Administração de Sistemas (ASIST)

Recuperação em Caso de Desastre (“disaster recovery”).
Plano de Continuidade de Negócio (BCP).

Outubro de 2014

Recuperação em Caso de Desastre ("disaster recovery")

Perante a ocorrência de uma falha deve iniciar-se um processo de recuperação da mesma (mesmo que se trate de um componente de um sistema redundante).

A expressão "recuperação em caso de desastre" está mais vocacionada para eventos de grande impacto que incluem desastres naturais catastróficos com possível destruição física quase total.

A "recuperação em caso de desastre" é fundamental para a "continuidade de negócio", o grande objetivo é reduzir ao máximo o tempo de paragem e eventuais perdas de dados.

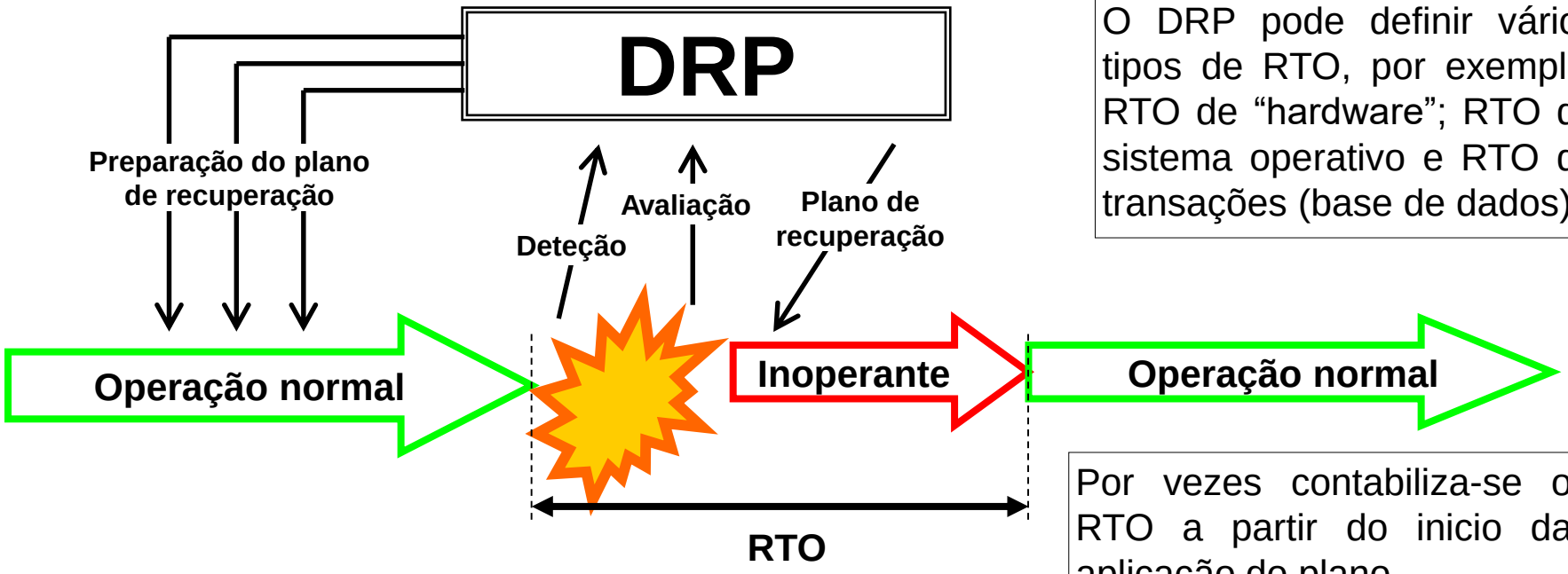
A "recuperação em caso de desastre" tem tudo a ver com preparação e planeamento:

- "mirroring" para local remoto
- "backups" regulares armazenados em local remoto
- "harware" de reserva armazenado em local remoto
- cenários de desastre e respectivos planos de recuperação

Plano de Recuperação de Desastre
(DRP – “Disaster Recovery Plan”)

O objetivo do DRP é reduzir ao máximo o tempo de paragem e perdas de dados em caso de desastre.

