

Universidade Lusófona de Humanidades e Tecnologias

Escola de Comunicação, Artes e Tecnologias da Informação

Plano de Recuperação de Dados

em caso de desastre provocado por fenómenos naturais

Alunos:

José Manuel Catarino Cascais Brás – 20070027
Vasco Joaquim da Conceição do Sacramento – 20070094

Orientador:

Professor Mestre Pedro Malta

Lisboa, 2010

Índice

Índice de tabelas	3
Índice de figuras	3
Siglas utilizadas	4
Resumo	5
Abstract.....	6
1. Introdução.....	7
2. Enquadramento teórico	8
2.1. Continuidade do negócio	10
2.2. Desafios na implementação de formas de continuidade do negócio	11
2.3. Recuperação de desastres.....	13
3. Método	16
4. Plano DRP (Disaster Recovery Plan).....	17
4.1. Objectivos do plano DRP	17
4.2. Requisitos.....	19
4.3. <i>Overview</i> do negócio	20
4.4. Âmbito	23
4.5. Gestão do risco.....	23
4.5.1. Minimização do risco	24
4.5.2. Controlo dos custos de TI.....	25
4.5.3. Risk IT	26
4.5.4. Levantamento e definição dos recursos críticos	29
4.6. Segurança.....	31
4.7. Business Impact Analysis (BIA).....	34
4.8. Gestão de contratos e serviços TI	37
4.8.1. ITIL.....	37
4.8.2. Val IT.....	39
4.9. Plano de <i>backup</i> global	40
4.9.1. Desafios	42
4.9.2. Metodologia de <i>backup</i> diária recomendada	43
4.9.3. Tipos de <i>backup</i>	43
4.9.4. Período de retenção	44
4.9.5. Rotação das <i>mídias</i>	44
4.9.6. Dispositivos de <i>backup</i>	46
4.10. Soluções tecnológicas para DRP	47

4.10.1. Análise de soluções	47
4.10.2. Solução proposta	49
4.11. Procedimento para recuperação dos sistemas definidos como críticos	53
4.11.1. Exclusões	53
4.11.2. Pressupostos	54
4.11.3. Abordagem do processo de recuperação	54
4.12. Sequência lógica de eventos.....	55
4.12.1. Activação do plano	55
4.12.2. Estratégia de recuperação	56
4.12.3. De volta à normalidade.....	59
4.13. Testar o plano de <i>disaster recovery</i>	60
4.14. Programa de manutenção do plano	63
4.15. Gestão da Mudança	63
5. Conclusões e trabalho futuro.....	65
Bibliografia.....	67
Anexos.....	71

Índice de tabelas

Tabela 1 - Diferenças entre conceitos.....	10
Tabela 2 - Tipos de falha e as suas causas.....	13
Tabela 3 - Demonstração de custos (valores fictícios)	14

Índice de figuras

Figura 1- Alta disponibilidade	11
Figura 2 - Opções para recuperação de Sistemas	15
Figura 3 - Mapa de localização	20
Figura 4 - Organigrama	21
Figura 5 - Matriz de negócio	23
Figura 6 – Framework ITIL.....	37
Figura 7 - Gráfico de análise de custos.....	56
Figura 8 - Ciclo de vida de um plano de disaster recovery	66
Figura 9 - Inserção de datas	71

Siglas utilizadas

Sigla	Expansão
AIT	Advanced Intelligent Tape
BIA	Business Impact Analysis
BSA	Business Software Alliance
CCTA	Central Computer and Telecommunications Agency
CCTV	Closed-circuit television
CFH	Custo dos funcionários por hora
CPD	Centro de Processamento de Dados
CPU	Computer Processor Unit
DLT	Digital Line Tape
DRP	Disaster Recovery Plan
DVD	Digital Video Disc
DVD+R	DVD recordable
DVD+RW	DVD-ReWritable
DVD-R	DVD recordable
DVD-RAM	DVD–Random Access Memory
DVD-RW	DVD-ReWritable
ECC	Error-correcting code
FTP	File Transfer Protocol
GNU	General Public License
HD	Hard drive
IDC	International Data Corporation
IFRS	International Financial Reporting Standards
IRS	Imposto sobre o Rendimento das Pessoas Singulares
IT	Information technology
ITIL	Information Technology Infrastructure Library
LTO	Linear Tape-Open
OGC	Office for Government Commerce
OLA	Operational Level Agreement
RAID	Redundant Array of Independent Drives
RMH	Rendimento Médio por Hora
RPO	Recovery point objective
RTO	Recovery Time Objective
SI	Sistemas de Informação
SID	System Identification
SLA	Service Level Agreement
SOX	Sarbanes Oxley
TI	Tecnologias de Informação
UPS	Uninterruptible Power Supply
XHTML	eXtensible Hypertext Markup Language

Resumo

Após o atentado às torres gémeas em Nova York, tem-se notado um aumento do investimento das empresas em planos de recuperação de desastres, é notório que grande parte das empresas ainda não os possui, e se os possui, não os testa de forma eficaz. Na prática estas empresas continuam em risco caso haja um desastre, de não poderem continuar o seu negócio, por não terem forma de recuperar os dados vitais para a sua continuidade.

O objectivo é fornecer um conjunto de boas práticas para ajudar a efectuar um plano de recuperação em caso de desastre, integrado com o plano de continuidade de negócio. Pretende-se que com um conjunto de boas práticas e aconselhamentos, apoiados num conjunto de *templates* e seguindo as indicações constantes no documento, seja possível garantir que uma empresa recupere eficazmente e no mais curto espaço de tempo possível, de um desastre de causa natural, de forma a não perder oportunidades de negócio, e em alguns casos até, evitar a falência.

Este trabalho explica qual necessidade de se ter um plano de recuperação bem estruturado, com normas e políticas específicas e de que deverão ser introduzidas no conjunto das suas políticas empresariais. Fornece também todas as instruções e *templates* necessários à recolha de informação necessária para a correcta elaboração de um plano de recuperação de desastre de causas naturais, para de uma forma simples se conseguir implementá-lo.

Abstract

After the twin towers attack, in New York, it has been noticed an increase in business investment in disaster recovery plans, but it is evident that most companies still don't have one, and if they do have, they don't test them effectively. In practice these companies remain at risk in the event of a disaster, and therefore cannot continue their business, for not being able to have a way to recover their vital data for its continuity.

This work aims to provide a set of good practices to help making a plan for a disaster recovery, integrated with the business continuity plan. It is intended that with a set of good practice and advices, supported by a set of templates and following the guidelines contained in the document, so that it can ensure that a company recovers effectively and as soon as possible, from a natural disaster, and be able not to lose business opportunities, and in some cases even to avoid bankruptcy.

This paper explains why it is essential to have a well-structured recovery plan, with specific standards and policies and that should be introduced in its business policies. Also provides all necessary instructions and templates for the collection of information needed for the proper preparation of a disaster recovery plan of natural causes, in order to implement it easily.

1. Introdução

Este trabalho tem como objectivo a criação de um documento que ajude na criação de um plano e respectiva documentação associada, onde se pretende que este se torne numa ferramenta de suporte à gestão garantindo a uma organização estar preparada para uma imediata recuperação de sistemas e aplicações de suporte às suas actividades críticas, isto na eventualidade de ocorrer um desastre natural.

Entende-se por desastre, um evento catastrófico resultante de causas naturais ou provocado pelo homem, que afecta seriamente ou impede por completo a normal continuidade das operações. Em caso de desastre durante o horário normal de funcionamento, o funcionário, elemento da segurança ou outro qualquer elemento que detecte o evento deverá informar imediatamente o Responsável de Segurança da companhia.

São inúmeros os exemplos de empresas Norte Americanas que quer pela positiva quer pela negativa, sofreram e recuperaram de desastres catastróficos. Os EUA já sofreram múltiplas situações do género, e disso é exemplo o desastre de Nova Orleães ou a queda das Torres Gémeas do World Trade Center, em que as empresas que tinham planos eficazes de continuidade de negócio recuperaram e reiniciaram a sua actividade pouco tempo depois.

Um exemplo de sucesso foi a Cantor Fitzgerald (que era a maior empresa de transacção de obrigações no Mundo), foi quase que imediatamente capaz de mudar suas funções para seus escritórios de Connecticut e Londres, fruto do seu plano de continuidade do negócio¹.

Maus exemplos como o Barclays Bank que não soube adequar o seu *site de disaster recovery* ao número de funcionários a receber em caso de desastre, resultou na

¹ De acordo com additional cases do livro Essentials of Management Information System em Pearson Education . (s.d.). *The World Trade Center Disaster: Who Was Prepared?* Obtido em 14 de Julho de 2010, de http://wps.prenhall.com/bp_laudon_essmis_6/21/5556/1422339.cw/content/index.

incapacidade de receber e deslocar os 1200 funcionários para as suas instalações de New Jersey, que tinha preparado para o efeito¹.

2. Enquadramento teórico

Como forma de enquadramento conceptual ao tema da recuperação após um desastre, convém definir o que significa "*Desastre*" em matéria de TI (Tecnologias de Informação), pois perder um único documento Word não é evidentemente uma catástrofe. Perder a base de dados com todos os clientes, incluindo os registo de contas a receber, provavelmente não é uma catástrofe se seus *backups* são razoavelmente actuais e o hardware está intacto. Um grande incêndio ou terramoto que destrói o *hardware* do sistema e todos os dados no seu sistema claramente podemos considerar como sendo um enorme desastre. É necessário portanto determinar caso a caso o que constitui para uma empresa um desastre e as medidas que deverão ser tomadas quando este for declarado.

O valor que uma empresa irá perder por hora num *downtime* é extremamente difícil de avaliar e quantificar. Claramente que se irão perder bastantes lucros, contudo este problema vai muito além de apenas capital. Está também em jogo a imagem da empresa, a sua reputação, perda de produtividade, novos negócios, cota de mercado e em que medida estão dispostos a esperar os seus clientes enquanto o seu sistema está em baixo.

Uma pesquisa recente do Gartner Dataquest² sobre tempo de inactividade de uma aplicação mostra que em média 40 % do tempo de inactividade é causada por falhas do próprio *software* (por exemplo, problemas de desempenho ou "bugs"), 40 % por erros do utilizador e aproximadamente 20% pelo sistema ou por falhas ambientais. A maioria das falhas (cerca de 60 %) de "sistema ou ambientais" são causadas por problemas de *hardware*. Em geral, menos de 5% do tempo de inactividade das aplicações são imputáveis a catástrofes (Wheatman, 2001), mas além de raras, quando as catástrofes

¹ De acordo com additional cases do livro Essentials of Management Information System em Pearson Education . (s.d.). *The World Trade Center Disaster: Who Was Prepared?* Obtido em 14 de Julho de 2010, de http://wps.prenhall.com/bp_laudon_essmis_6/21/5556/1422339.cw/content/index.

²Gartner, Inc. (2009). *The Aftermath: Disaster Recovery and Planning for the Future*. Obtido em 3 de Maio de 2010, de Web site da Gartner: http://www.gartner.com/5_about/news/disaster_recovery.html

acontecem, os danos provocados normalmente são muito elevados, o que dificulta bastante a recuperação dos sistemas, e o retomar das actividades normais da empresa, é exemplo dessa situação, o atentado às torres gémeas, onde todo o *hardware* ficou inutilizado.

É necessário determinar a janela de recuperação, dito de outra forma, é forçoso determinar quanto tempo uma empresa sobrevive sem os seus dados e sem o seu sistema central. Se a resposta é apenas umas horas e todo o *hardware* for destruído, é necessário ter um sistema alternativo enquanto adquire novo hardware. Se o caso for a perda do *site*, então nesse caso é necessário ter um *site* alternativo.

Disaster Recovery não é continuidade do negócio

2.1. Continuidade do negócio

A gestão da continuidade do negócio é um processo de gestão holística que identifica potenciais impactos que ameaçam uma organização e fornece uma estrutura para a construção de resiliência e a capacidade de uma resposta eficaz, que protege os interesses dos seus principais interessados, a reputação, a marca e a criação de actividades de valor.¹

Existe alguma confusão conceptual em torno do tema: a semântica da língua portuguesa leva-nos a confundir contingência, recuperação de desastres e continuidade de negócios.

Embora semelhantes, cada conceito traduz uma ideia distinta:

Tabela 1 - Diferenças entre conceitos

Planos	Descrição	Foco
Continuidade de Negócios	O Plano de Continuidade de Negócios tem o foco na manutenção das funções críticas do negócio de uma organização durante e após a ocorrência de um sinistro. Geralmente contém o plano de recuperação de desastres e o plano de contingência TI	Processos de negócio: questões relacionadas aos activos de TI somente abordadas no que se relaciona a sua importância para os processos críticos de negócio
Recuperação de Desastres	Fornece procedimentos detalhados para a recuperação das facilidades de TI em <i>sites</i> alternativos em caso de desastres	Activos de TI e sinistros com efeitos de longo prazo
Contingência	Fornece procedimentos e capacidades necessárias para a recuperação de uma aplicação específica ou sistemas complexos	Interrupções nos sistemas de TI com efeitos de curto prazo

Uma empresa sem um plano de continuidade = empresa em risco

43% das empresas que passaram por uma catástrofe nunca reabrem, e 29% acabam por fechar ao fim de dois anos ²

¹ PAS56.Com. (2006). *A Business Continuity Management and Risk Management Guide*. Obtido em 20 de Abril de 2010, de Web site de PAS56.Com: <http://www.pas56.com/>

² De acordo com a empresa de contabilidade McGladrey & Pullen, citada em Micro Solutions. (s.d.). *More Data Recovery Informations*. Obtido em 2 de Abril de 2010, de Web site de Micro Solutions, Data Recovery Lab : <http://www.micro-solution.net/micro5.html>

Continuidade de negócios é reduzir o tempo de inactividade:

- Tempo de inactividade previsto planeado
- Tempo de inactividade não previsto

Dois elementos-chave da continuidade do negócio:

- Alta disponibilidade (figura 1)¹
- Recuperação de desastres

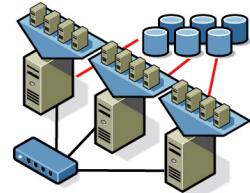


Figura 1- Alta disponibilidade

2.2. Desafios na implementação de formas de continuidade do negócio

Para algumas empresas pode ser muito caro desenvolver um plano de continuidade do negócio, pois para além do plano devem ser disponibilizados recursos para a contratação de pessoal qualificado, locais alternativos de processamento, equipamentos redundantes e formação específica aos colaboradores. No entanto todos estes investimentos são largamente compensados por permitirem a uma empresa a continuidade dos seus negócios no caso de um desastre. Colocam-se portanto alguns desafios às empresas.

Custos

- *Hardware* adicional
- Ferramentas adicionais
- Formação
- Locais alternativos de processamento

¹ Sistemas de alta disponibilidade oferecem resistência à falhas de software, hardware e energia, cujo objectivo é disponibilizá-los o máximo de tempo possível. Estes sistemas referem-se a soluções redundantes de equipamentos e serviços, a fim de manter o funcionamento contínuo destes sistemas. Pode-se dizer que se trata de um sistema alternativo de segurança, o qual, em momentos de falha do sistema principal, assume o funcionamento no menor tempo possível, mantendo a disponibilidade dos dados. – Adaptado de Alta Disponibilidade - Sua empresa disponível 24 horas todos os dias (Misturini, 2005).

Complexidade

- Gestão e provisionamento
- Novos aplicativos específicos para as necessidades de continuidade do negócio

Confiabilidade

- Incerteza sobre a possibilidade de atender aos objectivos de disponibilidade e recuperação
- Dificuldade em efectuar testes de soluções complexas

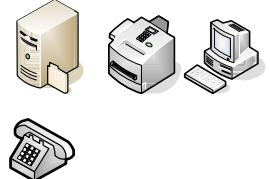
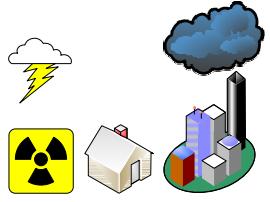
2.3. Recuperação de desastres

“Perda total de um ambiente de computação que serve de apoio ao negócio. Recuperação do ambiente computacional de um erro ou falha no *site* principal. Subconjunto de continuidade de negócios.”¹

O que pode dar origem a um desastre?

Um desastre pode derivar de várias causas, conforme explicado na tabela 2.

Tabela 2 - Tipos de falha e as suas causas

Falhas Lógicas		Bugs de <i>software</i> ; <i>Windows Update</i> ; Destrução de informação; Corrupção de dados;	DOS Attack; Erros de utilizador; Vírus; Spyware; Malware;
Falhas de componentes		Falha do CPU; Falha dos discos; Falha do RAID (Redundant Array of Independent Drives); Falha de energia;	Falha da <i>Motherboard</i> ; Falha das placas de rede; Falha do Sistema operativo;
Falha do Site		Tornados (Furacões); Cheias; <i>Tsunami</i> ; Tempestades eléctricas; Sabotagem; Atentado à bomba;	Fogo; Falhas de energia; Terrorismo/Guerra; Epidemias; <i>Cyber Attack</i> ;

¹ Texto adaptado de Challenges Faced by Services Oriented Industries (LAKHANI, 2009)

Quanto custa por hora um *downtime*?

Não é possível responder a esta pergunta, pois este custo depende de muitas variáveis, como por exemplo o custo de cada hora de mão-de-obra, o que como é sabido, varia de empresa para empresa, a tabela 3¹ pretende ilustrar como calcular alguns destes custos, para tal é necessário ter em consideração o seguinte:

- Custo dos funcionários por hora × a fracção dos funcionários afectados pela falha (CFH)
- Rendimento médio por hora × fracção do rendimento afectado pela paralisação (RMH)
- $Downtime = CFH + RMH$

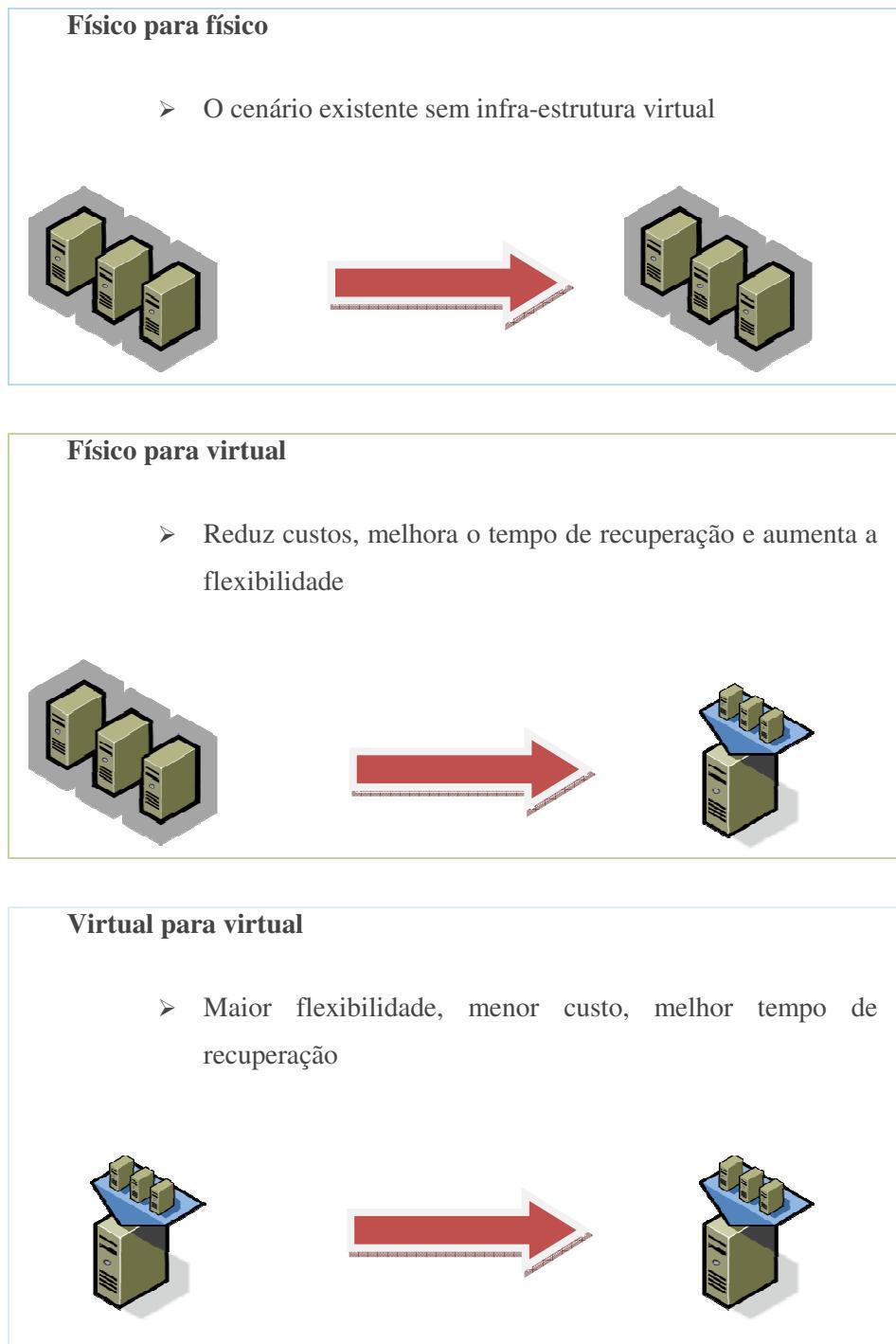
Tabela 3 - Demonstração de custos (valores fictícios)

Calculo	
Salário por hora	10 €
Seg. Social e IRS (+/-30%)	3 €
Custo por empregado por Hora	13 €
Vendas brutas anuais	2.000.000,00 €
40 horas/semana × 52 semanas	2080
Rendimento médio por hora	961,54 €
6 empregados a 13 €	78 €
100% de <i>downtime</i>	961,54 €
8 horas de <i>downtime</i>	8.316,32 €
Não inclui os seguintes custos:	
Satisfação do cliente	Quota de mercado
Responsabilidade	Reputação
Perda de produtividade	Perda de oportunidade

¹ Os dados utilizados para o cálculo são fictícios, não reflectindo qualquer média ou indicador de referência, são meramente ilustrativos.

