o desenvolvimento de um modelo de PCN para o Serviço de Informática dos CFM.

1.3 Objectivos

Devido aos problemas mencionados na secção anterior, segue o objectivo do presente trabalho.

1.3.1 Objectivo geral

- Analisar os principais constrangimentos relacionados à continuidade operacional do Serviço de Informática dos CFM e desenvolver um protótipo de Plano de Continuidade de Negócios adequado.

1.3.2 Objectivos específicos

- Realizar um apuramento estatístico relativamente ao conhecimento e uso das ferramentas de continuidade operacional por parte das empresas moçambicanas;
- Identificar os principais constrangimentos, fraquezas e ameaças à continuidade de negócios no Serviço de Informática dos CFM;
- Seleccionar o método de desenvolvimento de planos de continuidade de negócios, técnicas e ferramentas de continuidade operacional que mais se adequam ao caso de estudo;
- Desenvolver o protótipo de plano de continuidade de negócios que se adapte a realidade do Serviço de Informática dos CFM.

1.4 Estrutura do Trabalho

O presente trabalho se encontra dividido em 8 capítulos, a saber:

1. O primeiro capítulo apresenta uma breve introdução ao tema, a definição do problema e os objectivos deste trabalho;
2. No segundo capítulo são mencionados os materiais usados e os métodos empregues na elaboração do presente trabalho.
3. O terceiro capítulo traça os alicerces para o tema, apresentando conceitos básicos que serão posteriormente usados.
4. É neste capítulo que o conceito PCN é introduzido e explanado, sendo apresentados elementos envolventes e abordados detalhes técnicos.
5. O quinto capítulo apresenta o caso de estudo que servirá para o desenho do modelo do PCN que é apresentado na forma de um documento adjacente a este trabalho.
6. As conclusões e recomendações constam do sexto capítulo.
7. No sétimo capítulo é referenciada toda a bibliografia usada durante a elaboração deste trabalho.
8. Os anexos podem ser encontrados no último capítulo, nomeadamente o oitavo capítulo.

Adjacente a este documento, encontra-se o protótipo de Plano de Continuidade de Negócios para os CFM.

CAPÍTULO II

2 MATERIAL E MÉTODOS

Na secção 1.3. foram apresentados os objectivos deste trabalho, sendo os meios adoptados para alcançar estes objectivos descritos neste capítulo.

Para a realização do apuramento estatístico relativamente ao conhecimento e uso das ferramentas de continuidade operacional por parte das empresas moçambicanas foram efectuados inquéritos e entrevistas a empresas seleccionadas com base na pesquisa anual das 100 maiores empresas moçambicanas efectuada pela KPMG em 2006 que considera os resultados financeiros de 2004. O presente estudo foi realizado um ano após a divulgação do relatório, ou seja, em 2007.

O desenvolvimento do inquérito para o apuramento estatístico, visível no Anexo **A**, foi efectuado tendo como base inquéritos propostos por Doughty (2004) e Doswell (2000) em suas obras e ainda colhendo opiniões e sugestões de consultores no mercado moçambicano que tenham participado em projectos semelhantes. De seguida foram inquiridas empresas pertencentes ao universo em causa, sendo que apenas 29 se mostraram disponíveis a responder ao inquérito e participar do estudo.

As estatísticas derivantes destes inquéritos podem ser consultadas no Anexo E. Os resultados deste inquérito, associados à crescente necessidade de funcionamento ininterrupto das organizações foram um incentivo adicional à realização do trabalho subordinado ao tema Plano de Continuidade de Negócios.

Para a elaboração das estatísticas apresentadas foi usado o Microsoft Excel para auxílio na determinação dos resultados estatísticos.

Tendo em vista o objectivo seguinte, seguiu-se a revisão bibliográfica através da consulta a obras e literatura de interesse, consultas a organizações com planos de características similares, entrevistas informais a consultores independentes seguindo o guião apresentado no Anexo **C**, e ainda a consultas na *Internet*.

De forma a permitir a identificação dos principais constrangimentos, fraquezas e ameaças à continuidade de negócios nos CFM, foram igualmente efectuados inquéritos, que segundo D'Ascenção (2001) são uma excelente forma de angariar dados para cálculos estatísticos. O inquérito visava perceber o nível de preparação dos funcionários para fazer face a um incidente, o seu conhecimento e uso de ferramentas para garantia de continuidade e as condições organizacionais para a garantia de um funcionamento sem interrupções de vulto. Este inquérito pode ser encontrado no Anexo **B**, contudo, por questões relacionadas à confidencialidade da informação, os seus resultados não serão apresentados neste trabalho.

Foram também realizadas entrevistas segundo o guião de entrevistas constante no Anexo **D** e efectuadas leituras à documentação interna existente.

Devido à dimensão e complexidade organizacional encontrada, o escopo do estudo foi limitado ao Serviço de Informática, na qualidade de órgão responsável pela implementação, gestão e manutenção das TIC nos CFM.

Os processos anteriores permitiram analisar as características inerentes à Continuidade Operacional e identificar constrangimentos que representam riscos e ameaças ao funcionamento pleno do Serviço de Informática.

Os métodos de desenvolvimento de planos de continuidade, as ferramentas e técnicas de continuidade operacional foram seleccionadas após diversos debates individuais com os funcionários – chave do Serviço de Informática, tendo em consideração os objectivos de recuperação e os custos associados.

CAPÍTULO III

3 INTRODUÇÃO AO PLANO DE CONTINUIDADE DE NEGÓCIOS

Lei de Murphy: "Qualquer coisa que pode correr mal irá correr mal!"
(Reuvid, 2005)

3.1 Definição de Risco

A presente secção tem por objectivo situar o leitor, relativamente a um dos conceitos mais importantes inerentes ao tema, que é na realidade a razão de existência da Continuidade de Negócios. Tal conceito é Risco.

Na sociedade actual, é impossível retirar totalmente o risco presente nas actividades, e assim as organizações devem "aceitar" a exposição a um certo grau aceitável de risco (Doughty, 2001). Este risco é definido por Miguel (2003) como sendo o grau de exposição a acontecimentos considerados negativos. Esta será a definição assumida neste trabalho.

Mandia & Promise *apud* Mamede (2006) enfatiza ainda que os riscos podem passar despercebidos até ao ponto em que os mesmos se concretizam tornando evidente a sua existência, e dependendo da dimensão, natureza e outros factores relacionados com a própria organização, o risco ao realizar-se pode ter um impacto inconsiderável ou devastador.

Actualmente existem muitos riscos para as organizações, alguns herdados pela natureza das operações, outros naturais, globais ou até não relacionados. No presente mundo de crescente complexidade e incerteza, as organizações devem gerir os riscos de forma mais rigorosa possível. Surpreendentemente, a maior parte delas não o faz, provavelmente porque se sentem impotentes. Mas o mais preocupante

ainda é o facto de algumas delas permanecerem despercebidas aos riscos a que se encontram expostas (Reuvid, 2005).

A realização do risco é um evento que interrompe o procedimento normal de operações da organização, precipitando qualquer nível de crise. Segundo Doughty (2006), crises são situações inevitáveis numa sociedade crescentemente complexa e cada vez mais suportada por sistemas sócio-tecnológicos. O mesmo autor define crises como sendo condições ou situações necessitando de atenção ou acções urgentes. Uma reacção cuidadosa e organizada a uma crise pode representar a diferença entre a recuperação total e o desastre total. Qualquer crise é caracterizada por uma intensa pressão, pelo tempo e pelos constrangimentos de recursos, e não existem dois incidentes iguais e nenhum é abordado exactamente da mesma forma (Mamede, 2006).

A forma como as crises são geridas constitui a chave para a prevenção de desastres e subsequente minimização dos seus impactos (Doughty, 2001). O mesmo autor aborda o termo desastre no âmbito de Sistemas de Informação, afirmando que estes podem variar de uma inundação, incêndio ou terramoto até uma crise laboral ou a simples destruição de um arquivo de extrema importância.

Na secção seguinte será introduzido o conceito Continuidade de Negócios.

3.2 Definição de Continuidade de Negócios

Uma das perguntas mais pertinentes na actual Sociedade de Informação está ligada aos crescentes custos relacionados com problemas de segurança de informação. Uma das principais razões que aponta para tal é o facto de as organizações não estarem a acompanhar a curva tecnológica na sua íntegra, no que respeita à tomada de atitudes pró-activas de forma a melhorar as respectivas posturas face às questões de segurança (Mamede, 2006). Esta situação é apoiada por Doughty (2001), em sua obra, citando os recursos informáticos como uma área específica de preocupação.

A sensibilidade à perda de informação varia de organização para organização (Reuvid, 2005). Para Doughty (2004), a informação é um recurso valioso, não equiparável a um recurso material, que em certo momento pode ser substituído. Por mais que a organização possua seguros, instalações e infra-estruturas de suporte alternativas, ou contratos de manutenção e reposição de *hardware*, a integridade da informação deve ser mantida a todo o custo. Assim, a informação é um dos pilares para a continuidade operacional das organizações.

Esta continuidade operacional, ou Continuidade de Negócios, é definida por Sikich (2003) como sendo a combinação de estratégias, inteligência competitiva, gestão de eventos e conhecimento organizacional que irão assegurar a sobrevivência, crescimento, flexibilidade e viabilidade para a organização. Segundo Elliot *et al* (2002), as raízes da Continuidade de Negócios situam-se na protecção dos Sistemas de Informação. O pilar destes Sistemas de Informação – as TIC – são reconhecidas por Reuvid (2005), como sendo ferramentas essenciais para as estratégias de Continuidade de Negócios.

De acordo com Reuvid (2005), a Continuidade de Negócios fornece uma aproximação alternativa e mais rigorosa para a organização desenvolver a sua resposta a interrupções de serviço. Esta concentra-se no impacto do incidente e crucialmente na sua duração, em detrimento das suas causas. O mesmo autor menciona ainda a tentativa deste processo de identificar o ponto no tempo onde uma interrupção se torna intolerável, também conhecido por Objectivo Temporal de Recuperação (*Recovery Time Objective* – RTO). Outro conceito importante está relacionado com restauração da condição da

organização, a nível de estrutura de suporte às operações, há um ponto minimamente aceitável e funcional. Este conceito é denominado de RPO (*Recovery Point Objective*). O RTO e RPO podem ser únicos para toda a organização, mas na maior parte das situações existe um para cada departamento ou função vital da mesma.

Se uma organização pretende retornar às operações normais após uma interrupção, deve garantir a reactivação dos serviços e processos antes que os pontos supracitados sejam atingidos, deve incluir também na sua estratégia de Continuidade de Negócios, a Análise de Impacto nos Negócios e o Plano de Continuidade de Negócios (Doughty, 2004). A implementação desta estratégia é corroborada por Reuvid (2005) em sua obra, acrescentando ainda que a mesma deve espelhar a constante evolução da organização e o desenvolvimento das suas TIC. Salienta-se ainda a necessidade de existência de uma gestão centralizada da estratégia de Continuidade de Negócios e a importância do estabelecimento de uma rede de coordenadores por todos os departamentos da organização de forma a não excluir processos que provavelmente revelem-se vitais para o funcionamento organizacional.

A Continuidade de Negócios é recomendada e em alguns casos até imposta por alguns padrões e/ou legislações tais como:

- King I e King II – relatório publicado pelo Comité King com o objectivo de instaurar boas práticas de gestão corporativa na África do Sul;
- Sarbanes Oxley (Sarbox) – legislação Norte-Americana aprovada em 2002, que visa garantir a transparência na gestão financeira das organizações, credibilidade na contabilidade, auditoria e a segurança das informações para que sejam realmente fiáveis, evitando assim fraudes, fuga de investidores, etc;
- BS 25999 / BS 7799 / ISO 17799 – conjuntos de normas padrão e políticas de seguranças para área das TIC publicadas pelo Instituto de Padrões Britânicos (*British Standards Institute* – BSI) e Organização Internacional para a Normalização (*International Organization for Standardization* – ISO);
- Basel I e Basel II – padrão de continuidade de negócios publicado pelo Comité de Basel com o objectivo de regulamentar a gestão de risco de organizações do sector bancário internacionalmente.

Uma vez definida a Continuidade de Negócios, a secção seguinte irá abordar a definição do conceito Plano de Continuidade de Negócios.

3.3 Definição do PCN

Uma parte significativa do planeamento para prevenção de desastres pessoais é feita através de medidas preventivas que visam minimizar a probabilidade de um desastre recair sobre nós. Algumas destas medidas são tão básicas como garantir que o automóvel não fique sem combustível, instalar sistemas de seguranças nas nossas casas, verificar as condições do pneu sobressalente e as ferramentas necessárias para a sua substituição, etc. (Doughty, 2001). Para além destas medidas preventivas, desenvolvem-se também as capacidades de resposta a desastres, tais como, o procedimento para a mudança de um pneu furado ou de um fusível queimado.

Elliot *et al* (2002) e Fagundes (2004) são unânimes em definir o PCN da seguinte forma: Uma série de processos que tendem a identificar as ameaças internas e externas às quais uma organização está exposta de forma a sintetizar recursos que permitirão prover a mesma de uma prevenção e recuperação efectivas, sem perder a vantagem competitiva e o valor da integridade do sistema. Tais processos, previamente estruturados, são concebidos com o objectivo de eliminar decisões e atitudes desnecessárias imediatamente após a ocorrência de um desastre. A estratégia de recuperação deve estar sempre focada e vinculada aos processos de negócios, assim sendo, o envolvimento da alta gerência é um factor crítico.

Por outro lado, os processos são cada vez mais dependentes das TIC, considerando como aspecto negativo desta situação, a assumpção de que estas tecnologias estarão sempre disponíveis. Elliot *et* al (2002) cita Bangemann (1994), referindo que a gestão prudente das TIC e a exploração dos Sistemas de Informação em particular, são reconhecidas como habilidades – chave que ditam a vantagem organizacional na actual Sociedade de Informação. Assim, um PCN pode e deve ser conduzido pela área ou departamento responsável pelas TIC.

Um PCN bem estruturado deve rumar à simplicidade e flexibilidade. Não deve conter detalhes desnecessários, ser facilmente actualizável, e providenciar as alternativas necessárias. Por fim, o plano deve incluir um espaço dedicado ao seu próprio teste e manutenção (Doughty, 2001).

Este planeamento deve ainda determinar que recursos serão necessários e deverão ser usados para mitigar determinado evento ou potencial risco. Uma vez analisados e quantificados os potenciais riscos para a organização, e tomadas decisões relativamente às estratégias para a gestão de risco, estão reunidas as condições para fundamentar um PCN. Na sua forma mais simples, o PCN identifica as vulnerabilidades e traça as estratégias para lidar com elas. Deve cobrir no mínimo, a protecção e salvaguarda da informação vital para a organização: registos de clientes, facturação, ficheiro de pessoal, contactos, documentos de tesouraria, etc. (Canton, 2003).

Actualmente, um PCN não é mais uma luxúria ou ferramenta de organizações gigantescas, mas sim uma necessidade comum de qualquer organização. Contudo, a decisão de investir em um PCN é ainda em muitos casos forçada, por exemplo, por obrigações legais, por imposição de terceiros ou em caso pior, após a ocorrência de uma interrupção e como medida de prevenção de outras interrupções.

Serão de seguida apresentados alguns objectivos e benefícios do PCN.

3.4 Objectivos e Benefícios do PCN

De acordo com Elliot *et al* (2002), as organizações são parte de um ambiente caracterizado por incertezas e instabilidade, rumando sempre a novos desafios. Assim, o PCN deve ser capaz de acompanhar a evolução das organizações neste "mar agitado" conferindo o máximo de segurança e mínimo de exposição a riscos possíveis. A maior preocupação de um PCN está relacionada com a prevenção e gestão de risco, e só após isto a recuperação e resumo de actividades (Doughty, 2001). Assim, o principal objectivo de um PCN é garantir a operação da empresa com o mínimo impacto aos clientes em situações de contingência (Fagundes, 2004). Outros objectivos são:

- Garantir que os processos críticos de negócio possam ser restabelecidos antes de causar prejuízos sensíveis;
- Atender as exigências de ambientes que demandam alta responsabilidade;
- Dar confiança aos clientes, parceiros, funcionários e governo na continuidade do negócio pela recuperação plena das operações.

Muitos gestores têm ainda a concepção que os investimentos em PCN implicam consumo de recursos que poderiam ser aplicados em áreas sobre as quais a organização teria retorno. Contudo, esta abordagem não é a mais correcta considerando que o investimento em um PCN reflecte-se na protecção da vida da organização de forma a garantir que os retornos possam ser gerados e trazer outras vantagens para a mesma. A Módulo[4] cita em seu site algumas das vantagens do uso de um PCN:

- Redução de custos financeiros, derivados da paragem dos processos de negócios e redução dos riscos e impactos inerentes aos eventos inesperados;
- Redução do tempo de resposta, frente a indisponibilidade de componentes que suportam os principais processos de negócios;
- Aumento da credibilidade com os integrantes da cadeia produtiva, accionistas e clientes;
- Cumprimento de normas legais relacionadas com a Continuidade dos Negócios.

[4] Líder Brasileiro na área de segurança das TIC

CAPÍTULO IV

4 CICLO DE VIDA DO PCN

"Desastres podem ser devastadores para um negócio."

(Canton, 2003)

Segundo Doughty (2001) e Fagundes (2004), o desenvolvimento de um PCN é contínuo e dinâmico tal como o seu ciclo de vida representado na Figura 1.

Figura 1: Ciclo de vida do PCN

(Fagundes, 2004)

As três fases que compõem o ciclo de vida do PCN, serão abordadas em detalhes nas secções que se seguem, nomeadamente:

- Análise de Impacto no Negócio – onde são apurados os riscos e respectivas probabilidades aos quais a organização está sujeita;
- Desenvolvimento e Implementação – consiste na selecção e implementação das técnicas e ferramentas escolhidas para minimizar os riscos encontrados;

- Teste e manutenção – deve garantir que o PCN se encontre devidamente estruturado realizando testes e actualizações ao mesmo.

4.1 Análise de Impacto no Negócio

No uso de qualquer tecnologia, processo e/ou procedimento devem ser determinados onde consequências inesperadas e indesejadas podem ocorrer na aplicação destas tecnologias. È necessário que os gestores olhem para os seus objectivos e para as ferramentas usadas para alcançá-los, de forma a determinar os seus pontos críticos. (Doughty, 2001)

A Análise de Impacto no Negócio (*Business Impact Analysis*) – AIN, segundo Elliot *et al* (2002), é o termo usado para descrever o processo de medição das maiores probabilidades de ocorrência de determinado evento num conjunto de eventos, bem como das consequências dos mesmos. Doughty (2004) apresenta uma definição mais abrangente: É a ciência e arte de reconhecimento de ameaças ou riscos existentes, determinação das suas consequências sobre os recursos e aplicação de modificações de uma forma economicamente viável para manter as consequências sobre fronteiras (controladas). Um dos principais objectivos deste processo é garantir que a organização não esteja exposta à níveis de risco inaceitáveis, contudo este processo está sujeito a percepções e interpretações individuais (Miguel, 2003).

Uma AIN completa é normalmente um processo muito dispendioso em termos cronológicos, consumindo imensas horas de trabalho à medida que os especialistas analisam riscos internos e externos. É importante neste estágio despender algum tempo analisando a possibilidade de ocorrência dos riscos e a probabilidade dos mesmo interromperem o fluxo organizacional. É neste momento que uma grande parte dos riscos são reduzidos, mitigados ou ignorados, sendo o resultado final uma avaliação de risco que detalha os riscos que a organização enfrenta, de uma forma concisa que possa ser facilmente compreendida e que permita a tomada de acções concretas e eficazes. Em termos teóricos e de forma genérica, as organizações devem:

- Efectuar uma avaliação da informação e da relevância da mesma para a organização;
- Identificar os riscos à informação, quer sejam eles de origem humana ou natural, internos ou externos;

- Quantificar as probabilidades de materialização dos riscos identificados, incluindo aqueles que ultrapassem as medidas preventivas já existentes;
- Identificar as funções críticas que devem ter prioridade na recuperação em relação às outras funções;
- Desenhar metodologias de mitigação ou redução até pontos considerados aceitáveis das ameaças identificadas (Reuvid, 2005).