O DRP define cenários de desastre e os procedimentos de recuperação para cada um deles, com um determinado RTO (“Recovery Time Objective”).



O DRP pode definir vários tipos de RTO, por exemplo: RTO de “hardware”; RTO de sistema operativo e RTO de transações (base de dados).

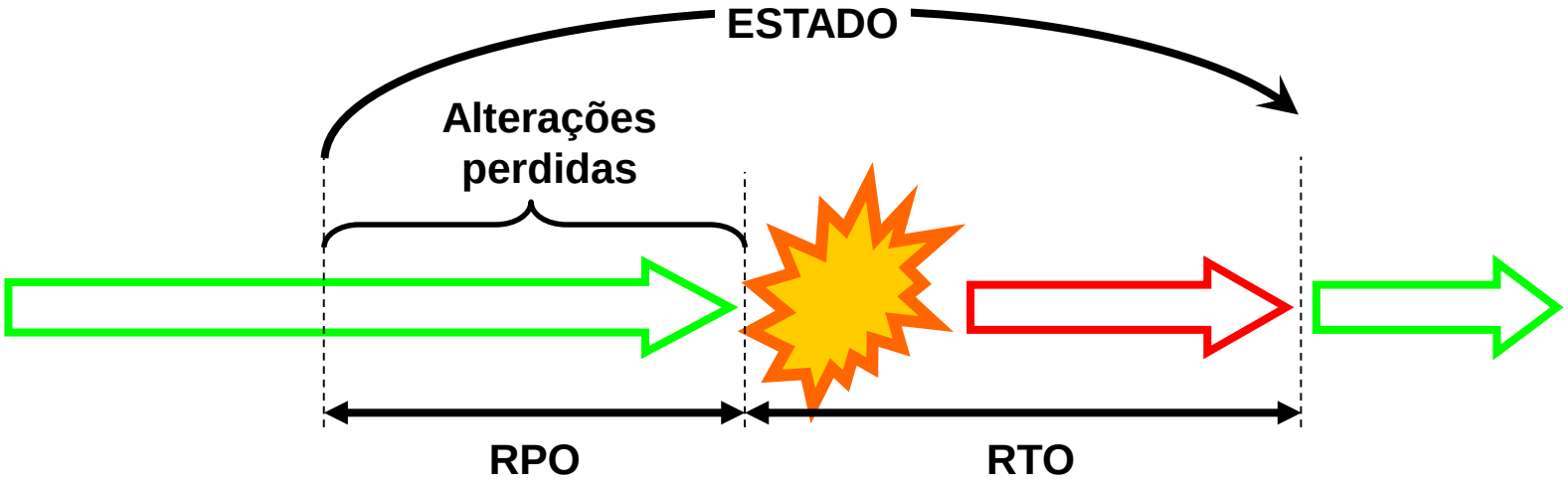
Por vezes contabiliza-se o RTO a partir do inicio da aplicação do plano.

RPO – “Recovery Point Objective”

Para serviços onde é admissível a perda de dados em caso de desastre, o RPO especifica a quantidade máxima de dados que se podem perder.

O RPO especifica um tempo de operação antes do desastre em que todas as alterações realizadas vão ser perdidas.

A periodicidade das cópias de segurança (“backup”) nunca pode ser superior ao RPO. Se for usado “mirroring” o RPO é nulo ou muito próximo de zero.



Plano de Continuidade de Negócio

(BCP – “business continuity plan”)

O BCP tem como objectivo definir um conjunto de condições e procedimentos que visam garantir a continuidade do negócio.

O DRP é um dos elementos mais importantes do BCP (por vezes confundem-se), mas o BCP é mais abrangente.

Plano de Continuidade de Negócio (BCP)

- Prevenção de falhas (“fault avoidance”)
- Tolerância a falhas (“fault tolerance”)
- Plano de Recuperação de Desastre (DRP)
- Equipa técnica, papeis, responsabilidades e autoridade.