Opções para recuperação de desastres:

Existem três tipos possíveis de recuperação de desastres, utilizando tecnologias diferentes, apresentando custos e vantagens diferentes, conforme ilustrado na figura 2.



Factos:¹

- 36% das empresas reportam não possuir um plano de recuperação em caso de um desastre;
- 6% de todos os computadores sofrerão um episódio de perda de dados numa determinada altura;
- 93% das empresas que perderam seus dados e que foram incapazes de recuperar em mais de 10 dias, foram à falência no prazo de um ano após o desastre;
- O erro humano representa 11% de toda a perda de dados;
- Quase três em cinco utilizadores já perderam um arquivo electrónico que achavam que estar armazenado correctamente;
- 30% de todas as empresas que sofrem um grande incêndio abrem falência ao fim de um ano devido à perda de dados;
- Os vírus informáticos representam 8% de toda a perda de dados;
- As empresas que não são capazes de retomar as operações até 10 dias após um desastre onde perderam os seus dados, não são susceptíveis de sobreviver;
- Duas das três empresas que possuem um plano de *backup* e recuperação de desastres sentem que seu plano tem vulnerabilidades significativas;
- 43% das empresas possuem quantidades significativas de dados críticos para o negócio armazenados em computadores individuais sem qualquer tipo de backup;
- *Software* corrompido representa cerca de 6% de toda a perda de dados;
- 100% das *hard drives* irão um dia falhar.

3. Método

Este trabalho foi elaborado recorrendo a pesquisas na internet de informação pertinente referente ao tema em estudo. Foram também consultados para o efeito, livros sobre as matérias em questão, alguns do espólio literário dos autores, outros da biblioteca desta Instituição.

¹ Adaptado de National Archives & Records Administration, Washington, D.C. citado em New Horizon I.T. Consulting, Inc. (2010). *Disaster Recovery*. Obtido em 35 de Maio de 2010, de New Horizon I.T. Consulting: <http://newhorizonitconsulting.com/disaster.htm>

Após efectuado o levantamento da informação atrás referida, a mesma foi analisada exaustivamente, com vista ao levantamento dos pontos críticos, bem como das falhas e necessidades das empresas, em matéria de recuperação de dados em caso de desastre, com vista a obtenção de soluções que possam ajudar as empresas a elaborar e manter um plano de recuperação de dados.

Foi factor decisivo para a elaboração deste trabalho, não só alguma experiência profissional dos elementos do grupo, mas sobretudo todos os conhecimentos adquiridos ao longo dos três anos desta Licenciatura em Informática de Gestão.

Como este trabalho se caracteriza por ser teórico¹ e abrangente, foram criados templates de forma a conseguir fazer o levantamento da informação necessária à elaboração de um plano de recuperação de dados em caso de desastre natural, e posterior implementação para a recuperação de dados.

4. Plano DRP (Disaster Recovery Plan)

4.1. Objectivos do plano DRP

O objectivo principal deste plano é desenvolver um conjunto de documentação onde se incluem regras, normas e procedimentos de forma a permitir que uma organização desenvolva um plano que a permita sobreviver a um desastre e que possa restabelecer as operações do seu negócio de uma forma célere e organizada.

Um plano deverá ser elaborado de forma a dar indicações de como minimizar os impactos em termos de recursos humanos, impactos operacionais e financeiros inerentes a uma situação de desastre e como recuperar os sistemas que suportam uma empresa.

Sendo que o objectivo será a recuperação de sistemas e a minimização de toda e complexidade em torno da mesma, são apenas dadas indicações de carácter geral para todos os processos complementares e acessórios a esta acção, este descreve as acções

¹ Nota dos autores: por dificuldade de comunicação com o elemento da Clínica São João de Deus indicado para nos prestar a informação necessária à elaboração de um trabalho com um teor mais prático, e, após recomendação do Orientador do trabalho procedemos apenas à elaboração de um plano teórico, passível de ser adaptado a várias empresas.

que deverão ser postas em prática, os recursos necessários e os procedimentos que deverão ser seguidos antes, durante e depois do desastre.

Para atender a esse propósito deve-se eleger uma metodologia que enfatize os seguintes pontos chaves:

- Como fornecer à gestão uma compreensão detalhada do esforço total requerido para tornar e manter eficaz, uma matriz de recuperação;
- Como obter o compromisso da gestão apropriado para suportar e participar no esforço de recuperação;
- Definição das exigências de recuperação na perspectiva do negócio;
- Documentar o impacto de uma perda prolongada às operações e ao negócio;
- Seleccionar as equipas do DRP para testes, actualizar e assegurar uma execução eficaz do plano;
- Definir como as premissas do DRP devem ser integradas aos processos de negócio para uma recuperação no tempo necessário para não haver ruptura nos processos de negócios;
- Estabelecimento antecipado de meios alternativos de operação.
- Definição de linhas orientadoras para garantir a segurança dos colaboradores;
- Como garantir uma resposta rápida e eficaz ao imprevisto através de uma estrutura de acções, procedimentos e protocolos capazes de gerir uma situação de desastre;
- Formas de recolha de informação crítica;
- Meios de mitigar o risco;
- Criação de *templates* para fácil recolha de informação;
- Ilustrações de como executar e estruturar passo-a-passo um correcto plano;
- Conjunto de melhores práticas;
- Noções de segurança em TI;
- Noções de *Governance*;

Para se atingir um planeamento eficaz é necessário que os elementos mais seniores da área de sistemas de informação e das áreas de negócios estejam envolvidos durante todo o projecto para o benefício da organização.

4.2. Requisitos

O desenvolvimento de um DRP envolve a criação de uma "matriz de recuperação total"¹ para restaurar os recursos computacionais com as funções vitais do sistema de informação para atender as necessidades do negócio da empresa. O plano deve procurar restabelecer todo o sistema de informação no menor tempo possível a fim de evitar um efeito catastrófico no negócio da empresa. O desenvolvimento de uma estratégia viável de recuperação não deve ser uma iniciativa exclusiva da área de sistemas de informação, mas de toda a organização de forma a proteger todos os interesses da empresa.

A fim de sobreviver, as empresas devem assegurar que as operações críticas possam recomeçar o processamento normal dentro de um espaço de tempo razoável. Para atingir esses objectivos o DRP deve atender os seguintes requisitos:

- Providenciar um ambiente seguro e pessoas preparadas para um desastre;
- Reduzir as perdas financeiras em casos de desastres;
- Identificar linhas de negócios críticas que requeiram suporte em situações de desastres;
- Identificar as fraquezas e executar um programa da prevenção de desastre;
- Minimizar a duração de uma paralisação das operações de negócio;
- Desenvolver uma "matriz de recuperação" que seja compreensível, fácil de usar e manter;
- Facilitar a coordenação eficaz de tarefas da recuperação;
- Reduzir a complexidade do esforço de recuperação;
- Minimizar interrupções nas operações normais;
- Limitar a extensão da interferência e dos danos;
- Minimizar o impacto económico da interrupção;
- Formar técnicos nos procedimentos de emergência; e,
- Proporcionar uma reposição simples e rápida do serviço.

¹ Esta Matriz de Recuperação Total resulta da compilação de informação vinda dos Sistemas Críticos e da Matriz de Recuperação de Software de uma empresa, os quais resultaram de informação proveniente do BIA.

4.3. *Overview do negócio*

Como os elementos que irão proceder à recuperação das operações, podem não conhecer correctamente a empresa (numa situação de catástrofe os elementos mais experientes poderão não estar disponíveis), ou por serem elementos com carácter meramente técnico ou por nem sequer pertencerem à empresa, será sempre desejável que lhes seja efectuado um prévio e correcto enquadramento da empresa cujos sistemas vão recuperar.

Deverá portanto o plano de DRP ter um capítulo onde será descrito o âmbito, missão e principal actividade da empresa, bem como o seu volume de negócios, áreas de actuação e constituição da empresa de forma a se ter a correcta dimensão da mesma e respectivo enquadramento do seu negócio.

Este tipo de informação reveste-se de particular importância, pois de acordo com a sua actividade, determinados sistemas ganham importância sobre outros.

Localização da empresa

É necessário detalhar com exactidão, a localização da empresa, através da sua morada, bem como um mapa de localização (figura 3) e diversas vias e formas de acesso à mesma, para que não possam existir dúvidas quanto à sua localização.

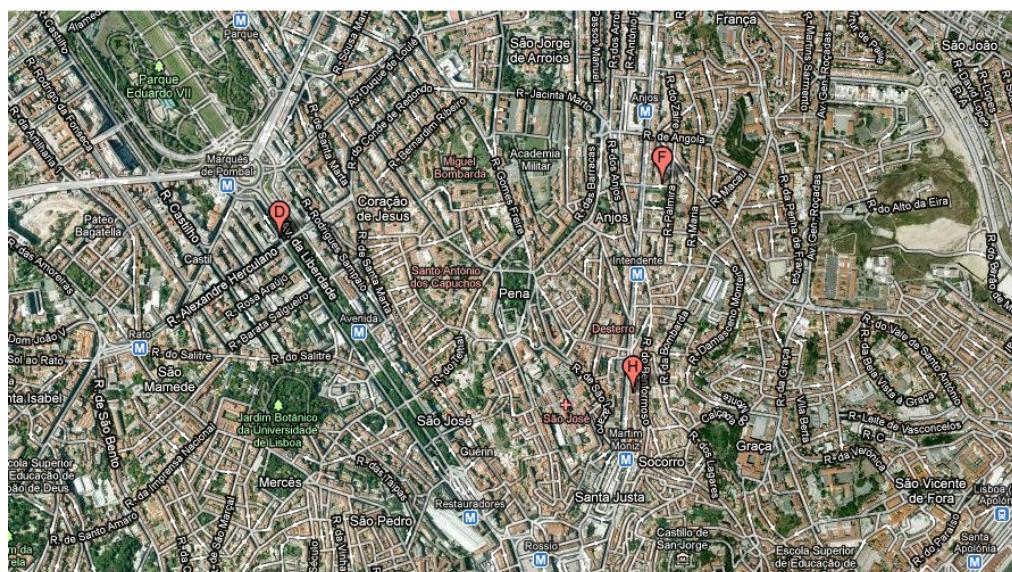


Figura 3 - Mapa de localização

Sucursais ou dependências

No caso de existirem sucursais ou dependências deve constar neste capítulo as referências às mesmas, a localização de cada uma acompanhada da morada, respectivo mapa de localização e principais vias de comunicação.

As várias dependências deverão ter o seu próprio plano de contingência que deverá ser englobado no plano de continuidade da empresa. Caso tenham um *Data Center* ou centro de processamento de dados, o seu plano de DRP deve ser feito em articulação com a sede, de forma a existir uma uniformidade de normas, critérios e uniformização de processos.

Organograma

Com o intuito de se saber quem faz o quê, e a quem em caso de necessidade, reportar as informações pertinentes, ou esclarecer dúvidas, é necessária a elaboração de um organograma da empresa (figura 4)¹.

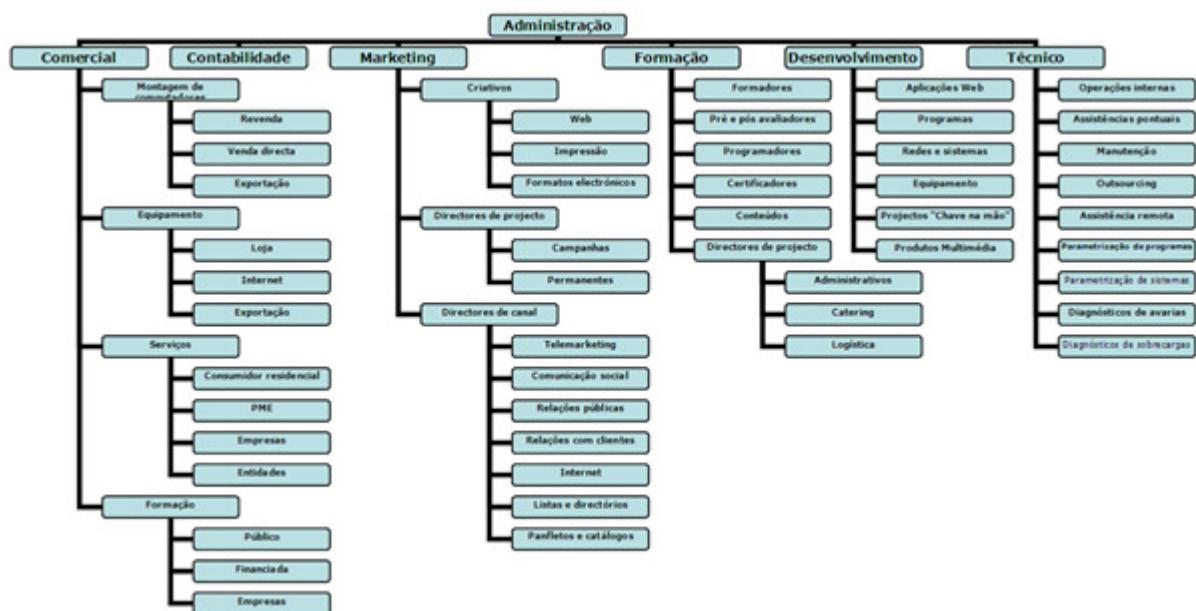


Figura 4 - Organograma

¹ Representação meramente ilustrativa

Missão

Entende-se como a missão de uma organização, a explicação do que esta se propõe fazer, e a quem vai servir com a sua actividade, ou seja, pretende dar uma visão de qual é o propósito da sua existência.

Ao explicar qual a sua missão, as organizações devem conseguir explicar qual a finalidade de estarem no mercado.

A definição da missão ajuda a orientar as organizações na gestão do seu plano estratégico de forma a canalizar os seus esforços para o que as organizações forem melhores. Este conceito serve de linha orientadora das organizações.

Para desenvolver a missão da companhia existem várias actividades que interagem entre si, sendo que algumas delas têm uma interacção directa com o cliente e distribuidores - Actividades Primárias. Contudo, o seu desempenho está dependente de vários outros processos - Actividades de suporte.

Será portanto necessária uma clara definição destas componentes (Actividades Primárias e Actividades de Suporte).

Actividades Primárias

No seguimento de um desastre interessa recuperar de imediato as actividades primárias bem como as actividades de suporte essenciais para esse objectivo.

A interacção entre todas estas actividades, clientes, distribuidores e outras entidades externas relevantes é efectuada através de processos organizacionais que geram entre si fluxos de informação.

Deverá ser criada uma matriz de negócio (ilustrada na figura 5) apresentando um resumo destes fluxos.

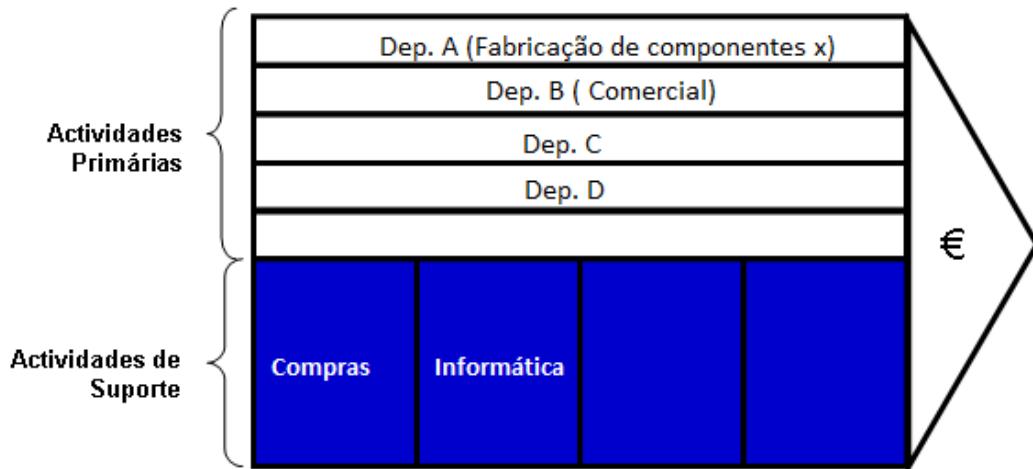


Figura 5 - Matriz de negócio

4.4. Âmbito

Este plano estabelece as estratégias, procedimentos e acções para responder e gerir uma situação de desastre natural, ajudando a definir todos os processos críticos dos sistemas designados como fundamentais para o negócio da empresa e todos os elementos necessários para garantir a sua recuperação (formulários, equipamentos, aplicações, bases de dados, sistemas, entre outros).

No âmbito do presente plano serão dadas indicações de como recuperar os locais, os processos organizacionais e os sistemas / aplicações.

4.5. Gestão do risco

A Gestão do Risco é um processo global de identificação, análise e avaliação do risco.

Para que a Gestão do Risco seja eficiente e eficaz, é essencial o patrocínio e suporte da gestão de topo da empresa. A mais-valia desta parceria é tornar mais fácil para a gestão de topo entender de Gestão de Riscos de segurança da informação relacionados com outras áreas de negócio.

Para se efectuar uma análise efectiva e que produza resultados eficazes, é necessário que a empresa tenha a noção de todos os activos existentes na empresa relacionados com TI para a sua correcta gestão e administração. Este processo vai desde a gestão dos activos de *software*, do controlo dos custos de TI, até à correcta noção do ambiente tecnológico

para que num caso de desastre se possa recuperar a situação original, minimizando o risco.

4.5.1. Minimização do risco

A gestão inexistente ou ineficiente dos seus recursos de *software* expõe as organizações a três tipos de riscos:

- **Riscos técnicos:** *software* que não está devidamente licenciado não beneficia de apoio técnico eficaz. Isso faz com que uma interrupção no serviço altere a qualidade do mesmo. O não controlo das instalações de *software* aumenta o risco de violação da segurança: a infecção por vírus, invasões, entre outros problemas.
- **Riscos jurídicos:** de acordo com a BSA (*Business Software Alliance*), a taxa média de pirataria de *software* foi de 35% na Europa em 2005 (França: 47%, Reino Unido: 27%, Espanha 46%, Itália: 53%, Portugal: 43%)¹. Isto representa uma quebra de receitas de cerca de 12 biliões de dólares para a indústria de *software* que, para proteger os seus interesses, investe recursos consideráveis em educação e repressão. Refira-se que a legislação europeia sobre a protecção de direitos de autor prevê a imposição de sanções severas aos infractores (multas, penas de prisão, etc.) e os elementos da gestão das TI estão, muitas vezes na linha da frente.
- **Conformidade com regras legais e financeiras:** SOX (*Sarbanes Oxley*)² e as IFRS (*International Financial Reporting Standards*) são apenas algumas das muitas normas jurídicas e de contabilidade que exigem registos de despesas para ser detectáveis e necessitam de uma gestão cuidadosa dos recursos, especialmente de *software*, que é mais difícil de apreender por causa da sua natureza imaterial. O não cumprimento destas normas pode causar custos financeiros e de imagem para uma organização.

¹ De acordo com o Terceiro Estudo Anual Global Sobre Pirataria de Software (Business Continuity Institute, 2010)

² Lei americana adoptada em 2002 para fortalecer o governo e restaurar a confiança dos investidores, no seguimento de um conjunto de escândalos financeiros, conforme A *Guide To The Sarbanes-Oxley Act* (Sarbanes-Oxley, 2002).

4.5.2. Controlo dos custos de TI

Para além do controlo dos riscos decorridos da inobservância de uma correcta gestão, é possível reduzir significativamente os custos directos e indirectos associados ao *software*:

- **Redução da aquisição de *software* em excesso:** Uma boa gestão do licenciamento existente permite reduzir custos, pois sai muito caro às organizações não gerirem devidamente o seu *software*, como por exemplo a compra de licenças em excesso (mais do que o número de estações de trabalho), a aquisição de versões de *software* completo quando bastaria efectuar uma actualização à licença inicial, a manutenção de software que não está em uso, a não utilização de licenças por parte de alguns utilizadores e por vezes é efectuado um deficiente planeamento de necessidades.
- **Melhor negociação com os fornecedores:** Um melhor conhecimento do *software* de uma organização permite-lhe negociar melhor com os fornecedores reduzindo o investimento e os orçamentos. Uma política eficaz permite à organização planear e agrupar as suas compras, fazer uma melhor utilização das opções de *upgrade* à sua disposição graças ao controlo sobre os contratos de licenciamento, permite também saber quando pode cancelar contratos de manutenção que já não estão em uso, entre outros aspectos.
- **Redução dos custos de suporte:** uma gestão de *software* apropriada também permite que as organizações conduzam os seus esforços para uma correcta e orientada formação dos seus funcionários, prestando desta forma o correcto apoio às necessidades reais dos utilizadores; como forma de antecipar incidentes através da distribuição de documentos de informação (como dicas ou bases de conhecimento), para personalizar o *software* de acordo com o tipo de utilizador ou com o tido de departamento, para adequar a sua implantação, etc. Ao reduzir as prováveis causas de incidentes, é possível reduzir significativamente os custos de apoio sem comprometer a qualidade do serviço.

