

Disaster recovery

1. Conceitos fundamentais
2. Noção de DRP
3. Sites partilhados

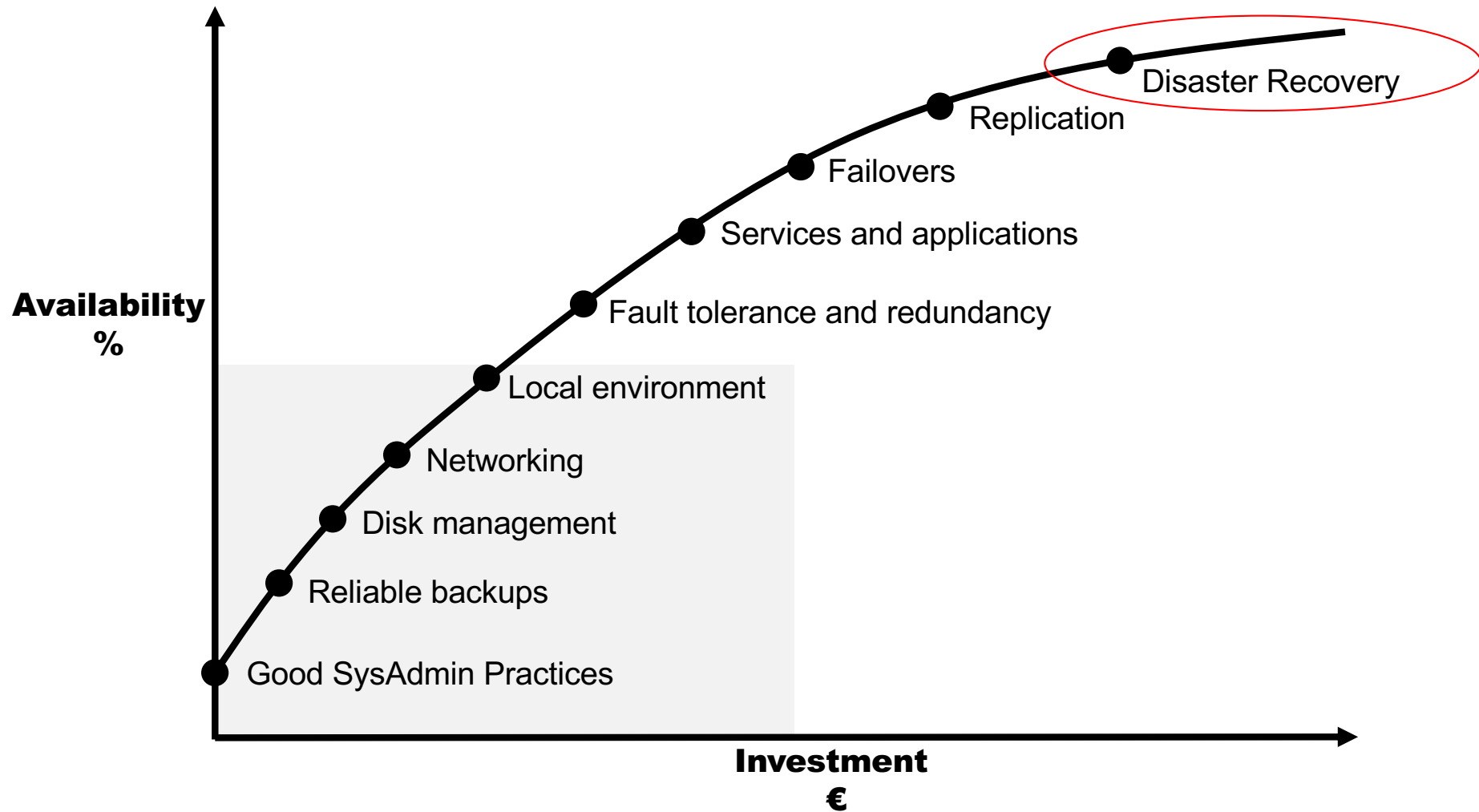
Enquadramento



www.disasterrecovery.org



Availability index

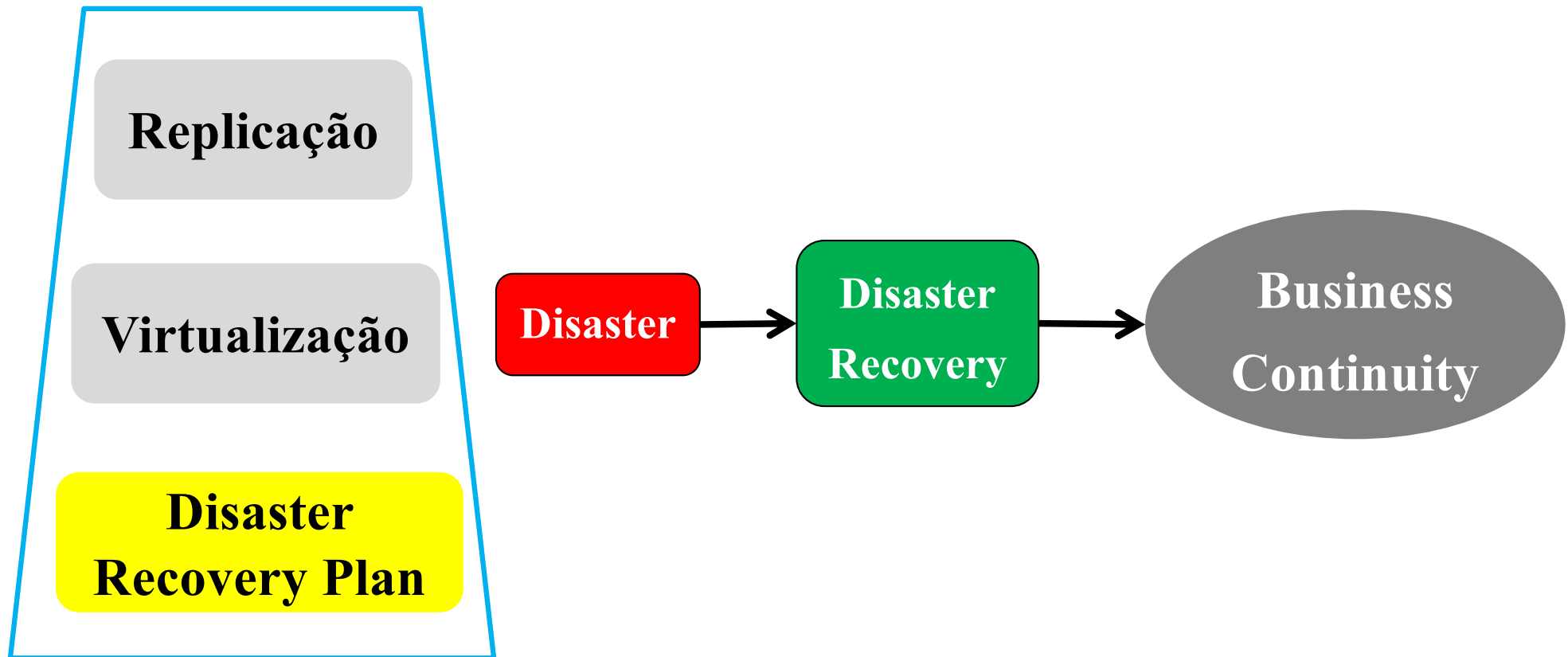


Adapted by Marcus E, Stern H., "Blueprints for high availability"; 2003; Wiley; ISBN: 0471430269;

Enquadramento




Enquadramento



Business continuity and DR planning

Business continuity \neq Disaster Recovery



*“**Risks and threats** to the ongoing availability of services, business functions and the organization **are actively reviewed and managed** at set intervals as part of the overall **risk-management process.**”*

*“Is the process by which **suitable plans and measures are taken** to ensure that, **in the event of a disaster**, the **business can respond appropriately** with the view to **recovering critical and essential operations** in a **little time possible.**”*

Disaster recovery plan

Objetivos fundamentais de um DRP:

1. Proteger os funcionários
2. Assegurar sobrevivência da empresa, durante e após o desastre
3. Assegurar a continuidade da empresa e do negócio

Disaster recovery plan

Conteúdo de um plano de DRP

NIST - Special Publication 800-34, Contingency Planning for Information Technology Systems, ISO/IEC 24762, BS 25777

- Definir um “*contingency planning policy statement*”
- Definir um “*business impact analysis (BIA)*”
- Identificar medidas de controlo preventivas
- Desenvolver estratégias de recuperação
- Desenvolver um plano de contingência para as TI
- Testar, treinar ... testar, treinar ... testar, treinar ...
- Atualizar ... atualizar ... atualizar ... atualizar ...