Desenvolvimento do BCP

1 - Análise

- Business Impact Analysis (BIA)
- Threat and Risk Analysis (TRA)
- Cenários de impacto

2 - Desenvolvimento da solução

Encontrar a solução de continuidade mais económica que satisfaz os requisitos determinados na fase de análise. Por exemplo valores de RTO e RPO.

3 - Implementação

Colocar em prática as medidas definidas na solução de continuidade.

4 – Testes e exercícios

Testar procedimentos, por exemplo procedimentos de recuperação

5 – Manutenção

Actualização de acordo com novas realidades. Testes e exercícios periódicos.

Certificação do BCP

Existem vários “standards” para a elaboração do BCP, a sua utilização possibilita a certificação externa que é um elemento de valorização importante para a organização, atestando a solidez da solução.

O “standard” mais recente é o ISO22301, o BS 25999-2 (UK) é ainda bastante utilizado. Outros países como Estados Unidos e Austrália possuem “standards” próprios.

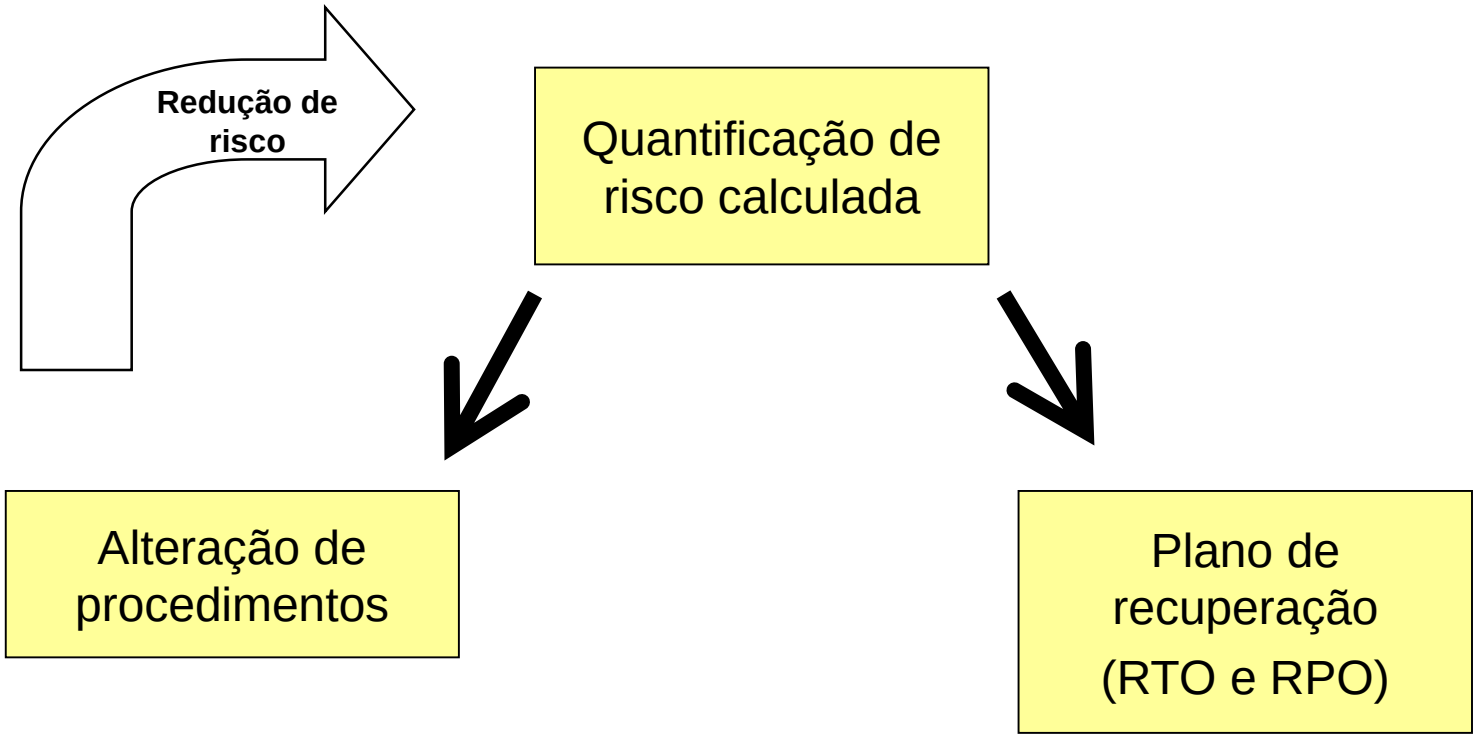
O BCP envolve aspectos fora do âmbito da administração de sistemas informáticos, por exemplo na área da gestão de pessoal e outros aspectos da gestão do negócio.