O processo de recuperação de uma organização após uma crise pode ser equiparado aos cuidados de primeiros socorros que são prestados em casos de acidentes. Devem ser primeiro restabelecidas as funções vitais de modo a garantir a sobrevivência e só então devemo-nos preocupar com as restantes funções. O primeiro passo na identificação das áreas de maior risco dentro da organização consiste em obter uma visão geral a alto nível. Este passo é importante de modo a perceber a magnitude do ambiente operacional. De forma a obter esta visão a um alto nível são recomendados os seguintes documentos: organigrama organizacional, políticas, padrões e procedimentos de segurança, diagramas de rede, listas de aplicações, ferramentas de gestão de rede e bases de dados, inventários e relatórios de análises anteriores. (Killmeyer, 2006)

Para a quantificação das probabilidades e riscos Canton (2003) sugere duas abordagens:

1. A mais simples consiste em atribuir um valor de 1 a 3, de acordo com a sua criticidade e probabilidade de ocorrência do desastre (Alto - 3; Médio - 2; Baixo - 1). Somando estes 2 factores poderá obter-se uma "pontuação total" de forma a classificar as ameaças tal como demonstra a Tabela 1.

Tabela 1: Medição simples de riscos

(Canton, 2003)

Desastre potencial	Probabilidade de ocorrência	Potencial impacto	Total
Incêndio	Baixa (1)	Médio (2)	3
Ataque terrorista	Baixa (1)	Alto (3)	4
Inundações	Média (2)	Baixa (1)	3
Falha no sistema de facturação	Alta (3)	Alta (3)	6

2. Também descrita por Reuvid (2005), esta abordagem é mais profunda e complexa e consiste em atribuir valores para uma série de factores inerentes à organização, e não só a criticidade e probabilidade como anteriormente proposto. Tal como se pode ver na Tabela 2, devem ser atribuídos valores ou "pesos" à probabilidade de ocorrência e ao impacto à nível humano, estrutural, comercial ou financeiro, e ainda ao impacto no que diz respeito à imagem da organização quer a nível interno como externo. Assim, e tendo em conta o mesmo modelo de soma dos valores aplicados no primeiro método, serão classificadas as ameaças a que a organização está mais exposta. A escala usada nesta matriz é variável, cabendo a decisão à equipa de Análise.

Tabela 2: Medição detalhada de riscos

(Reuvid, 2005)

Desastre	Probabilidade	Impacto humano	Impacto material	Impacto no negócio	Recursos internos para mitigação	Recursos externos para mitigação	Total	Recursos para mitigação
Incêndio	2	3	4	3	4	2	18	6
Ataque Terrorista	1	5	5	4	4	4	23	8
Inundações	3	3	2	3	2	2	15	3
Falha no Sistema de Facturação	4	1	1	5	3	1	15	4

Escala:

- Probabilidade
  - Baixa – 1
  - Alta – 5
- Impacto
  - Baixo – 1
  - Alto – 5

- Recursos para mitigação
    - Existentes – 1
    - Inexistentes – 5

È importante salientar que, por mais experientes e profissionais que sejam os consultores ou colaboradores envolvidos no processo de avaliação do risco, é necessária uma participação activa dos funcionários da organização, pois estes melhor que ninguém conhecem-na bem como seus processos vitais e eventualmente os riscos envolvidos e permitem dar uma visão interna da organização (Reuvid, 2005). Contudo, de acordo com Elliot *et al* (2002), a AIN apresenta algumas limitações. Uma delas está ligada à complexidade do sistema em estudo. Identificar todas as variáveis pode tornar-se extremamente difícil. Reuvid (2005) vai mais além, afirmando que em termos práticos a análise quantitativa pode demonstrar sérias complicações de implementação, sendo que as organizações na sua maioria classificam os riscos em termos de baixos, médios ou altos.

É importante não subestimar o papel da AIN, pois o PCN é simplesmente um esforço para mitigação de riscos. Somente após o término desta fase será possível proceder à implementação de um modelo de continuidade de negócios com a confiança necessária.

Este processo (AIN) constitui toda a espinha dorsal do processo de Continuidade de Negócios (Elliot *et al*, 2002).

4.2 Desenvolvimento e implementação do PCN

O PCN a ser implementado deverá assegurar que qualquer desastre ou interrupção tenha o mínimo de impacto possível sobre a organização. O plano deverá mencionar as razões que levaram a organização a desenvolvê-lo nas áreas funcionais da mesma, e que funcionários e recursos estão alocados de forma a tornar o plano funcional (Doughty, 2004). Contudo, de acordo com Elliot *et al* (2002), é importante que o PCN não crie uma imagem falsa de uma organização com excelentes práticas de gestão em geral e segurança em particular.

4.2.1 Desenvolvimento do PCN

Segundo Elliot *et al* (2002), o desenvolvimento de um PCN está longe de ser uma ciência. Contudo, existe uma série de recomendações e técnicas já desenvolvidas por diversos autores. Todas estas são flexíveis na sua implementação e passíveis de serem usadas simultaneamente. Esta é uma decisão a ser tomada pela equipa de implementação do PCN tendo em conta o ambiente no qual a organização se encontra inserida.

O PCN pode ser desenvolvido de duas formas (Elliott *et al*, 2002):

1. Usando um "esqueleto" (*template*) fornecido normalmente por uma organização especializada na área, quer seja na forma de uma aplicação (*software*) ou em papel, que de seguida deve ser adaptado, ou moldado, às necessidades e realidades da organização;
2. Criando uma estrutura de raiz, totalmente desenvolvida com o objectivo de servir às necessidades da organização sendo que esta opção, normalmente é levada a cabo por uma equipa de trabalho interina. Este tipo de desenvolvimento é geralmente conhecido pelo termo inglês *in the house development*.

Segundo Doughty (2001) o desenvolvimento pode ser dividido em duas partes:

1. Técnica: Tecnologias de Informação e Comunicação;
2. Negócios: Logística, contabilidade e administração, recursos humanos, etc.

Neste trabalho será abordado o PCN a nível das TIC. De acordo com Reuvid (2005), algumas das ferramentas mais usadas a este nível são:

- Políticas organizacionais, procedimentos e padrões (*standards*);
- Segurança física;
- Pacotes antivírus;
- Controlos de acessos;
- *Firewall*;
- Sistemas redundantes.

Estas ferramentas são, em grande número, implementadas sem uma AIN. Isto deve-se ao facto de serem consideradas boa prática ou de senso comum e outras vezes ainda podem ser usadas pela maioria. Contudo este raciocínio não é o mais correcto uma vez que não existem duas organizações iguais. Outra questão que deve ser levada em consideração está relacionada com políticas e legislações vigentes que devem ser respeitadas sob o risco de penalizações, que podem trazer um efeito totalmente oposto ao do desejado por um PCN.

Uma das melhores formas de iniciar o processo de implementação de um PCN é obtendo a aprovação de entidades superiores responsáveis pela estratégia organizacional por forma a tornar o PCN mais abrangente possível. O mesmo deverá preservar a integridade e a política dos negócios bem como ser detalhado o suficiente para que todo e qualquer funcionário da organização possa entendê-lo da forma mais clara e sucinta possível. Todos os funcionários – chave para o funcionamento do PCN, devem ser devidamente identificados assim como suas tarefas especificadas. Deve ser adoptada uma terminologia comum ao longo do plano de forma a clarificar o entendimento por todos (Doughty, 2001).

Toda a informação e documentação crítica e valiosa devem possuir uma cópia de segurança actualizada e devem ser estabelecidos os procedimentos para a restauração desta informação. O PCN deve estabelecer quais as informações vitais e a sua periodicidade de execução de cópias de segurança, testes, manutenção e todos outros procedimentos críticos. Deve também estabelecer as medidas de segurança necessárias em caso de desastre, bem como as medidas para as instalações alternativas, caso hajam. Normalmente é estruturado de forma que a informação que é necessária durante a fase de recuperação das operações esteja no início do documento, exceptuando procedimentos técnicos de recuperação e informação auxiliar (Doughty, 2001).

Uma das dificuldades que as equipas de implementação de um PCN muitas vezes enfrentam é a constante alteração do ambiente sobre a qual a organização se encontra inserida. O desejo de compor uma lista definitiva de todos os riscos e ameaças é penoso e muitas vezes não é alcançado. Assim, tentar lidar de forma específica com cada uma das ameaças pode tornar a implementação do PCN perpétua e esta situação deve ser controlada.

Durante o desenvolvimento do PCN é comum a falta de atenção sobre departamentos menos funcionais, que devem ser restaurados após os processos críticos. Os departamentos de informática são normalmente os primeiros na lista de recuperação, contudo está provado que o seu funcionamento isolado não garantirá a Continuidade de Negócios da organização. Devem ser detalhados também os pontos de interacção entre os departamentos (Doughty, 2001).

Outro factor bastante importante e que deve ser considerado na metodologia de desenvolvimento de um PCN são os serviços da organização que estão a cargo de terceiros. É comum nos dias de hoje que terceiros tenham um papel bastante activo nas organizações. Normalmente serviços especializados são encarregues a terceiros que demonstram ter maior aptidão e competência para determinada área para além de apresentar melhores custos.

Neste âmbito, muitos gestores consideram o risco associado aos serviços encarregues a terceiros como riscos extra-organizacionais, ou seja, riscos não pertencentes à organização. Nesta perspectiva, considera-se risco extra-organizacional mas tendo sempre em mente que a paragem de tais serviços pode ter consequências drásticas para a organização. Assim torna-se relevante analisar a fiabilidade de tais terceiros, no que concerne à continuidade de negócios de forma a garantir a existência da organização mesmo após uma interrupção inesperada (Doughty, 2001).

4.2.2 Estrutura do PCN

Apesar de não existir uma forma padronizada de elaboração de um PCN, segundo Canton (2003) existem 5 grandes secções que devem ser incluídas no PCN. Esta estrutura é também reconhecida por Doughty (2004) e corroborada por Doswell (2000) e é constituída pelas seguintes secções:

1. Introdução – Nesta secção devem ser descritos os objectivos do plano e apresentada uma breve apresentação da organização. De seguida deve ser indicado o escopo do plano, bem como as

exclusões e assumpções assumidas durante o desenvolvimento do plano. São ainda apresentados os resultados da AIN, as estratégias de continuidade já existentes e ainda as equipas que compõem o PCN e respectivo organigrama.

2. Informação Crítica – Esta é a secção que contém a informação crítica para o plano. Estão aqui contidos os detalhes relativos a cada uma das equipas, nomeadamente, seus responsáveis, listas de chamadas, tarefas, equipamentos e registos vitais necessários.
3. Manutenção – Todo o processo de revisão e manutenção do plano deve estar detalhado nesta secção, prevendo situações e momentos nos quais o plano deve ser actualizado.
4. Exercícios – A quarta secção do plano aborda todas as questões relacionadas com o exercício do plano de forma a divulgá-lo e familiarizar os funcionários aos procedimentos apresentados.
5. Apêndice – Apesar de ser a última secção do plano não é a menos importante. Nela estão contidos anexos tais como os procedimentos de restauração de sistemas operativos e bases de dados, diagramas de rede, localizações das cópias de segurança, entre outra informação crítica.

A Tabela 3 é sugerida por Canton (2003) com o intuito de auxiliar a equipa de desenvolvimento do PCN através de uma série de perguntas às quais o plano deve ser capaz de responder.

Tabela 3: Questões a serem respondidas pelo PCN

(Canton, 2003)

Secção		Questão a ser respondida
1	Escopo	Quem e o quê está incluído no plano?
	Objectivos	Qual o objectivo do plano?
	Pressupostos	O que assumimos?
	Estratégias	Como reagiremos em crise?
2	Equipas	Quem é o responsável? Quem é o líder?
	Notificações	Como divulgamos a informação?
	Materiais	O que precisamos?
3	Actualizações	Como e quando actualizaremos o plano?
4	Exercícios	Como nos preparamos?
5	Documentos de referência	Onde encontramos informação crítica?

4.2.3 Técnicas e ferramentas para garantia de continuidade

Proteger a informação vital e garantir que esta esteja sempre acessível devem fazer parte de um dos maiores desafios de qualquer organização (Reuvid, 2005). Este capítulo debruçar-se-á sobre algumas das técnicas e ferramentas existentes para a garantia da Continuidade de Negócios das organizações e elaboração de um PCN.

4.2.3.1 Segurança física

De acordo com Mamede (2006), as ameaças à segurança física e os controlos que podem ser implementados resumem-se à ameaças de causa natural e ameaças causadas pelo Homem. Para além das preocupações a nível físico, muito relacionadas com o meio ambiente que rodeia todo o sistema computacional, existem outras preocupações. Entre estas contam-se as medidas que podem ser tomadas ao nível do armazenamento de dados, de redundância de sistemas, de cópias de segurança e de sistemas de alimentação ininterrupta.

De entre as ameaças de causa natural salientam-se as seguintes:

- Incêndios: Os riscos causados por incêndio são o próprio fogo, o calor, o fumo e danos provocados por agentes supressores como extintores e água. Os controlos que podem ser implementados incluem a instalação de detectores de fumo, extintores automáticos ou manuais, utilização de extintores não líquidos nas áreas onde exista equipamento electrónico, a realização de exercícios frequentes de evacuação e a manutenção de todas as cópias de segurança fora das instalações.
- Terramotos: De forma a controlar o efeito desta calamidade natural deve-se manter todo o equipamento informático fora de zonas envidraçadas, instalar dispositivos anti-vibrações em todo esse equipamento e infra-estruturas.
- Inundações: Para prevenir que situações desta natureza tenham impactos negativos sobre a organização, é necessário garantir um sistema de drenagem funcional que possibilite o escoamento da água.
- Temperatura e humidade: Sem uma temperatura e humidade controladas, o *hardware* pode sofrer permanentemente de desempenho inconsistente e/ou falha completa. Os riscos implicados são o mau funcionamento ou a falha provocada por sobreaquecimento, não só nos

componentes sensíveis mas também em outros equipamentos. Outro aspecto prejudicial é a exposição à formas líquidas. Assim, todos estes factores têm de ser tomados em consideração para a monitorização de temperaturas e níveis de humidade nas salas onde se encontre o equipamento que suporta actividades críticas.

No que diz respeito às ameaças causadas pelo Homem, estas são frequentemente motivadas por três factores, a malícia, a oportunidade e o azar. Algumas destas ameaças podem ser o roubo ou a fraude, que podem provocar a perda de funcionalidades nos sistemas de informação, a perda de informação crítica ou confidencial e a perda financeira. Controlos possíveis são a vigilância activa e inspecção à todos os que abandonem as instalações, criação de uma consciência colectiva sobre a importância da segurança em toda a organização, auditorias regulares, boas práticas de controlo de imobilizado bem como relativas à chaves e zonas fechadas e também uma carteira de seguros adequada na contratação e saída de funcionários.

4.2.3.2 Redundância/Cópias de Dados

i. Cópias de segurança

Para garantir a continuidade operacional há que garantir a disponibilidade de acesso à informação. Um sistema de cópias de segurança só consegue ser medido até que a recuperação seja efectivamente necessária.

Existem muitas formas de efectuar cópias de segurança, embora seja mínima a diferença entre elas. Para além das especificações, todas elas servem ao mesmo propósito, que é a criação de um duplicado de informação. Uma vez efectuada esta duplicação, o objectivo seguinte é a colocação dessas cópias numa localização geográfica distinta daquela onde estão os dados originais. A razão desta deslocalização das cópias é a prevenção de situações de desastre que possam comprometer em simultâneo sistemas, dados originais, e cópias de segurança (Mamede, 2006).

De forma a possibilitar a recuperação de informação e recuperação das operações de negócios em tempos aceitáveis devem ser implementados regimes de cópias de segurança bem estruturados e seguidos de forma rígida. A frequência com que as cópias são efectuadas varia de organização para

organização, dependendo da sensibilidade e valor da informação, bem como do que a organização considera aceitável perder em qualquer eventualidade (Doughty, 2001).

O sistema de cópias de segurança pode ser tão simples como a cópia sistemática de ficheiros para suporte tipo *CD*, *DVD*, fitas magnéticas ou discos externos, até centros de processamento alternativos sincronizados em tempo real. Tudo dependerá do valor que se está a proteger, o que pode ser obtido com uma AIN efectiva. Actualmente a medida mais utilizada consiste em efectuar cópias de segurança utilizando cassetes de fita magnética de alta capacidade (Mamede, 2006).

ii. *Raid*

Os indivíduos e as organizações armazenam, hoje em dia, imensas quantidades de informação nos discos rígidos dos computadores pessoais e servidores. Os discos rígidos oferecem uma grande quantidade de espaço de armazenamento, e a capacidade de procurar dados de forma muito rápida. No entanto, os computadores são equipamentos passíveis de falha, incluindo-se aqui os dispositivos de armazenamento. Assim, torna-se importante estar preparado para uma possível situação de avaria total de um dispositivo de armazenamento. Para garantir que esta situação não seja mais do que uma inconveniência temporária, é necessário distribuir os dados de um disco por várias unidades, diminuindo a probabilidade de perda de dados uma vez que a possibilidade de avaria simultânea de dois ou mais dispositivos é extremamente baixa. A tecnologia que permite este tipo de suporte é conhecida por *RAID*.

A sigla *RAID* significa, no original em Inglês, *Redundante Array of Independent Disks*. Existem vários tipos de *RAID*, todos com o mesmo objectivo, ou seja fazer com que dois ou mais discos rígidos possam funcionar como uma "equipe". Normalmente, os dados são transferidos para os discos rígidos através de um controlador dos mesmos. Com a tecnologia *RAID*, esses dados são canalizados através de um controlador e espalhados por vários discos em simultâneo. Este controlador de *RAID* não é mais do que um dispositivo que permite garantir a sincronização entre vários discos rígidos.

Uma vez garantida esta sincronização, um disco rígido pode partilhar dados através de várias formas possíveis, dependendo da forma como foi configurada a aplicação da tecnologia. As formas possíveis de implementar *RAID* são o *stripping, mirroring e duplexing* (Chen *et al apud* Doughty, 2004):

- *Stripping* – O *stripping* de dados consiste na distribuição dos dados por múltiplos discos de forma a faze-los parecer um único disco, grande e rápido, o que faz com que aumente o desempenho do conjunto. Este desempenho é melhorado na medida em que várias operações de leitura e escrita podem ser executadas em paralelo. Paralelismo este que se reveste de dois aspectos que é importante referir: Por um lado, múltiplos pedidos independentes podem ser respondidos em paralelo por serem discos separados. Por outro, pedidos únicos de múltiplos blocos podem ser respondidos por múltiplos discos actuando de uma forma coordenada, o que aumenta a taxa efectiva de transferência para um pedido único (Mamede, 2006).

  Os discos sincronizados permitem a recuperação de dados através de um disco de paridade (Disco β na Figura 2) que leva à recuperação da informação perdida com base na informação que consta nos restantes discos constituintes do *array* redundante.