Disaster recovery plan

Conteúdo de um plano de DRP

NIST - **Special Publication 800-34**, Contingency Planning for Information Technology Systems, ISO/IEC 24762, BS 25777

- Documentar e prioritizar hw, sw e outros elementos
- Selecionar o site de DR
- Identificar pessoas chave, com posições críticas e correspondentes backups
- Criar e treinar equipas de resgate/emergência
- Implementar testes e exercícios práticos
- Atualização constante do plano

Disaster recovery plan

Business Impact Analysis (BIA)

Functional Area	Functional Name	Mail-zone	Risk Code F=Financial C=Customer R=Regulatory	Time Before Impact 0=week 2 or more 1=week 1 5=up to three days 10=day 1 20=4 hours 40=immediate	Customer Impact 0=none 1=Low 3=Med 5=High	Regulatory Impact 0=none 1=Low 3=Med 5=High	Financial Impact 0=none 1=0 to 10K 2=>10K but <100K 3=>100K but <500K 4=>500K but <1 Mil 5=>1 Mil	Rating Total Sum of 1 thru 4	Recovery Time Sensitivity Code	Alt. Site
Customer service	Call center	Z 45	C & F	40	5	1	3	49	AAA	Surviving sites then Smith Road
Customer service	Customer account maint.	Z 37	C	1	3	0	0	4	D	Work from home
Customer service	Customer monetary	Z 38	C & F & R	10	3	3	4	20	A	Smith Road


Exhibit 6.1 BIA Form.

Building an Enterprise-Wide Business Continuity Program; Kelley Okolita; 2009

Disaster recovery plan

Exemplos

- <http://searchdisasterrecovery.techtarget.com/>
- <http://www.drj.com/resources/sample-plans.html>

<COMPANY NAME>  Business Continuity Plan

BC 030204..Key Suppliers and Vendors and Emergency Contact Information

(TO ACCESS GUIDELINES ON COMPLETING THIS PART OF THE BUSINESS CONTINUITY PLAN, CLICK [HERE](#))

Listed below are the organisation's key suppliers who may need to be contacted in the event of an emergency. In the event of these regular suppliers not being able to provide the goods or services required in an emergency, an alternative list of suppliers has also been drawn up.

1. REGULAR SUPPLIERS

NAME OF SUPPLIER	KEY GOODS OR SERVICES PROVIDED	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS

2. ALTERNATIVE SUPPLIERS

NAME OF SUPPLIER	KEY GOODS OR SERVICES PROVIDED	NORMAL CONTACT DETAILS	EMERGENCY CONTACT DETAILS

COMPLETED BY: NAME: DATE:

REVIEWED BY: NAME: DATE:

- Documento assinado
- Compromisso assinado
- Vários templates disponíveis

Disaster recovery plan - preparação

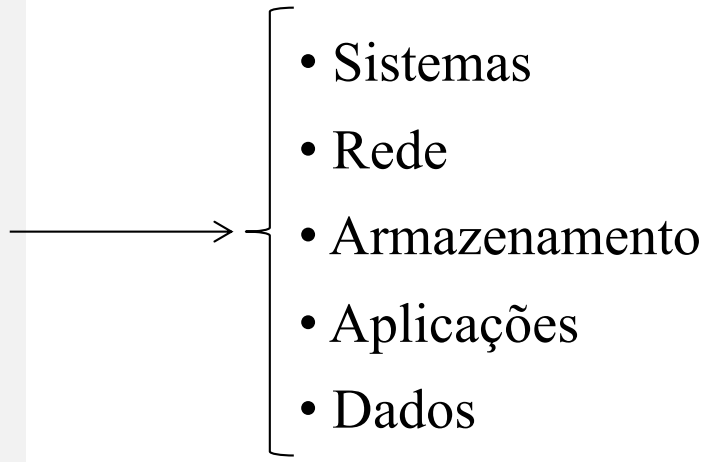
- Identificar coordenador(es) do DRP e backups
- Identificar e priorizar (todas) as funções do negócio
- Identificar um site de DR
- Estimar o tempo aceitável de recuperação após falha
- Definir metodologia de backups (*onsite e offsite*)
- Definir modelo de distribuição de informação crítica (números de telefone, passwords, planos, ...)