A fase de análise de riscos e cenários de impacto do BCP é de importância fundamental, nela devem ser identificados os processos críticos para o negocio que devem ser tratados com maior prioridade, destacando os potenciais SPOF.

De acordo com o carácter mais ou menos crítico de cada processo, serão definidos os valores de RTO e RPO contrabalançados com os custos para a sua obtenção.

Análise de risco (“Risk Assessment”)

A análise de risco pode ser feita com recurso a formulários/inquéritos que através da quantificação de um conjunto de parâmetros permite obter uma quantificação abstrata do risco no domínio em análise.



Análise de risco – matriz de risco

A análise de risco numa infra-estrutura informática deve ser levada ao ponto de se abordar falhas em elementos críticos do mesmo. É necessário considerar não apenas o impacto negativo da falha no componente, mas também a probabilidade de ela ocorrer:

RISCO = IMPACTO x PROBABILIDADE

Para quantificar o risco calculado desta forma IMPACTO e PROBABILIDADE são normalmente classificados com valores de 1 a 5.

	Impacto				
Probabilidade	**1**	**2**	**3**	**4**	**5**
5	**5 (baixo)**	**10 (médio)**	**15 (alto)**	**20 (muito alto)**	**25 (muito alto)**
4	**4 (baixo)**	**8 (médio)**	**12 (alto)**	**16 (alto)**	**20 (muito alto)**
3	**3 (baixo)**	**6 (médio)**	**9 (médio)**	**12 (alto)**	**15 (alto)**
2	**2 (baixo)**	**4 (baixo)**	**6 (médio)**	**8 (médio)**	**10 (médio)**
1	**1 (baixo)**	**2 (baixo)**	**3 (baixo)**	**4 (baixo)**	**5 (baixo)**

Os valores de RTO e RPO devem ser ajustados ao nível de risco determinado.

Plano de contingência (“contingency plan”)

AKA: Plano B

O plano de contingência é uma parte importante do BCP, define metodologias alternativas para manter o negócio em funcionamento quando os recursos “normais” ficam indisponíveis.

Nas organizações actuais, altamente dependentes dos sistemas informáticos pode ser difícil de implementar.

Deve definir:

- Que tipo de desastre deve levar ao arranque do plano de contingência.
- Definir os passos exactos para ser posto em prática.
- Definir necessidades em termos de pessoal e materiais ou equipamentos.
- Que procedimentos “normais” estão previstos no plano de contingência e quais os que ficarão indisponíveis (restrições ao funcionamento do negócio).
- De que forma os procedimentos realizados durante o plano de contingência vão ser integrados no sistema após a sua recuperação.

Plano de “backup/restore” - RPO

As cópias de segurança são um elemento importante do DRP, podem ser usadas sempre que o RTO e RPO não são muito exigentes. Para exigências maiores é necessário recorrer a “mirroring” que não é mais do que uma cópia de segurança permanentemente sincronizada com o original.

A cópia de segurança permite que após um desastre com perda de dados ou configurações de software seja possível recriar um sistema com estado idêntico à data em que foi realizada a última cópia.

Ao planear a periodicidade da realização das cópias de segurança fica definido o RPO máximo. A periodicidade da realização das cópias de segurança deve depender da frequência das alterações dos dados e por isso deverá ser ajustada de forma conveniente a cada elemento da infra-estrutura.

