DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

Administração de Sistemas

Turma 3DE

João Pires (1150455)
Sérgio Carreirinha(1180800)
César Ferreira (1180811)
José Cunha (1181494
Frasncisco Tavares (1181844)

Docente
André Moreira (ASC)

isep Instituto Superior de Engenharia do Porto

Índice

Glossário

DRP – Disaster Recovery Plan;

DRT – Disaster Recovery Team;

MDV – Master Data Viagens;

MDR – Master Data Rede;

SLA – Service-Level Agreement;

SPA – Single Page Application.

Introdução

No âmbito da unidade curricular de Administração de Sistemas, foi-nos proposto a elaboração de um plano de recuperação em caso de desastre em relação ao projeto desenvolvido na unidade curricular de Laboratório/Projeto V.

Este projeto necessita de serviços tecnológicos para o seu desenvolvimento, bem como para a própria implementação web. Como resultado desta dependência, os serviços tecnológicos exigem um plano de recuperação abrangente, para garantir que estes possam ser restabelecidos rapidamente e completamente em caso de desastre.

Este plano resume os resultados de uma análise de risco para todos os serviços e fornece etapas gerais que serão realizadas para restaurar as suas funções e dados. Fornece também recomendações para fortalecer a estrutura tecnológica.

Objetivos

O objetivo principal deste plano de recuperação em caso de desastre (DRP) é ajudar a garantir a continuidade da gestão de negócio, fornecendo a capacidade para recuperar os serviços da empresa em causa com sucesso.

Os objetivos específicos deste plano em relação a uma emergência são:

- Detalhar um curso geral de ação a seguir em caso de desastre;
- Minimizar confusão, erros e despesas para o negócio;
- Implementar uma recuperação rápida e completa dos serviços.

Os objetivos secundários são:

- Reduzir os riscos da perda dos serviços;
- Fornecer proteção aos serviços;
- Garantir a viabilidade deste plano.

Sistema

Este projeto está divido em duas partes. Sendo estas *backend* e *frontend*:

Backend:

- MDV – Master Data Viagens, é uma WEB.API desenvolvido em ASP.NET;
- MDR – Master Data Rede, é uma WEB.API desenvolvido em Node.JS;
- PLANNING – Planeamento, é uma API desenvolvido em prolog.

Frontend:

- SPA (Single Page Application):
    - Registo + Login – Registo e login para aceder ao frontend da plataforma;
    - Painel de Administrador – Painel usado para efetuar alterações de dados.

Maximum Tolerable Period of Disruption (MTPD)

O MTPD ou Maximum Tolerable Period of Disruption é o termo usado para definir o tempo máximo de desempenho inferior aos requisitos da infraestrutura informática. Por outras palavras, o MTPD é o período máximo aceitável resultante de um incidente que limita os recursos, afetando o bom funcionamento do sistema.

A equipa considera que o tempo máximo seria de 1 hora. Este limite de tempo será o mais adequado para que o negócio volte à normalidade, sem que afete os utilizadores (Data Administrators e Clients).

Maximum Tolerable Downtime (MTD)

O MTD ou Maximum Tolerable Downtime é o tempo máximo de inoperacionalidade da infraestrutura informática. Ou seja, o MTD é o período máximo em que o sistema está em baixo sem que afete os utilizadores.

A equipa considera que o tempo máximo de inoperabilidade do sistema seria de 15 minutos. Imaginando que um novo utilizador está a tentar aceder ao sistema, não pode estar mais do que 15 minutos, sem poder ver viagens ou horários de autocarros disponíveis para o seu trajeto.

Minimum Business Continuity Objective (MBCO)

O Minimum Business Continuity Objective é a especificação de o nível mínimo que deve ser mantida durante uma rotura na infraestrutura. Interpretando de outra maneira, é o serviço mínimo que o sistema tem de disponibilizar a todos os utilizadores da aplicação de modo a serem pouco prejudicados.

A equipa definiu que o MDV seria o componente obrigatório em caso de desastre. Desta forma, é garantido aos utilizadores a consulta das viagens e das passagens, pois contém informação necessária para o bom funcionamento da aplicação.

E tal como no SLA, é dada continuidade em termos de segurança, integridade e disponibilidade que é pretendido por todas entidades envolvidas.

Business Impact Analysis (BIA)

O Business Impact Analysis identifica o impacto que uma disrupção iria causar no negócio.

Para a aplicação foram definidos os seguintes impactos:

- Insatisfação do cliente;
- Perdas de rendimento;
- Custos de manutenção;
- Penalidades contratuais;

Risk Assessment (RA)

O Risk Assessment descreve os possíveis cenários que afetam a continuidade de negócio, a sua probabilidade e o seu impacto.

A equipa definiu os seguintes riscos, conforme a tabela em baixo:

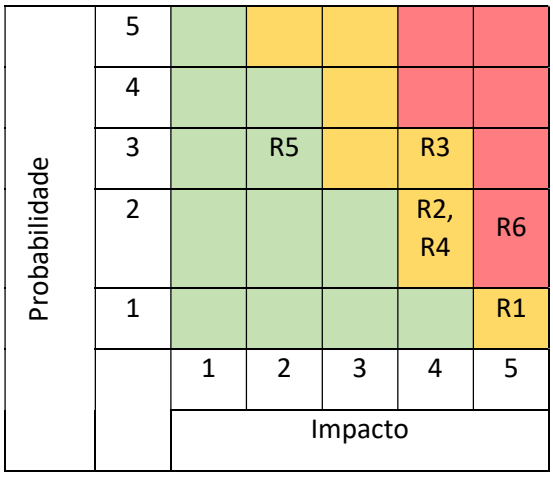

Figura 1 – Matriz do RA

Id Risco	Risco	P(R)	I(R)	Descrição
R1	Desastres Naturais	1	5	Desastres relacionados à infraestrutura dos servidores (incêndios, terramotos, cheias, etc.).
R2	Falha de eletricidade	2	4	Falta de eletricidade relacionado à infraestrutura.
R3	Falha de ligação à Internet	3	4	Problemas de ligação à internet relacionados com a operadora.
R4	Corrupção nos discos	2	4	Corrupção de dados relacionados com o servidor.
R5	Falha humana	3	2	Erros relacionados com manutenção.
R6	*Cyber* Ataque	2	5	*Cyber* ataque por parte de terceiros ao servidor.