As organizações para serem competitivas, inovadoras e empreendedoras, nos dias de hoje, têm forçosamente que utilizar meios informáticos, fazendo parte desses recursos o *hardware* e o *software*. As vantagens competitivas geradas com estes meios são mais associadas ao aumento de produtividade, velocidade e agilidade. Desta forma, a gestão

dos seus activos (devidamente equipados com um software adequado) permite às organizações:

- Aumento da produtividade dos utilizadores, pois reduz-se o tempo de indisponibilidade da sua infra-estrutura de TI, sendo isto conseguido com formação específica dos seus técnicos de TI;
- Antecipação de incidentes;
- Melhoria de segurança de TI;
- Uma melhor gestão de *backups*;
- Implantação de um novo *software* ou *upgrades* de forma mais eficiente através do correcto conhecimento das configurações instaladas;
- Absorção rápida das mudanças organizacionais, tais como: reorganizações, fusões ou aquisições;
- Minimização do *downtime* em caso de um desastre, seja ele natural (provocado terramoto, tsunami, incêndio, entre outras situações) ou de causas tecnológicas.

Melhores práticas recomendadas:

1. Estabelecimento de uma política para a organização de *software*, licenciamento e *hardware*;
2. Criação de uma organização específica;
3. Aplicação dos procedimentos pré-estabelecidos para gerir as licenças e o seu ciclo de vida na empresa;
4. Comunicar aos responsáveis.

4.5.3. Risk IT

A *framework* Risk IT baseia-se num conjunto de processos de negócio, de forma a disponibilizar orientações à gestão. Complementa as *frameworks* Cobit e Val IT (Value Governance of IT Investments) e aborda questões relacionadas com gestão de risco de Tecnologias de Informação.

A Risk IT deve ser adaptada a cada empresa e ao seu tipo de negócio, a sua implementação começa com a identificação e categorização dos riscos, esta *framework* contempla entre outros controlos e métricas, a construção de matrizes com os fluxos de

comunicação do risco e guias de técnicas de como os riscos se relacionam com os domínios e processos.

A *framework* Risk IT rege-se pelos seguintes princípios (Gonçalves, 2009):

Gestão empresarial eficaz dos riscos de TI

- Sempre ligado aos objectivos do negócio;
- Alinha a gestão de TI (riscos de negócio relacionados com a gestão do risco global da empresa);
- Equilibra os custos e benefícios da gestão de riscos.

Gestão eficaz dos riscos de TI

- Promove a comunicação aberta dos riscos de TI;
- Estabelece a forma correcta de como a gestão de topo pode efectuar a sua gestão, enquanto define e aplica critérios de responsabilidade pessoal para operar dentro de níveis de tolerância aceitáveis e bem definidos;
- O processo é contínuo e parte de actividades diárias.

A Risk IT inclui três áreas de conhecimento, o Risk Governance, o Risk Evaluation e o Risk Response.

Compete ao **Risk Governance** criar e manter uma visão dos riscos, integrar-se com a gestão dos riscos corporativos e consciencializar os decisores para os riscos nas decisões de negócio.

O **Risk Evaluation** tem por finalidade, a recolha de dados, a análise de riscos e a manutenção de um perfil dos riscos.

Finalmente, cabe ao **Risk Response** a articulação e gestão dos riscos, e a reacção aos vários eventos.

O Risk IT integra-se totalmente com o CobiT e com o Val IT. A forma desta *framework* apresentar os seus resultados, é em tudo idêntica ao CobiT, pois também apresenta para

cada processo, metas vinculadas aos indicadores de negócio, processos e actividades, entre outras.

A relação entre o Risk IT e o Cobit funciona da seguinte forma: todos os eventos e actividades de TI são controlados pelo Cobit este avalia-os quanto aos riscos e oportunidades, e gera informação para a gestão de risco, ou seja para o Risk IT.

Perante o exposto é necessário, de uma forma automatizada ou manual ter inventários com o seguinte:

Servidores em produção

Esta listagem (Anexo 1 – Inventário de servidores) permite ter uma visão geral de todos os servidores em produção, respectiva importância para o negócio e seleccionar quais os servidores a colocar como prioritários na matriz de recuperação global.

Computadores pessoais

Com a listagem dos computadores pessoais (Anexo 2 - Inventário de computadores) pode-se obter uma visão geral de todos os postos de trabalho existentes, quais as suas características e funções. Oferece-nos também uma visão, por departamento, de quais os computadores que é necessário recuperar.

Equipamentos de comunicações

Relação dos equipamentos existentes que suportam a função de comunicações de uma empresa (Anexo 3 - Inventário de *hardware* de comunicações)

Equipamentos de telecomunicações

O inventário dos equipamentos existentes que suportam a função de telecomunicações de uma empresa pode ser inserido no *template* “Inventário de *hardware* de telecomunicações” (Anexo 4).

Nº de licenças activas

Pretende-se que sejam listadas todas as licenças existentes (Anexo 5 - Inventário de licenças), permitindo assim controlar os contratos existentes, bem como as respectivas quantidades.

4.5.4. Levantamento e definição dos recursos críticos

Para que as acções de recuperação dos recursos críticos numa situação de desastre sejam efectuadas com sucesso e de modo a suportar a continuidade do negócio, é necessário que estes sejam priorizados com a correcta organização. Para isso é fundamental que seja efectuado um levantamento de todo o equipamento e sistemas em uso e que seja efectuada uma relação entre as respectivas funções e os sistemas e operações que suportam e por fim que seja estabelecida uma ordem de recuperação associada à sua importância.

Hardware

A listagem de todo o *hardware* não categorizado pelos restantes *templates*, mas que seja necessário estar registado pela sua função e processos envolvidos, pode ser inserida no *template* “Inventário de *hardware*” (Anexo 6).

Sistemas críticos

O levantamento de todos os sistemas considerados críticos devido à sua função ou processos que suportam deve ser efectuado utilizando para tal o *template* “Inventário de sistemas críticos para o negócio” (Anexo 7), no entanto é necessário ter em conta que podem existir sistemas que não têm processos ou funções associadas mas que por sua vez suportam outros que são críticos.

Aplicações existentes

Deve ser elaborada uma lista de todas as aplicações existentes para que possam ser inventariadas, categorizadas e priorizadas de acordo com as recomendações do negócio, para tal deve ser utilizado o *template* “Inventário de aplicações” (Anexo 8).

Application owners

A definição dos *application owners* de cada aplicação é necessária para que exista a responsabilização formal para o seguinte:

- Definição de requisitos de funcionalidades;
- Solicitação e aceitação de alterações;
- Autorizações de acessos;
- Definição de RTO (*Recovery Time Objective*)¹ e OLA (*Operational Level Agreement*)² de cada aplicação.

Deverá ser efectuado um levantamento de todas as aplicações existentes e respectiva atribuição a um *application owner*, utilizando para tal o template “Lista de Application Owner” (Anexo 9).

Software

A listagem de todo o *software* não categorizado pelos anteriores *templates* necessita de estar registado e categorizado de acordo com o *template* “Matriz de recuperação de *software*” (Anexo 10).

Este levantamento servirá à equipa de recuperação em caso de desastre, como forma de verificar e controlar se todos os sistemas são ou não recuperados.

¹ Um *Recovery Time Objective* é a duração do tempo e um nível de serviço dentro do qual um processo de negócios deve ser restaurado após um desastre (ou interrupção) de modo a evitar consequências inaceitáveis associadas a uma quebra na continuidade de negócios; já um RPO define o que a organização considera um nível aceitável de perda de dados. Por exemplo, se um serviço tem um SLA de 99%, com medição mensal, isso significa que o RTO é de 7 horas e 18 minutos. Se combinar isso com um RPO de, digamos, 24 horas, poderão definir-se técnicas e gestão de *backups* com precisão.

² O objectivo do OLA é apresentar uma descrição clara, concisa e mensurável de relacionamentos de suporte interno do provedor de serviços. Os OLAs descrevem, basicamente, os contratos entre diferentes grupos de TI que actuam no suporte a um SLA, inclusive os tempos de processamento e resposta para o fornecimento dos serviços. Supondo-se que temos um *site* crítico com uma meta de SLA de 99,99%, mas uma base de dados da qual ele depende para obter conteúdo, tem uma meta de disponibilidade de apenas 95%. O OLA ajuda a solucionar essas divergências e a alinhar as equipas de TI no sentido de uma meta comum.

4.6. Segurança

Efectuar uma avaliação de risco é fazer um exame cuidadoso a todas as variáveis que podem causar danos aos sistemas informáticos, prejudicando o correcto funcionamento dos sistemas e como consequência falha na continuidade do negócio da empresa a quem dão suporte.

Uma incorrecta avaliação do risco pode levar a que os sistemas fiquem expostos a riscos, podendo levar a interrupções de serviço muito prejudiciais a uma empresa. Deverão, portanto, ser elaborados planos para controlar os riscos.

As cinco medidas a seguir são:

1. Identificar os perigos.
2. Decidir o que pode ser prejudicado e como.
3. Avaliar os riscos e decidir quais as medidas a tomar.
4. Documentar as soluções e implementá-las.
5. Rever o processo de avaliação e actualiza-lo se necessário.

Não complicar o processo. Em muitas organizações, os riscos são bem conhecidos e as medidas de controlo necessárias são fáceis de aplicar. Por exemplo, provavelmente o processo de guarda das *tapes* de *backup* da empresa, é feito no mesmo edifício onde estão todos os sistemas, numa sala sem acesso restrito, sem condições ambientais propícias à guarda deste tipo de equipamento (controlo de humidade e temperatura), sem protecção contra inundações e fogo. Os sistemas de suporte a actividades críticas, tais como as comunicações estão com protecção deficiente. Por exemplo, tipicamente os bastidores de comunicações estão em armários sem segurança e em locais públicos, facilmente alguém desliga um cabo de rede, porque até necessita de um igual em sua casa e pode-se demorar horas até se descobrir onde falham as comunicações. É típico não existir documentação das ligações existentes e de quais os locais onde estão interligadas.

Outro exemplo é a sala de sistemas ou *Data Center*, não estar com acesso vedado a estranhos e com sistemas de controlo de entradas, onde por questões de segurança deverá existir um *log* de entradas com as respectivas autorizações, onde deverá constar a

descrição da actividade efectuada, hora e duração da mesma. Claro que o respectivo nível de segurança deverá ser adequado de acordo com a criticidade dos sistemas e meios envolvidos.

Associados a estes controlos estão processos de auditoria, que têm como função a consolidação de todos os processos de controlo para minimizar o risco.

Um processo de auditoria ao CPD (Centro de Processamento de Dados) ou *Data Center* é um dos passos obrigatórios no processo de auditoria TI.

Segue-se uma lista de verificação dos pontos-chave a serem usados:

Políticas & Processos

- Tem o CPD políticas e procedimentos escritos em prática?
- Estão eles suficientemente descritivos e em detalhe para orientar a sua organização e correcto funcionamento?
- Está o pessoal que frequenta o CPD suficientemente consciente dessas políticas e procedimentos?
- São eles actualizados com regularidade?

Pessoal

- São atribuídas responsabilidades em regime de rotatividade ao pessoal do CPD e aos operadores?
- Existe um log sobre o funcionamento do CPD e para o registo de quaisquer eventos significativos e as respectivas medidas tomadas pelo operador?
- O *log* de operador é inspeccionado diariamente pela gestão?

Tratamento de incidentes

- Os operadores sabem exactamente o que fazer quando diferentes tipos de emergências com fogo ocorrem?
- Existem outros elementos que saibam exactamente o que fazer quando ocorrer uma emergência de fogo?

- Existe treino para outras situações de emergência? Quais? Com que frequência?

Alarme de incêndio

- Estão as caixas de activação de alarme de incêndio e as opções de corte de energia de emergência, claramente visíveis e desobstruídas?
- Existem instruções de anti-fogo claras, adequadas e publicadas em todos os locais chave?
- Existem caixas de activação de alarme de incêndio na área dos computadores em quantidade suficiente?
- Os operadores são treinados periodicamente no combate a incêndios?
- São atribuídas responsabilidades individuais aos operadores em caso de incêndio?
- Qual a frequência com que são realizados exercícios de simulação de fogo?

Meios de extinção de incêndios¹

- Sistemas de Aspersão ou Sprinklers
- Halon
- FM200 (Agentes Halogenados)

Fornecimento de energia ao CPD

- Existe redundância no fornecimento de energia ao CPD?
- Existem fases de energia distintas para o CPD?
- Existem UPS (*Uninterruptible Power Supply*)? Com contratos de manutenção e assistência técnica? São testadas? Existem evidências dos testes?
- Existem alarmes para a falha de algum desses elementos? Com registo de ocorrências?

¹ De acordo com as normas nacionais retirado de Síntese Normativa (APSEI , s.d.)

Ar condicionado

- Está a fonte de energia do ar condicionado separada da fonte de energia principal do edifício?
- Tem uma UPS?
- Existe um contrato de manutenção?
- Qual é a frequência com que o ar condicionado é revisto?
- Quais os seus SLA (*Service Level Agreement*)?

Controle de ambiente

- Gestão da cablagem existente.
- Os produtos combustíveis devem ser proibidos.
- Controlo de humidade e temperatura.
- Chão elevado para evitar que inundações afectem o *hardware*.
- Alarme de aviso para os pontos de controlo.
- Águas e líquidos devem estar localizados fora *Data Center*.
- Como é protegido o CPD? Secure ID? Impressão digital? Bloqueio com chave de acesso (código)?
- Tem câmaras de CCTV com gravação automática?

4.7. Business Impact Analysis (BIA)

Informação geral

Uma análise de impacto de negócios (BIA) é uma forma de avaliar o impacto que uma interrupção tem nos processos de negócios de uma organização. Durante o processo, todas as funções de negócios são identificadas e avaliadas, em função do seu impacto nas operações e no lucro da empresa. O BIA avalia: o impacto que as perdas causam no negócio; o retorno do investimento; o serviço ao cliente; as transacções; a reputação; a vantagem competitiva; a quota de mercado; as responsabilidades legais; entre outras áreas. O BIA é um elemento-chave na construção de uma base realista para um programa de continuidade de negócio e é uma ferramenta eficaz no apoio às necessidades de um programa de continuidade de negócios abrangente. As informações

resultantes constituem a base para priorizar o processo de recuperação com base na perda desses processos para os negócios.

Resultados BIA

- Identifica riscos e quantifica impactos no negócio.
- Identifica processos e funções que são necessários para a sobrevivência do negócio.
- Determina a ordem na qual os processos precisam de ser recuperados.
- Identifica recursos essenciais utilizados para executar essas funções.
- Identifica dependências operacionais da empresa (os que uma organização depende e os que dependem dela, a montante e a jusante).
- Suporta a justificação das estratégias de continuidade de negócios e suas despesas.

Exemplo de etapas - Executar uma análise de impacto nos negócios

O BIA pode ser repartido pelas seguintes etapas básicas:

- Definir metas de negócios actuais e futuras;
- Identificar todas as funções e processos de negócio;
- Desenvolver os diagramas do processo de fluxo de trabalho;
- Identificar dependências internas e externas ao negócio;
- Definir os objectivos de recuperação de negócios;
- Quantificar o impacto, (por ex.: financeiro, legal, normativo, operacional, cliente, etc.);
- Definir objectivos de tempo de recuperação (RTO) e objectivos de pontos de recuperação (RPO (*Recovery point objective*)));
- Compilar dados e desenvolver documento de relatório do BIA;
- Analisar e validar com a gestão.

O processo de considerar os impactos financeiros e não financeiros associados à perda de uma função de negócios ou de um processo auxilia a gestão de negócios no desenvolvimento de quadros de tempo de recuperação adequados e objectivos. As áreas a serem consideradas incluem:

Impactos financeiros

- A perda de receitas resultantes de rescisão ou atrasos na transformação de produtos ou prestação de serviços.
- Perda de quota de mercado ou do seu valor em bolsa resultando em rescisão ou atrasos na produção de produtos ou prestação de serviços.

Impactos legais, normativos e de conformidade

- A potencial violação de um contrato ou da incapacidade de atender aos requisitos normativos.
- Incapacidade de atender aos principais requisitos de documentação e relatórios.
- A incapacidade de manter registos em conformidade com os princípios contabilísticos geralmente aceites e requisitos de impostos.
- A incapacidade de cumprir ordens judiciais ou acordos aplicáveis de liquidação ou litígio.

Impactos operacionais

- Incapacidade de atender a clientes, unidades de negócios e às expectativas de desempenho do grupo de trabalho.
- Custo das amortizações, causados por atrasos de processamento.
- Custo criado pelas encomendas em carteira e requisitos de recursos necessários para as resolver.

Impactos de serviço ao cliente

- Perda de confiança por incapacidade de cumprir os requisitos ou as expectativas dos clientes e potenciais clientes.
- O nível de impacto específico para as operações da unidade de negócios. No caso de um *call center*, menos impacto referem-se à incapacidade para atender 100 chamadas por hora *versus* o impacto da incapacidade de 1000 chamadas por hora de serviço.

- Consequências de não cumprir acordos contratuais e/ou contratos de nível de serviço.

Outras considerações

O impacto será documentado considerando interrupção das operações que ocorrem no pior momento possível (pior cenário). Isso inclui:

- Operações cíclicas chave (final de semana, mês, trimestre, ano);
- Perda de componentes de fluxo de trabalho crítico ou suas dependências.

Para a introdução dos dados necessários à análise de impacto de negócios (BIA) deve ser utilizado o documento constante no *template “Business Impact Analysis”* (Anexo 11).

4.8. Gestão de contratos e serviços TI

Uma empresa que tenha um clara ideia dos serviços que deve prestar em termos de suporte de TI à sua empresa quer sejam eles fornecidos com pessoal interno ou contratado, reduz o risco e melhora o processo de gestão bem como o planeamento estratégico. O enfoque na gestão dos contratos de TI reduz os problemas de falta de serviço de um fornecedor em caso de necessidade de recuperação de desastre, pois é nessa hora mais crítica que uma empresa necessita deles. Neste capítulo serão abordadas duas *frameworks* que ajudam a gestão na tomada de decisão quanto à escolha dos seus fornecedores e parceiros.

4.8.1. ITIL

Não se pretende dar indicações de como implementar o ITIL, mas sim tentar explicar que é uma ferramenta essencial para uma correcta adopção das melhores práticas em gestão de TI.

O ITIL permite a criação de uma

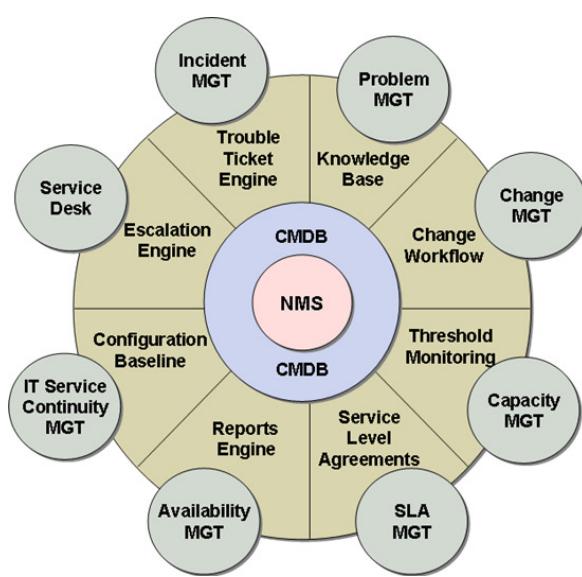


Figura 6 – Framework ITIL

linguagem e conceitos partilhados entre os elementos das equipas técnicas da organização e os seus utilizadores, fornecedores, subcontratados e parceiros, facilitando o entendimento e a definição de abordagens comuns.

Information Technology Infrastructure Library (ITIL) é um conjunto de boas práticas a serem aplicadas na infra-estrutura, operação e manutenção de serviços de tecnologia da informação (TI). Foi desenvolvido no final dos anos 1980 pela CCTA (*Central Computer and Telecommunications Agency*) e actualmente está sob custódia da OGC (*Office for Government Commerce*), Inglaterra.

O ITIL procura promover a gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação (TI). O ITIL lida com estruturas de processos para a gestão de uma organização de TI apresentando um conjunto abrangente de gestão de processos e procedimentos, organizados em disciplinas, com os quais uma organização pode fazer sua gestão táctica e operacional com vista a alcançar o alinhamento estratégico com os negócios.

O ITIL dá uma descrição detalhada sobre importantes práticas de TI com *checklists*, tarefas e procedimentos que uma organização de TI pode adaptar para as suas necessidades, o ITIL embora extenso é essencialmente uma metodologia para gestão da infra-estrutura de TI de uma organização. É constituído por um conjunto das melhores práticas que tem como objectivo principal alinhar os serviços prestados pelas tecnologias e sistemas de informação com os requisitos de negócio através da gestão da qualidade dos seus componentes e serviços. As organizações que implementam o ITIL beneficiam assim, da experiência acumulada desde a década de 1980 e da utilização desta metodologia associada a um conjunto global de boas práticas.

O enfoque em termos de contratos assenta em dois grandes grupos de serviços, a saber: o “*Services Delivery*” – que estrutura os serviços que são oferecidos - e o “*Support Services*” – que determina os meios de suporte aos serviços que serão oferecidos e geridos. É neste tipo de contratos que uma organização deve ter o seu enfoque, tendo particular atenção a determinados aspectos na altura de estabelecer o contrato de prestação de serviços e de controlar os seus níveis de serviço.