A hora exacta da realização das cópias de segurança deve ajustar-se ao horário de funcionamento do negócio. Para cópias diárias, geralmente o horário após expediente é o mais adequado.

Plano de “backup/restore” - RTO

A escolha dos meios de armazenamento para as cópias de segurança afecta o RTO, por razões económicas opta-se muitas vezes por meios de armazenamento de acesso lento. Esta opção afecta o tempo necessário para a reposição dos dados (“restore”), aumentando o RTO.

Atualmente estão disponíveis discos de elevada capacidade a baixo custo, sempre que possível esta solução deve ser preferida em detrimento de soluções mais tradicionais do tipo fita magnética de acesso muito lento.

Esses meios mais lentos são mais adequados para cópias de arquivo do que cópias de segurança.

Os meios de armazenamento lentos colocam problemas também durante a realização de cópias tornando a operação mais demorada. As operações de “backup” podem ter impacto na disponibilidade dos sistemas. Normalmente os objectos como ficheiros têm de ser bloqueados para evitar que sejam realizadas alterações sobre os mesmos durante a cópia.

Plano de “backup/restore”

Uma forma de reduzir a duração das operações de cópia é recorrer a cópias incrementais ou cópias diferenciais. Em qualquer dos casos o ponto de partida é sempre uma cópia integral.

Uma cópia incremental contém os dados que foram alterados desde a cópia incremental anterior (ou cópia integral se for a primeira).

Uma cópia diferencial contém os dados que foram alterados desde última cópia integral.

Estas técnicas, além de reduzirem a duração do processo de “backup” reduzem também o espaço de armazenamento necessário.

A sua utilização tem a importante desvantagem de tornar a reposição dos dados mais lenta, em especial para a variante incremental.

Além da reposição da cópia integral é necessário de seguida efectuar a reposição sucessiva das várias cópias incrementais ou a reposição da uma única cópia diferencial.

Plano de “backup/restore”

O ciclo de criação de cópias incrementais ou diferenciais deve ser limitado e interrompido periodicamente por uma nova cópia integral, caso contrário os efeitos são:

- cópias incrementais: um grande número de cópias incrementais tem de ser mantido, além do espaço ocupado a operação de reposição torna-se muito morosa.
- cópias diferenciais: o volume da cópia diferencial vai crescendo à medida que se vão acumulando alterações relativamente à cópia integral.

Novamente aqui os horários de negócio devem ser respeitados, muitas vezes a opção é a realização de uma cópia integral ao domingo e cópias incrementais ou diferenciais durante os outros dias da semana.

Uma cópia de segurança nunca deve ser eliminada sem estar concluída com sucesso a cópia de segurança seguinte, pelo contrário é desejável manter pelo menos uma cópia anterior, muitas vezes opta-se por manter várias.

A cópia de segurança anterior pode ser movida para um meio de armazenamento mais económico antes de realização de uma nova cópia.

Plano de “backup/restore”

Sendo o objectivo da cópia de segurança a recuperação em caso de desastre, não podemos correr o risco de a perder num mesmo desastre que afecte o original.

Embora a cópia de segurança possa sem mantida no local, encerrada num cofre à prova de fogo, o ideal é que se encontre num local geográfico distinto (off-site).

É possível realizar localmente a cópia de segurança e de seguida transportar a mesma para local remoto, mas não é a solução mais cómoda. Além disso para efeitos de reposição seria necessário aguardar pelo transporte em percurso inverso.

O ideal é realizar a cópia através da rede, por exemplo directamente entre duas SAN de dois CPD da organização. Uma alternativa mais económica é contratar um dos muitos serviços de “backup” “online” disponíveis.

Existem alguns inconvenientes:

- Segurança: é necessário assegurar a autenticação confidencialidade (ex.: VPN).
- Velocidade de acesso: afecta o tempo necessário para a cópia e o RTO.
- Fiabilidade: só é possível a recuperação se a ligação de rede estive operacional.