Business Continuity Plan (BCP)

O Business Continuity Plan documenta os procedimentos a efetuar para responder, recuperar, retomar e restaurar a um nível pré-definido de operação após o desastre.

Risco	Procedimento
R1	Ativar uma equipa especializada em recuperação após desastres naturais
R2	Verificar se existe uma reparação rápida, senão utilizar outra fonte de energia elétrica
R3	Verificar se existe uma reparação rápida, senão contactar a operadora
R4	Verificar a existência de hardware para substituição
R5	Reparar o erro, e melhorar a instrução dos profissionais.
R6	Contratar uma *task force* para eliminar o intruso.

Risco R1

Após uma ocorrência de risco R1, é ativada uma equipa especializada em recuperação em desastres naturais. A equipa tem que:

- Estabelecer novas ligações com as infraestruturas de *failover* dentro de 2 horas úteis;
- Restaurar os principais serviços dentro de 6 horas uteis após o desastre;
- Até 24 horas após o desastre, tem de estar estabelecido o funcionamento normal dos serviços.

Risco R2

Após a ocorrência de risco R2, é esperado que:

- A fonte de energia da infraestrutura seja um gerador de *Backup*;
- Dentro de uma hora, detetar onde se encontra a falha e consertá-la;
- Restaurar a principal fonte a energia.

Risco R3

Após a ocorrência de risco R3, e conforme definido em termos contratuais, a resolução do problema terá de ser feita dentro do tempo estipulado para uma falha. Se o mesmo não acontecer, tem de ser verificado a penalidade e/ou indemnização acordada.

Risco R4

Após a ocorrência de risco R4, deve-se:

- Verificar a existência de hardware extra, e proceder à sua substituição;
- Caso seja necessário adquirir hardware extra, proceder à sua compra.

Risco R5

Após a ocorrência de risco R5, a empresa terá de:

- Proceder à reparação do erro, juntando uma equipa com profissionais mais experientes;
- Instruir melhor o(s) funcionário(s), para que não ocorra o mesmo erro.

Risco R6

Após a ocorrência de risco R6, a empresa tem o dever de:

- Reunir uma *task force* especializada na remoção de *hackers/vírus* e danos causados;
- Reforçar as medidas de segurança dos servidores;
- Melhorar as práticas de segurança dos funcionários.

Disaster Recovery Plan (DRP)

O Disaster Recovery Plan também é parte integrante do BCM. Se o MBCO ou o MTD não são afetados, o BCM deve conter os procedimentos necessários para recuperar o SLA dos serviços em disrupção. Se são afetados, o DRP assume o controlo até à recuperação da situação pretendida.

Num cenário em que não só todos os serviços estão inativos (MDV, MDR, SPA) mas também os servidores principais e de *failover* não respondem aos pedidos, deve-se optar por uma resposta urgente, *id est*:

- Contactar um fornecedor de servidores remotos e subscrever um plano de curto prazo;
- Fazer nova ligação ao serviço de nível mínimo (MBCO) num período máximo definido pelo MTD;
- Definir um limite de acessos concorrentes entre utilizadores e informá-los de falhas técnicas;
- Reunir uma equipa especializada em recuperação de desastres (DRT);
- Transferir toda a informação novamente para os servidores próprios.

Fault Avoidance

Fault Avoidance, que em português significa prevenção de falhas, procura evitar a ocorrência de falhas no sistema que questiona a continuidade do negócio. Existem várias formas de evitar falhas que das quais se destacam:

- Monitorização (Controlo da temperatura dos servidores, controlo da humidade, controlo da utilização dos recursos dos discos, CPU, etc);
- Testagem continua do software;
- Adotar boas práticas de trabalho e modularidade;
- Controlo de competências dos ativos.

Fault Tolerance

Fault tolerance é propriedade do sistema que permite a operação normal dos componentes em caso de falhas.

Caso o serviço mantenha o funcionamento normal dizemos que estamos perante um *Full Fault Tolerant*. Se ocorrer uma degradação temporária, é uma *Graceful Degradation.* Por outro lado, se esta degradação for significativa, então terá de ser considerado um *Fail Soft.* Se a falha torna o serviço inativo, porém mantém a integridade, considera-se um *Fail Safe*.

Backup

De forma a não perder os dados, em caso de uma disrupção, adota-se uma técnica de *Mirroring,* apesar de implicar duplicação de dados, e prejudicar na disponibilidade de operações. Porém, esta técnica pode ser assíncrona ou síncrona, em que o WRT (Work Recovery Time) e o RTO (Recovery Time Objective) são quase nulos ou até mesmo nulos, respetivamente. Deste modo, deve-se praticar um *Mirroring* bidirecional.

No que toca às copias de segurança foi definido pela equipa que seriam feitas cópias incrementais diariamente, à exceção do último dia útil da semana em que seria feita uma cópia integral do sistema. Durante as cópias de segurança, o sistema deve continuar ativo e com um funcionamento normal.