Uma das disciplinas do ITIL é a gestão da continuidade de serviços de TI, este papel tem a responsabilidade sobre o serviço de continuidade das TI e deve idealmente ser parte do grupo que assegura a “Continuidade do Negócio”. Em organizações menores esta função pode estar combinada com as funções de Disponibilidade e Capacidade. Este papel pode, também, ser combinado com papéis de segurança, especialmente em organizações que procuram certificar-se em processos de segurança.

4.8.2. Val IT

A aplicação efectiva dos princípios, processos e práticas contidas no Val IT permitirá que as organizações:

- Aumentem a probabilidade de seleccionarem investimentos com potencial para gerar retornos elevados;
- Aumentem a compreensão e transparência dos custos, riscos e benefícios, resultando em divisões de gestão muito melhor informadas;
- Aumentem a probabilidade de sucesso na execução de investimentos seleccionados, de modo a atingirem ou excederem o seu retorno potencial;
- Reduzam os custos, através da não realização de coisas que não deveriam ser feitas, ou mesmo do cancelamento de investimentos que não disponibilizam o seu potencial esperado;
- Reduzam o risco de fracasso, especialmente o fracasso de grande impacto;
- Reduzam as surpresas relativas aos custos e disponibilização de TI e, ao fazerem isto, aumentem o valor de negócio, reduzam os custos desnecessários e aumentem o nível global de confiança nas TI.

Em resumo, a correcta gestão de contratos e serviços permite a uma empresa o seguinte:

- Identificar necessidades e negociar contratos;
- Estabelecer e controlar níveis de serviço;
- Gerir fluxos financeiros;
- Selecção dos fornecedores mais adequados;
- Definição de contratos de prestação selectivos de serviços baseados no cumprimento de níveis de serviço.

Fornecedores e respectivos contratos

É necessário manter uma listagem dos contratos por fornecedor, pois esta fornece uma visão de quais os contratos activos, quais as datas de início e fim de cada um e qual o seu âmbito, para tal foi criado um *template* para o preenchimento destes dados (Anexo 12 - Listagem dos contratos).

O correcto preenchimento do *template* (Anexo 13 - Listagem de fornecedores), oferece-nos uma visão geral de quem são os fornecedores da empresa, de modo que se possa segmentá-los de acordo com o seu campo de acção, solidez financeira e estrutural.

O nível de SLA permite às empresas gerir o nível de serviço previamente contratado e criar relatórios com base no referencial contratado, para a sua correcta interpretação, recomendamos a utilização do *template* Lista de níveis de SLA (Anexo 14).

4.9. **Plano de backup global**

Existem muitos factores que irão determinar qual a melhor estratégia a *backups* e independentemente do tamanho da empresa, o processo de definição da estratégia deve ser o mesmo. Os principais factores a ter em conta são: a complexidade dos processos envolvidos, a gestão da mudança, a quantidade de dados (e o tipo de dados) que estão a ser geridos, a rapidez com que será necessário repor dados, sistemas e processos que estão a operar, e tendo em conta os RTOs e RPOs pré-definidos, deve então o plano de *backups* global ser adaptado de acordo com esse referencial.

O armazenamento de dados em meios electrónicos é cada vez mais frequente e esta tendência torna necessária a procura de formas de protecção que sejam realmente eficazes, rápidas e de custo aceitável. A automatização dos processos de *backup* e restauro são obrigatorias (a actividade humana é susceptível ao erro como por exemplo uma operação inadequada ou um esquecimento).

Esta preocupação aumenta quando os dados devem estar disponíveis integralmente e de imediato, principalmente quando estes foram identificados como sendo críticos para o negócio. Deve-se como consequência garantir a fiabilidade e integridade dos dados.

Uma vez que os aplicativos e o *hardware* também podem falhar, não importa a confiabilidade de um PC, servidor ou dispositivo usado para gravar dados, é extremamente importante ter uma solução de *backup* que seja tolerante a falhas. Não menos importante, é garantir que o *hardware* que suporta os dados é confiável e que mantém a integridade dos mesmos. Os sistemas de armazenamento em *raid* permitem ter um conjunto de características que permitem garantirem a fiabilidade e integridade da informação lá armazenada, nomeadamente esquemas de paridade¹ e ECC (*Error-correcting code*)².

Devem ser adoptadas medidas de tolerância a falhas ao nível do *hardware* dos servidores:

- Processadores redundantes;
- Fontes de alimentação redundantes;
- Fontes de refrigeração redundantes;
- Discos em *array* ou em *raid*³ (existem várias formas);
- Discos *hot spare*;
- Servidores em *clustering*;
- *On-line storage*.

Ao nível do ambiente do *Data Center*:

- Ar condicionado redundante;

¹ As mensagens são partidas em vários blocos de bits (uns e zeros numa transmissão digital). O número de ocorrências do "1" é contado. Depois é activado um bit de paridade - 1 se o número de "1" for ímpar e 0 se o número de "1" for par. Quando a mensagem chega, é testado o bit de paridade para verificar se está de acordo com o número de "1" da mensagem. Este esquema tem o problema de falhar quando o número de erros na transmissão é ímpar. (Fonte: http://pt.wikipedia.org/wiki/Detect%C3%A7%C3%A3o_e_corre%C3%A7%C3%A3o_de_erro).

² Código de correcção de erros. O ECC é um código no qual cada sinal de dados está em conformidade com regras específicas de construção. Os desvios dessas regras podem ser detectados e corrigidos. Esta técnica é normalmente usada em armazenamento de dados no computador (por exemplo: memória flash) e em transmissões de dados. Alguns códigos podem detectar e corrigir um certo número de bits de erros. Se apenas corrigirem um erro, são chamados códigos de correcção de erro único, ou SEC - single error correcting, e os que conseguem detectar dois erros são chamados de detecção de erro duplo, ou DED - double error detecting. (Fonte:http://pt.wikipedia.org/wiki/Detect%C3%A7%C3%A3o_e_corre%C3%A7%C3%A3o_de_erro).

³ Mais informação sobre este assunto pode ser consultada em <http://pt.wikipedia.org/wiki/RAID>

- Fontes de energia redundantes - duas ou mais fases de energia redundantes, UPS redundantes;
- Sistemas de detecção e combate a incêndio redundante.

4.9.1. Desafios

Colocam-se alguns desafios na concretização do sucesso na recuperação da informação crítica e respectivos sistemas, eis alguns:

- Garantir 99,99% da disponibilidade dos dados;
- Gerir o aumento do volume de dados;
- Categorização e priorização dos dados tendo em conta a natureza dos mesmos;
- Interferir o menos possível no ambiente operacional da organização, a menos que esta estabeleça uma rede dedicada de *backup*;
- Armazenamento dos *backups* em local seguro e com condições controladas (temperatura e humidade controlados);
- A recolha das tapes de *backup* diariamente para armazenamento *off-site*;
- Cópia de *backups*, usando o método cópia (ou *clone*);
- Descentralizar o armazenamento de dados mantendo-os redundantes em pontos distantes geograficamente;
- Restringir o acesso aos *backups* apenas a pessoal autorizado;
- Definição de uma política de entrega e recolha diária de *backups* das imagens dos servidores e tapes de *backups* de dados;
- Definição de uma política de retenção e dados;
- Definição de normas e procedimentos definindo a periodicidade e tipo de testes a efectuar aos *backups* existentes (servidores e tapes de *backups*);
- Definição de processos de controlo às normas e procedimentos em uso;
- Definição de um protocolo de autorização ao levantamento dos *backups* em caso de desastre (deverá mencionar quais os elementos autorizados a levantar o material necessário), deverá compreender a recolha das últimas tapes de *backup* e imagens de servidores guardadas, e kit de emergência (caso haja) com os manuais do DRP e instruções a seguir.

4.9.2. Metodologia de *backup* diária recomendada

Backup pode ser entendido como sendo um mecanismo para realizar cópias de segurança de arquivos, directórios e demais conteúdos pertinentes para uma possível recuperação caso seja necessário. O método a utilizar (ver capítulo 4.9.3 – Tipos de *backup*) será o que for mais recomendado para a exigência de tempo de reposição de dados, tendo em conta também o referencial para os custos associados.

4.9.3. Tipos de *backup*

A escolha da metodologia e estratégia de *backup* deve ser ajustada de acordo com as necessidades de reposição de uma empresa, descreve-se abaixo as mais comuns:

- Diário - Executa o *backup* dos directórios, unidades de rede, etc. Efectua o *backup* mesmo que nenhum arquivo tenha sido alterado. Ao repor os dados sabemos que a última *tape* de *backup* é a que tem os dados mais actuais.
- Cópia (ou *clone*) - Cria uma cópia do *backup* diário sem que os arquivos sejam marcados como sendo cópias, o que ocorre no método diário. Utilizado quando envolvidos os métodos do tipo Diário e Incremental. Também utilizado quando existe a necessidade de transporte para outro local sem que os *backups* “oficiais” sofram alterações.
- Incremental - Utilizado em conjunto com o diário, efectuando apenas o *backup* de arquivos criados ou alterados desde o último *backup* diário. Faz uso de menos tempo e ocupa menos espaço na *tape*. Existe o detalhe de no momento de restauração do *backup*, ser necessário o *backup* diário inicial e todos os incrementais criados na sequência da sua criação.
- Diferencial - Pode ser utilizado em conjunto com o *backup* diário ou incremental. Efectua o *backup* de todos os arquivos que sofreram modificações ou foram criados desde o último *backup* diário ou incremental. Necessita apenas do último *backup* diário e o diferencial. Possui um tamanho grande, porém um tempo menor de restauração.

4.9.4. Período de retenção

O período de retenção refere-se ao tempo de guarda que uma empresa tenciona manter os seus dados. Hoje em dia, e por questões legais¹ existem determinados tipos de dados que necessitam de períodos relativamente longos de retenção, nomeadamente dados relativos a conversações electrónicas e acessos à internet. No entanto por medida de segurança, períodos alargados são mais adequados para permitir a uma empresa proteger-se contra surpresas desagradáveis, permitindo maior flexibilidade na recuperação de um dado histórico de uma informação. Se uma empresa possuir apenas um "set" de *mídias*² para ser usado no *backup*, o seu período de retenção é extremamente curto e isto poderá comprometer o esquema de recuperação dos dados.

4.9.5. Rotação das *mídias*

De acordo com o período de retenção dever-se-á utilizar um conjunto de *mídias* maior ou menor, isto fará com que o tempo de retenção proteja mais adequadamente os vários tipos de problemas com perda de informações que podem ser restaurados de uma maneira mais versátil. A quantidade de *mídias* usadas minimizará possíveis falhas com os seus dispositivos de cópias. Isto significa uma longevidade maior das cópias e dos seus dispositivos também. Em geral, o uso de vários conjuntos de *mídias* possui um custo elevado. Isto pode ser um importante factor na tomada de decisão para escolha de qual o esquema de *backup* a utilizar e os dispositivos adoptados que serão mais adequados para as necessidades de *backup*.

Rotação mínima

O esquema mínimo de rotação que se pode considerar utiliza dois conjuntos de *mídias* que serão rodados alternadamente, isto permite um nível de protecção relativa, eliminando a hipótese da perda da cópia de segurança, caso surjam falhas no processo de *backup*. Todavia, não é uma grande protecção pois o período de retenção destas *mídias* é muito curto. Se se usar este tipo de esquema, será necessário determinar com

¹ ANACOM. (14 de Agosto de 2009). *Retenção de dados de acesso à Internet*. Obtido em 29 de Abril de 2010, de Web site da ANACOM: <http://www.anacom.pt/render.jsp?contentId=970264>

² Do Inglês - Mídia ou Computer data storage – refere-se a componentes usados para armazenamento de dados dos computadores e podem ser de diversa natureza e capacidade (tapes, discos rígidos, RAM, ROM, CDs, entre outros – ver cap. 4.9.6).

muito critério qual a periodicidade com que serão realizados os *backups* dos sistemas críticos e guardadas cópias de segurança. Para as empresas onde a informação não é crítica, este esquema pode fazer algum sentido, e suas cópias podem ser semanais. Mas em sistemas críticos e que necessitam de *backups* diários, não é possível adoptar este esquema.

Rotação média

Os *backups* são realizados numa unidade de fita magnética ou outro dispositivo removível qualquer, com capacidade suficiente de armazenamento total numa única unidade. Os grupos que este método utiliza são dois conjuntos de *mídias* diferentes. O primeiro para o *backup* diário, o segundo para o *backup* semanal. Se se usar o sistema apenas para os dias de semana (*business day*), serão necessárias cinco *mídias* rotuladas de Seg; Ter; Qua; Qui. e Sex., para a semana completa serão necessário adicionar-se mais duas *mídias*, rotuladas de Sáb. e Dom. respectivamente. Para o *backup* semanal, será efectuado um *backup* completo, que deverá ser armazenado *off-site* e sairá fora do esquema de rotação. O esquema usado é o incremental e dever-se-á ter em conta que se houver necessidade de repor dados a uma quinta-feira, é necessário usar as tapes dos dias anteriores até ao último *backup* completo (neste caso sexta-feira), sendo esta operação mais morosa.

Rotação alta

Backups feitos geralmente em unidades de grande capacidade. Todos os *backups* são completos, não havendo necessidade de backups incrementais desde que sejam executados sobre uma unidade cuja janela de *backup*¹ seja aceitável. Este sistema usa dois conjuntos de *mídia* diferentes, o primeiro é para um esquema de rotação diário, o segundo para um esquema mensal. O número de unidades a serem utilizadas depende do período de retenção desejado, normalmente são em média dez unidades para o *backup*

¹ **Janela de backup.** É bastante frequente ouvir-se falar de *backup window*. Esta expressão caracteriza o tempo que demora a completar-se uma operação de *backup*, sendo um factor de avaliação da sua prestação. Pela parte do sistema protegido, a janela temporal dedicada ao *backup* é definida pelo tempo que um sistema fica dedicado exclusivamente à operação de *backup*, situação em que é exigida a paragem total ou parcial dos seus serviços, retirado de: <http://www.dotecome.com/infoimagem/info28/28art6.htm>

diário e 22 para o mensal. Isto permite obter uma “fotografia” diária das duas semanas anteriores.

A rotação da *mídia* é efectuada em diferentes dias do final do mês, os *backups* são feitos usando o esquema de rotação diário das unidades, primeiro a unidade #1, depois a unidade #2 e assim por diante, até atingir a unidade #10, voltando para a unidade #1. A unidade #10 normalmente fica armazenada *off-site*. No final do mês, o esquema diário de rotação é saltado um dia e a unidade de *backup* é utilizada para sair fora do esquema de rotação.

Considerações acerca do plano geral de *backups*

Numa situação de desastre natural (seja ele de que tipo for) o tempo de recuperação irá certamente ser crítico, independentemente dos RTOs e RPOs definidos. É uma altura de muito *stress* e irá ser uma luta contra o tempo, onde todos os minutos despendidos a mais, serão valiosos. Assim, tendo em conta essa lógica e as referências definidas para tempos de recuperação, o método mais rápido será o diário, mas é em simultâneo o mais dispendioso, pois necessita de um maior nº de tapes para armazenamento de dados. O tempo de restauro dos Sistemas que fazem *backups* incrementais exige mais tempo para restauro em caso de um incidente. Na avaliação deste item, deverá ser considerado o tempo em que os activos ficarão paralisados. A indisponibilidade de serviços é considerada uma ameaça para a segurança do negócio. O período de retenção das *mídia* será o mais alargado possível para permitir a manutenção de dados históricos durante maior período de tempo possível.

4.9.6. Dispositivos de *backup*

Independentemente da técnica utilizada é preciso ter em mente que os dados de uma empresa necessitam de ser armazenados em *mídias* confiáveis. Existem os mais diversos tipos para cada necessidade.

Flash Memory - Utilizados para *backups* de pouca informação. Possuem durabilidade de aproximadamente 10 anos. Os dados não são corrompidos por fontes magnéticas.

DVD Backup – Os DVD incluem tecnologias DVD-RW, DVD + RW, DVD-R, DVD + R, DVD-RAM, assim como tecnologias DVD *dual-layer*. Um DVD *single-layer* pode armazenar até 4,7 GB de dados. Um DVD de dupla camada pode armazenar até 8,5 GB.

Disco Rígido - Devido ao baixo custo dos discos rígidos, estes têm sido utilizado com frequência.

Tapes de backup¹ - estão disponíveis em diversas capacidades como as de 4 milímetros e de 8 milímetros para sistemas de médio porte. AIT, DLT e LTO para sistemas de grande porte. Comparando com outros meios de armazenamento, as tapes de *backup* fornecem alta capacidade de armazenamento a baixo custo. Possuem a desvantagem de escrever de forma sequencial e consequentemente mais lenta.

On-line Storage – Este é um dos mais recentes métodos de *backup*. Os dados são todos armazenados *online*. Os dados são enviados (*upload*) para servidores dedicados e seguros. Fazem uso dos três princípios da segurança da informação: disponibilidade, integridade e confidencialidade.

4.10. Soluções tecnológicas para DRP

4.10.1. Análise de soluções

Conversão de virtual para virtual

Sem dúvida uma das melhores soluções, pois permite efectuar a passagem de um sistema virtualizado para outro *host* muitas vezes em questão de segundos e sem *downtime*, agiliza processos, e poupa dinheiro em investimentos para novo *hardware*, e algo muito importante e em voga, ajuda a diminuir a pegada de carbono deixada pelas empresas. Permite criar redundância de uma forma fácil e de certa forma simples (basta para isso duplicar a imagem virtual), permite criar sistemas de alta disponibilidade e tolerante a falhas com o uso das propriedades de *clustering* oferecidas por alguns fabricantes (umas nativas e outras dos sistemas operativos que suportam), agregadas a soluções de *load balancing*. Existem no entanto algumas preocupações com a performance dos *backups* visto que estes podem estar a ser feitos a máquinas virtuais

¹ Informação sobre *tapes* de *backup* disponível em <http://www.data-backup-and-storage.com/tape-backup-drives.html>

noutros *data-centers* e esta sair degradada. Os *backups* a servidores de Exchange em máquinas virtuais necessitam de ser efectuados ao próprio Exchange (para limpar os *logs* das transacções) e não apenas à máquina virtual. Em soluções de alta disponibilidade a limitação a dois nós num *cluster* deve ser algo a considerar. O investimento inicial na tecnologia que dá suporte à virtualização pode ser um pouco elevado (desde o *hardware* ao *software*), mas é largamente compensado pelo benefício que dela advém.

Conversão de físico para virtual

Sem dúvida que a virtualização oferece uma agilidade sem precedentes na recuperação de sistemas em caso de desastre, mas e quanto aos sistemas físicos que não são bons candidatos à virtualização? E quando os custos associados à virtualização ainda não estão contemplados? Nestas situações é necessário encontrar uma alternativa credível e fiável para a recuperação de sistemas. A solução de conversão de físico para virtual necessita de cópias dos sistemas físicos com alguma regularidade, sendo que para controladores de domínio essa regularidade tem de ter em conta outros factores, nomeadamente o tempo em que são renovados os SID (*System Identification*), questão crítica para alguns sistemas. Mas nem todos os sistemas têm esta particularidade e para os restantes, será tão regular quanto as alterações a eles efectuadas. É necessário portanto estabelecer procedimentos para se efectuar cópias dos sistemas em produção, para que estes possam vir a ser repostos noutros ambientes ou *hardware*.

Conversão de físico para físico

A solução para sistemas em que a virtualização não é solução, deve ter em conta algumas funcionalidades que assegurem o restauro do sistema de origem no de destino, assim sendo deve o *backup* de sistemas deve ser feito automaticamente (através de agendamentos ou com base em eventos), enquanto o mesmo está em produção para evitar a interrupção de serviço. Deve assegurar que a recuperação para um *hardware* diferente (quer com a tecnologia *Restore Anywhere* ou similar), permitindo a cópia de *backup* para um local externo *via* FTP (*File Transfer Protocol*) ou unidade de disco secundária, como forma de oferecer recursos melhorados de recuperação após desastres. Conversões ininterruptas de físico em virtual e vice-versa, em ambientes virtuais (VMware, Microsoft e Citrix).

4.10.2.Solução proposta

Não existe uma solução única para todas as empresas, sendo que cada caso tem de ser analisado ao pormenor e encontrada uma solução para cada situação. Cada empresa tem uma complexidade tecnológica muito própria, pois pode ir desde os desenvolvimentos à medida, ao *hardware* muito específico. No entanto existem muitas similaridades entre todas as empresas e é nessas situações que já existe um conjunto de soluções para permitir a uma empresa voltar a operar mais rapidamente. Nas restantes situações deve-se avaliar o impacto dos elementos em estudo, e optar por criar redundância.

Pontos-chave:

- Comunicações internas (Voz e dados);
- Comunicações para o exterior (voz, dados e internet), onde estão englobadas as comunicações com as dependências (caso as haja);
- Reposição de sistemas críticos;
- Segurança;
- Postos de trabalho para utilizadores;
- Impressoras;

Virtualização

Um pouco de história:

Apesar da tecnologia de virtualização de servidores receber actualmente tanta atenção, o seu conceito em si não é novo. Na verdade a ideia surgiu na metade dos anos de 60, quando os enormes e caros computadores da época atingiram uma elevada capacidade de processamento mas mostravam-se ineficientes em aproveitar o seu caro tempo de cálculo, isto devido ao facto de a gestão dos seus processos ser efectuada de uma forma manual pelo operador.

Verificou-se que para tirar melhor proveito seu caro processamento computacional seria necessário executar vários processos em paralelo. Com esse procedimento surgiu o

conceito de tempo partilhado (*time sharing*¹) de processamento, aproveitando os tempos de espera do processador, que culminou com a ideia de virtualização.