Categorias de Continuidade de Negócio

De acordo com as técnicas usadas e consequentes valores de RTO, as soluções de "disaster recovery" são classificadas em 7 categorias ou níveis ("tiers"):

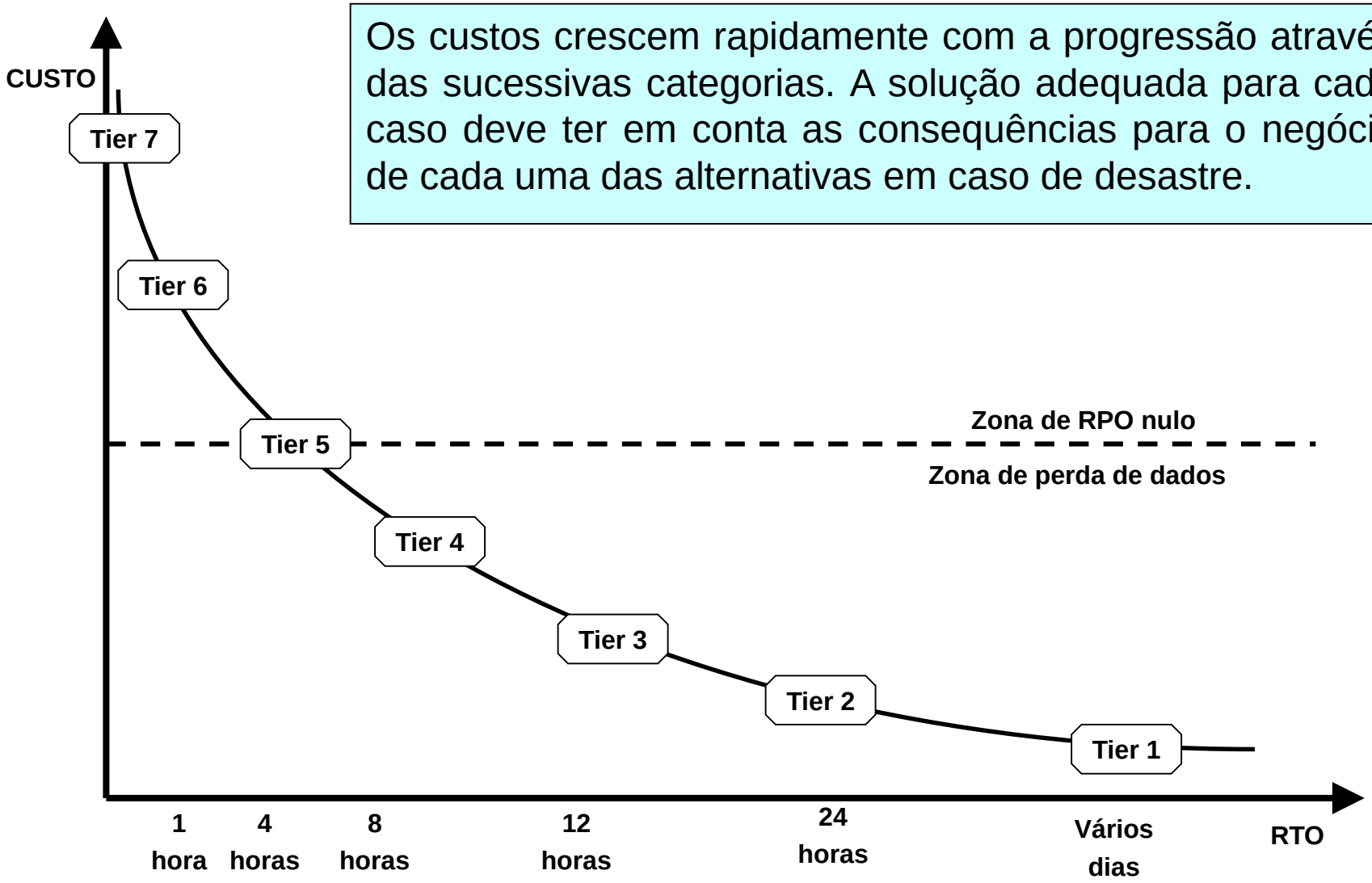
Tier 1: Data backup with no hot site
Tier 2: Data backup with a hot site
Tier 3: Electronic vaulting
Tier 4: Point-in-time copies
Tier 5: Transaction integrity
Tier 6: Near-zero data loss
Tier 7: Highly automated, business integrated solution