Disaster recovery plan - preparação

- Definir equipas de recuperação
- Recolher informação específica e crítica sobre a rede
- Coligir informação confidencial
- Sinalizar fornecedores críticos
- Identificar outros serviços: p.e. apoio psicológico
- Disponibilizar treino contínuo do DRP para todos

Disaster recovery plan - preparação

Equipas de recuperação:

- Gestão de desastre
 - Comunicações
 - Recuperação de infraestrutura TI
 - Contacto com fornecedores
 - Análise de destruição
 - Interface com o negócio
 - Logística
- 
- The diagram illustrates the relationship between disaster recovery teams and IT infrastructure components. A list of seven disaster recovery tasks is shown on the left, with the task 'Recuperação de infraestrutura TI' highlighted. An arrow points from this task to a bracketed list of five IT infrastructure components on the right: Sistemas, Rede, Armazenamento, Aplicações, and Dados.
- Sistemas
 - Rede
 - Armazenamento
 - Aplicações
 - Dados

Disaster recovery plan – escolha do site de DR

1. Localização física

- Acesso aos dados apenas através de uma única SAN?
- Ambos os sites partilham *facilities*?
- Próximo de serviços de saúde, bombeiros, etc...?
- Nível de *low-key* do site?
- Está bem dimensionado?
- Partilha de recursos para DR com outras companhias.

2. Segurança

- Regras de acesso ao equipamento (emergência declarada ou não)

3. Quanto tempo?

Disaster recovery plan – modelo de distribuição

1. Restrito?

- Documento **escrito** apenas pelo(s) coordenador(es) do DRP e pelo(s) backups
- Cópia digital em vários sítios, com acesso controlado
- Coordenadores têm DRP da sua área/secção/departamento

2. Abrangente?

- Documento disseminado por papel e em formato digital, por todos os colaboradores

Disaster recovery plan – conteúdo

- Contactos de telefone pessoais
- Passwords privilegiadas e regulares
- Procedimentos de emergência
- Hierarquia de contactos (1ª linha, 2ª linha, ...)
- Organigrama da organização
- Localização física dos sites (alguns podem ser secretos)
- Informação proprietária sobre contactos de fornecedores, identificação de patentes e projetos em curso

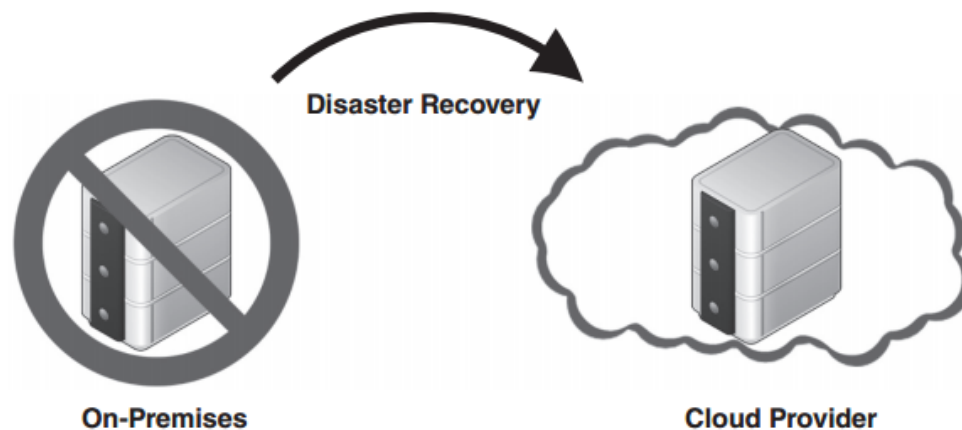
Informação sensível que deve ser mantida em ambiente restrito.
Prevenir fugas de informação através de colaboradores dispensados.