Em 1972, o cientista Norte-americano, Robert P. Goldberg (Goldberg, 1974), lançou a base teórica da arquitectura para sistemas computacionais virtuais, na sua dissertação na universidade de Harvard. No mesmo ano a IBM lançou um *mainframe* capaz de executar simultaneamente diferentes sistemas operativos sob a supervisão de um programa de controlo – o *hypervisor*.

O sistema 370 da IBM foi o primeiro computador inteiramente projectado para virtualização, que com o sistema operativo CP/CMS, permitia executar múltiplas instâncias em simultâneo. Este sistema foi seguido pelo IBM z/VM, que se aproveitava da virtualização via *hardware* de uma forma mais completa, onde todas as interfaces de hardware eram virtualizadas. O VM/CMS ficou muito bem conceituado no meio académico e foi amplamente distribuído na indústria. Várias abordagens modernas de virtualização devem muito às suas implementações em computadores de grande porte da IBM.

Com o passar dos anos a virtualização começou a cair no esquecimento devido a criação de novas aplicações cliente/servidor e ao declínio da plataforma mainframe que perdeu força frente à ascensão da plataforma x86. De acordo com a VMWare², a ampla adopção do Windows e Linux como sistema operativo em servidores na década de 1990, acabaram por definir a arquitectura x86 como padrão da indústria.

Devido ao elevado custo de aquisição de um mainframe, as empresas passaram a adquirir servidores de plataforma x86 de acordo com as suas necessidades, processo este chamado de *low-end* (várias máquinas pequenas a fazer o trabalho de um grande servidor). Neste cenário, em vez de ter um elevado custo inicial com a aquisição de um

¹ Time Sharing: Este conceito significa partilha de tempo de processamento, ou seja, só tempos inactivos entre os processos são partilhados com outros processos para dinamizar o sistema. Múltiplos jobs são executados simultaneamente, sendo que a CPU atende cada job por um pequeno tempo, um a um em sequência. Os tempos dedicados para cada job são pequenos o suficiente para que os utilizadores consigam interagir com cada programa sem que percebam que existem outros programas em execução.

² VMware, Inc. (2007). *Understanding Full Virtualization, Paravirtualization, and Hardware Assist*. Obtido em 3 de Junho de 2010, de Web site da VMware: http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

mainframe, optava-se por adquirir servidores de menor capacidade de acordo com as necessidades.

O impacto dessa nova estratégia foi que para garantir uma boa margem de folga contra problemas de dimensionamento de hardware, grande parte destes servidores foram usados para servir uma única aplicação. De acordo com a IDC (*International Data Corporation*)¹, as arquitecturas cliente/servidor tradicionalmente apenas podem utilizar cerca de 10 a 20% da CPU (*Computer Processor Unit*) total disponível em servidores (O'Donnell, 2007). Já as arquitecturas de virtualização podem aproveitar mais de 90% dos recursos da CPU. Assim, e em cada implementação de um típico servidor x86, o máximo do uso da sua CPU era subaproveitada. Os servidores eram superdimensionados para a aplicação que iriam executar, e por consequência, acabavam por sofrer do mesmo problema dos mainframes da década de 1960, isto é, não se aproveitava toda a sua capacidade computacional, eram assim subutilizados.

Então, em 1999, a VMWare Inc. introduziu o conceito de virtualização na plataforma x86 como uma maneira mais eficiente para utilizar o equipamento desta plataforma, aproveitando os servidores x86 para fornecer uma estrutura computacional que possibilitasse o total aproveitamento dos recursos computacionais deste tipo de servidores.

A partir de 2005, fabricantes de processadores como Intel e AMD deram mais atenção à necessidade de melhorar o suporte via hardware nos seus produtos, a Intel com a sua tecnologia Intel VT e a AMD com a AMD-V. Estas plataformas de hardware contêm funcionalidades explícitas que permitem que *hypervisors* melhorados sejam utilizados com a técnica de virtualização completa (*full virtualization*), que tornam mais fácil a implementação e potencializa a melhoria de performance.

Desta forma a virtualização é um processo que permite executar vários sistemas operativos num único computador. Sendo uma máquina virtual um sistema operativo completo que se comporta como se fosse um computador independente. Ao utilizar a virtualização, um servidor pode ter vários sistemas operativos em utilização. A

¹Estudo efectuado para a IDC por Bob O'Donnell, *Virtualization Moves from the Back Office to the Front Office* (O'Donnell, 2007).

virtualização ao mesmo tempo que possibilita uma diminuição do parque informático permite também a criação de redundância ao criar duplicados das máquinas virtuais.

Um ambiente virtual contempla de um modo geral dois componentes principais, o *host* e o *guest*, sendo que o *host* é o sistema operativo que é instalado e executado directamente no *hardware* ou servidor. O sistema operativo *guest* é o ambiente virtual que se executa sobre o *host*, tornando-se assim numa máquina virtual. Ao contrário das máquinas físicas, os *hosts* podem executar em simultâneo vários sistemas *guest*.

A virtualização, ao permitir que vários sistemas operativos e aplicações sejam executados em simultâneo numa única máquina física, pode ajudar a melhorar de forma significativa os planos de recuperação de dados, pois os elementos da equipa não têm de se preocupar com a reconfiguração dos vários sistemas. E em alguns casos (dependendo do tipo de software de virtualização utilizado) não existe sequer a preocupação do *hardware* ter de ser igual ao original.

Existe no mercado uma ampla oferta de *software* de virtualização, não só de carácter comercial mas também de código aberto¹, sendo que por vezes o custo associado à utilização deste último acabe por ser mais elevado do que o custo do software pago, pois o apoio técnico é escasso e mais caro.

No que respeita à oferta de *software* de virtualização, esta é grande e variada, ficam aqui apenas alguns exemplos. Quanto ao *software* comercial, podemos escolher o VMware², o Hyper-V³ da Microsoft entre outros. Quanto ao *software* gratuito ou livre (*Open Source*) apresentamos como sugestão o Xen Hypervisor⁴ e o VirtualBox⁵, ambos licenciados sob a GNU (*General Public License*).

Assim nas soluções físico para físico deve ter-se em atenção as soluções de *backup* em **tempo real** dos servidores, pois nas soluções onde a opção virtualização não é solução por não ser passível de ser usada, é necessário efectuar imagens dos servidores para se ter backups actualizados e nos dias de hoje parar um sistema para se criar uma imagem

¹ Do Inglês *open source*, criado pela OSI (*Open Source Initiative*) também conhecido por software livre.

² Versão *trial* para download em <https://www.vmware.com/tryvmware/?p=default>

³ Integrado no Windows Server 2008 R2

⁴ Download em http://www.xen.org/products/xen_archives.html

⁵ Download em <http://www.virtualbox.org/wiki/Downloads>

é muito complicado ou mesmo inaceitável. A compatibilidade entre as camadas de *hardware* tem de ser vista com especial cuidado, pois uma imagem de um servidor pode não ser compatível com o de contingência, caso não seja o mesmo modelo, marca e processador. Seria incomportável para uma empresa manter ou exigir ao provedor do serviço do *site* alternativo a manutenção de redundância de equipamentos para os seus clientes a fim de manter a compatibilidade entre equipamentos. Para os casos em que a virtualização ainda não é solução e em caso de contingência do número de servidores disponíveis no *site* de recuperação, a solução física para virtual é uma boa alternativa para a recuperação de sistemas que dão suporte ao negócio. Aqui, mais uma vez, as soluções de *backup* em **tempo real** dos servidores permitem programar a frequência dos backups e em simultâneo efectuar uma conversão para virtual. Estas soluções permitem a abstracção da camada física da máquina e permite o restauro de uma máquina para qualquer *hardware* (*Restore anywhere*), retirando a problemática da escolha do *hardware* onde restaurar o servidor.

No caso de *mainframes*, a hipótese de replicação no *site* passa pelo apoio do fabricante na solução a encontrar. Outras situações particulares devem ser devidamente analisadas e encontrada uma solução para cada uma delas, desde que satisfaça os desígnios do negócio ou que se assuma o risco pela não reposição do sistema em causa.

4.11. Procedimento para recuperação dos sistemas definidos como críticos

4.11.1. Exclusões

No decurso de um desastre, e devido à limitação de recursos, irá haver necessidade de desenvolver planos de acção no próprio momento do desastre para algumas áreas em virtude da sua complexidade e necessidade de recursos demasiado específicos. Por vezes existe determinado tipo de serviços e por estarem associados e *hardware* muito específico não serão passíveis de ser recuperados, por exemplo em empresas a operar na área da saúde, o aparelho de radiologia ou aparelhos oftalmológicos entre outros, os serviços associados a estes ou a outros aparelhos específicos, só são repostos se existir um duplicado dos respectivos aparelhos no *site* de recuperação. Noutras áreas e devido à escassez de recursos humanos, o normal funcionamento poderá dar lugar ao indispensável para uma operação de sobrevivência e deverão ser identificadas quais as

áreas e serviços abrangidos pela exclusão e quais as alternativas aos mesmos. Por exemplo, em caso de emergência a impressão da facturação, que era efectuada *in-house*, pode passar a ser efectuada em regime de *outsourcing*; o processamento de salários entre outros.

4.11.2.Pressupostos

Para a elaboração deste plano foram tidos em conta os seguintes pressupostos:

- Existe pelo menos um sobrevivente em cada departamento;
- As instalações alternativas a utilizar, estão intactas;
- Os elementos críticos deste plano, nomeadamente equipas técnicas e de comando existente têm as *skills*¹ necessárias para a interpretação e execução das indicações fornecidas no plano em vigor.

4.11.3.Abordagem do processo de recuperação

Para dar uma visão geral de qual a abordagem a este plano de recuperação, foi elaborado um diagrama de casos de uso (Anexo 15) que ilustra o comportamento do sistema.

Foram também criados diagramas de actividades que ilustram os processos envolvidos no plano e fluxos de informação. De forma a facilitar a visualização e interpretação das actividades relacionadas com o plano, foram criados os seguintes diagramas:

- Actividades do DRP – Representa as actividades deste plano, sem contudo pormenorizar as actividades executadas por cada uma das equipas envolvidas (Anexo 16);
- Actividades do responsável pelo DRP – Representa as actividades a executar pelo responsável do plano de recuperação (Anexo 17);
- Actividades da equipa de comando – Representa as actividades que a equipa de comando deve executar ao longo de todo o processo de DRP (Anexo 18);

¹ Skill – do Inglês, **Habilidade** (do latim *habilitate*) é o grau de competência de um sujeito concreto frente a um determinado objectivo. Entenda-se portanto por *Skills* necessários, como sendo as habilitações, o treino ou formação específica na área.

- Actividades da equipa de recuperação de SI (Sistemas de Informação) – Representa as actividades que a equipa de recuperação deve executar, com vista à recuperação de todos os sistemas (Anexo 19).

4.12. Sequência lógica de eventos

Depois de efectuada a declaração de desastre, o responsável pelo DRP é responsável por entrar em contacto com os fornecedores e iniciar os procedimentos técnicos a fim de assegurar a recuperação de serviços estabelecidos no contrato correspondente.

Os principais passos a seguir são os seguintes:

- Recolha do material de DRP;
 - *Tapes de backup* com dados.
 - Imagens de servidores (o suporte pode estar em tape ou *HD*).
 - Manual de recuperação.
- Dirigir-se para o *site* de recuperação;
- Iniciar a recuperação dos sistemas indicados como críticos.

4.12.1. Activação do plano

Depois de ter sido efectuada a Declaração de Desastre, o Plano de Recuperação é activado através de chamadas, preferencialmente para telemóvel de acordo com uma árvore de chamada (Anexo 20 - Árvore de chamada).

Caso não se consiga falar com algum dos colaboradores da árvore de chamada deve ser deixada uma mensagem no *voice-mail* do telemóvel do tipo:

“Plano de Recuperação foi activado. Contacte assim que possível um dos elementos da sua Equipa de Gestão da Continuidade”.

Se se tratar de elementos da 1^a e 2^a vaga da árvore de chamada deve ser tentado o 2º contacto da opção aí indicado. Nesta situação o referido 2º contacto ficará responsável por contactar os elementos das vagas seguintes que iriam ser contactados pelo colaborador que se encontra indisponível.

4.12.2.Estratégia de recuperação

Como estratégia de recuperação dos sistemas de TI, e resultante da definição dos RPO¹ e RTO², deve ser definido que tipo de *site* é necessário para a empresa. Este deve ser escolhido tendo em conta alguns factores, nomeadamente a relação custo/tempo de recuperação (figura 7) versus necessidades do negócio.

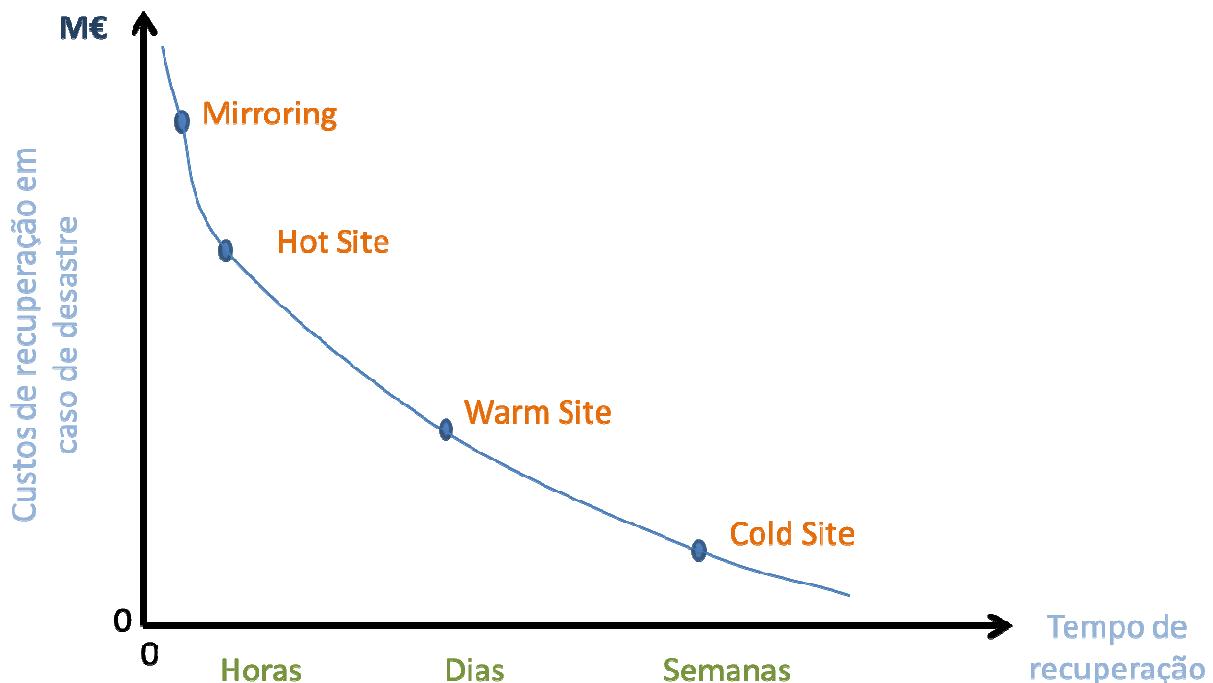


Figura 7 - Gráfico de análise de custos

Tipos de *sites* de contingência:

Partilhados

- **Mirroring** – É uma cópia exacta do local primário da empresa, com sistemas informáticos completos ou em sistema de virtualização. Estes sistemas estão a ser actualizados em tempo real e são um espelho do *site* primário, sendo por isso

¹ Ponto como objectivo para recuperação (RPO) descreve a quantidade aceitável de perda de dados medidos no tempo. RPO (Recovery Point Objective) é o ponto no tempo para o qual se deve recuperar dados conforme definido pela organização. Isto é geralmente uma definição que uma organização determina como uma perda de "aceitável" numa situação de desastre. Se o RPO de uma empresa é de 2 horas e o tempo necessário para obter os dados de volta para a produção é de 5 horas, o RPO ainda é de 2 horas. Com base no presente RPOS os dados devem ser restaurados para dentro de 2 horas da catástrofe.

² Recovery Time Objective é a duração do tempo e um nível de serviço dentro do qual um processo de negócios deve ser restaurado após um desastre (ou interrupção) de modo a evitar consequências inaceitáveis associadas a uma quebra na continuidade de negócios.

chamado de *mirroring*. O *mirroring* ou, traduzido literalmente, "espelhamento", é uma operação unidireccional (*a one-way operation*) enquanto a *synchronization* ou "sincronização" é *uma operação bidireccional (two-way)*. Este *site* contém todos os recursos necessários para a imediata continuidade do negócio. É o *site* alternativo que melhores condições oferece, mas é simultaneamente o mais dispendioso e que mais trabalho dá para manter.

- ***Hot Site*** - Recebe este nome por ser uma estratégia pronta para entrar em operação assim que uma situação de desastre ocorre. O tempo de operacionalização desta estratégia está directamente ligado ao tempo que for definido para tolerância a falhas de serviço. O *hot site* é um recurso alternativo totalmente equipado, onde um negócio pode ser realocado com perdas mínimas para as operações normais após um desastre. Pode ou não conter cópias dos *backups* diários dos dados e informações da empresa, pois o local de armazenamento das cópias dos *backups* pode ser efectuado noutro local. Para a gestão dos registos do negócio também contempla mesas, cadeiras, telefones, aparelhos de fax, fotocopiadoras e acesso à internet para ajudar as empresas a manter as suas operações comerciais. Um *hot site* contém computadores em *standby*, sistemas ambientais, recursos de comunicação e outros equipamentos necessários para apoiar plenamente os requisitos do imediato processamento de dados de uma organização em caso de crise ou de desastre. *Hot site* é um termo que se originou no ambiente de processamento de dados, mas o conceito aplica-se igualmente bem para a designação de um local alternativo para um escritório, espaço de trabalho ou área industrial. Este tipo de *site* alternativo pode ser instalado e estar funcional em questão de horas e é uma necessidade para as empresas que devem retomar as operações normais tão rapidamente quanto possível. Um *hot site* também pode ser usado como uma base alternativa de operações em circunstâncias normais. Capaz de suportar períodos curtos ou longos de indisponibilidade. Devem ser realizados testes anuais de funcionamento.
- ***Warm site*** - Dentro da classificação nas estratégias anteriores, esta propõe uma alternativa de contingência a partir de um ambiente com os **recursos mínimos** de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto, aplicável à situação com tolerância de indisponibilidade

ainda maior. Esta estratégia aplica-se portanto quando é definida uma maior tolerância à ausência de serviço, podendo uma empresa sujeitar-se à indisponibilidade por mais tempo, até ao retorno operacional da actividade. É um local de *backup* e é equipado com computadores e *hardware* semelhante ao local original da empresa, mas não inclui cópias de backup de dados e informações. Para a gestão dos registos do negócio também contempla mesas, cadeiras, telefones, aparelhos de fax, fotocopiadoras e acesso à internet para ajudar as empresas a manter suas operações comerciais.

- **Cold site** - é o tipo de *site* mais barato de local alternativo para um negócio operar. Para a gestão dos registos de negócios oferece mesas, cadeiras, telefones, aparelhos de fax, fotocopiadoras e acesso à internet para ajudar as empresas a manter as suas operações comerciais. O *site* não inclui computadores, *hardware* ou *backup* das cópias dos dados e informações do local original. Este tipo de *site* requer menos recursos para operar, pois permite que os clientes utilizem os seus próprios computadores.

Próprio – *site* redundante

Principais características:

- Propriedade da própria empresa;
- Com as mesmas características do *Hot site* ou *Mirroring*;
- Maior flexibilidade;
- Possibilidade de balanceamento de carga;
- Maior custo;
- Em alguns casos, exigência legal ou reguladora.

Vantagens / desvantagens

Hot site* e *Mirroring

Vantagens

- Entram em operação em poucas horas ou até mesmo de imediato.
- Alta disponibilidade.

- Podem ser usados para soluções de curto ou longo prazo.
- Possibilidade de testes anuais.

Desvantagens

- Alto custo.
- Limitação da escolha de *hardware* ou software.

Warm e Cold site

Vantagens

- Menor custo que o *hot site* ou o *Mirroring*.
- Disponibilidade por períodos maiores devido ao menor custo.
- Possibilidade de uso de *hardware* ou *software* proprietário.

Desvantagens

- Entrada em operação mais demorada.
- Maior dificuldade para realização de testes.

Como complemento à estratégia de recuperação em termos de *sites* a escolher, deverá seguir-se um conjunto de boas práticas, nomeadamente ter-se em conta a localização do *site* (longe o suficiente do local primário para não ser atingido pela situação lá ocorrida), fora de uma zona sísmica, longe da orla marítima, zonas de aluvião, encostas, confluência de rios, ou seja a escolha do local deve seguir critérios rígidos de segurança e não critérios puramente comerciais ou económicos.

4.12.3.De volta à normalidade

Existe uma altura em que os desastres terminam e a zona afectada volta ao seu normal funcionamento. O plano de recuperação de desastres também deve abordar esta fase (como regressar ao local de origem). Apesar de esta fase não ter a mesma natureza crítica em relação ao factor tempo no que respeita aos preparativos para reposição dos dados e sistemas (não é necessário cumprir os RTO ou RPO), tal como o foi na fase em que o desastre foi declarado. Mas como os *sites* de *backup* custam dinheiro todos os dias

que estão em uso, devido às questões económicas e de organização deve-se retornar à normalidade o mais rápido possível. O novo centro de processamento de dados deve estar equipado com todo o *hardware* e *software* necessário para o retomar das operações. Todos os sistemas e dados (sem excepção) serão retomados, pois já não existirá qualquer contingência, face ao *site* temporário.