Categoria	Carateristicas	RTO (horas)	RPO (horas)
Tier 7	"tier 6", com arranque automático do "harware" alternativo	< 2	0
Tier 6	"tier 5", com "mirror" de discos	1 a 6	0
Tier 5	"tier 4", com "mirror" de base de dados (integridade de transações)	4 a 8	0 (*)
Tier 4	"tier 3", com cópias mais frequentes e rápidas em disco	6 a 12	4 a 8
Tier 3	"tier 2", com cópias de segurança realizadas "on-line"	12 a 24	6 a 12
Tier 2	"tier 1", com "hardware" alternativo "off-site"	> 24	12 a 24
Tier 1	Cópias de segurança "off-site"; sem "hardware" alternativo	> 48	> 48
"Tier 0"	"Não há DRP"		

(*) – apenas para a base de dados

Categorias de Continuidade de Negócio - Custo

Os custos crescem rapidamente com a progressão através das sucessivas categorias. A solução adequada para cada caso deve ter em conta as consequências para o negócio de cada uma das alternativas em caso de desastre.



Política de segurança

A “Política de segurança” é um documento que estabelece um conjunto de regras obrigatórias visando a proteção da infra estrutura e dados.

É um elemento importante para assegurar a continuidade de negócio, em especial no domínio da prevenção de falhas.

A “Política de segurança” deve ser mais abstrata do que um manual de utilização, deve indicar “o que não se pode fazer”, “o que se pode fazer”, mas não deve incluir o “como fazer”.

Por motivos de segurança e de forma a facilitar a sua adaptação à evolução da organização, não deve conter aspectos técnicos da implementação.

A “Política de segurança” deve concisa, de fácil leitura e interpretação, sugere-se a utilização dos 5 Ws do jornalismo: Who, What, Where, When, Why

O caráter mais ou menos restritivo da “Política de segurança” deve resultar de uma avaliação prévia do potencial de risco de segurança.

Através de questionários sobre a organização / negócio e respectiva infra-estrutura, é possível quantificar um nível de risco de ataque.

Política de segurança – caraterísticas

- documento público, facilmente acessível a todos os utilizadores
- de leitura obrigatória para todos os utilizadores
- identifica os vários atores na organização (utilizadores, administradores, …)
- define claramente os objetivos de segurança
- alerta os utilizadores para as várias ameaças a que o sistema está sujeito
- destaca a importância de todos sem excepção respeitarem as regras
- justifica a razão de ser das regras impostas (os atores devem concordar)
- identifica os contactos para esclarecimento de questões duvidosas
- define o tratamento de situações omissas na "política de segurança"
- estabelece as consequências da violação de regras
- destaca a manutenção de registos de actividades para auditorias
- é consistente na profundidade da abordagem das várias vertentes
- é possível impor aos atores (é possível fiscalizar o cumprimento das regras)

Política de segurança – politicas

Uma política deve dizer o que é permitido, proibindo tudo o resto.

É mais arriscado dizer o que é proibido, permitindo tudo o resto.

Política de …

- autenticação
- acesso físico
- acesso lógico
- utilização da rede interna (ligação de dispositivos à rede, …)
- utilização da internet (acesso a sites, controlo de conteúdos, …)
- “passwords” (regras na definição, armazenamento e manuseamento)
- utilização de e-mail
- privacidade (confidencialidade; registos de actividades e acesso aos mesmos)
- gestão de postos de trabalho

Referências bibliográficas

[1] Lhamas A. (2010-2011). Aulas Teóricas de ASIST.

(…)