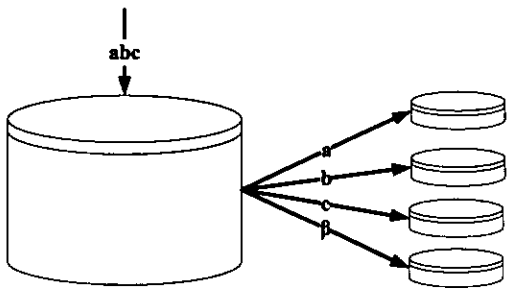


Figura 2: Discos redundantes usando disco de paridade

(Chen *et al apud* Doughty, 2004)

- *Mirroring e Duplexing* – Esta tecnologia permite a réplica exacta de um disco em outro de forma a prevenir uma falha no disco. Ou seja, para cada disco constituinte do *RAID*, existe um duplicado, e através de um controlador toda a informação é armazenada simultaneamente em ambos discos. Apesar de altamente confiável, esta tecnologia torna-se dispendiosa pela necessidade de um número de discos dobrado como se pode ver na Figura 3.

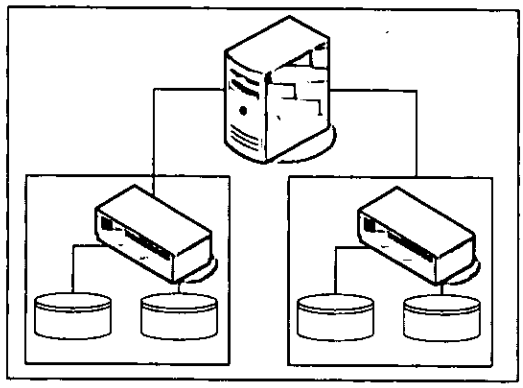


Figura 3: Discos redundantes em *mirrorring* e *duplexing*

(Chen *et al apud* Doughty, 2004)

As tecnologias citadas podem também ser usadas em combinação resultando em níveis de confiabilidade e redundância extremamente elevados.

4.2.3.3 Redundância de redes locais

Não é possível imaginar, nos dias de hoje uma organização que possua mais de um computador e que os mesmos não estejam interligados em rede (Doughty, 2004). Uma rede fiável é aquela que continua a servir o seu propósito apesar da falha de um elemento crítico.

Apesar das organizações optarem pela conectividade ininterrupta, alguns problemas podem ocorrer por diversas razões. A conectividade não é responsabilidade de uma entidade. A conexão de um *router* para a *Internet* envolve o próprio *router*, a conexão *CSU/DSU*, energia eléctrica, cabeamento e inúmeros administradores – cada um com influências sobre diferentes partes da conexão. A qualquer momento, erros humanos, de aplicações, físicos, ou situações imprevisíveis, tais como mau estado do tempo, podem colocar em risco a conectividade (Halabi, 2001).

Tipicamente, os elos mais fracos de uma rede são os dispositivos de distribuição, tais como *switches* e *hubs*, pois são os responsáveis pela disseminação do sinal aos terminais ou outros dispositivos de comunicação criando uma espécie de árvore. Nestes casos a redundância pode ser alcançada providenciando múltiplos caminhos para o tráfego de informação (Halabi, 2001). Deve-se ter em conta, que em redes existem caminhos físicos e lógicos, e criando uma redundância de caminho lógico é inútil.

A solução passa por criar caminhos físicos redundantes tal como a Figura 4 demonstra, aplicando um protocolo que permita esta implementação sem ciclos infinitos no tráfego. Este protocolo é conhecido por *Spannig Tree Protocol* (STP). O STP aplica um algoritmo específico à rede, baseado na sua topologia tendo como resultado uma rede sem ciclos lógicos.

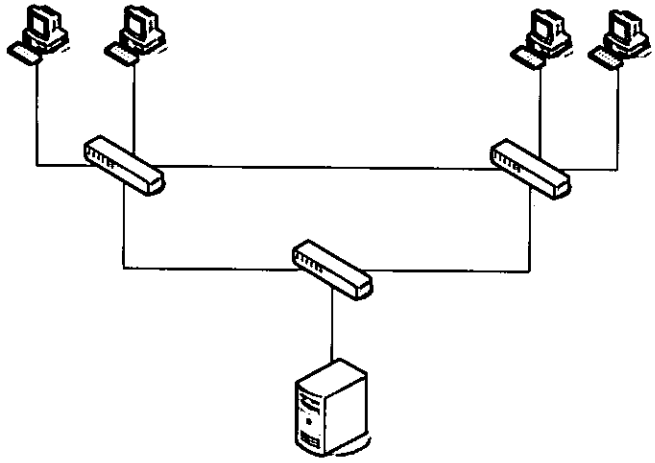


Figura 4: Rede com caminhos físicos redundantes

(Halabi, 2001)

A Figura 5 apresenta outra técnica, bastante aplicada devido à sua simplicidade de implementação e custos relativamente diminuídos que consistem no uso de um dispositivo de distribuição em *stand-by,* o qual em caso de falha do dispositivo principal possa facilmente substitui-lo sendo apenas necessário para tal a alteração de uma conexão.

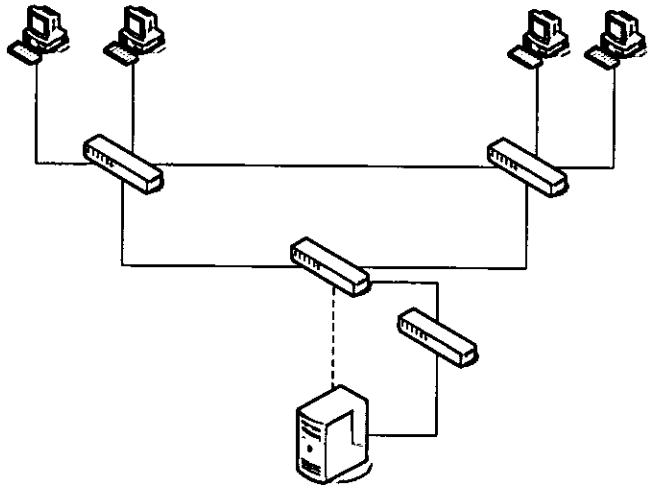


Figura 5: Rede com dispositivo redundante em *stand-by*

(Halabi, 2001)

4.2.3.4 Redundância de comunicações

Nesta Era globalizada, a dispersão geográfica das organizações torna-se preponderante na sua competitividade. Contudo, esta dispersão se traduz na necessidade de estabelecer comunicações fiáveis entre as diversas localizações físicas de forma a garantir a sua comunicação. Assim, as Redes de Longa Distância, ou WAN (*Wide-Area Network*) na sua sigla em inglês, passam a desempenhar um papel crítico no funcionamento de organizações geograficamente dispersas mas com necessidade de comunicação frequente e centralização de informação (Doughty, 2001).

Devido aos elevados custos do estabelecimento de uma WAN, estes serviços são na sua maioria contratados a fornecedores especializados e assim a garantia de continuidade passa pelas garantias oferecidas pelo fornecedor e pela redundância de conexões entre os locais.

De acordo com Halabi (2001), esta redundância pode ser estabelecida de duas formas tendo em conta os custos e a característica das conexões necessárias:

A primeira forma consiste na contratação de serviços que providenciem duas ligações permanentemente activas para que caso uma das conexões seja interrompida, o fluxo possa ser garantido pela segunda conexão. Nestes casos, o equipamento deve ser configurado de forma a executar uma distribuição dos dados entre as duas conexões com o objectivo de incrementar a disponibilidade e velocidade da rede e ainda evitar que uma das conexões esteja ociosa em detrimento da outra.

Esta forma apresenta grandes vantagens em termos de continuidade operacional pois a comunicação não sofre interrupções mesmo em caso de paragem de uma das conexões, contudo os seus custos de implementação, manutenção e configuração revelam-se bastante elevados.

A segunda opção apresenta custos relativamente inferiores, contudo necessita de um intervalo de tempo para efectuar a passagem para a conexão secundária e sua velocidade de transmissão é consideravelmente baixa. Esta opção passa pela contratação de um serviço de discagem (*dial-up*) que é

usado apenas quando a conexão primária for interrompida. Este serviço consiste na marcação telefónica por meio de um *modem* para um provedor de serviço que irá garantir a comunicação entre os locais.

Sikich (2003) aponta ainda um factor importante e independente do tipo de conexão que está relacionado com a infra-estrutura usada pelo fornecedor do serviço, pois a contratação de dois fornecedores baseados na mesma infra-estrutura não torna as conexões redundantes. A opção correcta passa pelo uso de conexões suportadas por infra-estruturas distintas (fibra óptica e satélite por exemplo).

4.2.3.5 Redundância de Servidores

Para além de se poder arquitectar soluções de servidor com redundância em quase todo o *hardware* e dispositivos de armazenamento, pode-se incrementar ainda mais o nível de segurança recorrendo à redundância de servidores ou *clustering*. Esta tecnologia permite que um determinado número de servidores actue como se de um único servidor se tratasse, através da partilha de recursos. A Figura 6 apresenta um conjunto de servidores em *cluster*, actuando como um só e a servir os restantes dispositivos da rede.

O nível de partilha depende do objectivo que se procura atingir com a implementação do *cluster*, ou seja, se o objectivo for o melhor desempenho, então os servidores podem partilhar memória e capacidade de processamento. Se o objectivo for disponibilidade, os servidores podem ser sincronizados, replicando os dados e aplicações em cada um das máquinas intervenientes (Mamede, 2006)

O *clustering* oferece um grande número de vantagens, assim como um elevado desempenho e elevada disponibilidade. Contudo os custos são igualmente elevados, o que constitui a grande desvantagem desta ferramenta. A instalação e configuração de um *cluster* é algo que tem de ser devidamente planeado e realizado, pois um *cluster* instalado com deficiências pode causar mais problemas de disponibilidade de serviços de rede e ficheiros do que um servidor simples

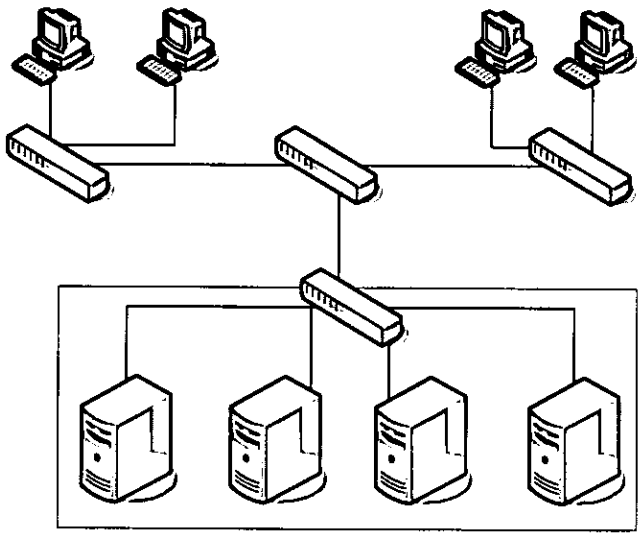


Figura 6: Servidores em *cluster*

(Mamede, 2006)

Na realidade, um *cluster* é um grupo de computadores independentes que se combinam para trabalhar como um único sistema redundante. Se um dos servidores falhar, o outro assume de imediato as suas funções, para que os utilizadores nem sequer se apercebam de tal falha.

4.2.3.6 Sistemas de alimentação eléctrica ininterrupta

Os sistemas de alimentação eléctrica ininterrupta, *uninterruptable power supplies – UPS*, no original em Inglês, são sistemas de baterias que disponibilizam energia em situações de falha de alimentação eléctrica principal. Os sistemas de UPS garantem ainda uma estabilização da corrente eléctrica, o que favorece o tempo de vida das fontes de alimentação dos equipamentos. Estes sistemas não foram concebidos com o objectivo de assegurar a continuidade das operações em situação de falha na alimentação principal, mas sim para assegurar a possibilidade de se efectuarem de forma adequada os procedimentos de encerramento dos sistemas sem perda ou corrupção de dados e aplicações.

A instalação destes sistemas é relativamente simples, e destina-se a ligar os servidores e computadores pessoais que executam aplicações críticas. Destina-se também a alimentar dispositivos activos de rede, para que as sessões possam ser terminadas de forma normal e para que os servidores possam comunicar entre si durante a situação de falha na alimentação (Mamede, 2006).

Se for realmente necessário que os sistemas fiquem disponíveis por longos períodos de tempo em caso de falha na alimentação eléctrica, então devem ser considerados sistemas geradores, normalmente constituídos por motores *diesel* concebidos para gerarem energia eléctrica. Estes motores arrancam no instante a seguir à falha de corrente eléctrica, enquanto os computadores estão a ser suportados pelas unidades de UPS. Quando a corrente volta a normalizar, estes motores desligam-se automaticamente.

Um elemento usualmente esquecido quando se define uma estratégia para situações de falha na corrente eléctrica é o sistema de ar condicionado nas salas de servidores. Se os servidores continuam a trabalhar, durante um determinado período de tempo, mais ou menos longo alimentados pelos sistemas eléctricos alternativos, a temperatura dentro destas salas tende a subir rapidamente já que os sistemas de ar condicionado estarão sem corrente eléctrica. Assim, deve ser considerada a instalação de um gerador para alimentar estes sistemas.

4.2.3.7 Locais alternativos

Uma das alternativas para permitir a continuidade é a construção ou aluguer de locais de trabalho alternativos. Estes locais possuem as condições mínimas para que a organização possa executar as suas funções básicas de modo a permitir a sua sobrevivência, ou seja, são criadas condições de trabalho para os elementos e operações – chave (Reuvid, 2005).

Assim, o PCN deve mencionar quais os colaboradores e/ou funcionários que devem continuar as suas operações no local alternativo e ainda que operações devem ser desempenhadas. Esta escolha deve ser bastante acautelada de modo a que não sejam usados recursos para realizar tarefas menos críticas, ou que por outro lado tarefas críticas não sejam realizadas por insuficiência de recursos.

De acordo com o mesmo autor, o local alternativo deve ser cuidadosamente escolhido, e duas situações consideradas:

- Se muito próximo às instalações principais, corre-se o risco de o desastre afectar ambos;
- Se muito distante a acessibilidade pode tornar-se um grande obstáculo.

Tipicamente, as organizações interessadas nestes serviços firmam contratos anuais com taxas de pagamento mensais com empresas provedoras de locais alternativos, caso a construção própria não seja

economicamente viável. Se a organização usar o local alternativo, normalmente são acrescidas taxas diárias de acordo com os serviços prestados (Sikich, 2003).

De um modo geral existem 3 tipos de locais alternativos, conhecidos pelas suas palavras inglesas:

- *Hot-Site* – São locais alternativos completamente equipados com toda a estrutura de suporte organizacional necessário para o reinício imediato das actividades. Um *hot-site* possui suporte a nível de *hardware*, *software* e cópias de segurança actualizadas. Na maior parte dos casos, os *hot-sites* representam uma redundância completa de servidores e informação em tempo real, tornando possível o arranque imediato das operações a partir do local alternativo (Elliot *et al,* 2002)
- *Cold-Site* – Os *cold-sites* são os locais alternativos de custo mais reduzido. Este tipo de alternativa não oferece qualquer suporte à nível de TIC, sendo apenas disponibilizado o espaço de trabalho. Toda a restante estrutura de suporte deve ser disponibilizada, instalada e configurada pela própria organização. A falta de *hardware* e *software* previamente configurados implicam tempo de recuperação mais elevado comparativamente aos outros tipos de locais alternativos (Elliot *et al,* 2002).
- *Warm-Site* – Este tipo de local alternativo encontra-se equipado com o *hardware* semelhante ao usado pela organização em causa, contudo não existe suporte a nível aplicacional (*software*) nem a nível de cópias de segurança da informação (Elliot *et al,* 2002).

4.3 Exercício e manutenção do PCN

Foi mencionado nos capítulos anteriores que o desenvolvimento de um PCN só é possível com o apoio e suporte da gestão de topo. Este apoio não se refere apenas ao desenvolvimento do plano mas deve se estender também à actualização e exercício do mesmo. Um PCN não tem valor nenhum se no momento em que houver algum evento crítico ele não funcionar. Assim é fundamental que haja um planeamento de exercícios e actualização do plano (Fagundes, 2004).

4.3.1 Exercício

Uma vez criada a estratégia de continuidade e implementado o plano é essencial para a organização a avaliação e exercícios regulares sobre o plano de forma a garantir a sua integridade (Reuvid, 2005). Segundo Doughty (2001), para muitas organizações uma vez construído o PCN, os gestores executivos assumem que as suas responsabilidades terminaram, o que é absolutamente incorrecto. Os testes sobre o plano podem ser efectuados em vários estágios, variando de exercícios simples sobre uma unidade isolada até simulações completas fazendo uso das tecnologias e dos serviços alternativos ou ainda, de evacuações de emergência (Reuvid, 2005).

É nesta fase que deve ser provada a viabilidade do plano. Neste momento as omissões, factos assumidos invalidamente, ou soluções inadequadas devem ser detectadas, e não no momento da ocorrência de uma interrupção. (Doughty, 2004)

De acordo com o mesmo autor existem quatro razões básicas para se exercitar um PCN:

1. Verificar se o PCN é funcional e se vai de acordo com os requisitos de continuidade do negócio;
2. Identificar os pontos fracos do plano de modo a corrigi-los antes da ocorrência de um desastre;
3. Permitir aos funcionários familiarizarem-se com o plano e com os seus procedimentos, evitando assim surpresas na altura de utilização do plano;
4. Satisfazer alguns dos requisitos legais impostos por uma grande parte de organizações.

Diversos tipos de exercícios podem ser aplicados aos PCN, e estes podem ser categorizados em quatro formas:

1. Auditoria: Esta forma tem como objectivo verificar a disponibilidade dos recursos mencionados no PCN. Este tipo de exercício deve ser efectuado periodicamente de forma a verificar a existência e funcionamento de cópias de segurança, os dispositivos e recursos alternativos, validade dos contratos com terceiros entre outros. Infelizmente este método está limitado à validação dos recursos existentes e não identifica novos pontos de falha nem recursos necessários.
2. Simulações: Estas permitem avaliar a disponibilidade dos recursos e o nível de preparação dos funcionários. Neste processo são reunidos os funcionários e é apresentado um cenário de desastre. Com base nos dados apresentados os funcionários devem rever os procedimentos mencionados no PCN de forma a familiarizarem-se com o mesmo, contudo o plano não é invocado como tal. Este tipo de exercício é fácil de conduzir, de custo reduzido e efectivo no sentido de verificar se os recursos foram correctamente identificados.
3. Teste em tempo real: Este tipo de exercício é frequentemente realizado no Centro de Processamento de Dados ou no local alternativo de trabalho (*hot-site*). Este tipo de teste permite obter maior grau de segurança embora seja também muito dispendioso em termos de tempo e custos.
4. Exercício – surpresa: Caracteriza-se como sendo uma variação dos exercícios anteriormente mencionados com o factor surpresa adicionado. Este tipo de exercício é muito discutido contudo pouco usado pois os inconvenientes que traz para os funcionários e o mal-estar que pode gerar dentro da organização, ultrapassa as suas vantagens. Os benefícios obtidos por este tipo de testes podem ser alcançados em outros testes dedicando uma especial atenção e incluindo formas de controlo de modo a evitar fraudes.

Na realização dos exercícios, independentemente do seu tipo, são importantes aspectos tais como (Doughty, 2001):

- Escopo: é importante, antes do início do exercício definir um escopo claro e sucinto. É importante também que todos os funcionários envolvidos no teste estejam cientes e entendam a definição do escopo.

- Fraudes: Durante a realização do exercício, deve ser nomeado um observador independente. Devem ser igualmente estabelecidos métodos de controlo por forma a garantir que apenas os recursos mencionados no plano sejam usados, sendo que excepções ao plano devem ser anotadas para posterior análise.
- Documentação de Resultados: Os resultados dos exercícios efectuados devem ser sempre documentados. Se possível devem também ser documentadas as actividades posteriores ao teste, identificadas correcções e definidas responsabilidades. Os resultados e a restante documentação devem ser comunicados aos participantes do teste e à gestão de topo. Em casos de sucesso, este deve ser reconhecido, tal como as pessoas que contribuíram para tal sucesso. No caso contrário, os constrangimentos encontrados devem ser documentados de um ponto de vista positivo e motivador, com ênfase para as acções correctivas.