Devem-se então fazer os últimos *backups* do *site* de contingência e enviá-los para o novo centro de processamento de dados. Após os dados serem restaurados no ambiente principal, a produção poderá ser iniciada no novo centro de processamento de dados. Neste ponto, o centro de processamento de dados de contingência pode ser descontinuado, com a disposição de todo o *hardware* temporário e a eliminação de todos os dados e sistemas colocados em produção nesse local.

4.13. Testar o plano de *disaster recovery*

O Plano deve ser testado regularmente para assegurar que a empresa terá capacidade efectiva de recuperar os seus processos críticos numa situação de desastre.

O objectivo dos testes/simulações é validar o plano de recuperação e efectuar os ajustes necessários de acordo com não conformidades encontradas ou procedimentos indicados para serem revistos. Lembrando que os ambientes de negócio e processamento de dados são dinâmicos, os planos de recuperação devem ser constantemente revistos, actualizados e testados.

Num cenário típico de testes ao plano de *Disaster Recovery*, é necessário efectuar testes cíclicos às suas componentes de recuperação, estes testes são efectuados aos diferentes níveis de componentes a serem executados e todo o processo de teste é normalmente, circular e periódico. O teste consiste em assegurar que cada teste efectuado se torna mais complexo ao longo do tempo. É importante notar que os testes de recuperação de desastres são diferentes do teste de continuidade de negócios.

Tipos de testes individuais às componentes:

- **Testes por meio de uma lista de verificação¹** - São usadas listas de verificação como forma de revisão da equipa de recuperação, para determinar se as componentes do plano são actuais e se estão disponíveis e completas;
- **Testes à documentação** - São executados através da realização da revisão dos procedimentos e documentação do plano e serve para testar por exemplo uma lista de contactos;
- **Testes de Bancada** - São testes do plano de recuperação em que as acções não são realmente executadas;
- **Teste Passo-a-Passo** - É efectuada uma revisão verbal do plano;
- **Testes Passo-a-Passo estruturados** - Neste tipo de testes, as equipas vão executar e rever todos os passos do plano, sem realmente dar início aos procedimentos de recuperação.
- **Revisão do Plano de Exercício em Sala de Formação** – Permite explicar numa sala qual o cenário para o exercício de interrupção completa do negócio, descrevendo todos os passos do processo de recuperação. Fazer uma moderação que permita a todos os responsáveis pelas equipas de continuidade darem feedback de modo a rever o Plano de Continuidade e a própria estratégia de exercícios.

¹ Nota: Lista de verificação de um teste é também um método utilizado para testar um plano de Continuidade de Negócios e Disaster Recovery Plan. Por exemplo, o plano é distribuído e comentado por Unidades de Negócio em relação à sua exactidão do seu conteúdo, rigor e eficácia.

Testes a todas as componentes:

- **Testes paralelos** - Requerem que seja testada a funcionalidade de processamento no local de contingência.

Testes combinados às componentes:

- **Teste de transferência dos sistemas** – Este teste prepara e assegura que os sistemas de recuperação podem apoiar as funções críticas de negócio.
- **Teste de interrupção completa do negócio** - É um exercício em que todos os processos de recuperação e estratégia são testados. É na verdade uma réplica de um desastre por meio de simulação da interrupção da produção. Proporciona situações o mais próximas possível do cenário real, por exemplo, quem fizer o exercício não saberá a que horas e quando irá intervir, são efectuados teste de *stress* às equipas de recuperação, que podem ser jornadas *non-stop* com a equipa de recuperação, colocação propositada de erros nas componentes, substituição de um elemento, etc., isto permite aferir da capacidade de resistência e da capacidade de reacção ao imprevisto;

Exercício de Evacuação

- Evacuar todos os colaboradores do edifício sede e/ou dependências ou sucursais – permite testar e avaliar a sua eficácia;
- Testar o know-how das equipas de 1^a intervenção – permite aferir se estas equipas estão aptas a desempenhar o seu papel.

Relatório de testes

Todos os participantes no exercício de larga escala têm um formulário (Anexo 21 - Relatório de exercício de testes) onde constará a descrição dos testes a realizar, os objectivos a atingir e respectivos resultados esperados. Estes formulários permitem registar o sucesso ou insucesso de cada teste levado a cabo, bem como todas as observações pertinentes para a sua avaliação.

Adicionalmente dever-se-á se preencher um formulário de resumo e validação do exercício (Anexo 22) que servirá essencialmente para registar recomendações ou sugestões de alterações aos exercícios.

Com base nestes formulários, deverá ser preparado um relatório global sobre o exercício com os seguintes elementos:

- Disponibilidade, resposta e competência demonstrada no desenrolar do exercício por parte dos elementos envolvidos;
- Adequação e clareza dos manuais e material de apoio fornecido;
- Adequação das instalações usadas;
- Adequação dos *backups*, e documentação existente para suporte à recuperação dos processos/funções;
- Proposta de soluções para resolver problemas/fraquezas detectados;
- Os relatórios dos testes devem ser revistos de modo a avaliar a efectividade do plano. Também deve ser assegurado que as recomendações destes relatórios tenham reflexo no processo de revisão de um Plano de Continuidade.

4.14. Programa de manutenção do plano

A manutenção do plano é um factor crítico para o sucesso de uma recuperação real. O plano de recuperação deve reflectir as mudanças efectuadas nos ambientes reais. É crítico que os processos existentes sejam revistos e a necessária alteração no plano seja efectuada. Nas áreas onde a gestão da mudança não existe, esse procedimento deve ser implementado. Muitos produtos de *software*¹ de recuperação possuem a facilidade de gestão da mudança.

4.15. Gestão da Mudança

Tendo em conta que a estratégia de recuperação passa pela utilização de instalações alternativas, deve ser tomada em consideração a compatibilidade entre essas instalações alternativas e as instalações normalmente utilizadas.

¹ Já focados no capítulo 4.10.1em soluções físico para físico (características de *Restore Anyware*)

Decisões de compra de *hardware*, *software*, equipamentos de telecomunicações ou outras alterações na infra-estrutura de TI devem ser tomadas tendo em consideração os impactos na relação de compatibilidade acima referida. Esta avaliação será feita pelos responsáveis pelas referidas decisões de compras que devem informar o responsável do DRP.

Simulação periódica do plano e adequação do manual de DRP

Deverá existir um planeamento e adequação do plano a alterações do nível tecnológico, processos de negócio, aumento ou diminuição dos activos de TI e novas implementações em produção.

Deverão ser definidas linhas de orientação quanto à periodicidade com que devem ser feitos os exercícios de teste (sempre de acordo com a frequência, complexidade e criticidade das alterações introduzidas). Aconselha-se efectuar reuniões de alinhamento com o negócio de preferência mensais, onde existirá um alinhamento do plano com as necessidades do negócio. O plano deve ser testado preferencialmente duas vezes por ano e nunca menos do que uma vez. Deve calendarizar-se essa planificação e apresenta-la à gestão.

Este calendário poderá prever etapas preliminares até ao teste completo, passando pelas várias opções de testes às componentes existentes.

O manual de DRP deverá então ser actualizado e distribuído a todos os elementos identificados para receber uma cópia do mesmo. Na opinião dos autores, uma das formas de complementar as opções tradicionais para garantir que o manual esteja realmente ao alcance de todos os elementos atrás citados, é a disponibilização do plano através da inclusão de toda a informação constante do mesmo num *web site*¹ seguro, assim, a informação fica disponível em qualquer local, em qualquer altura, para todos os elementos autorizados, desde que exista a possibilidade de aceder à internet.

¹De forma a ilustrar como se torna fácil a qualquer elemento autorizado, consultar a informação do plano de DRP, foi elaborado um site em XHTML para que possa ser consultado em computadores pessoais (*desktops ou laptops*) ou em dispositivos móveis (por exemplo PDAs). O site inclui todo este trabalho e é fornecido em formato digital incluído no CD que acompanha o trabalho.

Regulamentação

Os regulamentos internos de uma empresa são extremamente importantes, pois são eles que normalizam o respectivo funcionamento e criam regras gerais de actuação, dentro dos limites do que é definido como normal e aceitável. Deve-se então regular os procedimentos internos no que respeita a todas as actividades relacionadas com o plano de recuperação em caso de desastre (bem como todas as outras), divulgar e formar periodicamente todos os elementos envolvidos no processo. No entanto como este processo é transversal a toda a empresa, a sua divulgação deve abranger todos os funcionários, para que estes tomem conhecimentos das regras internas da empresa no que a este assunto diz respeito. Como suporte à criação de normas internas foi criado o *template* “Criação de normas internas” (Anexo 23), que servirá para registar a elaboração dos documentos, as suas revisões ao longo do tempo, departamento de origem, a data de divulgação, a entrada em vigor e a última actualização efectuada. É importante também, para além do seu conteúdo, sabermos quais os documentos que o actual regulamento revogou (caso existam), quem é o seu autor e as respectivas aprovações. Em suma, todo o histórico de revisões ao regulamento deve ser mantido.

5. Conclusões e trabalho futuro

Um plano de recuperação em caso de desastre pode significar a diferença entre sobreviver a um desastre e continuar a operar no mercado, ou não ter a capacidade de recuperar dele e sucumbir. O sucesso de um plano de recuperação em caso de desastre muito depende do resultado obtido com a recolha da informação necessária, da metodologia usada para a recolha da informação, da formação dos seus elementos, da comprovação do seu sucesso, através de testes e do programa de manutenção do mesmo.

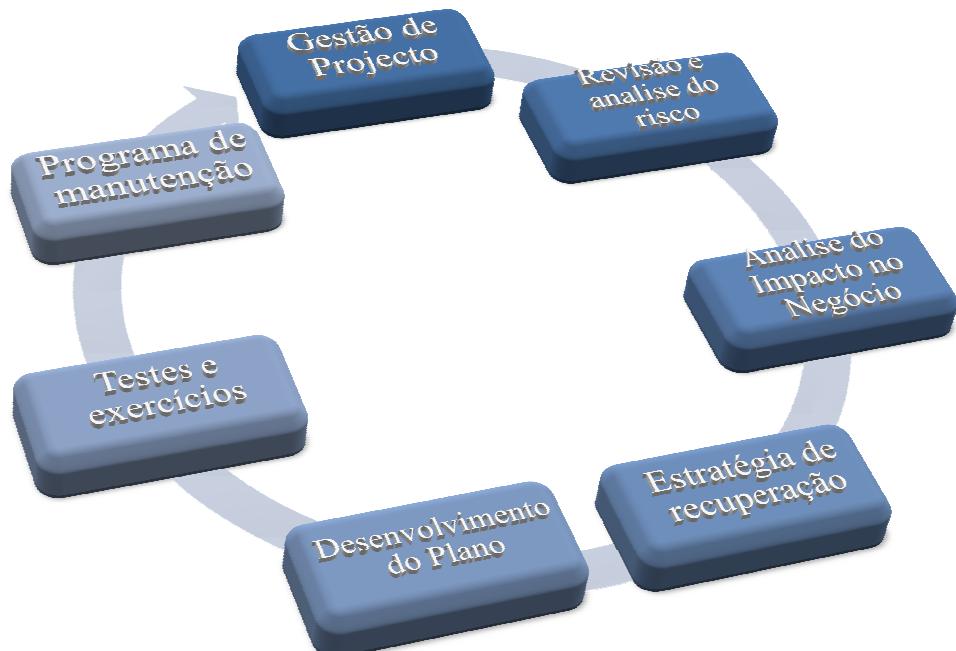
Em muito contribui também a documentação usada para recolher a informação (sem ela não existiriam as métricas e os referenciais) necessária para a eficaz recuperação dos sistemas de suporte às funções críticas. Deve-se planear e coordenar o plano, definir objectivos, políticas, directrizes, responsabilidades e exercitar as especificações indicadas no plano, validando-as através de testes periódicos. Dessa forma avalia-se a eficácia dos procedimentos e melhores práticas neles indicados. Durante a fase de testes,

é necessário estabelecer e coordenar os exercícios adequados, avaliando-os, para depois proceder à actualização do plano e informar a gestão executiva dos seus resultados.

No futuro, consideramos importante desenvolver uma base de dados com toda a informação obtida através dos *templates* agora criados. Esta base de dados pode servir para efectuar o cruzamento e tratamento dos dados recolhidos, podendo permitir a automatização do preenchimento de uma matriz de recuperação, de forma a optimizar a recuperação dos sistemas.

Criar mecanismos que possibilitem o preenchimento e actualização *online* dos formulários representados nos *templates* actuais, de forma a garantir que a informação disponível é a mais correcta possível, ficando também assim garantida a possibilidade de aceder à informação, em qualquer local, desde que consiga aceder à Internet.

Um plano de recuperação em caso de desastre tem um ciclo de vida típico (ilustrado pela figura 8) que pode ser utilizado como referencial para orientação das etapas base a percorrer ao longo da sua existência.



Fonte: Adaptado de *Business Continuity Management Institute*

Figura 8 - Ciclo de vida de um plano de disaster recovery

Bibliografia

ANACOM. (14 de Agosto de 2009). *Retenção de dados de acesso à Internet*. Obtido em 29 de Abril de 2010, de Web site da ANACOM: <http://www.anacom.pt/render.jsp?contentId=970264>

APSEI . (s.d.). *Síntese Normativa*. Obtido em 12 de Junho de 2010, de APSEI - Associação Portuguesa de Segurança Electrónica e de Protecção de Incêndio: <http://www.apsei.org.pt/index.php>

Association of Contingency Planners. (2007). *Welcome to ACP* . Obtido em 3 de Maio de 2010, de Web site de ACP - Association of Contingency Planners: <http://www.acp-international.com/>

Bakshi, S., & Rafeq, A. (2005). *Information Systems Control Journal*. Obtido em 7 de Julho de 2010, de Information Systems Audit and Control Association: <http://www.isaca.org/Journal/Past-Issues/2005/Volume-3/Documents/jpdf053-The-Asian-Tsunami.pdf>

Braiotta, L., Gazzaway, R., Colson, R., & Ramamoorti, S. (2010). *The Audit Committee Handbook* (5^a ed.). New Jersey: John Wiley & Sons, Inc.

Business Continuity Institute. (2010). *Página inicial do BCI - Business Continuity Institute*. Obtido em 2010 de Maio de 26, de Web site do BCI - Business Continuity Institute: <http://www.thebci.org/>

Business Continuity Management Institute. (13 de Novembro de 2008). *Disaster Recovery Glossary*. Obtido em 15 de Junho de 2010, de Web site da BCMpedia: <http://pt.bcmpedia.org>

Business Software Alliance. (Maio de 2006). *Terceiro Estudo Anual Global Sobre Pirataria*. Obtido em 29 de Abril de 2010, de BSA: <http://w3.bsa.org/portugal/resources/upload/BSA%20Portugal%202006%20IDC%20Whitepaper.pdf>

Casa dos Bits. (6 de Maio de 2010). *Empresas europeias não acautelam perda de dados*. Obtido em 7 de Maio de 2010, de Web site do TeK - Canal de Tecnologia do SAPO: <http://tek.sapo.pt>

Chen, K., Chu, D., Dutta, P., Kamil, A., & Mettler, A. (2005). *Core Systems Papers*. Obtido em 12 de Maio de 2010, de Web site de UC Berkeley: <https://www.cs.ucsb.edu>

Compute-rs.com. (s.d.). *Open Source Software Proprietário vs Software Livre? Dicas para Integração de Tecnologia*. Obtido em 2 de Maio de 2010, de <http://www.compute-rs.com/pt/conselho-835437.htm>

Comunidade ISMS Portugal. (2007). *Continuidade de Negócio*. Obtido em 20 de Maio de 2010, de Blog da Comunidade Portuguesa de Segurança da Informação: <http://www.ismspt.blogspot.com/>

data.backup-and-storage.com. (2010). *What Tape Backup Drives Solution Is Best For Your Computer or Network*. Obtido em 7 de Junho de 2010, de Web site de data.backup-and-storage.com: <http://www.data-backup-and-storage.com/tape-backup-drives.html>

Disaster Recovery Journal. (2009). *Página inicial do DRJ*. Obtido em 18 de Abril de 2010, de <http://www.drj.com/>

DRI International. (2010). *Home page do DRI - the Institute dor Continuity Management*. Obtido em 18 de Maio de 2010, de <https://www.drii.org/>

Fazio, A. (2010). *Backup e recuperação de desastre para a virtualização de servidores*. Obtido em 2 de Maio de 2010, de TechNet Magazine - Microsoft Corporation: <http://technet.microsoft.com/pt-br/magazine/2008.10.disasterr.aspx>

Gallagher, M. (2003). *Business Continuity Management “How to protect your company from danger”*. Harlow, UK: Prentice Hall.

Gartner, Inc. (2009). *The Aftermath: Disaster Recovery and Planning for the Future*. Obtido em 3 de Maio de 2010, de Web site da Gartner: http://www.gartner.com/5_about/news/disaster_recovery.html

Gestão Organizacional e Design, Lda. (2010). *ISO/IEC 27001:2005*. Obtido em 8 de Maio de 2010, de Web site de DQA: <http://www.dqa.pt/>

Global Continuity. (2010). *Home page de Global Continuity Group*. Obtido em 28 de Maio de 2010, de <http://www.globalcontinuity.com/>

Goldberg, R. P. (Junho de 1974). *Survey of Virtual Machine Research*. Obtido em 5 de Julho de 2010, de Honeywell Information Systems and harvard University: <https://www.cs.ucsb.edu/~ravenben/papers/coreos/Gol74.pdf>

Gonçalves, J. P. (2 de Novembro de 2009). Risk IT - Enterprise Risk: Identify, Govern and Manage IT Risk. *Cadernos de Gestão e Tecnologias de Informação* . (L. DecisionMaster - Sistemas de Informação e Suporte à Decisão, Ed.) Lisboa, Portugal.

Haletky, E. L. (18 de Março de 2010). *Virtualization's Disaster Plan*. Obtido em 29 de Abril de 2010, de Forbes.com LLC: <http://www.forbes.com/2010/03/18/virtualization-disaster-recovery-technology-haletky.html?boxes=Homepagechannels>

Hewlett-Packard Development Company, L.P. (2010). *O que é virtualização e o que ela pode fazer pela minha empresa?* Obtido em 29 de Abril de 2010, de HP.com Brasil: http://www.hp.com/latam/br/pyme/solucoes/apr_solucoes_01.html

IFRS Foundation. (2010). *Welcome to IFRS*. Obtido em 25 de Maio de 2010, de Web site de IFRS: <http://www.iasb.org/Home.htm>

Instituto de Meteorologia - Gabinete de Relações Externas. (7 de Outubro de 2003). *Dia internacional para redução dos desastres naturais*. Obtido em 12 de Maio de 2010, de Web site da Universidade de Coimbra: <http://student.dei.uc.pt>

Instituto de Meteorologia, IP. (2008). *Home page do Instituto de Meteorologia*. Obtido em 6 de Maio de 2010, de <http://www.meteo.pt/pt/>

Intel Corporation. (s.d.). *Virtualização*. Obtido em 29 de Abril de 2010, de Web site da INTEL: <http://www3.intel.com/portugues/technology/virtualization/index.htm>

International Data Corporation. (2010). *IDC*. Obtido em 6 de Maio de 2010, de Web site da IDC - International Data Corporation: <http://www.idc.com/>

International Organization for Standardization (ISO). (2010). *ISO*. Obtido em 3 de Junho de 2010, de Web site da International Organization for Standardization: <http://www.iso.org>

ISACA - Information Systems Audit and Control Association. (2006). *Conheça a ISACA*. Obtido em 8 de Maio de 2010, de Web site da ISACA: <http://www.isaca.org.br/novoportal/>

IT Governance Institute. (2007). CobiT 4.1. Illinois, USA.

LAKHANI, A. K. (9 de Maio de 2009). *Challenges Faced by Services Oriented Industries*. (GOOGLE, Ed.) Obtido em 10 de Abril de 2009, de Knol: <http://knol.google.com/k/cs-uet/challenges-faced-by-services-oriented/3rlivhv1qrg4y/1>

Linux Journal. (12 de Janeiro de 2006). *Xen Virtualization and Linux Clustering, Part 1*. Obtido em 5 de Julho de 2010, de Web site de Linux Journal: <http://www.linuxjournal.com/article/8812>

Micro Solutions. (s.d.). *More Data Recovery Informations*. Obtido em 2 de Abril de 2010, de Web site de Micro Solutions, Data Recovery Lab : <http://www.micro-solution.net/micro5.html>

Misturini, D. (Dezembro de 2005). *Alta Disponibilidade - Sua empresa disponível 24 horas todos os dias*. Obtido em 1 de Julho de 2010, de Tech Journal: http://www.tracesistemas.com.br/tech_journal/2005/dezembro/artigo_destaque.htm

National Institute of Standards and Technology. (10 de Maio de 2010). *Página inicial da NIST*. Obtido em 28 de Maio de 2010, de Web site da NIST: <http://www.nist.gov>

New Horizon I.T. Consulting, Inc. (2010). *Disaster Recovery*. Obtido em 35 de Maio de 2010, de New Horizon I.T. Consulting: <http://newhorizonitconsulting.com/disaster.htm>

Nogueira, M. D. (28 de Março de 2009). *Backup e Disaster Recovery para a virtualização de servidores*. Obtido em 3 de Junho de 2010, de <http://getvirtual.org/blogs/mdnoga>

Nolasco, J., & Bastos, P. (21 de Julho de 2000). *Backup e Arquivo - Conceitos e Fundamentos*. Obtido em 25 de Maio de 2010, de Info Imagem - Jornal da Gestão Electrónica de Imagens, Documentos e Processos: <http://www.dotecome.com/infoimagem/infoimagem/info28/28art6.htm>

O'Donnell, B. (Maio de 2007). *virtualization whitpaper by IDC*. Obtido em 5 de Julho de 2010, de Web site da Compaq: http://gem.compaq.com/gemstore/sites/k12/Q4t5735/pdfs/virtualization_whitpaper_by_idc.pdf

PAS56.Com. (2006). *A Business Continuity Management and Risk Management Guide*. Obtido em 20 de Abril de 2010, de Web site de PAS56.Com: <http://www.pas56.com/>

Pearson Education . (s.d.). *The World Trade Center Disaster: Who Was Prepared?* Obtido em 14 de Julho de 2010, de http://wps.prenhall.com/bp_laudon_essmis_6/21/5556/1422339.cw/content/index.