Business continuity – cloud environment

Domain 3

Characteristics of the cloud environment to consider in BCDR plan

1 On premises (local) and cloud as BCDR



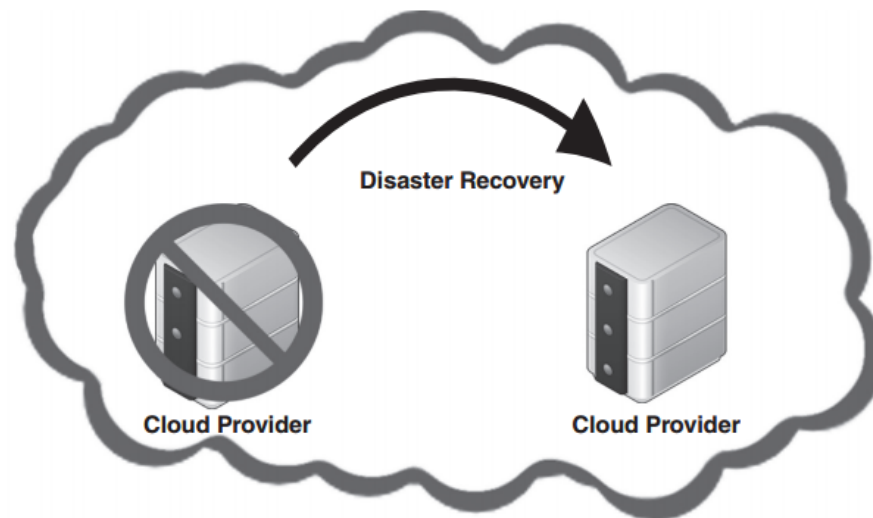
- Traditional failover strategy
- Endpoint is the cloud

Business continuity – cloud environment

Domain 3

Characteristics of the cloud environment to consider in BCDR plan

2 Cloud service consumer, primary provider BCDR



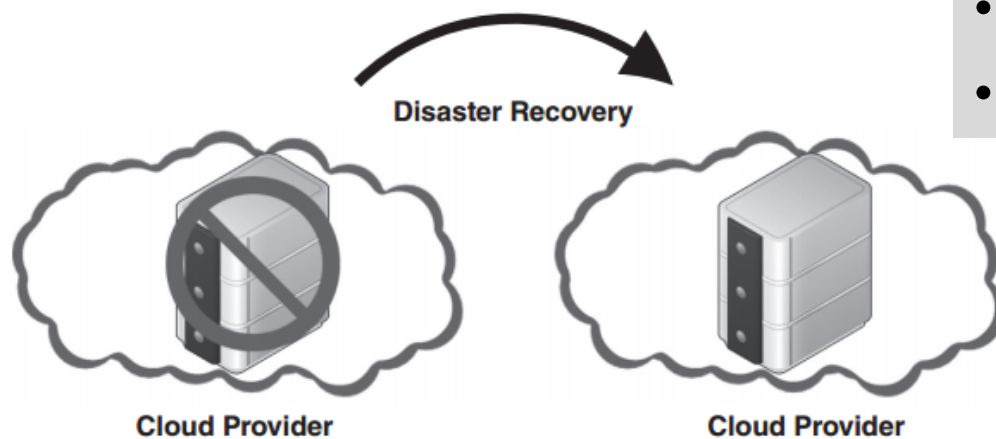
- Both sites are on a CSP
- ... in different regions