Segundo Doughty (2001), os exercícios devem ser estruturados com o objectivo de:

- Determinar o estado de preparação dos departamentos individualmente, para responder à grandes desastres;
- Analisar a habilidade que vários departamentos e unidades auxiliares ou de suporte tem ao interagirem de forma eficiente e eficaz;
- Verificar se os equipamentos de recuperação existentes no local ou em locais alternativos são adequados para suportar a recuperação de todas as funções de negócio;
- Confirmar se o plano foi correctamente criado e/ou actualizado e responde às necessidades da organização.

Os exercícios são reconhecidos como sendo consumidores de tempo e dinheiro e por isso devem ser explorados ao máximo para demonstrar o maior nível de segurança possível no PCN e saturar o mesmo ao máximo com vista a encontrar quaisquer falhas ou negligências cometidas (Doswell, 2000).

4.3.2 Manutenção

De acordo com Doughty (2001), a manutenção do PCN é vista como uma sobrecarga sobre um funcionário por natureza extremamente atarefado. A competição entre a manutenção do PCN e as responsabilidades diárias constitui uma das principais razões pela qual o PCN não é actualizado. É

imperativo também que estejam abertos os canais de comunicação, para que as alterações organizacionais relevantes sejam comunicadas com vista à manutenção e actualização do plano.

Aquando da realização de uma alteração com impacto sobre actual PCN, o coordenador ou responsável pela manutenção do mesmo deve desenvolver um plano de acção para a actualização do PCN. De acordo com a estrutura e dimensão da organização e do plano, e tendo em conta a natureza da alteração ocorrida poderá ser necessário o estabelecimento de um projecto para a actualização do plano (Doughty, 2001).

Uma cultura a ser desenvolvida e que pode ser de grande ajuda está relacionada com a "posse" ou "propriedade" do plano. Um PCN é em termos legislativos propriedade da organização, mas em termos conceptuais deve ser considerado como posse dos que irão realmente usá-lo em caso de desastres. Dificilmente manter-se-á um PCN actualizado se esta filosofia não for adoptada incorrendo num crescente risco de não conseguir a recuperação das operações de forma esperada. A propriedade do PCN pode ser atribuída de diversas formas, dependendo do seu escopo, dimensão e complexidade, e ainda de factores inerentes à organização, podendo ser atribuída de forma departamental, por unidade ou até por função. Segundo Doughty (2004), outra forma de garantir que o plano se mantenha actualizado consiste na realização periódica de AIN com vista a avaliar quaisquer alterações que tenham ocorrido.

Um detalhe muitas vezes ignorado está relacionado com o controlo de versões do plano. Esta questão é mais perceptível em organizações com alterações constantes nas quais o PCN se encontra repetidas vezes em actualização sendo que existem dificuldades no controlo destas versões. Ao final de um período de alterações podem se encontrar departamentos com diferentes versões do PCN o que faz com que se perca completamente a noção de qual o plano a seguir e quais os procedimentos actualizados. Assim, durante o processo de actualização de um PCN, uma sólida estrutura de controlo de versões e distribuição das mesmas deve ser implementada para assegurar que todos dentro do escopo do plano estejam actualizados com a última versão.

O mesmo autor afirma ainda que existem duas categorias de manutenção de um PCN:

- Manutenção Programada – Este tipo de manutenção é essencialmente regulado pelo tempo, ou seja, por acções inicialmente agendadas que irão ocorrer num período de tempo bem conhecido. Exemplos de acções que possam despoletar manutenções programadas são testes que estejam agendados, alterações estruturais na organização previamente definidas, etc.
- Manutenção Não – Programada – Este tipo de manutenção é imprevisível e não programável. É essencialmente baseado em eventos em contraste à categoria anteriormente citada. Alguns dos casos mais comuns que originam manutenções não – programadas são a saída repentina de funcionários – chave, alterações significativas no fluxo ou até na estrutura organizacional, o surgimento de uma nova ameaça como um paiol, por exemplo.

CAPÍTULO V

5 APLICAÇÃO DO PCN NO CFM

5.1 A escolha do caso de estudo

Na qualidade de um dos inquiridos para o questionário destinado às 100 maiores empresas moçambicanas, segundo o relatório de 2006 da KPMG, foi efectuado o pedido ao CFM para sua participação como caso de estudo para o presente trabalho o qual foi imediatamente aprovado.

A pré-disposição dos responsáveis e colaboradores, aliados ao facto de os CFM terem a sua gestão actualmente assente sobre as TIC e sem um PCN tornaram os CFM um caso de estudo excelente.

Após a aprovação para a realização do estudo, foi efectuado um estudo preliminar à estrutura organizacional e devido à complexidade e dimensão encontradas o escopo do trabalho foi reduzido ao Serviço de Informática.

Este serviço possui actualmente a responsabilidade de prover os CFM de todos os serviços relacionadas com as TIC e assim, um PCN sobre este serviço revelar-se-á um PCN virado às TIC.

5.2 OS CFM

5.2.1 Apresentação

A empresa Portos e Caminhos-de-Ferro de Moçambique, E.P., abreviadamente designada por CFM, é uma entidade colectiva de direito público, dotada de personalidade jurídica e com autonomia administrativa, financeira e patrimonial, exercendo a sua actividade na subordinação do Ministério dos Transportes e Comunicações.

Os CFM regem-se pela Lei nº 17/91, de 3 de Agosto, pelos presentes estatutos, pelas disposições legais e regulamentares que especialmente lhe forem aplicáveis e finalmente, no que não estiver especialmente regulado, pelas normas de direito privado.

A defesa do interesse público que orientará toda a actividade da empresa, será assegurada pelo Governo, através do Ministério dos Transportes e Comunicações, salvo nos casos em que estiver expressamente definido de outro modo na Lei ou nos presentes estatutos.

A sede dos CFM está situada na cidade de Maputo, e a organização exerce a sua actividade em todo o território nacional podendo criar delegações em outros pontos do país desde que assim seja aprovado pelo Conselho de Administração. Este conselho delibera igualmente o estabelecimento de representações comerciais no estrangeiro.

O transporte ferroviário de pessoas e carga e a prestação de serviços portuários constituem o objecto da organização, sendo que esta pode ainda subscrever participações financeiras para a constituição de empresas mistas, desde que tal seja autorizado pelos Ministros dos Transportes e Comunicações e das Finanças.

5.2.2 Missão

Os CFM assumem como sua actual missão:

- A reconstrução do sistema de transporte ferro – portuário, para torná-lo moderno, competitivo, eficiente, orientado para o mercado e financeiramente viável.
- O investimento, promoção e desenvolvimento estratégico das infra-estruturas ferro – portuárias.
- Diversificação da sua intervenção empresarial, como forma de promover a sua sustentabilidade à longo prazo e rentabilizar os seus activos.

5.2.3 Objectivos

Na sua página inicial da *Internet*, os CFM estabelecem os seguintes objectivos:

- Promover e desenvolver as infra-estruturas ferro – portuárias e serviços;
- Promover o desenvolvimento das actividades de transporte e logística através da participação crescente do sector privado na sua operação e gestão;
- Envolver-se, em associação com o sector privado, na operação dos sistemas ferro – portuários de forma sustentável, segura, eficiente e proveitosa para o transporte de passageiros e carga e prestação de serviços portuários;
- Maximizar a utilização de forma racionalizada e rentável dos seus activos.

5.2.4 Organigrama

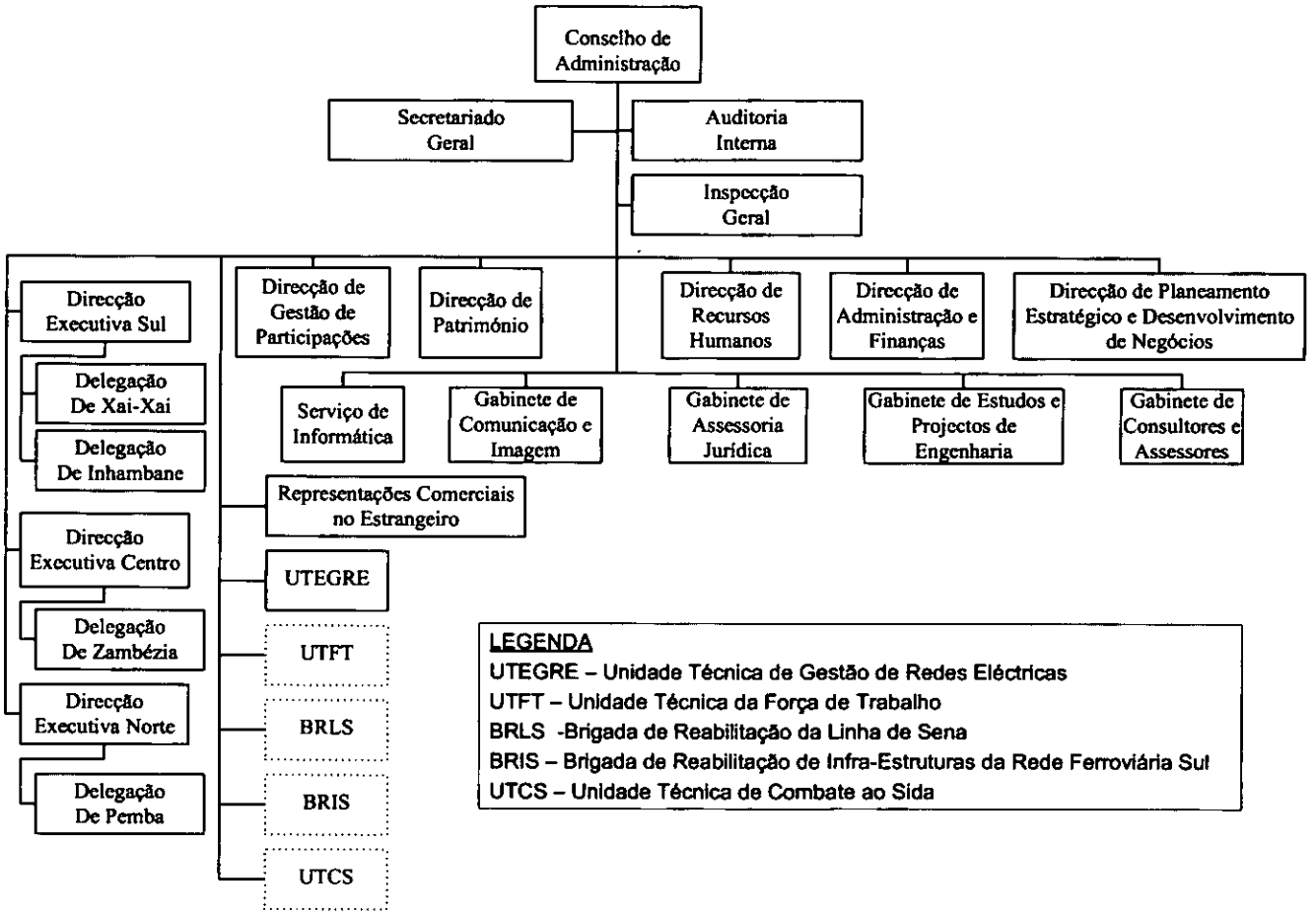


Figura 7: Organigrama dos CFM

5.3 O Serviço de Informática

O Serviço de Informática dos CFM foi criado com dois grandes objectivos:

- Estabelecer e implementar Políticas Informáticas para os CFM;
- Promover e garantir suporte na área das TIC à organização, de modo a auxiliar o maior número possível de áreas administrativas e operacionais.

Actualmente este Serviço presta apoio na aquisição e manutenção de material e aplicações informáticas e de gestão, actuando como provedor de serviços de *Internet* e *e-mail*. O crescente número de funcionários usando o *e-mail* e *Internet*, assim como a recente introdução de um *ERP*, para gestão integrada que absorve a maior parte dos processos organizacionais tornam o Serviço de Informática preponderante e crítico para a continuidade operacional da organização.

O crescimento deste Serviço deve ser acompanhado por um incremento das suas capacidades de resposta, confiabilidade e garantia de prestação de serviços contínua ou com o mínimo de sobressaltos possíveis.

5.4 Métodos e procedimentos aplicados para desenvolvimento do PCN

Para o desenvolvimento do PCN apresentado em anexo, foram efectuadas leituras à documentação existente relativamente ao funcionamento dos CFM, sua estrutura organizacional, processos, e ainda à estrutura tecnológica e de comunicação.

Com o objectivo de obter um grau de detalhes mais elevado, foi feito o acompanhamento durante uma semana, das actividades principais desempenhadas pelos colaboradores do Serviço de Informática, aos quais foram posteriormente efectuadas entrevistas, formais e informais, e submetidos questionários. As mesmas formas de recolha de informação foram aplicadas aos responsáveis pelas áreas de Sistemas de Informação e Infra-estrutura.

Este processo caracterizou a fase inicial do ciclo de vida do PCN, relativa à Análise de Impacto no Negócio. A fase seguinte, relacionada ao Desenvolvimento e Implementação, foi realizada em concordância com funcionários chave e chefes de secção de forma a escolher as ferramentas e métodos que melhoram se adequam ao Serviço de Informática dos CFM.

Para a terceira fase do ciclo de vida do PCN, o protótipo desenvolvido foi submetido aos responsáveis pelo Serviço de Informática de forma a obter os seus comentários e críticas. Desta forma, o desenvolvimento do PCN foi acompanhado por membros da organização garantindo que o mesmo cubra as suas necessidades.

5.5 Estrutura Actual

Do estudo efectuado, foram constatados os seguintes factores:

1. Todos inquiridos afirmaram não possuir uma lista de contactos de emergência, tais como polícia, bombeiros, responsáveis de segurança, etc.
2. Em relação aos procedimentos de segurança e planos de continuidade no departamento as opiniões foram divergentes, representando por si só visões dispersas da mesma realidade. Este tipo de situação, de acordo com Miguel (2003) resulta da fraca divulgação dos métodos operacionais.
3. A totalidade dos inquiridos foram unânimes em afirmar que uma paragem no funcionamento do Serviço de Informática traria impactos severos a nível de gestão da organização, visto que quase todos os processos de gestão são neste momento suportados por este Serviço.
4. Relativamente à reacção em casos de emergência, apenas 35% dos inquiridos afirmaram não conhecer as suas funções ou responsabilidades. Contudo, dos restantes 65% todos afirmaram que as suas reacções seriam resultado de avaliações individuais e não estruturadas de acordo com o que seria o objectivo da organização.
5. De acordo com a média efectuada pelas respostas do Director do Serviço de Informática, e pelos três Chefes de Serviço, foram estabelecidos RPOs e RTOs por serviço apresentados na Tabela 4:

Tabela 4: RPOs e RTOs por serviço

Serviço	RTO	RPO
Antivírus e *firewall*	4 horas	-
Internet e *e-mail*	1 dia	-
ERP	1 dia	1 dia
Ligações remotas	2 dias	-
SIGRH	5 dias	1 dia
Hospedagem de páginas de *Internet*	15 dias	30 dias
Restantes serviços	15 dias	-

5.5.1 Aplicações/Ferramentas e Sistemas de Informação

O Serviço de Informática dos CFM fornece à organização, entre outros, uma série de ferramentas de apoio à gestão. Estas ferramentas são baseadas em TIC e compostas basicamente por Sistemas de Informação para a Gestão Administrativa, Financeira e Operacional, acesso à rede interna, *Internet* e *e-mail*. Para tal, estão instalados no seu CPD uma série de servidores e outros equipamentos que permitem prover aos CFM este leque de serviços. Os principais servidores são:

- Servidor de *e-mails;*
- *DHCP, DNS Local* e *File Server;*
- Servidor do sistema de Processamento salarial actualmente em desuso, servindo apenas para dados históricos e estatístico;
- Servidor de antivírus;
- Servidor de Sistema de Gestão Integrada (*ERP*)
- *Terminal Service* para ligações remotas
- *DNS* Secundário
- *DNS* Primário, Controlador de Domínio, Servidor da Página de *Internet* dos CFM, *TACACS*
- *Firewall*

Existem ainda uma série de outras aplicações e sistemas, alojados em computadores que funcionam como "*stand – alones*", nas respectivas Direcções Executivas e Departamentos. Estes sistemas têm níveis de criticidade, importância e uso variáveis mas relativamente inferiores em comparação com os sistemas alojados no CPD, embora muito raramente são sujeitos a manutenções ou a realização de cópias de segurança. Estes Departamentos e respectivas Direcções Executivas encontram-se fora do âmbito do presente trabalho, e deverão ser analisados num estudo mais abrangente.

5.5.2 Estrutura de *hardware*

A nível de estrutura interna de *hardware*, os principais dispositivos que compõem a infra-estrutura tecnológica actual dos CFM, há que salientar as seguintes características:

1. Os servidores de *ERP* e *Terminal Service* possuem discos redundantes e comunicações para a rede redundantes;

2. Os servidores de *ERP*, *Terminal Service*, anterior sistema de processamento salarial e *DHCP* possuem fontes de alimentação eléctrica redundantes;
3. O *router* não possui redundância activa, contudo existe em *stand-by* um *router* capaz de o substituir;
4. Todos os restantes dispositivos não possuem qualquer forma de redundância.

5.5.3 Rede informática

O Serviço de Informática possui uma rede informática responsável pela comunicação das diversas Direcções Executivas, seus departamentos e áreas operacionais a nível nacional. Contudo, existem ainda locais sem acesso a esta rede devido à sua localização recôndita e consequente falta de meios de comunicação.

Pela crescente necessidade de prestar mais e melhor serviços, o Serviço de Informática desenvolve paulatinamente a sua estrutura, estando neste momento com capacidade de interligar quatro províncias, nomeadamente Maputo, Beira, Nampula e Tete, recorrendo para tal a comunicações via cabo *UTP*, fibra óptica, satélite, ondas de rádio, redes sem fio e circuitos dedicados.

O processo de extensão desta rede sofreu no último semestre de 2006 uma aceleração significativa devido aos objectivos à longo prazo dos CFM de permitir o uso de *Internet* e *e-mail* a nível organizacional e ainda pela introdução de um *ERP*, que se concretizou no início de 2007. De salientar que esta rede cresce à medida que os provedores nacionais de serviços de comunicação estendem as suas coberturas.

5.5.4 Rede eléctrica

Com o objectivo de garantir o fornecimento contínuo de energia eléctrica dentro do Serviço de Informática estão implementadas as seguintes estruturas:

- Gerador diesel com uma autonomia de funcionamento de até 8 horas;
- Um circuito isolado, ligado a um *rack* de UPS com uma autonomia de cerca de 20 minutos.

5.5.5 Segurança lógica

A nível de segurança lógica, o único ponto de "contacto" exterior, para a *Internet*, é um *gateway* com *firewall* incorporado, responsável pela filtragem de todos os pacotes que entrem e saiam da rede. Este computador possui instalada uma aplicação de filtragem e encaminhamento de pacotes de rede, e tem como funções principais garantir a segurança das redes internas, encaminhar todos os pacotes de e para a *Internet* e actuar também como *anti-spyware*.

Está também instalado na rede um serviço de antivírus, e existe para tal um servidor dedicado exclusivamente a este serviço, que garante a actualização automática e protecção em tempo real de todos os computadores pertencentes à rede e nos quais esteja instalado o antivírus.

Relativamente à gestão de senhas, no momento da criação do utilizador, o colaborador responsável atribui ao utilizador a respectiva senha, a qual deverá forçosamente ser alterada da próxima vez que a conta for acedida. Esta política é aplicável às contas de e-mail e aos utilizadores do *ERP*. De salientar que a nível de autenticação na rede, esta encontra-se na forma de *Workgroup*.