Sarbanes-Oxley. (2002). *A Guide To The Sarbanes-Oxley Act*. Obtido em 25 de Maio de 2010, de Web site de Sarbanes-Oxley: <http://www.soxlaw.com/>

Service Level Agreement Example, Presentation, Guide and Audit. PN. (2008). *The SLA Toolkit*. Obtido em 30 de Maio de 2010, de Web site de Service Level Agreement Example, Presentation, Guide and Audit. PN: <http://www.service-level-agreement.net/>

Snedaker, S. (2007). *Business Continuity and Disaster Recovery Planning for IT Professionals*. Burlington, Massachusetts, USA: Syngress Publishing, Inc.

Standards Direct. (s.d.). *Standards Direct - International Standards And Documentation*. Obtido em 22 de Maio de 2010, de Web site da Standards Direct - International Standards And Documentation: <http://17799.standardsdirect.org/>

The British Standards Institution. (2009). *Página inicial da BSI*. Obtido em 9 de Maio de 2010, de Web site de The British Standards Institution: <http://www.bsigroup.com/>

VMware, Inc. (2007). *Understanding Full Virtualization, Paravirtualization, and Hardware Assist*. Obtido em 3 de Junho de 2010, de Web site da VMware: http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

Wezards. (2010). *Porquê Opensource*. Obtido em 2 de Maio de 2010, de Web site da Wezards: <http://www.wezards.com/wezards/opensource/porque-opensource>

Wheatman, V. (21 de Setembro de 2001). Aftermath: Disaster Recovery. U.S.A.: Gartner, Inc.

Anexos

Informações pertinentes relativas aos anexos

Devido à necessidade de normalizar os documentos finais apresentados pelos templates em anexo, alguns deles, apresentam opções com vista à limitação das escolhas possíveis, ou como auxílio à inserção dos dados pelo utilizador, assim, alguns têm funcionalidades às quais não é possível aceder em formato “pdf”, para que possam ser visualizadas todas as opções, são fornecidos no CD que contém o trabalho, dentro do directório “templates”, todos os templates em formato “docx”. Sem prejuízo do atráis exposto, foram colocadas no *template* que possibilita opções, uma ilustração do seu funcionamento, é de salientar também que em todos os quadros em que é solicitado a inserção de data, esta pode ser inserida por escolha, tal como demonstrado na figura 9.

1 [Escreva o nome]	Click para colocar a data.	Click para colocar a data.	[Breve descrição do que está em contrato]
2 [Escreva o nome]	Click para colocar a data.	1 Click para colocar a data.	[Breve descrição do que está em contrato]
3 [Escreva o nome]	Click para colocar a data.	2 Julho 2010	[Breve descrição do que está em contrato]
4 [Escreva o nome]	Click para colocar a data.	S T Q Q S S D	[Breve descrição do que está em contrato]
5 [Escreva o nome]	Click para colocar a data.	28 29 30 1 2 3 4	[Breve descrição do que está em contrato]
6 [Escreva o nome]	Click para colocar a data.	5 6 7 8 9 10 11	[Breve descrição do que está em contrato]
7 [Escreva o nome]	Click para colocar a data.	12 13 14 15 16 17 18	[Breve descrição do que está em contrato]
8 [Escreva o nome]	Click para colocar a data.	19 20 21 22 23 24 25	[Breve descrição do que está em contrato]
		26 27 28 29 30 31 1	[Breve descrição do que está em contrato]
		2 3 4 5 6 7 8	[Breve descrição do que está em contrato]
		Hoje	[Breve descrição do que está em contrato]
			[Breve descrição do que está em contrato]

Figura 9 - Inserção de datas

Conforme também explicado no trabalho, foi também colocado no CD referido no parágrafo anterior, uma versão do trabalho em formato XHTML, que se encontra no directório “site_tfc”. Foi também criada uma pasta de nome “utilitários”, onde estão os utilitários necessários para a visualização dos documentos nele contidos¹.

¹Pode ser efectuado o download de versões actualizadas do Word Viewer em <http://www.microsoft.com/downloads/details.aspx?familyid=3657ce88-7cfa-457a-9aec-f4f827f20cac&displaylang=en> e do Adobe Acrobat reader em <http://get.adobe.com/br/reader/>.

Inventário de Servidores

Trabalho de Fim de Curso

Anexo 1

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Inventário de Computadores

Trabalho de Fim de Curso

Anexo 2

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

#	Nome do Computador	Sistema Operativo	Processador (Mhz)	Memória	Tipo (CS/P) ¹	Fabricante	Data de aquisição	Departamento	Localização	Função que suporta	Observações
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											
16											

¹ Legenda: CS – Computador de Secretária; P - Portátil

Inventário de Hardware de Comunicações

Trabalho de Fim de Curso

Anexo 3

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Inventário de Hardware de Telecomunicações

Trabalho de Fim de Curso

Anexo 4

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Inventário de Licenças

Trabalho de Fim de Curso

Anexo 5

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

#	Nome do Software	Qtd	Fabricante	Data de aquisição	Data de Inicio do contrato	Data de Fim do contrato	Nº do Contrato	Observações
1	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
2	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
3	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
4	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
5	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
6	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
7	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
8	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
9	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
10	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
11	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
12	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
13	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
14	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
15	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
16	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
17	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		
18	[Escreva o nome]			Colocar a data	Colocar a data	Colocar a data		

Inventário de Hardware

Trabalho de Fim de Curso

Anexo 6

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Inventário de Sistemas Críticos para o Negócio

Trabalho de Fim de Curso

Anexo 7

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Inventário de Aplicações

Trabalho de Fim de Curso

Anexo 8

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

#	Nome da aplicação	Servidor / Hardware de suporte	Funções Suportadas	Origem	RTO	RPO	Observações
1	[Escreva o nome]						
2	[Escreva o nome]						
3	[Escreva o nome]						
4	[Escreva o nome]						
5	[Escreva o nome]						
6	[Escreva o nome]						
7	[Escreva o nome]						
8	[Escreva o nome]						
9	[Escreva o nome]						
10	[Escreva o nome]						
11	[Escreva o nome]						
12	[Escreva o nome]						
13	[Escreva o nome]						
14	[Escreva o nome]						
15	[Escreva o nome]						
16	[Escreva o nome]						
17	[Escreva o nome]						
18	[Escreva o nome]						

Listas de Application Owner

Trabalho de Fim de Curso

Anexo 9

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

#	Nome da aplicação	Owner	Contacto	Iniciais	Área de Responsabilidade	Assinatura Valida
1	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
2	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
3	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
4	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
5	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
6	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
7	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
8	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
9	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
10	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
11	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
12	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
13	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
14	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
15	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
16	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
17	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	
18	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de Responsabilidade	

Este template contempla a seleção de opção na coluna Área de Responsabilidade, pode ser visto um exemplo na imagem da página seguinte

#	Nome da aplicação	Owner	Contacto	Iniciais	Área de Responsabilidade	Assinatura Valida
1	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	<input type="text"/> Escolha a área de Responsabilidade	
2	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Escolha a área de responsabilidade .	
3	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Recursos Humanos	
4	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Financeira	
5	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Contabilidade	
6	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Tesouraria	
7	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Cobranças	
8	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Informática	
9	[Escreva nome da aplicação]	[Escreva nome do Responsável]	Colocar Contacto	Colocar Iniciais	Comercial	
					Marketing	
					Pré-Venda	
					Serviços Gerais	
					Escolha a área de Responsabilidade	

Matriz para Recuperação de Software

Trabalho de Fim de Curso

Anexo 10

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Business Impact Analysis

Trabalho de Fim de Curso

Anexo 11

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

DESENVOLVIMENTO DE FLUXOS DE TRABALHO – Desenvolvimento de diagramas de fluxos de trabalho

O planeamento deve abordar as interdependências de fluxo de trabalho entre a função que está a ser analisada e outras unidades de negócios e/ou fontes externas. Através do desenvolvimento de fluxos de trabalho, a função e as suas dependências são representadas e documentadas. É altamente recomendável que desenvolva a função de negócios a um alto nível diagramas de fluxos para cada que seja identificada na secção A#2. Identificar todas as dependências grupos de dependências internas e externas e dependências de sistemas, adicionar páginas adicionais de acordo com o necessário para diagramas de fluxo de trabalho adicionais.

IDENTIFICAÇÃO DE DEPENDENCIAS

O responsável pelo preparação do plano deve identificar *inputs*, aplicativos e resultados para se assegurar de uma completa recuperação de processos de todas as funções de negócios e o fluxo de processo de negócio. Entradas para um processo de negócio são fontes de informações ou serviços recebidos das unidades de negócios internos (suporte para áreas – técnica, negócios), bem como parceiros de negócios externos (fornecedores – provedores de dados do mercado, impressoras) que são necessários para executar tarefas principais. Os *inputs* vêm numa variedade de formatos e exemplos incluem, mas não estão limitados a: Dados electrónicos, transmissão de relatórios, chamadas de telefone, email, fax, livros, fornecedores de medias magnéticas, microfichas, etc.

O responsável pela preparação do plano precisa identificar não só os aplicativos que aparentemente são necessários para o sucesso do desempenho das funções de negócios, mas também as aplicações que se alimentam nesses programas; Os responsáveis pela preparação podem achar necessário falar com application owners ou outro pessoal/fornecedores de aplicativos, para obter ajuda na identificação destas famílias de aplicativos.

Os resultados de um processo devem ser identificados – embora esses resultados possam não ser críticos para a unidade de negócios que os produziu, podem ser entradas críticas para outro processo ou função e devem, portanto, ser identificadas.

Após a identificação dos *inputs*, aplicativos e respectivos *outputs*, o responsável pela preparação do plano deve iniciar um diálogo com os responsáveis por essa informação para que compreendam qual é a importância do seu contributo para um processo crítico de negócio. Em alguns casos, o diálogo resultará num "upgrade" à criticidade da unidade de negócio que fornece um *input* ou aplicação; *outputs* não-críticos de uma

unidade de negócio podem tornar-se entradas que são essenciais para processos de outra unidade. Esta informação é importante na elaboração dos seus planos de continuidade de negócio. Esta informação irá delinear claramente como este negócio irá comunicar e interagir com grupos interdependentes durante uma interrupção do negócio.

ASSIGNAR RTOs e RPOs

RECOVERY TIME OBJECTIVES, (RTO)

O objectivo de tempo de recuperação (RTO), é o tempo máximo que uma função de negócio ou serviço poderá estar sem ser executada antes de afectar de forma significativa os objectivos gerais da empresa (Por exemplo, a quantidade de tempo que uma unidade de negócios pode sobreviver sem executar a sua função de negócio ou serviço). Se o objectivo de tempo de recuperação é dependente do tempo do mês ou ano (períodos de pico de processamento), deve basear-se os intervalos de tempo pela métrica mais vulnerável onde possa ocorrer uma interrupção do negócio. Depois de identificar o RTO do negócio, todos os aplicativos e dados de suporte são classificados por essa referência.

RECOVERY POINT OBJECTIVES, (RPO)

(Restauro da informação e ponto de sincronização)

O Recovery Point Objectives (RPO) identifica o ponto no processo de que uma actividade empresarial precisa de ser restaurada antes de afectar significativamente os negócios em geral. Identificar o RPO deve ser elaborado em conjunto com o RTO. Isso pode ser visto como a quantidade máxima de dados que podem ser perdidos pelo negócio isto é $\frac{1}{2}$ dia útil, um dia útil, etc. tal como na estratégia de backup e restauro de dados. É fundamental o RPO seja conhecido pelo negócio e seja aceitável para o negócio. Caso contrário, a estratégia de backup e restauração de dados deve ser reforçada para atender aos requisitos de negócios.

Business Impact Analysis

A. Informação Geral

Nome da Organização: [Colocar o nome da empresa]

Departamento: [Colocar o departamento]

Manager: [Colocar o nome do responsável] Alternativo: [Colocar o nome do substituto]

1. Headcounts por função

Manager: [Colocar o nº de managers]

Especialistas: [Colocar o nº de especialistas]

2. Funções chave do negócio e processos de suporte

Função chave do negócio: [Designar a função, ex.: Contabilidade]

Objectivos do negócio: [Designar o(s) objectivo(s) para a função]

Lista dos processos chave: [Lista com os processos chave da função, ex.: Reconciliações bancárias]

3. Impactos

Volume de transacções anuais: [Colocar valor]

Aproximado Impacto diário:[Colocar valor]

Meta anual de receitas [Colocar valor]

Aproximado Impacto diário: [Colocar valor]

B. Requisitos iniciais para a recuperação dos departamentos

1. Pessoas (Todas as funções)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
Full-time					
Part-time					
Temporário					
[Desriminar]					

2. Equipamento de secretária

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
Telefone(s)					
PC(s)					
[Desriminar]					
[Desriminar]					

3. Equipamento especial (Impressão de cheques, etc)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Designar equipamento]					
[Designar equipamentos]					
[Designar equipamentos]					
[Designar equipamentos]					

4. Registos Vitais (ficheiros em papel, set de backups, documentação de suporte, etc)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					

5. Sistemas (unidades de disco de patilha, unidades de armazenamento)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					
[Descreminar documentos e informação de suporte]					

6. Aplicações (MS Office, Aplicações cliente / Servidor) / Equipamento de secretária

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descriminar]					

7. Dependências internas (Outros departamentos)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descriminar]					

8. Dependências externas (Fornecedores, parceiros, etc.)

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descriminar]					

9. Resultados do departamento

	Ambiente corrente	0 – 24 horas imediatas	2- 3 dias até 72 horas	4- 5 dias mesma semana	> 6 dias duas semanas
[Descriñinar]					

C. Impactos operacionais

<< Se uma ameaça parar as operações neste departamento, quão rapidamente afectará ela os pontos de a. até h. Coloque um X na coluna apropriada abaixo - menos de 1 dia, 1 a 2 dias, 3 a 5 dias 2 semanas, 3 a 4 semanas. Deixe em branco se não houver nenhum impacto para cada item de linha.>>

JUSTIFICAR OS IMPACTOS OPERACIONAIS DE CIMA

OBSERVAÇÕES

RESUMO DA RECUPERAÇÃO DE NEGÓCIO RTOs e RPOs – em ordem dos RTOs

Para as funções e processos identificados na secção A questão #2

Função de negócio ou serviço	RTO / RPO	Função de negócio ou serviço	RTO / RPO
[Descriminar]	/	[Descriminar]	/
[Descriminar]	/	[Descriminar]	/
[Descriminar]	/	[Descriminar]	/

DIAGRAMAS DE FLUXO DE PROCESSO DE ALTO NÍVEL

Listagem de Contratos

Trabalho de Fim de Curso

Anexo 12

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Listagem de Fornecedores

Trabalho de Fim de Curso

Anexo 13

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Listas de Níveis de SLA

Trabalho de Fim de Curso

Anexo 14

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

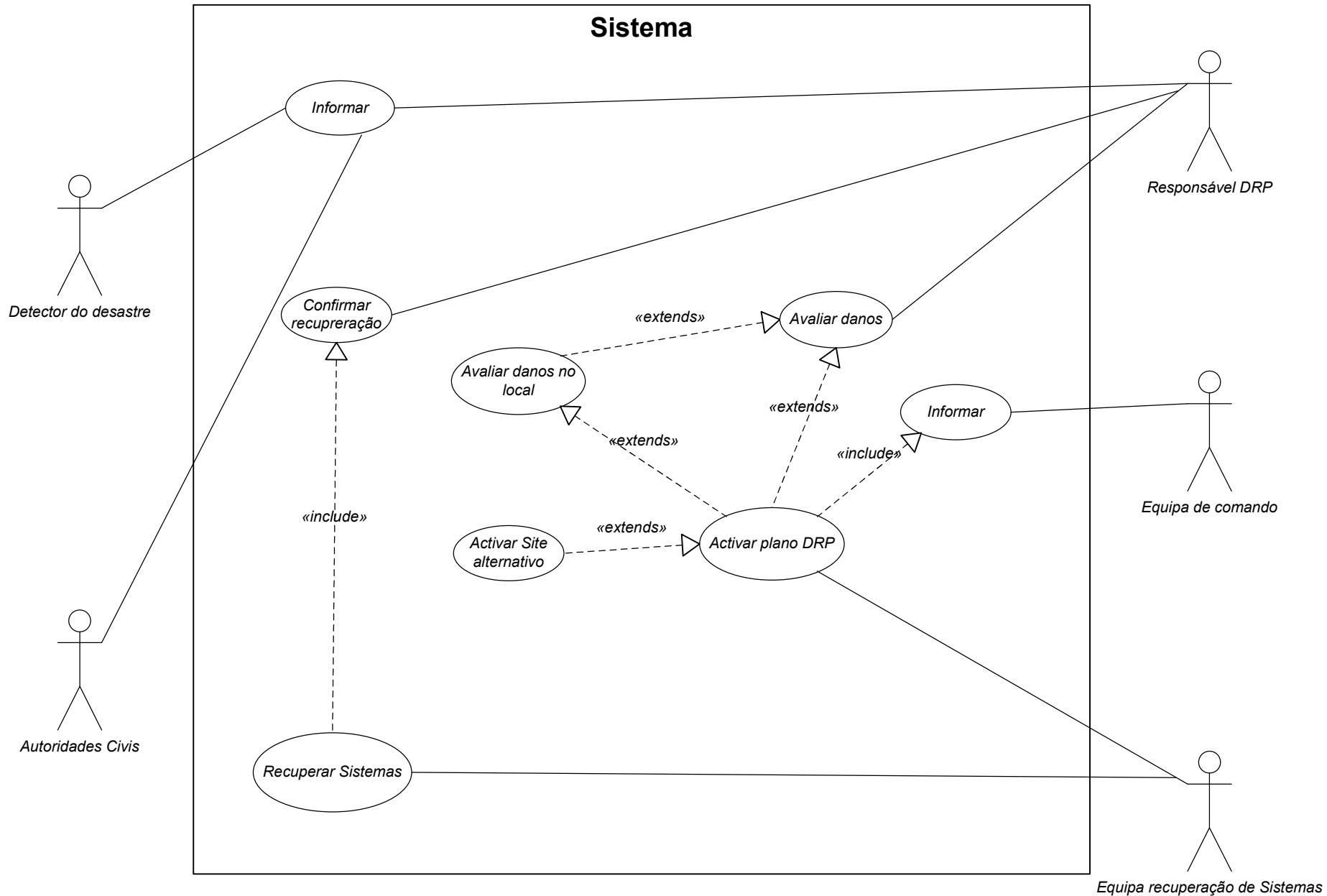
Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]



Notas:

Disciplina:

Trabalho de fim de curso

Tema: – DRP – Desastre Natural

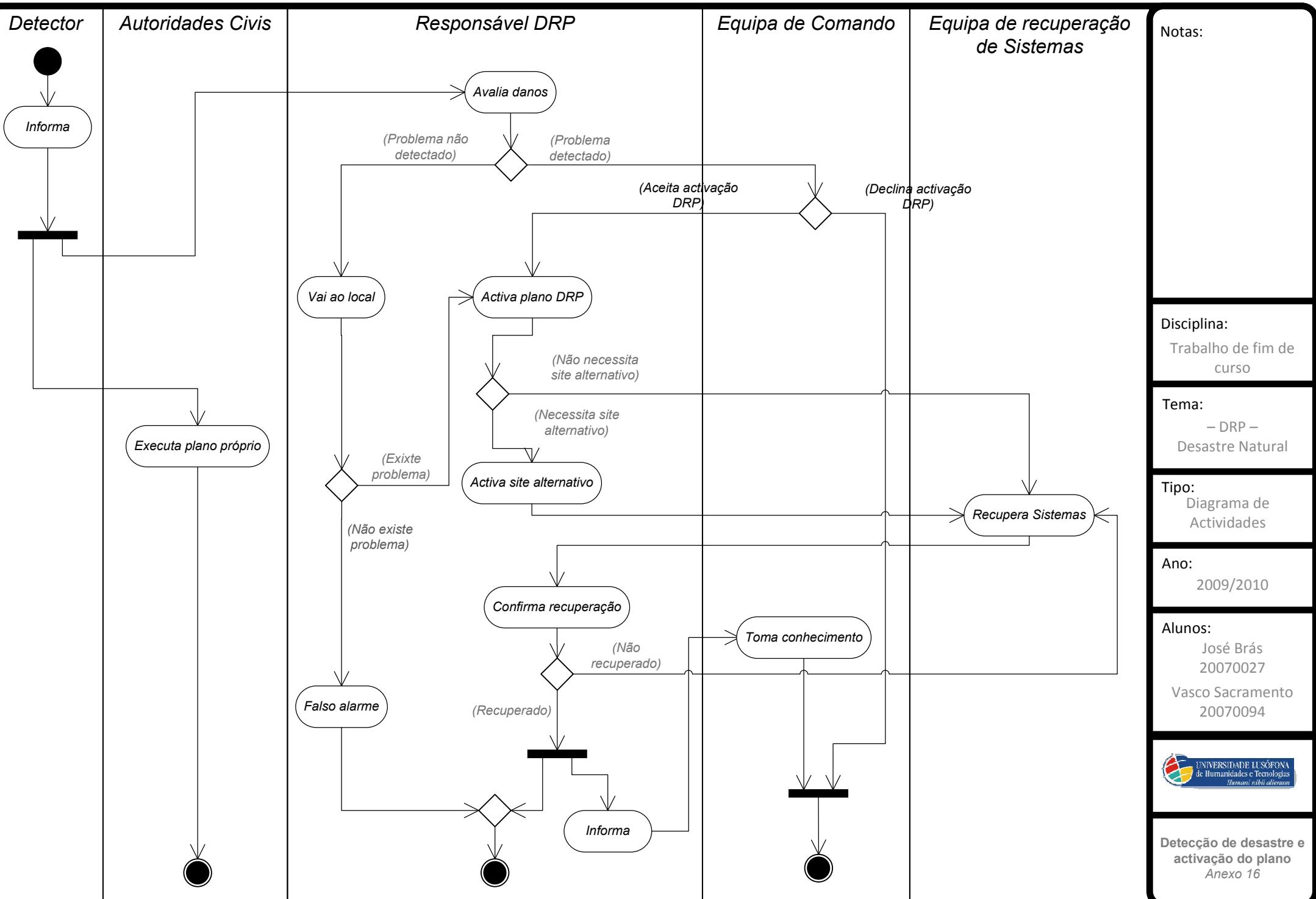
Diagrama de Use Case

Ano:
2009/2010

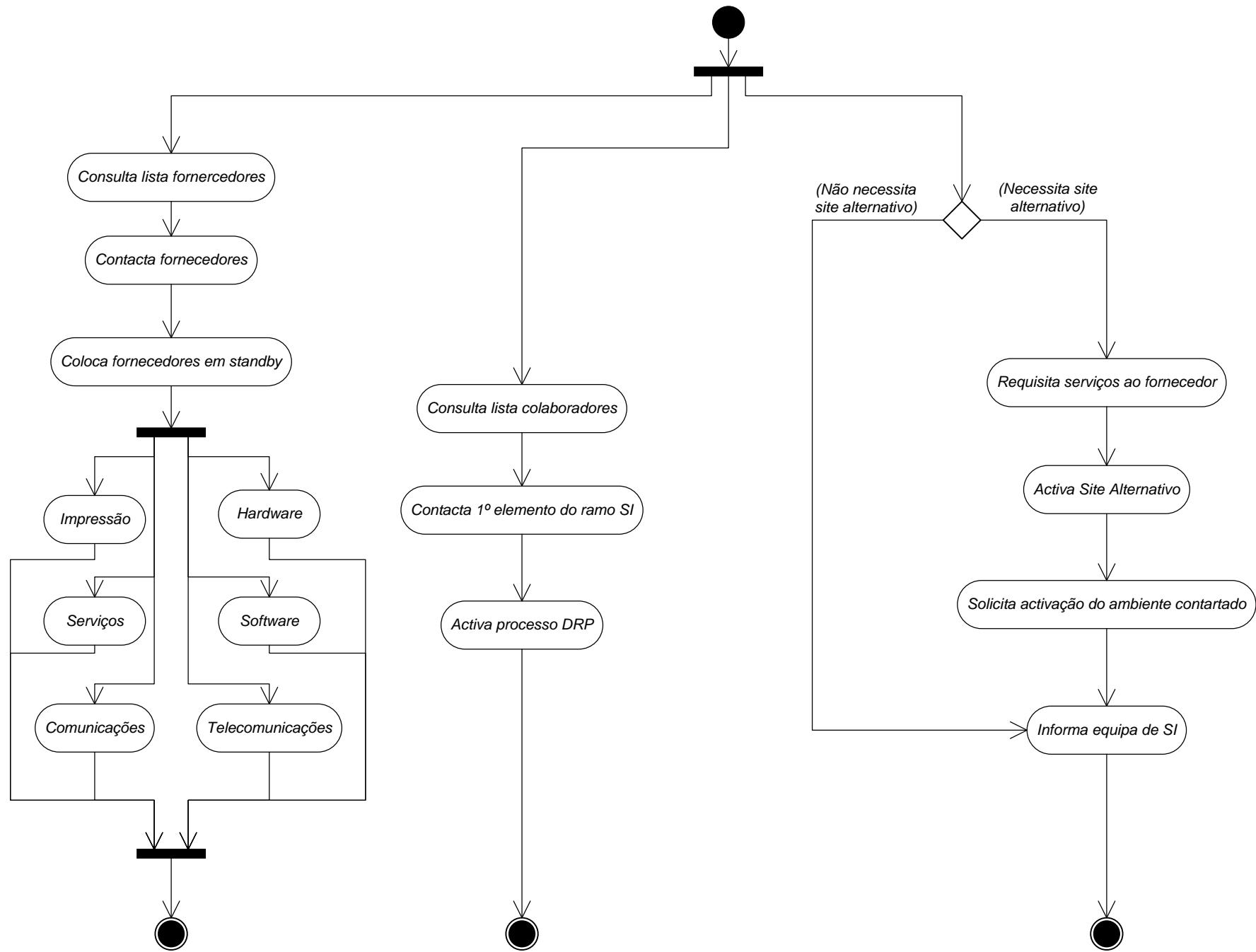
Alunos:
José Brás
20070027
Vasco Sacramento
20070094



Casos de uso
Anexo 15



Notas:



Disciplina:
Trabalho de fim de
curso

Tema:
– DRP –
Desastre Natural

Tipo:
Diagrama de
Actividades

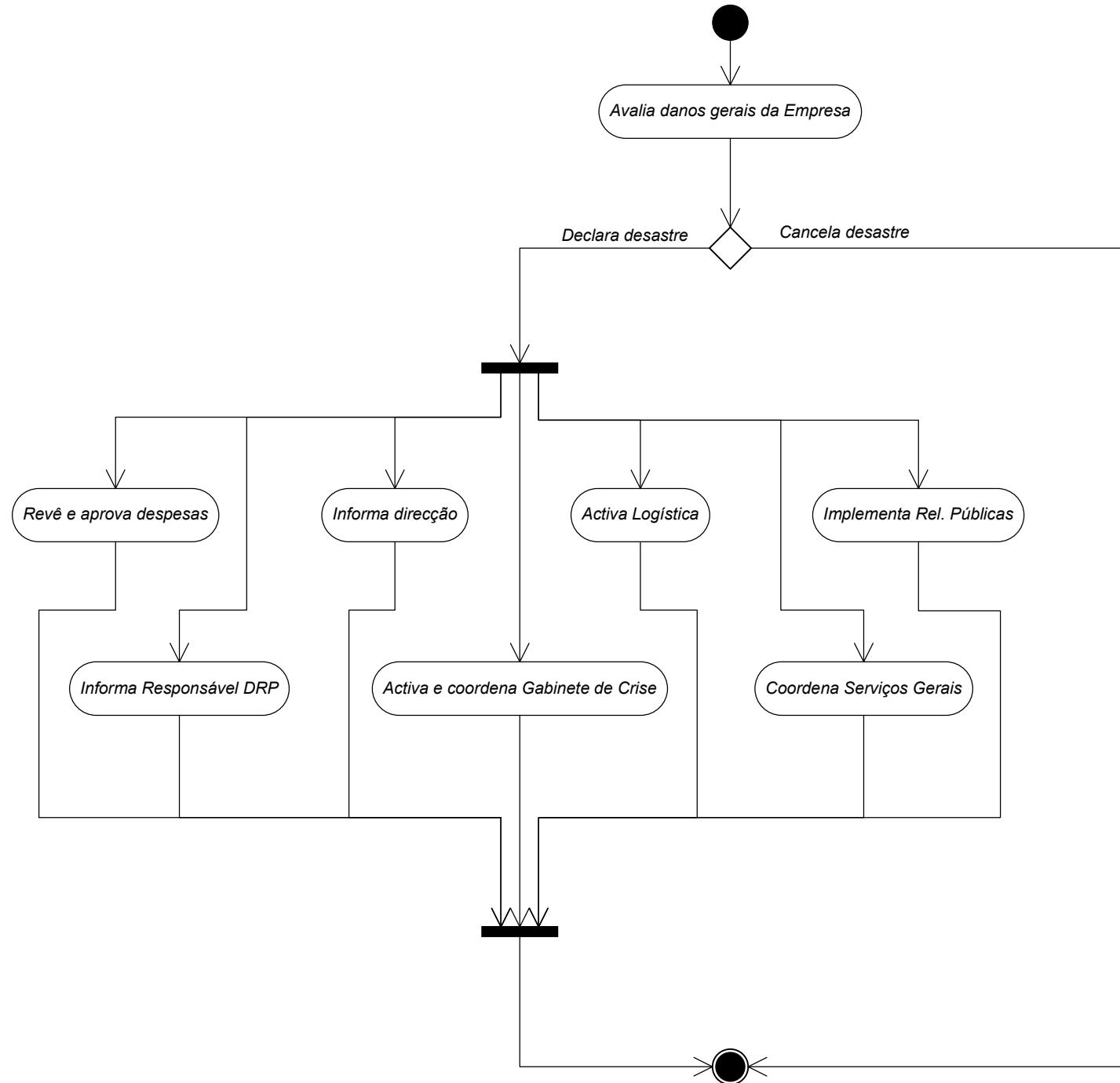
Ano:
2009/2010

Alunos:
José Brás
20070027
Vasco Sacramento
20070094



Sequências lógicas
após declaração de
desastre
Anexo 17

Notas:



Disciplina:
Trabalho de fim de
curso

Tema:
– DRP –
Desastre Natural

Tipo:
Diagrama de
Actividades

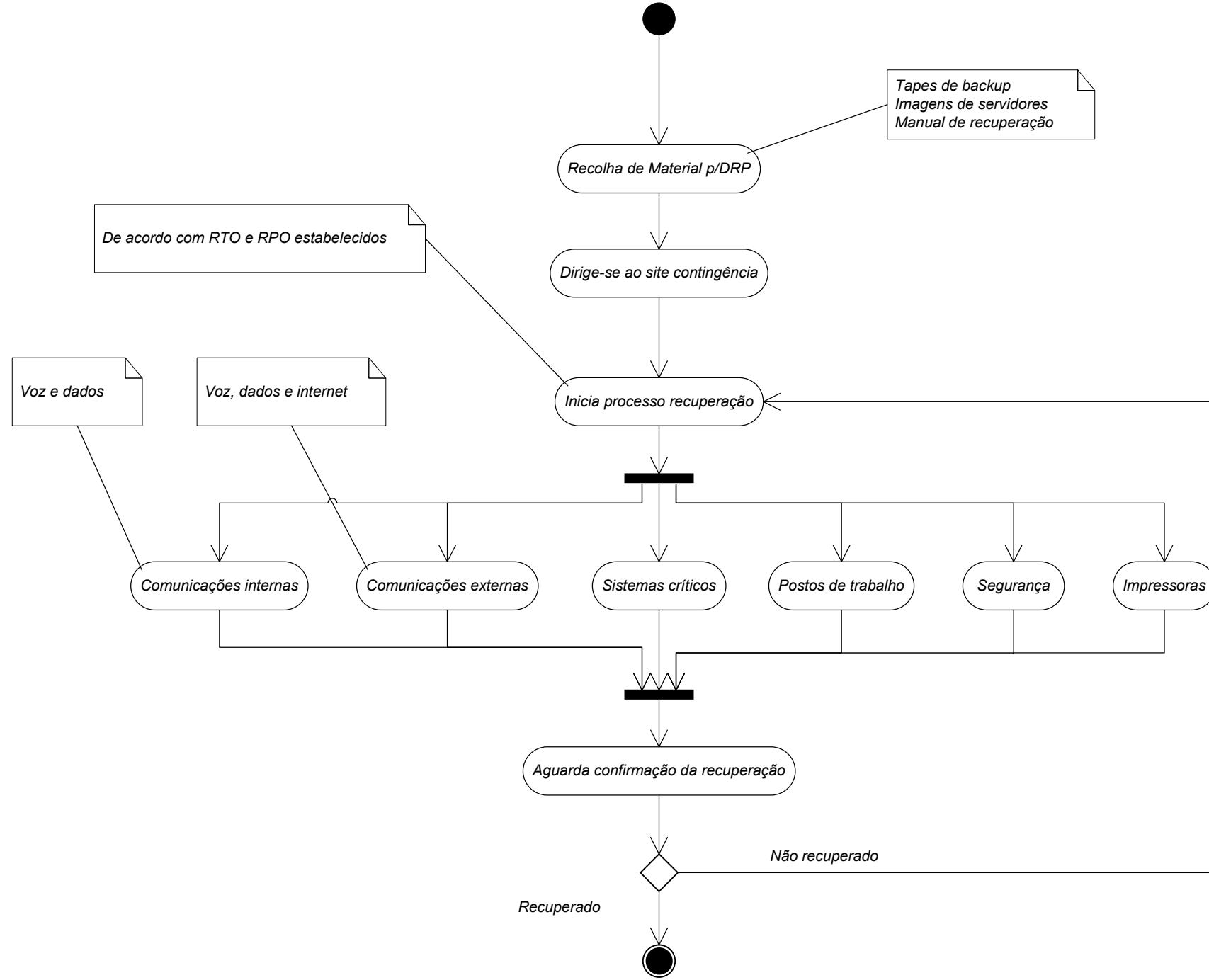
Ano:
2009/2010

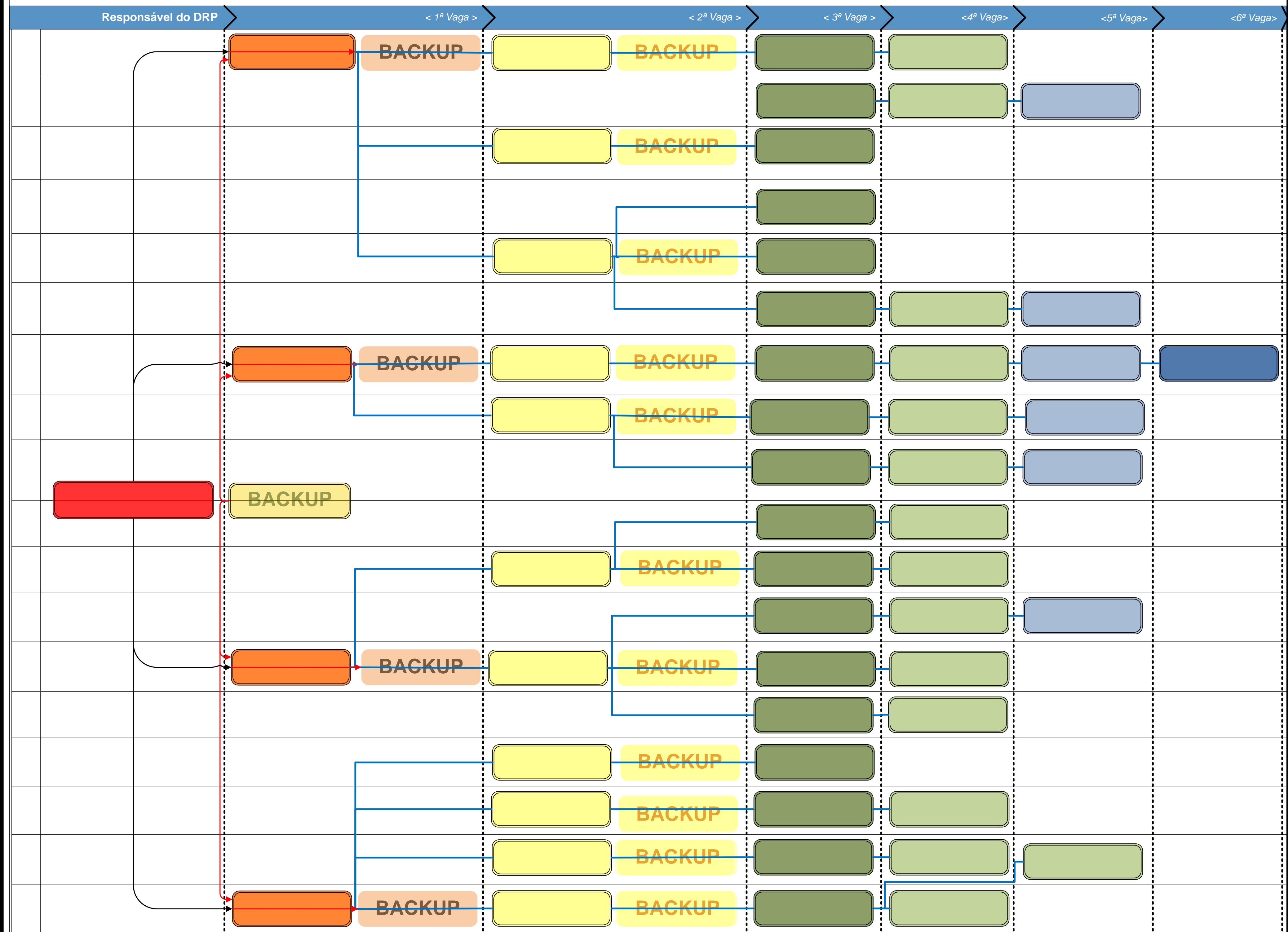
Alunos:
José Brás
20070027
Vasco Sacramento
20070094



Actividades da Equipa
de comando
Anexo 18

Notas:





Anotações:

Disciplina:

Trabalho de fim de curso

Tema:

– DRP –

Desastre Natural

Ano:

Alunos:

20070027
Vasco Sacramento
20070094



Árvore de Chamada

Anexo 20

Relatório de Exercício de Testes

Trabalho de Fim de Curso

Anexo 21

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Sumário

- Os testes tiveram lugar *colocar local* em *colocar Cidade* no dia Clicar para colocar a data., tendo os mesmos sido efectuados por xx colaboradores;
- Em termos gerais, a avaliação do exercício é *colocar avaliação geral*:
 - Todos os testes das restantes áreas atingiram/não atingiram os objectivos principais;
 - Todo o desenrolar do exercício foi documentado *colocar a forma como foi documentado*
- Para o próximo exercício, as principais recomendações são:
 - *colocar recomendações*

Processos chave & Pessoas envolvidas

#	Processo	Nome	Departamento
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Resultados do exercício

Aspectos positivos

Aspectos a melhorar

Resumo e Validação do Exercício

Trabalho de Fim de Curso

Anexo 22

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Tema: [Escreva texto]

Objectivo: [Escreva texto]

Entidades envolvidas: [Escreva texto]

Participantes: [Escreva texto]

Data da última actualização: [Clicar para colocar a data]

Resumo

A ser preenchido pelo Responsável da Equipa

A fim de dar como terminado o exercício de **DRP**, cada equipa envolvida no exercício, terá de preencher este formulário de resumo e validação. Esta ficha tem dupla funcionalidade, em primeiro lugar registar os resultados deste exercício e em segundo lugar identificar o actual restabelecimento da unidade de negócio. Ambas as respostas são exigidas a fim de serem revistas pela Direcção, Departamento de Auditoria e, em algumas organizações, por agências reguladoras.

Por favor escolha O QUE se aplica:

No geral, o exercício alcançou TODOS os objectivos principais.	<input type="checkbox"/>
No geral, o exercício alcançou NA GRANDE MAIORIA os objectivos principais.	<input type="checkbox"/>
No geral, POCOS objectivos principais foram alcançados.	<input type="checkbox"/>

Os objectivos específicos abaixo indicados necessitam de ser novamente testados no próximo exercício.

1	
2	
3	
4	

(Recomendações / sugestões de modificação de testes)

Validação

Por favor complete o seguinte:

O exercício de recuperação de desastre de hoje demonstrou, para o caso de surgir um eventual incidente/desastre nas instalações primárias, os recursos críticos e de suporte, necessários à retoma da actividade e dar continuidade às operações de negócio são suficientes e satisfatórios.

ESTÃO assegurados.

NÃO ESTÃO assegurados.

Por favor explique:

Assinatura:

Data: Clicar para inserir data.

Nome legível

Titulo:

Assinatura Responsável do negócio:

Data: Clicar para inserir data.

Nome legível

Titulo:

Criação de Normas Internas

Trabalho de Fim de Curso

Anexo 23

2009/2010

José Brás 20070027

Vasco Sacramento 20070094

Informática de Gestão

Assunto: [Escreva texto]

Objectivo: [Escreva texto]

Departamento de origem: [Escreva texto]

Participantes: [Escreva texto]

Área: [Escreva texto]

Divulgação: Clicar para inserir data.

Entrada em vigor: Clicar para inserir data.

Data da última actualização: Clicar para inserir data.

Revisões

Versão	Comentário	Data
		Clicar para inserir data.
		Clicar para inserir data.
		Clicar para inserir data.

Descrição

[Escreva texto]

Índice

[Escreva texto]

Texto

[Escreva texto]

Revogações

[Escreva texto]

Certificação

	Elaboração:	Revisão:	Aprovação:
[Colocar nome]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Colocar nome]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
[Colocar nome]	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>