Business continuity – cloud environment

Domain 3

Characteristics of the cloud environment to consider in BCDR plan

3 Cloud service consumer, alternative provider BCDR



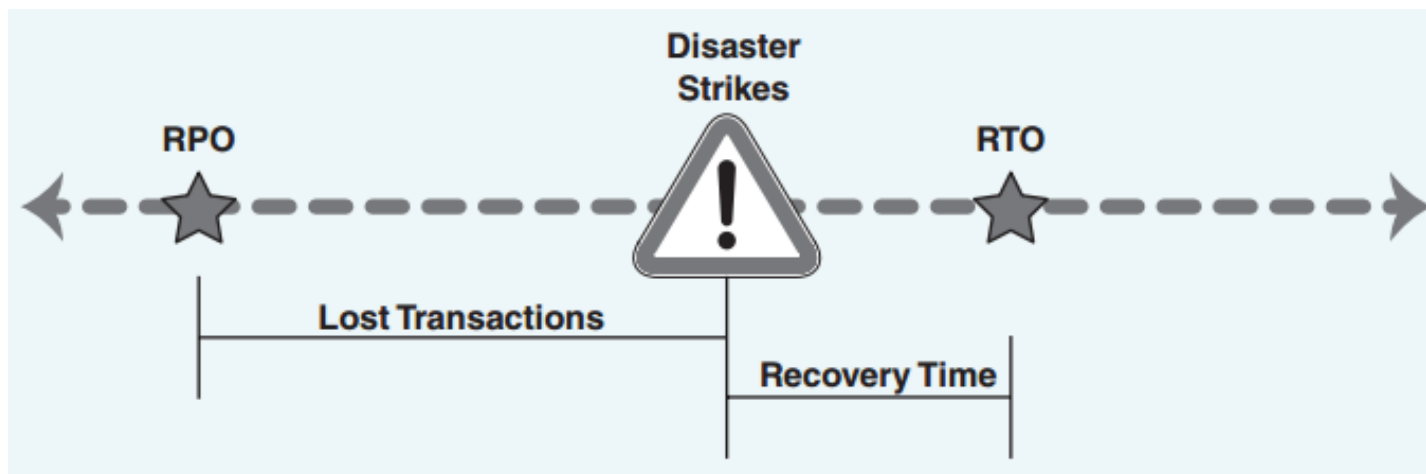
- Both sites are on different CSP
- Avoid risk of complete CSP failover

Business continuity – business requirements

Domain 3

How much data can the company afford to lose?

How fast you need a system to be up and running after a disaster?



RPO = Recovery Point Objective

RTO = Recovery Time Objective

Business continuity – BCDR strategy

- Is data sufficiently valuable for additional BCDR strategies?
- What is the required RTO?
- What is the requires RPO?
- What “disasters” were included in the analysis?
- Does that include CSP failure?

How BCDR can differ in a **cloud environment** from the **traditional approaches** that exist in noncloud environments?

Disaster recovery – main SLA components

1. SPoF should be all documented
2. Migration strategies to alternate providers should be possible
3. Alternate CSP should support all components in failover events
4. Controls should be enabled for data integrity
5. Users should select incremental backup settings
6. SLA should be revised at regular intervals

Disaster recovery – main SLA components

ISO/IEC documents regarding SLA items:

- ISO/IEC DIS 19086-1, “Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework—Part 1: Overview and Concepts”
- ISO/IEC NP 19086-2, “Information Technology—Cloud Computing—Service Level Agreement (SLA) Framework and Technology—Part 2: Metrics”
- ISO/IEC CD 19086-3, “Information Technology –Cloud Computing—Service Level Agreement (SLA) Framework and Technology—Part 3: Core Requirements”
- ISO/IEC AWI 19941, “Information Technology –Cloud Computing—Interoperability and Portability”
- ISO/IEC CD 19944, “Information Technology—Cloud Computing—Data and Their Flow Across Devices and Cloud Services”
- ISO/IEC FDIS 20933, “Information Technology—Distributed Application Platforms and Services (DAPS)—Access Systems”

Disaster recovery plan – sites de DR partilhados

- | | |
|---------------------------------|-----------------------------------|
| 1. Experiência | ✗ Equipamento partilhado ... |
| 2. Poupanças financeiras | ✗ ... perda de controlo |
| 3. Segurança remota | ✗ Testes tornam-se mais complexos |
| 4. Atualização do DRP e do site | |
| 5. Serviços extra | |

DR site Partilhado *versus* dedicado

PME → site partilhado

Grandes instituições → site dedicado

Disaster recovery plan – conclusões

- Desenho e teste de um bom DRP implica uma redução no tempo de recuperação após desastre.
- DR pode ser (é!) complexo e sujeito a erros. Capacidade de olhar para os detalhes poderá minimizar complexidade e erros.
- Um bom DR depende de ... pessoas! Poderão colaborar mais ou menos, conforme o grau de motivação e entrosamento na companhia.

Bibliografia

- Luiz André Barroso, Jimmy Clidaras, Urs Holzle; “The datacenter as a computer”; Morgan and Claypool Editors; ISBN: 978-1627050098; 2013 [pdf]
- Marcus E, Stern H., “*Blueprints for high availability*”; 2003; Wiley; ISBN: 0471430269