5.5.6 Cópias de segurança

A informação é o coração e a alma de qualquer organização. Aceitar a importância da informação é o primeiro passo para alocar os recursos necessários para garantir que esta mantenha-se acessível, legível e recuperável (Doughty, 2001).

Actualmente, os CFM possuem a maior parte da sua informação financeira concentrada no *ERP*. São feitas cópias de seguranças diárias automáticas da base de dados deste sistema e arquivadas localmente no disco do servidor.

Está instalado um *tape – loader* com capacidade para 10 *tapes*, contudo este não se encontra actualmente em uso devido a falta de licenciamento. Este dispositivo esteve em funcionamento numa fase inicial, sob licenciamento de teste que se encontra neste momento expirado. As *tapes* então produzidas, eram enviadas para um cofre à prova de fogo localizado no mesmo edifício, contudo existem grandes dificuldades da catalogação das mesmas de forma a facilitar a sua procura.

Existe ainda um grande volume de informação espalhada por diversos computadores pessoais sobre os quais não são efectuadas cópias de segurança, salvo aqueles em que os utilizadores efectuam as suas cópias individuais.

Apesar da criticidade de realização, teste e documentação das cópias de segurança, o Serviço de Informática não possui ainda uma política formalmente definida para tal. Não existem igualmente procedimentos para teste e documentação das mesmas.

Estão a ser realizados esforços para aquisição de licenças para o uso do *tape – loader* e para a instalação de um servidor em réplica localizado na Direcção de Finanças da Direcção Executiva Sul.

5.5.7 Segurança física

A nível da segurança física, as instalações do Serviço de Informática estão guarnecidas a tempo inteiro por seguranças trabalhando em regime de turnos. Os acessos aos diversos compartimentos, incluindo o CPD, são controlados por chaves que se encontram na posse dos respectivos colaboradores. De salientar que está em curso um projecto para a implementação de Câmaras de Circuito Fechado e de portas electrónicas com acesso controlado por cartão magnético.

Relativamente à prevenção de desastres naturais, está instalado no CPD um sistema de detecção e combate a incêndios, com 9 botijas de Halon, accionadas automaticamente por um dispositivo electrónico ou por aumento da temperatura.

Contudo, a central de comando deste sistema já não se encontra em funcionamento, daí que o sistema tenha perdido a capacidade de detecção de incêndios e resposta imediata. Neste âmbito, estão em curso diligências para a instalação de um sistema moderno, que irá ainda substituir as botijas de Halon, dado que este componente é canceroso.

O CPD está localizado no quarto andar de um edifício sendo assim reduzidas, ou quase nulas, as probabilidades de ocorrência de inundações. O acesso para o mesmo tem uma rampa de elevação e o

chão é falso, o que garante que mesmo em caso de problemas com a canalização ou de infiltração de água de chuva o escoamento seja feito de forma a garantir a integridade do CPD.

5.6 Avaliação do desenvolvimento do PCN

O PCN desenvolvido apresenta-se como um protótipo para o que seria um documento final e passível de implementação. O protótipo desenvolvido tem como escopo o Serviço de Informática dos CFM sobre a sua vertente de TIC e não cobre os restantes processos do CFM, pelo que a sua implementação no actual estágio não é recomendada.

O estudo efectuado está além da real necessidade dos CFM e caso a organização decida pela implementação, o documento deverá ser revisto, suas fronteiras alargadas e suas variáveis reanalisadas.

Contudo, o desenvolvimento deste protótipo despertou situações relacionadas principalmente com a segurança de informação, que estão neste momento em estudo e implementação no Serviço de Informática do CFM.

Neste estudo foi igualmente possível constatar a grande disponibilidade para contribuir para a melhoria do Serviço de Informática por parte dos seus funcionários, que, de forma geral, se mostraram bastante prestativos.

De forma geral, o processo de desenvolvimento do protótipo de PCN para o Serviço de Informática do CFM pode ser considerado muito bom e bastante interessante.

CAPÍTULO V

6 CONCLUSÕES E RECOMENDAÇÕES

6.1 Conclusões

O conceito Continuidade vem adquirindo, particularmente na última década, uma elevada importância nas organizações. Este conceito está directamente ligado ao PCN, ferramenta esta que apesar de extremamente valiosa e útil é ainda pouco aplicada devido ao fraco conhecimento dos benefícios que a sua implementação traz para a organização ou dos riscos inerentes à falta de sua implementação.

A espinha dorsal de um PCN é a sua AIN, que requer uma análise profunda à organização de forma a não ignorar riscos que possam mais tarde mostrar-se críticos. Para tal é necessário incluir na equipa de implementação, para além dos especialistas, funcionários chave das áreas em análise e a gestão de topo de forma a permitir uma visão interna e superior respectivamente.

O processo de desenvolvimento do PCN é cíclico e contínuo, e jamais se deve considerar a implementação como concluída pois o ambiente em que as organizações se encontram inseridas está em constante flutuação. Não existe um método rígido para o desenvolvimento do PCN, sendo a sua estrutura variável de acordo com a organização

A fase de teste e manutenção do PCN é facilmente subavaliada e nestes casos deverá se tomar algum cuidado para que estes processos sejam devidamente efectuados. De nada servirá um PCN onde os funcionários não estejam familiarizados, ou ainda, que não responde às necessidades organizacionais.

No actual ambiente tecnológico, existem inúmeras técnicas e ferramentas que podem garantir a continuidade operacional contudo, esta escolha deve ser efectuada com base numa AIN e Análise de

Custo - Benefício respeitando assim os parâmetros de tolerância estabelecidos e a capacidade de investimento da organização.

Relativamente ao estudo efectuado no Serviço de Informática dos CFM, apresentam-se as seguintes conclusões:

- Os CFM encontram-se neste momento numa fase de informatização dos seus processos, trazendo à tona questões relacionadas com a segurança de informação e continuidade operacional;
- Correntemente, os CFM não possuem um PCN deixando assim à deriva qualquer garantia de continuidade operacional;
- A realização de uma AIN no Serviço de Informática dos CFM revelou-se morosa e complexa, principalmente devido à ocupação dos funcionários chave e a complexidade organizacional. Contudo, este processo foi bastante interessante e é consideravelmente satisfatório.

6.2 Recomendações

Destacam-se as seguintes recomendações:

- Que seja feita a implementação de um PCN no Serviço de Informática dos CFM, prestando especial atenção aos seguintes aspectos:
    - Deverá ser feita uma AIN o mais detalhada possível;
    - Deverão ser estabelecidas políticas e directrizes de trabalho e estas devem ser amplamente divulgadas com o objectivo de consciencializar a massa laboral sobre a estratégia delineada e visão de topo;
    - Deverão ser realizadas acções de formação na perspectiva de capacitação dos funcionários em matéria de segurança no ambiente de trabalho, segurança de informação e ainda reacção em casos de eventos inesperados.
- Que a implementação do PCN seja expansiva ao resto dos CFM preferencialmente de forma faseada seguindo a AIN. Esta abordagem é recomendada tendo como factor principal a dimensão e complexidade organizacional.

CAPITULO VI

7 BIBLIOGRAFIA

- Canton, L. (2003). Guard Force Management. Burlington, EUA - Elsevier
- Carruthers, P. (2006). CrashProof your Business. Cape Town, África do Sul – Aardvark Press Publishing (Pty) Ltd.
- Cumbe, A. (2002). Reaplicação entre bases de dados Oracle e os métodos de resolução de conflitos. Tese de Licenciatura. Maputo, Moçambique.
- D'Ascenção, Luís Carlos (2001). M. Organização, Sistemas e métodos: Análise, redesenho e informatização de processos administrativos. 1ª Edição. São Paulo, Brasil – Editora Atlas S.A.
- Miguel, S.(2003). Integração de Sistemas de Informação. Lisboa, Portugal. – FCA – Editora de Informática.
- De Oliveira, Jayr F. (2004). Sistemas de Informação versus Tecnologias de Informação. São Paulo, Brasil. – Editora Érica Lda.
- Doswell, B. (2000) A guide to Business Continuity Management. Leicester, Reino Unido. – Perpetuity Press.
- Doughty, Ken. (2001). Business Continuity Planning. Florida, EUA. – Auerbach Publications.
- Elliot, D. *et al* (2002). Business Continuity Management. Londres, Reino Unido – Taylor and Francis Group
- Francisco, B. (2004). Estudo sobre a implementação de um ERP: Caso da CETA. Tese de Licenciatura. Maputo, Moçambique.
- Freeman, R. (1989). Telecommunication System Engineering. EUA – John Wiley & Sons, Inc.
- Halabi, S. (2001). Internet Routing Architectures. Indianápolis, EUA – Cisco Press.
- Hillbritch, R. (199). Economia Monetária. São Paulo, Brasil. – Editora Altas.
- Killmeyer, J. (2006). Information Security Architecture. Florida, EUA – Auerbach Publications.
- Macome, E. (1995). Introdução a metodologia de investigação. Maputo. DMI-UEM.

- Mamede, H. São (2006). Segurança Informática nas Organizações. Lousã, Portugal – FCA – Editora de Informática.
- Razac, A. Vahid (2001). Reengenharia Informática – Avaliação da sua implementação no BSTM. Tese de Licenciatura. Maputo, Moçambique.
- Regulamento do trabalho de licenciatura para os cursos da faculdade de Ciências (1994), Maputo, DMI-UEM.
- Reuvid, J. (2005). Managing Business Risk. 2ª Edição. Londres, Reino Unido – Kogan Page
- Rodrigues, A. (2005). Oracle 10g e 9i. Lisboa, Portugal – FCA – Editora de Informática.
- Sikich, Geaty W. (2003). Integrated Business Continuity. Oklahoma, EUA – PenWell Corporation

- http://www.17799.com (última consulta a 15-07-2008)
- http://www.bis.org (última consulta a 15-07-2008)
- http://www.bs25999.com (última consulta a 15-07-2008)
- http://www.cfmnet.co.mz/ (última consulta a 15-07-2008)
- http://www.efagundes.com (última consulta a 15-07-2008)
- http://www.infopol.gov.mz (última consulta a 15-07-2008)
- http://www.iodsa.co.za (última consulta a 15-07-2008)
- http://www.kddi.com/english/index.html (última consulta a 15-07-2008)
- http://www.kpmg.co.mz (última consulta a 15-07-2008)
- http://www.safeintheknowledge.com/statistics.php (última consulta a 20-10-2008)
- http://www.soxlaw.com (última consulta a 15-07-2008)
- http://www.unisdr.org/africa (última consulta a 15-07-2008)
- https://www.govnet.gov.mz (última consulta a 15-07-2008)

CAPÍTULO VII

8 ANEXOS

8.1 Anexo A

Questionário às organizações

O questionário 1 foi apresentado à diversas organizações com sede estabelecida na cidade de Maputo, com vista ao apuramento estatístico de dados relacionados com o conhecimento e uso de PCN.

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Questionário

O presente questionário destina-se a obtenção de dados estatísticos em relação ao entendimento e aplicação do PCN nas organizações em Moçambique de forma a avaliar o uso desta ferramenta por parte das mesmas e apresentação de dados estatísticos em um Trabalho de Licenciatura a ser efectuado no Departamento de Matemática e Informática da Universidade Eduardo Mondlane.

Algumas definições

Tecnologia de Informação e Comunicação (TIC) – Conjunto de ferramentas baseadas em sistemas informáticos que permitem a recolha, processamento, armazenamento, protecção e transmissão de informação.

Plano de Continuidade de Negócios (PCN) – uma série de procedimentos para restaurar a operacionalidade normal após um desastre e com a máxima velocidade e mínimo impacto nas operações.

Para o preenchimento do questionário por favor escreva nos locais traçados ou circunscreva a opção desejada

Toda a informação recolhida será considerada confidencial e usada apenas para os fins mencionados.

- **Dados gerais**

Data: ____/_____/_____ Hora de Início: ____:____

Hora de Término: ____:____

Nome[1]: _____

Contacto[1]: _____ E-mail[1]: _____

Instituição[1]: _____ Categoria[1]: _____

Profissão[1]: _____ Cargo[1]: _____

Anos de Serviço na Organização[1]: _____ Anos de existência da organização[1]: __

Sector de Actividade[2]: _____ Nº de funcionários[1]: _____

- **Em relação à situação actual da organização**

1. Como classifica o nível de dependência da organização em relação as TIC?
   a. Totalmente dependente
   b. Muito dependente
   c. Dependente
   d. Pouco dependente
   e. Independente
   f. Sem comentários
2. A organização possui uma infra-estrutura alternativa de TIC que possa ser usada em caso de paragem da estrutura primária por qualquer eventualidade?
   Sim Não
3. Em caso afirmativo, esta estrutura foi alguma vez testada?
   Sim Não
4. A organização possui um sistema automático de cópias de segurança (*backups*) de dados e aplicações?
   Sim Não

[1] Opcional
[2] Serviços; Pescas; Hotelaria e Turismo; Agricultura; Seguros; Banca e Leasing; Comunicações; Construção; Alimentação e Bebidas; Comércio; Transporte; Indústria; Energia

5. Se sim, as cópias efectuadas foram alguma vez testadas?

   Sim Não

6. As cópias de segurança efectuadas encontram-se num local seguro fora das instalações da organização e estão facilmente acessíveis?

   Sim Não

7. Quantas pessoas tem conhecimento e acesso as cópias de segurança? Por favor especifique os seus cargos.

   a. _____ pessoas

   _____

   _____

8. Possui meios para garantir a continuidade manual dos processos e do fluxo organizacional em caso de paragem das TIC?

   Sim Não

9. Conhece o custo diário de paragem da organização? Em caso afirmativo, por favor indique um valor aproximado.

   Sim Não

   Confidencial? ☐ _____ MT

10. Por favor indique os sectores (caso estejam identificados) cuja paragem originaria uma crise nos seguintes intervalos de tempo:

Tempo de paragem	**Sectores identificados como críticos**
Entre 0 e 3 dias	
Entre 3 e 7 dias	
Superior a 7 dias	

11. A organização já esteve sujeita a alguma paragem devido a eventos inesperados (naturais ou humanos) e que tenham causado prejuízos consideráveis? Em caso afirmativo, por favor descreva resumidamente o evento e a forma como foi contornado.

    Sim Não

_____

_____

12. Qual o tempo de paragem aceitável para a organização?
    a. Recuperação imediata
    b. Até 4 horas
    c. De 4 a 24 horas
    d. De 24 a 72 horas
    e. Mais de 72 horas
    f. Sem comentário
13. A organização esteve sujeita a introdução ou actualização do Sistema Informático e das ferramentas de suporte às TIC nos últimos 5 anos?
    Sim Não
14. Em caso afirmativo, o processo representou algum tempo de paragem para a organização? Em caso afirmativo, por favor especifique o tempo de paragem em dias.
    Sim Não
    _____ dias
15. A organização esteve sujeita a algum tempo de paragem durante a transição para o Metical da Nova Família? Em caso afirmativo, por favor indique o tempo de paragem em dias.
    Sim Não
    Confidencial? ☐ _____ dias

1. **Em relação ao PCN**

16. Que situação melhor descreve o nível de Planeamento de Continuidade de Negócios para a organização?
    a. Nenhum planeamento
    b. Desenvolvendo planos
    c. Planos locais em uso
    d. Planos organizacionais em uso
    e. Sem comentário
17. Existe alguma percentagem do orçamento organizacional dedicado a Continuidade de Negócios? Em caso afirmativo, por favor indique a percentagem.

Sim Não

Confidencial? ☐ _____ %

18. A organização faz uso estratégico do PCN para fins publicitários (marketing)?

Sim Não

Comentários

_____

_____

_____

Por favor preencha a Hora de Término.

Muito obrigado!!!

Contacto:

Mahomed Akil Ashraf

Telemóvel: 82 – 7864810 / 82 – 7864811

E-mail: m_akil_a@yahoo.com / m_akil_a@hotmail.com

8.2 Anexo B

Questionário aos funcionários

Direccionado aos funcionários do Serviço de Informática dos CFM, este questionário teve como objectivo o apuramento dos pontos considerados críticos para o departamento e o estado de preparação dos funcionários para eventos inesperados.

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Questionário

O presente questionário destina-se a avaliação dos pontos críticos do departamento e suas consequências, bem como o estado de preparação dos funcionários do mesmo em relação a desastres ou eventos inesperados.

Algumas definições

Tecnologia de Informação e Comunicação (TIC) – Conjunto de ferramentas baseadas em sistemas informáticos que permitem a recolha, processamento, armazenamento, protecção e transmissão de informação.

Plano de Continuidade de Negócios (PCN) – uma série de procedimentos para restaurar a operacionalidade normal após um desastre e com a máxima velocidade e mínimo impacto nas operações.

Centro de Processamento de Dados (CPD) – Instalação física usada para albergar sistemas informáticos críticos para a organização e respectivos componentes.

Toda a informação recolhida será considerada confidencial e usada apenas para os fins mencionados.

- **Dados gerais**

Data: ____/_____/_____ Hora de Início: ____:____

Hora de Término: ____:____

Nome[1]: _____

Contacto[1]: _____ E-mail[1]: _____

Anos de Serviço na Organização[1]: _____ Categoria[1]: _____

Profissão[1]: _____ Cargo[1]: _____

1. Indique os riscos (independentemente da sua natureza e origem) e a respectiva probabilidade de ocorrência, impacto nas funções do departamento e formas de mitigações possíveis (1-Menos provável / Impacto quase nulo → 5-Muito Provável / Impacto Devastador)

Risco	Probabilidade	Impacto	Forma de mitigação

2. Está informado da existência ou não de procedimentos de segurança no departamento?
   Sim Não
3. Está informado da existência ou não de um PCN dentro do departamento?
   Sim Não
4. Considera o departamento apto para responder a uma paragem inesperada?
   Sim Não
5. A informação crítica para o funcionamento do departamento possui cópias de segurança?
   Sim Não
6. Em caso afirmativo, estas cópias encontram-se em um local seguro e de acesso fácil fora da organização?
   Sim Não
7. Quantas pessoas possuem acesso as cópias de segurança?
   _____ pessoas
8. Que aplicações são usadas para garantir o funcionamento do departamento?

[1] Opcional

_____

_____

_____

9. As bases de dados de suporte a estas aplicações possuem cópias de segurança efectuadas em intervalos de tempo aceitáveis?

   Sim Não

10. Está disponibilizada uma lista com nomes e contactos de emergência tais como Polícia, Bombeiros, empresas de manutenção e responsável pela segurança do Centro de Processamento de Dados?

    Sim Não

11. Indique resumidamente os possíveis impactos para organização, originados pela paragem do seu departamento.

    _____

    _____

    _____

    _____

12. Estão definidas as operações críticas e prioritárias para a restauração do funcionamento do departamento?

    Sim Não

13. Caso aconteça algum desastre sabe o que deve fazer, ou quais as suas funções? Em caso afirmativo, por favor descreva-as resumidamente.

    _____

    _____

    _____

Por favor preencha a Hora de Término.

Muito obrigado!!!

8.3 Anexo C

Guião de Entrevista a Consultores

O guião de entrevistas seguinte foi apresentado a consultores e outros gestores com experiência relativamente à implementação de PCN.

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Guião de entrevista para definição de ferramentas e técnicas de desenvolvimento de Planos de Continuidade de Negócios

O presente guião de entrevistas tem como objectivo a recolha de opiniões de diversos especialistas e consultores com experiência na área de Continuidade de Negócios, com vista a obter uma visão mais abrangente e de forma a permitir um melhor entendimento do tema e a definição de um modelo apropriado de Plano de Continuidade de Negócios.

Algumas definições

Tecnologia de Informação e Comunicação (TIC) – Conjunto de ferramentas baseadas em sistemas informáticos que permitem a recolha, processamento, armazenamento, protecção e transmissão de informação.

Plano de Continuidade de Negócios (PCN) – uma série de procedimentos para restaurar a operacionalidade normal após um desastre e com a máxima velocidade e mínimo impacto nas operações.

Toda a informação recolhida será considerada confidencial e usada apenas para os fins mencionados.

- **Dados gerais**

Data: ____/_____/_____ Hora de Início: ____:____

Hora de Término: ____:____

Nome[1]: _____

Contacto[1]: _____ E-mail[1]: _____

Instituição[1]: _____ Categoria[1]: _____

Profissão[1]: _____ Cargo[1]: _____

Anos de Serviço na Organização[1]: _____ Anos de existência da organização[1]: _

Sector de Actividade[2]: _____ Nº de funcionários[1]: _____

1. O que é um PCN?
2. Quais os objectivos de um PCN?
3. Já participou em projectos de implementação de PCN? Que tarefa desempenhou?
4. Quais são as principais fases de um PCN? Pode descreve-las?
5. Que metodologias de implementação de PCN conhece? Qual delas recomendaria? Porquê?
6. Que mais valia, representa o PCN para uma organização?
7. A que tipo de empresas aconselharia a implementação de um PCN?
8. Qual seria a percentagem de reserva orçamental para a implementação e manutenção de um PCN dentro de uma organização?
9. Quais as principais dificuldades encontradas no processo de implementação de um PCN? Como ultrapassa-las?

Por favor preencha a Hora de Término.

Muito obrigado!!!

[1] Opcional

[2] Serviços; Pescas; Hotelaria e Turismo; Agricultura; Seguros; Banca e Leasing; Comunicações; Construção; Alimentação e Bebidas; Comércio; Transporte; Indústria; Energia

8.4 Anexo D

Guião de Entrevista aos Funcionários

O seguinte guião de entrevista foi apresentado aos funcionários do Serviço de Informática dos CFM, para recolha de informação adicional sobre o departamento e complemento ao questionário 2.

UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Guião de entrevista para recolha de informação relativa ao funcionamento do departamento

O presente guião de entrevista tem como objectivo a recolha de informação relativa ao departamento em estudo e análise dos principais constrangimentos e fraquezas do mesmo. Permitirá um entendimento maior do seu funcionamento interno, de forma a estruturar o modelo de Plano de Continuidade de Negócios às exigências do departamento.

Algumas definições

Tecnologia de Informação e Comunicação (TIC) – Conjunto de ferramentas baseadas em sistemas informáticos que permitem a recolha, processamento, armazenamento, protecção e transmissão de informação.

Plano de Continuidade de Negócios (PCN) – uma série de procedimentos para restaurar a operacionalidade normal após um desastre e com a máxima velocidade e mínimo impacto nas operações.

Toda a informação recolhida será considerada confidencial e usada apenas para os fins mencionados.

- **Dados gerais**

Data: ____/____/_____ Hora de Início: ____:____

Hora de Término: ____:____

Nome[10]: _____

Contacto[11]: _____ E-mail[1]: _____

Anos de Serviço na Organização[1]: _____ Categoria[1]: _____

Profissão[1]: _____ Cargo[1]: _____

1. Quais as principais operações desempenhadas pelo departamento?
2. Que funções, suportam e garantem, o cumprimento destas operações?
3. Qual a posição do departamento na estrutura da organização?
4. Em que períodos a procura de serviços do departamento é mais elevada?
5. Quais seriam os impactos da paragem de funcionamento do departamento a nível organizacional?
6. Estão identificadas operações críticas e respectivos procedimentos de restauração em caso de interrupção?
7. O departamento possui algum procedimento para a realização de cópias de segurança para a informação? Onde são arquivadas estas cópias? Quem tem acesso a elas?
8. A localização do Centro de Processamento de Dados (CPD) é adequada em termos de segurança?
9. Está instalado algum sistema de detecção e combate a incêndios para o CPD?
10. Qual o grau de proximidade do CPD em relação a postos de gasolina, paióis, zonas com radiação electromagnética, etc.?
11. Podem ocorrer inundações no CPD ou no departamento?
12. Existe algum plano de emergência para o evento de uma catástrofe? Este plano é testado regularmente? Já alguma vez foi usada? Está devidamente documentado e encontra-se em local seguro? Está disseminado pelos funcionários?
13. Existem dispositivos alternativos para o fornecimento de energia eléctrica? Estão sujeitos a manutenção regular?
14. Existem dispositivos alternativos para o fornecimento da estrutura de TIC? Estão sujeitos a manutenção regular?
15. Como classificaria o nível de preparação dos funcionários relativamente a ocorrência de uma catástrofe?
16. Descreva alguma das principais fragilidades relativamente a continuidade operacional do departamento. Como estas fragilidades podem ser minimizadas?

[10] Opcional
[11] Opcional

Por favor preencha a Hora de Término.

Muito obrigado!!!

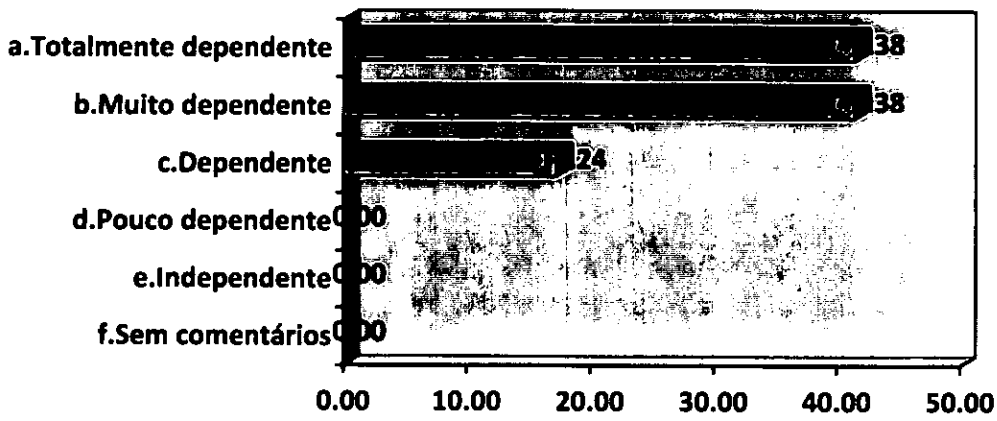
8.5 Anexo E

Resultados estatísticos do inquérito às organizações seleccionadas com base na pesquisa das 100 maiores empresas moçambicanas, efectuada pela KPMG em 2006.

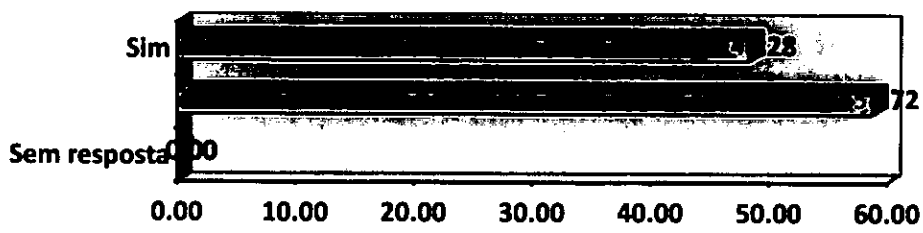
Os resultados estão apresentados na forma percentual, tendo em consideração o universo de inquéritos respondidos.

- **Em relação à situação actual da organização**

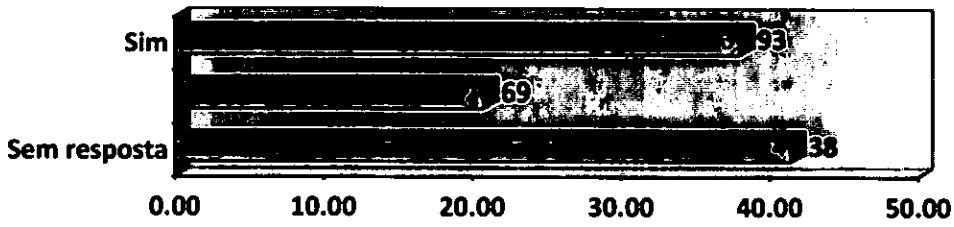
1. Como classifica o nível de dependência da organização em relação as TIC?



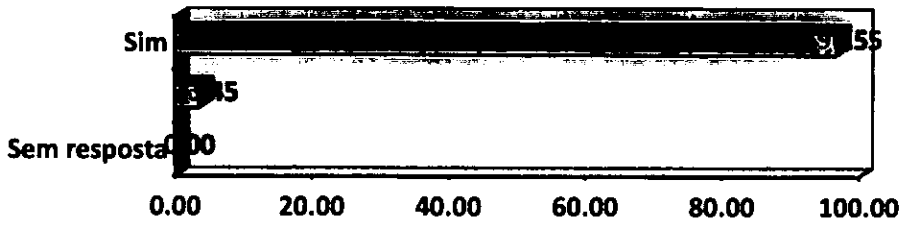
2. A organização possui uma infra-estrutura alternativa de TIC que possa ser usada em caso de paragem da estrutura primária por qualquer eventualidade?



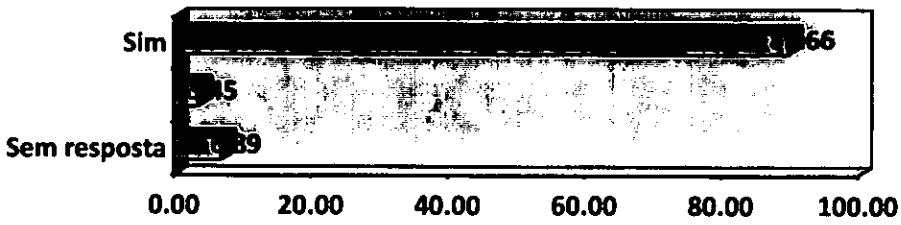
3. Em caso afirmativo, esta estrutura foi alguma vez testada?



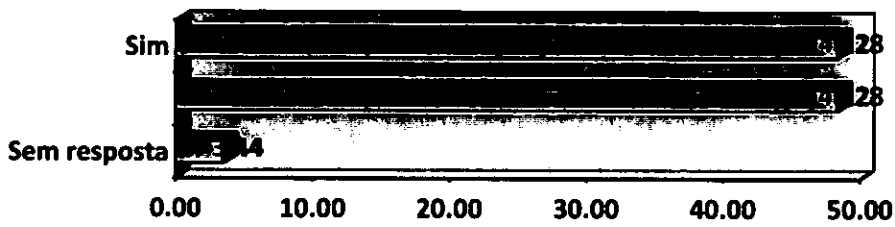
A organização possui um sistema automático de cópias de segurança (*backups*) de dados e aplicações?



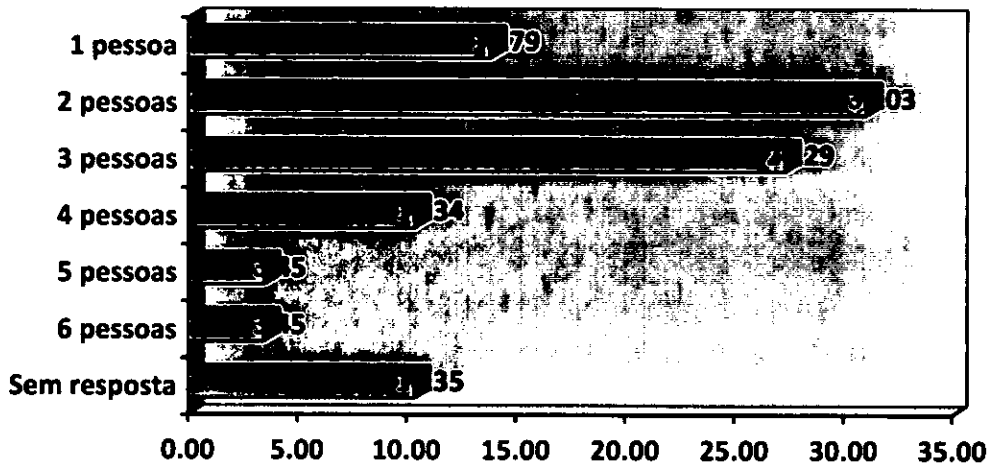
4. Se sim, as cópias efectuadas foram alguma vez testadas?



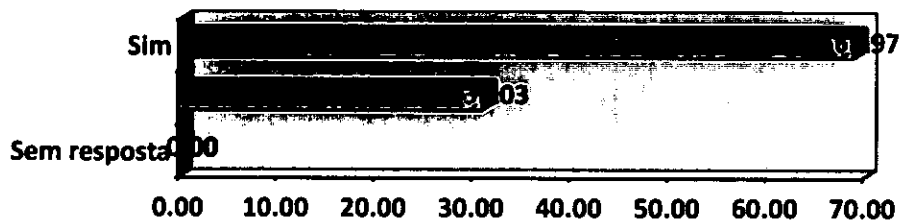
5. As cópias de segurança efectuadas encontram-se num local seguro fora das instalações da organização e estão facilmente acessíveis?



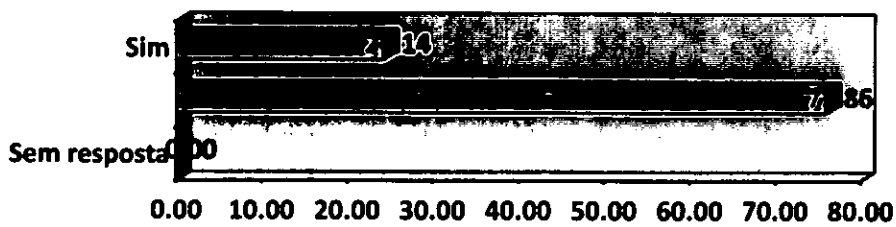
6. Quantas pessoas tem conhecimento e acesso as cópias de segurança? Por favor especifique os seus cargos.



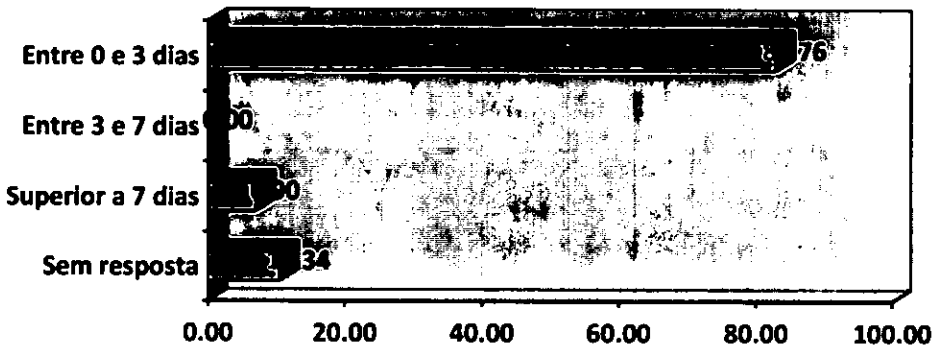
7. Possui meios para garantir a continuidade manual dos processos e do fluxo organizacional em caso de paragem das TIC?



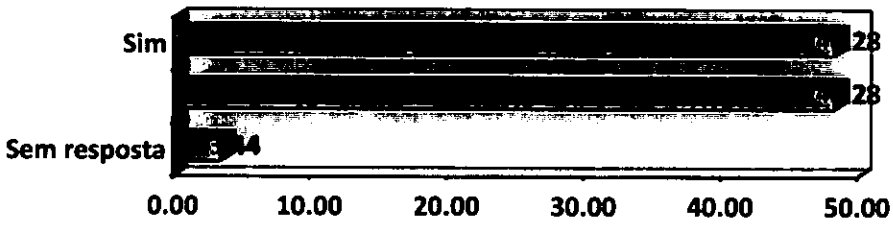
8. Conhece o custo diário de paragem da organização? Em caso afirmativo, por favor indique um valor aproximado.



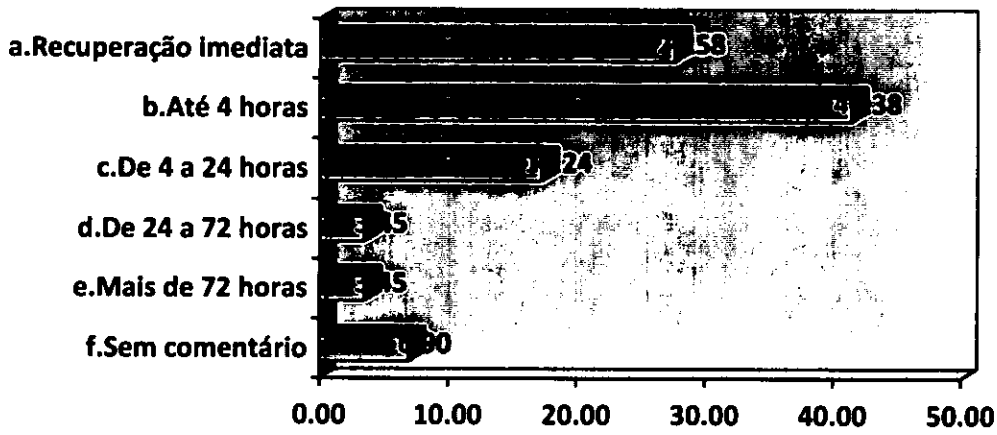
9. Por favor indique os sectores (caso estejam identificados) cuja paragem originaria uma crise nos seguintes intervalos de tempo:
   (Percentagem calculada com base no menor intervalo de tempo com pelo menos um sector crítico.)



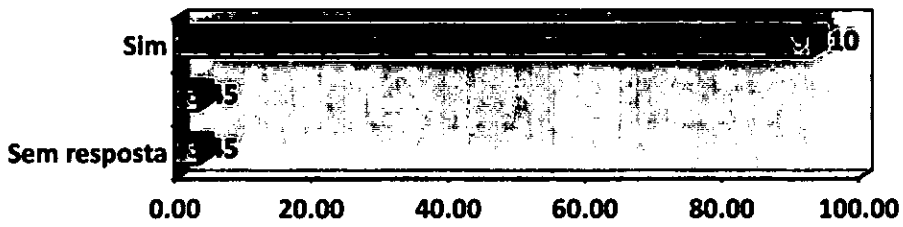
10. A organização já esteve sujeita a alguma paragem devido a eventos inesperados (naturais ou humanos) e que tenham causado prejuízos consideráveis? Em caso afirmativo, por favor descreva resumidamente o evento e a forma como foi contornado.



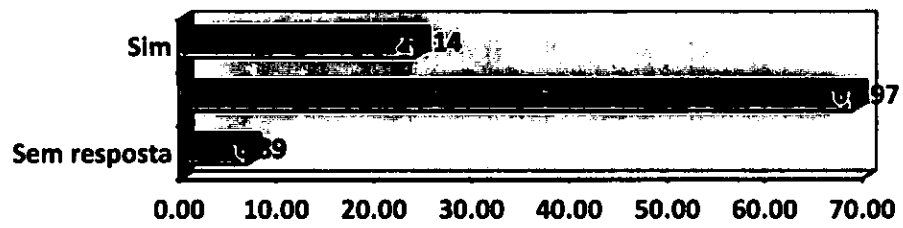
11. Qual o tempo de paragem aceitável para a organização?



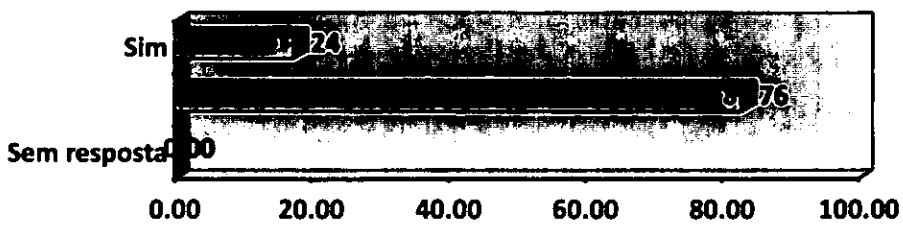
12. A organização esteve sujeita a introdução ou actualização do Sistema Informático e das ferramentas de suporte às TIC nos últimos 5 anos?



13. Em caso afirmativo, o processo representou algum tempo de paragem para a organização? Em caso afirmativo, por favor especifique o tempo de paragem em dias.

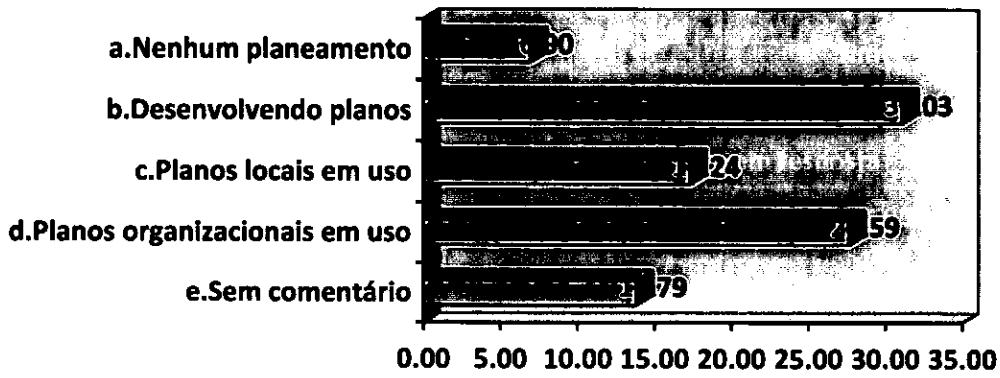


14. A organização esteve sujeita a algum tempo de paragem durante a transição para o Metical da Nova Família? Em caso afirmativo, por favor indique o tempo de paragem em dias.

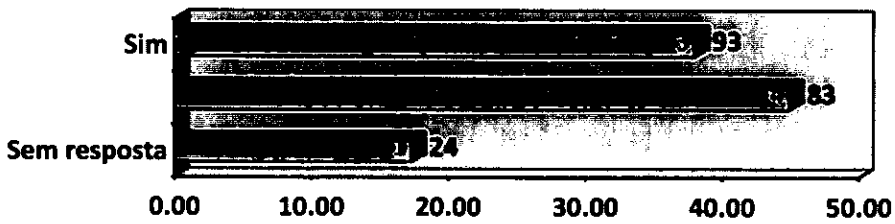


- **Em relação ao PCN**

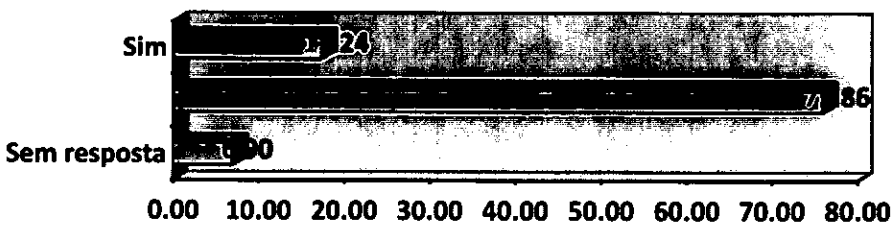
15. Que situação melhor descreve o nível de Planeamento de Continuidade de Negócios para a organização?



16. Existe alguma percentagem do orçamento organizacional dedicado a Continuidade de Negócios? Em caso afirmativo, por favor indique a percentagem.



17. A organização faz uso estratégico do PCN para fins publicitários (marketing)?



UNIVERSIDADE EDUARDO MONDLANE
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA E INFORMÁTICA

Protótipo de Plano de Continuidade de Negócios para os CFM

Mahomed Akil Ashraf

Fevereiro de 2009

Declaração de Confidencialidade

O presente Plano de Continuidade de Negócios e todo o seu conteúdo estão classificados como confidenciais e restritos só e somente aos funcionários abrangidos pela sua lista de distribuição.

Os mesmos não possuem qualquer direito de reutilização, cópia, e/ou divulgação deste documento nem do seu conteúdo.

Actualizações / Versões

Versão	Documentado por	Aprovado por	Data
«Versão»	«Nome do Responsável pela Documentação»	«Nome do Responsável pela Aprovação»	«Data da Versão»

Lista de Distribuição

Nome	Localização	Contacto	Contacto Alternativo
«Funcionário 1»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
«Funcionário 2»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
«Funcionário 3»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
«Funcionário 4»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
«Funcionário 5»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
«Funcionário 6»	«Seu gabinete»	«Contacto»	«Contacto Alternativo»
…	…	…	…

Siglas

- AIN – Análise de Impacto no Negócio
- CFM – Caminhos de Ferro de Moçambique
- CPD – Centro de Processamento de Dados
- DHCP – *Dynamic Host Configuration Protocol*
- DNS – *Domain Name System*
- ERP – *Enterprise Resource Planning*
- IP – *Internet Protocol*
- LAN – *Local Area Network*
- PCN – Plano de Continuidade de Negócios
- RPO – *Recovery Point Objective*
- RTO – *Recovery Time Objective*
- SIGRH – Sistema Informático de Gestão de Recursos Humanos
- TIC – Tecnologias de Informação e Comunicação
- UPS – *Uninterruptible Power Supply*
- WAN – *Wide-Area Network*

Índice de Figuras

Índice de Tabelas

Índice

1 INTRODUÇÃO

1.1 Objectivos

Este documento tem como objectivo delinear as acções, funções, responsabilidades e actividades chave que devem ser executadas de forma a permitir a recuperação de serviços críticos ao negócio, localizados no CPD, do Serviço de Informática da empresa Portos e Caminhos de Ferro de Moçambique (CFM), em casos de interrupção nos serviços.

Nota: Em caso de interrupção dos serviços por favor refira imediatamente para o Capítulo 2 deste documento.

1.2 Os CFM

1.2.1 Apresentação

A empresa Portos e Caminhos-de-Ferro de Moçambique, E.P., abreviadamente designada por CFM, é uma entidade colectiva de direito público, dotada de personalidade jurídica e com autonomia administrativa, financeira e patrimonial, exercendo a sua actividade na subordinação do Ministério dos Transportes e Comunicações.

O CFM rege-se pela Lei nº 17/91, de 3 de Agosto, pelos presentes estatutos, pelas disposições legais e regulamentares que especialmente lhe forem aplicáveis e finalmente, no que não estiver especialmente regulado, pelas normas de direito privado.

A defesa do interesse público que orientará toda a actividade da empresa, será assegurada pelo Governo, através do Ministério dos Transportes e Comunicações, salvo nos casos em que estiver expressamente definido de outro modo na Lei ou nos presentes estatutos.

A sede do CFM está situada na cidade de Maputo, e a organização exerce a sua actividade em todo o território nacional e poderá criar delegações em outros pontos do país desde que assim seja aprovado pelo Conselho de Administração. Este conselho delibera igualmente o estabelecimento de representações comerciais no estrangeiro.

O transporte ferroviário de pessoas e carga e a prestação de serviços portuários constituem o objecto da organização, sendo que esta pode ainda subscrever participações financeiras para a constituição de empresas mistas, desde que tal seja autorizado pelos Ministros dos Transportes e Comunicações e das Finanças.

1.2.2 Missão

O CFM assume como sua actual missão:

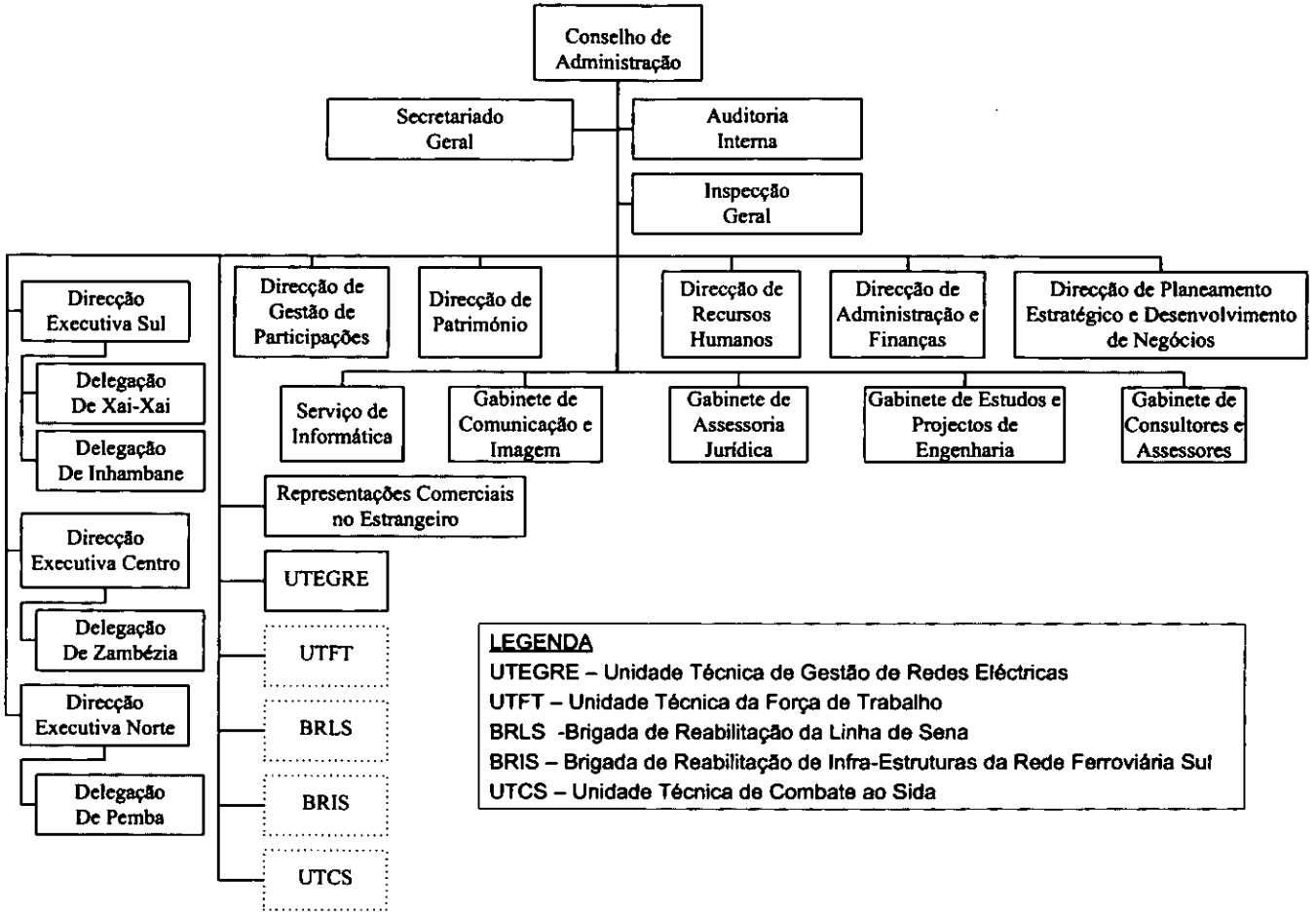
- A reconstrução do sistema de transporte ferro-portuário, para torná-lo moderno, competitivo, eficiente, orientado para o mercado e financeiramente viável.
- O investimento, promoção e desenvolvimento estratégico das infra-estruturas ferro-portuárias.
- Diversificação da sua intervenção empresarial, como forma de promover a sua sustentabilidade a longo prazo e rentabilizar os seus activos.

1.2.3 Objectivos

Na sua página inicial da *Internet*, o CFM estabelecem os seguintes objectivos:

- Promover e desenvolver as infra-estruturas ferro-portuárias e serviços;
- Promover o desenvolvimento das actividades de transporte e logística através da participação crescente do sector privado na sua operação e gestão;
- Envolver-se, em associação com o sector privado, na operação dos sistemas ferro-portuários de forma sustentável, segura, eficiente e proveitosa para o transporte de passageiros e carga e prestação de serviços portuários;
- Maximizar a utilização de forma racionalizada e rentável dos seus activos.

1.2.4 Organigrama



1.3 O Serviço de Informática

O Serviço de Informática do CFM foi criado com dois grandes objectivos:

- Estabelecer e implementar Políticas Informáticas para o CFM;
- Prover e garantir suporte na área das TIC à organização, de modo a auxiliar o maior número possível de áreas administrativas e operacionais.

Actualmente este Serviço presta apoio na aquisição e manutenção de material e aplicações informáticas e de gestão, actua como provedor de serviços de *Internet* e *e-mail*. O crescimento número de funcionários usando o *e-mail* e *Internet*, a recente introdução de um *ERP*, para gestão integrada que absorve a maior parte dos processos organizacionais tornam o Serviço de Informática preponderante e crítico para a continuidade operacional da organização.

O crescimento deste Serviço deve ser acompanhado por um incremento das suas capacidades de resposta, confiabilidade e garantia de prestação de serviços contínua ou com o mínimo de sobressaltos possíveis.

1.4 Escopo

O escopo definido para este documento limita-se ao Serviço de Informática do CFM. As demais Direcções e Serviços com dependências deste devem ser analisadas de forma a incluir suas prioridades e objectivos em planos mais abrangentes.

1.5 Exclusões

Os seguintes itens foram excluídos deste plano, e devem ser alvo de análise em futuros planos mais abrangentes:

- Continuidade operacional em casos de danos maiores ao edifício do Serviço de Informática;
- Identificação de processos e documentos que deverão ser alvo de redigitação em caso de recuperação com base em cópias de segurança anteriores;

- Material e procedimentos de emergência, saúde e segurança em caso de incidentes com consequências físicas;
- Resposta à comunicação social de forma a preservar a imagem organizacional e evitar informações destorcidas;
- Material e procedimentos de reparação em caso de incidentes com danos materiais e/ou estruturais;
- Material e procedimentos para operações de busca e salvação;
- Equipamento e procedimentos para a criação de local alternativo de trabalho;
- Plano de emergência para recuperação de computadores individuais;
- Questões sociais e de natureza não técnica.

1.6 Medidas de Prevenção

Com o objectivo de reduzir a probabilidade de invocar ou declarar uma situação de emergência, uma série de medidas foram implementadas de modo a incrementar a confiabilidade dos serviços prestados pelo Serviço de Informática. Estas medidas incluem:

- Gerador a diesel e *UPS* para alimentação contínua e estabilizada de energia eléctrica;
- Seguimento das recomendações contidas no manual do gerador;
- CPD localizado no 4º andar e com rampa de acesso de modo a evitar a entrada de água resultando em inundações;
- Chão e tecto falso para gestão da cablagem e possível expansão para sistema de detecção e combate de incêndios e sistema de detecção de inundações;
- Servidor de *ERP* (Servidor Bilene) e de ligações remotas (Servidor Limpopo) com *array* de discos redundantes;
- Servidor de *ERP* (Servidor Bilene), de ligações remotas (Servidor Limpopo), de SIGRH (Servidor Bazaruto) e *DHCP/DNS* (Servidor Índico - Sul) com fontes de alimentação redundantes;
- Antivírus e *Firewall* de forma a prevenir e minimizar as possibilidades de impacto derivados de ataques lógicos;

- Cópias de segurança automáticas diferenciais diários configurados para a base de dados do *ERP*;
- Cópias de segurança automáticas completos semanais configurados para a base de dados do *ERP*;
- Câmaras de circuito fechado de televisão para monitoria da segurança física na Direcção;
- *Router* em *stand-by* para substituição em caso de avaria de um *router* activo;
- Cópias diárias das configurações do *firewall*;
- Disco - duro em *stand-by* para o *firewall;*
- Placa *serial* em *stand-by* para *router;*
- Licenciamento devido para os sistemas operativos e aplicações.

1.7 Assumpções

Com base em entrevistas efectuadas aos funcionários do Serviço de Informática foram estabelecidos os seguintes parâmetros que irão determinar as estratégias e técnicas de recuperação:

Tabela 1: Parâmetros de recuperação

Serviço	RTO	RPO
Antivírus e *firewall*	4 horas	-
Internet e *e-mail*	1 dia	-
ERP	1 dia	1 dia
Ligações remotas	2 dias	-
SIGRH	5 dias	1 dia
Hospedagem de Página de Internet	15 dias	30 dias
Restantes Serviços	15 dias	-

1.8 Análise de Impacto no Negócio (AIN)

Neste capítulo é feita uma análise das ameaças detectadas e seus respectivos impactos a vários níveis, tal como as suas formas de mitigação. De salientar que os impactos encontram-se numa escala de 1 a 5, sendo 5 a indicação de impacto maior ou menores recursos de mitigação.

Tabela 2: Análise de Impacto no Negócio

Desastre/ Risco	Análise	Probabilidade	Impacto Humano	Impacto Material	Impacto no Negócio	Recursos Internos p/Mitigação	Recursos Externos p/Mitigação	Total	Recursos para Mitigação	Formas de redução
Incêndio	O Serviço de Informática não possui neste momento um sistema de combate e detecção de incêndios. A maioria dos extintores não estão sujeitos a manutenções regulares e os funcionários não possuem treino	1	3	5	5	2	4	14	6	• Instalação de sistemas automáticos de detecção e combate a incêndios para o CPD; • Revisão regular dos extintores; • Instalação de bocas incêndios com mangueiras de água; • Treino do pessoal para reacção

	para o seu uso. Não existem saídas de emergência.									e uso das ferramentas de combate a incêndios; • Criação de saídas de emergência.
Confidencialidade da informação	A rede dos CFM encontra-se conectada em forma de grupo de trabalho (*WorkGroup*), não existem sub-redes definidas e as pastas partilhadas em qualquer computador dentro da rede podem ser acedidas por qualquer outro colaborador.	3	0	0	2	5	5	5	10	• Colocação da rede em domínio; • Criação de sub-redes com controlo de acesso bem delineado; • Educação dos utilizadores em relação ao uso de senhas, e em relação à segurança e confidencialidade da informação.

Politicas para regência das cópias de segurança	Não existem políticas formais para a gestão das cópias de segurança. Estas são arquivadas localmente no mesmo servidor, não estão sujeitas a teste para verificação da sua integridade/ Não existem cópias regulares para um local no exterior/ Informação crítica encontra-se espalhada em maquinas individuais e não sujeita a cópias de segurança	4	0	0	4	3	5	8	8	• Definição de políticas de cópias de segurança estruturadas de acordo com a criticidade e importância da informação a ser copiada; • Realização de testes das cópias de segurança efectuadas; • Armazenamento de cópias de segurança em localização física distinta; • Criação de espaços individuais em forma de *File Server*, sincronizados com as máquinas individuais de forma a manter cópias de segurança.
Baixa formação e informação relativa à segurança	As medidas de segurança implementadas, procedimentos e estruturas de trabalho não estão divulgadas pelo departamento pelo que as reacções em casos de emergência não serão estruturadas e estarão sujeitas a juízo individual	2	1	2	4	3	2	9	5	• Divulgação de informação relativa à segurança e formação dos funcionários nesta matéria.

Climatização deficiente no CPD	Os aparelhos de ar condicionado instalados no CPD são deficientes e podem parar de funcionar repentinamente	3	0	0	4	5	1	7	6	• Renovação do sistema de climatização do CPD; • Manutenção regular.
Inoperacionalidade da rede de comunicações	A rede informática representa actualmente a espinha dorsal de todos os serviços que o Serviço de Informática presta a organização, sendo crucial o seu funcionamento sem interrupções	3	0	0	4	2	1	7	3	• Criação de vias de comunicação alternativas tais como comunicação sem fios, circuito dedicado ou outras.
Vírus/ *Spyware*/ *Malware*/ Outros ataques lógicos	Com o crescente uso da *Internet* e suas ferramentas, e com um cada vez maior número de utilizadores de dispositivos portáteis de transporte de informação estrutura de TIC torna-se cada vez mais propensa à "infecção"	3	0	0	5	1	1	8	2	• Actualização das aplicações; • Monitoria e responsabilizações dos *scans;* • Melhoramento do controle de acessos à *Internet* e educação dos utilizadores em relação ao uso de dispositivos de armazenamento de informação.
Funcionários estagiários	Os funcionários estagiários acedem ao CPD, estando propensos a erros e/ou falhas devido a sua incapacidade	2	0	0	3	1	0	5	1	• Treino e acompanhamento aos estagiários de forma a prepará-los para o ambiente de trabalho real com a mínima propensão a erros;

	técnica e/ou falta de conhecimento e domínio da estrutura e procedimentos									• Abertura de diálogo de forma a permiti-los expor as suas lacunas livremente.
Incapacidade de resposta a emergências	Em casos de emergência, não estão definidos procedimentos standard para a forma como os funcionários deve actuar e responder ao evento	2	1	1	3	2	1	7	3	• Definição de serviços críticos e prioritários; • Estabelecimento de um plano de emergência.

1.9 Estratégia de Continuidade de Negócios

Considerando a anterior AIN, os parâmetros de recuperação apresentados, e uma análise de custo benefício, as seguintes estratégias serão propostas de forma a garantir a Continuidade Operacional dentro dos parâmetros definidos.

- Instalação de Sistema de Detecção e Combate automático de incêndios para o CPD;
- Adequação do equipamento de climatização existente no CPD, de forma a controlar a temperatura e humidade;
- Migração da rede para uma estrutura em domínio (*Active Directory*) de forma a permitir melhor exploração dos recursos de rede garantindo ao mesmo tempo o controle de acesso tendo em conta a confidencialidade da informação;
- Reestruturação da cablagem de rede de forma a aumentar a sua performance e facilitar a manutenção;
- Inclusão de elementos redundantes na estrutura da rede informática de forma a garantir comunicação com os principais centros regionais em casos de corte da ligação primária. Estes elementos não devem necessariamente permitir a redundância em tempo real, mas sim garantir a comunicação dentro dos parâmetros estabelecidos;
- Consciencialização dos utilizadores relativamente ao uso e manutenção de recursos de rede e segurança de informação;
- Definição de políticas de partilha de informação com o objectivo de reduzir o acesso e disseminação de informação confidencial;
- Criação de uma estrutura *File Server* para armazenar informação individual dos colaboradores, evitando assim a grande dispersão de informação;
- Definição de políticas para a realização de cópias de segurança e testes dos mesmos, de forma a garantir os *RPOs* definidos para cada serviço;
- Responsabilização da execução e teste das cópias de segurança a funcionários distintos de forma a detectar atempadamente cópias corrompidas ou inacessíveis;
- Passagem periódica das cópias de segurança para tapes, em duplicado, de forma a armazenar uma cópia no cofre localizado no Serviço de Informática e outra em edifício distinto mas de fácil acesso;

- Criação de um servidor em *stand-by*, em localização distinta do CPD, que permita a substituição de qualquer um dos servidores primários, sendo apenas necessário a instalação do serviço e renomeação da máquina (nome e *IP* de forma a garantir a indexação por parte dos clientes);
- Estabelecimento e responsabilização de *scans* de *vírus*, *spyware* e *malware*;
- Verificação e manutenção periódica da cablagem eléctrica de forma a evitar curtos circuitos ou outros incidentes do género;
- Treino, acompanhamento e consciencialização de funcionários estagiários em relação à segurança física e lógica.

1.10 Equipas do PCN e Organigrama

1.10.1 Equipas e suas responsabilidades

1.10.1.1 Equipa de Gestão Executiva

A equipa de Gestão Executiva é composta pelos membros seniores e responsável pela orientação geral, tomadas de decisões e aprovações necessárias para a implementação do PCN. Normalmente, esta é a única equipa responsável pela activação do plano.

1.10.1.2 Coordenador de Continuidade de Negócios

Responsável por apoiar a activação do plano, o coordenador de continuidade de negócios deve ser o indivíduo com o conhecimento mais detalhado sobre o plano.

1.10.1.3 Equipa de TIC e Telecomunicações

Responsável por todas as comunicações de voz e dados dentro das instalações ou no local alternativo. Esta equipa tem também a função de restaurar as aplicações que se revelem críticas para a organização e os terminais dos utilizadores.

1.10.1.4 Equipa de Segurança

Responsável pela manutenção da segurança no interior e áreas anexas e circunvizinhas às instalações ou ao local alternativo.

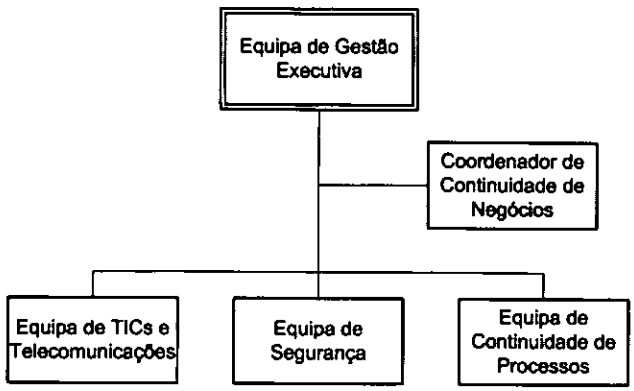
1.10.1.5 Equipa de Continuidade de Processos

Equipa composta de utilizadores finais, que irão colaborar na manutenção de operações vitais e recuperação de dados caso necessário.

1.10.2 Organigrama

A
Figura 1 apresenta o organigrama para as equipas que compõem o PCN.

Figura 1: Organigrama das equipas do PCN



2 INFORMAÇÃO CRÍTICA AO PCN

2.1 Em caso de emergência

Caso tenha detectado alguma anomalia, situação adversa, risco eminente, ou qualquer outro acontecimento que possa perigar a saúde e segurança dos funcionários, integridade das instalações e sua infra-estrutura, funcionamento normal do Serviço de Informática, segurança e/ou integridade da informação e TIC, por favor contacte um dos seguintes elementos:

Tabela 3: Contactos de emergência

Nome	Contacto	Contacto Alternativo
«Director do Serviço»	«Contacto»	«Contacto Alternativo»
«Chefe de Serviço A»	«Contacto»	«Contacto Alternativo»
«Chefe de Serviço B»	«Contacto»	«Contacto Alternativo»
«Chefe de Serviço C»	«Contacto»	«Contacto Alternativo»

2.2 Equipa de Gestão Executiva

2.2.1 Responsáveis

Tabela 4: Responsáveis da Equipa de Gestão Executiva

Ordem	Nome	Contacto	Contacto Alternativo
1	«Administrador do Pelouro»	«Contacto»	«Contacto Alternativo»
2	«Director do Serviço»	«Contacto»	«Contacto Alternativo»
3	«Chefe de Serviço A»	«Contacto»	«Contacto Alternativo»
4	«Chefe de Serviço B»	«Contacto»	«Contacto Alternativo»
5	«Chefe de Serviço C»	«Contacto»	«Contacto Alternativo»

2.2.2 Lista de Chamadas

Tabela 5: Lista de chamadas da Equipa de Gestão Executiva

Função	Nome	Contacto	Contacto Alternativo
Coordenador de Continuidade	«Coordenador de Continuidade»	«Contacto»	«Contacto Alternativo»

2.2.3 Lista de Tarefas

- Analisar o Incidente
- Invocar o plano
- Coordenação geral das actividades de recuperação
- Monitorar o processo de recuperação
- Reportar ao CA

2.2.4 Lista de Equipamentos

- 1 Telemóvel

2.2.5 Lista de Aplicações

N/A

2.2.6 Lista de Provedores de Serviços

N/A

2.2.7 Lista de Registos Vitais

- PCN
- Listagem de senhas

2.3 Coordenador de Continuidade de Negócios

2.3.1 Responsável

Tabela 6: Coordenador de Continuidade de Negócios

Nome	Contacto	Contacto Alternativo
«Coordenador de Continuidade»	«Contacto»	«Contacto Alternativo»

2.3.2 Lista de Chamadas

Tabela 7: Lista de chamadas do coordenador de Continuidade de Negócios

Equipa	Nome	Contacto	Contacto Alternativo
TIC e Telecomunicações	«Responsável dos Serviços de TIC e Telecomunicações»	«Contacto»	«Contacto Alternativo»
Segurança	«Responsável pela Segurança»	«Contacto»	«Contacto Alternativo»
Continuidade de Processos	«Responsável pela Continuidade de Processos»	«Contacto»	«Contacto Alternativo»

2.3.3 Lista de Tarefas

- Garantir a distribuição do plano
- Comunicar às restantes equipas
- Coordenar actividades das equipas
- Comunicação com provedores de serviços caso necessário
- Garantir o cumprimento do processo de recuperação
- Relatório do processo de recuperação
- Comunicação à equipa de Gestão Executiva
- Coordenar a actualização do plano

2.3.4 Lista de Equipamentos

- 1 Telemóvel

2.3.5 Lista de Aplicações

N/A

2.3.6 Lista de Provedores de Serviços

Tabela 8: Lista de provedores de serviço

Nome	Endereço	Contacto	Responsável	Contacto
«Provedor de Serviços A»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
«Provedor de Serviços B»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
«Provedor de Serviços C»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
…	…	…	…	…

2.3.7 Lista de Registos Vitais

- PCN

2.4 Equipa de TIC e Comunicações

2.4.1 Responsável

Tabela 9: Responsável da Equipa de TIC e Comunicações

Nome	Contacto	Contacto Alternativo
«Responsável dos Serviços de TIC e Telecomunicações»	«Contacto»	«Contacto Alternativo»

2.4.2 Lista de Chamadas

Tabela 10: Lista de chamadas da Equipa de TIC e Comunicações

Ordem	Nome	Contacto	Contacto Alternativo
1	«Técnico1 de TIC e Telecomunicações»	«Contacto»	«Contacto Alternativo»
2	«Técnico2 de TIC e Telecomunicações»	«Contacto»	«Contacto Alternativo»
3	«Técnico3 de TIC e Telecomunicações»	«Contacto»	«Contacto Alternativo»

2.4.3 Lista de Tarefas

- Operacionalizar a rede (*LAN* e *WAN*) de forma a possibilitar o trabalho da Equipa de Contabilidade
- Garantir capacidade de processamento de forma a satisfazer os requisitos da Equipa de Contabilidade
- Prover circuitos de telefonia fixa
- Prover acesso à *Internet* e *E-mail*
- Operacionalizar os servidores de aplicações críticas
- Garantir assistência técnica às restantes equipas

2.4.4 Lista de Equipamentos

- Cabo *UTP Cat5*
- Fichas *RJ45*
- Fichas *RJ11*
- Alicate de Crampagem
- 1 Computador Portátil
- Material para substituição de componentes danificados
- Telemóvel

2.4.5 Lista de Aplicações

- *MS - Windows Server 2003*
- *MS – Windows Server 2000*
- *MS – Windows Vista*
- *MS – Windows XP*
- *MS – Windows 2000*
- *MS – SQL Server 2005*
- *Astaro*
- *VNC*
- *Symantec Antivírus*
- *Mail - Server*

- *PHC 2007*

2.4.6 Lista de Provedores de Serviços

N/A

2.4.7 Lista de Registos Vitais

- PCN
- Cópia de segurança do *PHC*
- Cópia de segurança de SIGRH
- Cópia de segurança das configurações do *firewall*
- Cópia de segurança das configurações de *router*
- Diagrama de rede
- Diagrama de comunicações

2.5 Equipa de Segurança

2.5.1 Responsável

Tabela 11: Responsável da Equipa de Segurança

Nome	Contacto	Contacto Alternativo
«Responsável pela Segurança»	«Contacto»	«Contacto Alternativo»

2.5.2 Lista de Chamadas

N/A

2.5.3 Lista de Tarefas

- Avaliar as necessidades de segurança
- Comunicar empresa provedora de segurança
- Comunicar bombeiros caso necessários
- Comunicar serviços hospitalares de necessário
- Garantir a segurança das instalações

2.5.4 Lista de Equipamentos

- 1 Telemóvel

2.5.5 Lista de Aplicações

N/A

2.5.6 Lista de Provedores de Serviços

Tabela 12: Lista de provedores de serviço para a Equipa de Segurança

Nome	Endereço	Contacto	Responsável	Contacto
«Provedor de Serviços A»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
«Provedor de Serviços B»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
«Provedor de Serviços C»	«Endereço»	«Contacto»	«Responsável»	«Contacto»
…	…	…	…	…

2.5.7 Lista de Registos Vitais

- Plano de Continuidade de Negócios
- Planta do edifício

2.6 Equipa de Continuidade de Processos

2.6.1 Responsável

Tabela 13: Responsável da Equipa de Continuidade de Processos

Nome	Contacto	Contacto Alternativo
«Responsável pela Continuidade de Processos»	«Contacto»	«Contacto Alternativo»

2.6.2 Lista de Chamadas

Tabela 14: Lista de chamadas da Equipa de Continuidade de Processos

Ordem	Nome	Contacto	Contacto Alternativo
1	«Técnico1 de Continuidade de Processos»	«Contacto»	«Contacto Alternativo»
2	«Técnico2 de Continuidade de Processos»	«Contacto»	«Contacto Alternativo»
3	«Técnico3 de Continuidade de Processos»	«Contacto»	«Contacto Alternativo»
…	…	…	…

2.6.3 Lista de Tarefas

- Garantir a continuidade operacional dos principais processos de negócio

2.6.4 Lista de Equipamentos

- 7 Computadores de mesa
- 1 Computador portátil
- 1 Impressora

2.6.5 Lista de Aplicações

- *PHC*
- *SIGRH*

2.6.6 Lista de Provedores de Serviços

N/A

2.6.7 Lista de Registos Vitais

- PCN

3 MANUTENÇÃO DO PLANO

3.1 Revisões calendarizadas

O PCN deve ser alvo de revisões dentro dos seguintes intervalos de tempo:

- Mensal
  - Actualização das listas de chamadas;
  - Actualização dos contactos da lista de chamadas;
  - Actualização dos contactos da lista de provedores de serviço.
- Trimestral
  - Verificação da disponibilidade dos registos vitais.
- Anual
  - Revisão da análise de impacto nos negócios.

3.2 Revisões não calendarizadas

O PCN deve acompanhar as transformações às quais a organização está sujeita, e nem sempre estas são previsíveis. Assim, as seguintes alterações devem despoletar uma revisão no PCN:

- Entrada/Saída de funcionários;
- Alterações no organigrama organizacional;
- Alterações na estrutura de *hardware*;
- Alterações na estrutura da rede informática ou de comunicações;
- Alterações na estrutura física das instalações;
- Introdução de novas aplicações;
- Alterações nos regimes de cópias de segurança;
- Alterações dos parâmetros de recuperação (*RPO* e *RTO*).

4 EXERCICIO DO PCN

O exercício do PCN possui dois objectivos, nomeadamente:

- Criar um ambiente de aprendizagem para que todos os participantes possam se familiarizar com o Plano;
- Documentar alterações, actualizações e omissões sobre o Plano.

Em qualquer exercício, todos os participantes devem ser instruídos a restringir as suas acções ao uso apenas dos recursos disponibilizados pelo plano, e ainda a anotarem toda e qualquer actualização necessária ao plano. Estas anotações devem ser apresentadas ao Coordenador de Continuidade no final do exercício.

4.1 Simulação

A simulação é uma forma de exercício na qual, perante o cenário apresentado, os utilizadores percorrem o PCN com o objectivo de familiarizar à sua estrutura, ao mesmo tempo que são verificadas se as situações previstas correspondem aos requisitos reais de recuperação. Durante a simulação não são realizados testes ao equipamento e processos. Estes apenas são revisitados e seu fluxo analisado.
Semestralmente, deverá ser feito uma simulação sobre o PCN, com os seguintes objectivos:

- Familiarizar os participantes com os procedimentos do PCN;
- Validar as listas de recursos, tarefas e chamadas definidas no PCN verificando se mostram-se suficientes para o processo de recuperação;
- Verificar se a actual versão do plano responde as necessidades organizacionais.

É de seguida apresentada a estrutura para a realização da simulação:

- Marcação antecipada da data do exercício de forma a garantir a presença de todos os intervenientes;
- Garantir a presença de observadores externos e independentes;
- Determinação do cenário (Exp. Corte de energia, terramoto, falha de comunicação);
- Breve apresentação do cenário aos participantes;

- Revisão completa dos procedimentos de recuperação, garantindo que todos os recursos usados sejam disponibilizados no PCN.

4.2 Teste em tempo-real

Anualmente, deverá ser feito um teste completo as estratégias de continuidade implementadas. Contrariamente à simulação, para os testes em tempo-real não existe necessidade de determinação de um cenário, visto que todos os processos de recuperação devem ser revistos em ambiente de teste.
Este tipo de exercício deve focar as suas atenções em:

- Marcação antecipada da data do exercício de forma a garantir a presença de todos os intervenientes;
- Testar os dispositivos de redundância e replicação;
- Verificar integridade dos dados replicados;
- Testar o equipamento redundante e respectivos processos de inicialização;
- Testar vias de telecomunicação alternativas;
- Seguir procedimentos de reinstalação de servidores e clientes de aplicações críticas;
- Efectuar simulações de lançamento de registos para os sistemas críticos.

A presença de observadores externos é também recomendada, de forma a garantir o seguimento dos processos e relatório de situações que devem ser melhores e/ou corrigidas.
O objectivo deste exercício é validar de uma forma genérica a capacidade de resposta do plano às diversas adversidades que a organização possa encontrar, bem como avaliar a capacidade de resposta dos funcionários tendo em conta os constrangimentos relacionados com tempo e recursos.

4.3 Relatórios

4.3.1 Avaliação do Exercício

Após cada exercício, deve ser elaborado o relatório de avaliação do exercício, que deve conter os seguintes detalhes:

- Participantes
- Cenário apresentado;

- Desempenho individual e por equipas;
- Alterações e omissões detectadas;
- Comentários finais;
- Relatório dos observadores externos em anexo.

Este relatório é responsabilidade do Coordenador de Continuidade de Negócios e deve ser apresentado à Equipa de Gestão Executiva, com uma cópia para cada participante.

5 Anexos

5.1 Procedimentos para arranque manual do gerador

5.2 Diagrama de rede informática

5.3 Diagrama de rede eléctrica

5.4 Diagrama de rede de comunicação

5.5 Características dos servidores

5.6 Aplicações críticas dos servidores

5.7 Localização de cópias de segurança

5.8* Localização do *router* em *stand-by

5.9 Procedimentos de substituição do *router*

5.10* Procedimentos de instalação do *MS – Windows 2003 Server

5.11 Procedimentos de instalação do *MS – Windows 2000 Server*

5.12 Procedimentos de instalação do *MS – Windows Vista*

5.13 Procedimentos de instalação do *MS – Windows XP*

5.14 Procedimentos de instalação do *MS – Windows 2000*

5.15 Procedimentos de instalação do *Astaro*

5.16 Procedimentos de instalação do *VNC*

5.17 Procedimentos de instalação do *Mail – Server*

5.18 Procedimentos de instalação do *MS-SQL Server 2005*

5.19 Procedimentos de restauração de bases de dados

5.20 Procedimentos de instalação do *Symantec Antivírus*

5.21 Procedimentos de instalação do *Gateway* e *Firewall*

5.22 Procedimentos de instalação do *PHC 2007*

5.23 Procedimentos de instalação do SIGRH

***5.24* Procedimentos de instalação do WebServer**

5.25 Procedimentos de configuração das Ligações Remotas

5.26 Planta do edifício

5.27 Relatórios de exercícios anteriores