Instituto Superior de Engenharia do Porto

Disaster Recovery Plan

2021/2022

Turma 3NA

Grupo 74

1140858 _ Carlos Moutinho

1171602 _ Rui Marinho

1181882 _ Rafael Soares

1181892 _ Sara Silva

1181895_ Fábio Silva

Índice

Introdução

Em TI, se forma a manter a rentabilidade de qualquer negócio e garantir que os serviços tecnológicos sejam restabelecidos rapidamente, é extremamente importante ter um plano de ação para qualquer interrupção que possa acontecer, por exemplo, por intrusão de hackers, incêndio, falta de energia, desastre natural ou outro tipo de crise.

Para isso, no âmbito do projeto da unidade curricular de Laboratório/Projeto V e em resposta a unidade curricular de Administração de Sistemas, foi requerida a elaboração de um plano de recuperação em caso de desastre.

Em função da necessidade e da dependência dos vários serviços tecnológicos para o desenvolvimento e implementação do projeto acima referido, surgiu a tal necessidade prioritária da realização do plano de forma a minimizar efetivamente as consequências negativas de um desastre.

O plano detalha os resultados de uma análise de risco para todos os serviços e demonstra as atividades que serão realizadas para restaurar os sistemas e dados. Contém também recomendações de forma a reforçar a estrutura.

Contexto

A *Graphs4Social, S.A*. é uma *startup* com sede no Porto (Portugal) cuja missão é fornecer aplicações de manipulação e visualização de grafos de redes sociais. A empresa decidiu recentemente expandir o sue portfolio de produtos entrando na área de jogos, mas mantendo o foco nos grafos de redes sociais.

A empresa decidiu recorrer à subcontratação de serviços de desenvolvimento uma vez que não possui capacidade livre de momento.

Os sistemas implementados são de importância vital para a atividade da empresa, tais como:

- **Módulo de navegação e visualização 3D**: Este módulo web é responsável pela visualização em 2D e 3D do grafo da rede social do utilizador. Também é responsável por demonstrar as relações e os respetivos caminhos do grafo.
- **Módulo de inteligência artificial:** O módulo de inteligência artificial está integrado e comunica com o restante projeto e tem algumas funcionalidades tais como, determinar caminhos, tamanhos de rede, sugerir rotas e relações.
- **Módulo Site:** Uma aplicação web cuja principal função é o registo de utilizadores, permitir ao utilizador construir a sua rede social associando-se a outros utilizadores (indicando *tags* e força dessa relação) e diversas consultas.
- **Módulo Publicações e Comentários:** Este módulo responsável pela gestão dos *feeds* de utilizadores, entre eles, os comentários e os *posts*.

Businness Impact Analysis (BIA)

Identificação das atividades críticas da organização e as suas dependências e também permite desta forma priorizar as operações de recuperação após uma disrupção.

A tabela abaixo representa os tempos de recuperação, de perda de dados e os tempos necessários para repor os dados.

Serviços Críticos	**RPO** (1)	**RTO** (2)	**WRT** (3)
Módulo Master Data Rede Social (Aplicação + Base de dados)	0	90 min	30 min
Módulo Master Data Posts (Aplicação + Base de dados)	0	90 min	30 min
Módulo SPA (Website)	0	30 min	30 min
Serviços Não Críticos	**RPO** (1)	**RTO** (2)	**WRT** (3)
Módulo de Planeamento	180 min	30 min	30 min

(1) *Recovery Point Objective* (RPO) é o tempo máximo de perda de dados aceite.
(2) *Recovery Time Objective* (RTO) é o tempo médio de recuperação dos sistemas e infraestruturas.
(3) *Work Recovery Time* (WRT) é o tempo necessário para repor os dados e aplicações e testá-los.

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

Categoria	Características	RTO (horas)	RPO (horas)
Tier 7	"tier 6", com arranque automático do "hardware" alternativa	<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"		

Para que a continuidade do negócio da empresa fique totalmente assegurada, em função dos tempos calculados para os sistemas críticos serem reduzidos, enquadra-se numa classificação ***Tier 7***.

Maximum Tolerable Period of Disruption (MTPD)

O MTPD ou *Maximum Tolerable Period of Disruption* (Tempo Máximo Tolerável de uma Interrupção), é o termo usado para definir o tempo máximo que um serviço ou produto pode permanecer indisponível sem gerar danos significativos que ameacem a sobrevivência da empresa.

Para calcular o MTPD é necessário ter em conta as expectativas do cliente, assim como questões de reputação e financeiras.

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.

Maximum Tolerable Downtime (MTD)

O *MTD* ou *Maximum Tolerable Downtime* é o tempo máximo de inoperacionalidade da infraestrutura informática, ou seja, 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 2 horas.

Fault Avoidance

Fault Avoidance, que significa prevenção de falhas, procura evitar ou minimizar a ocorrência de falhas no sistema que coloque em causa a continuidade do negócio. Para maximizar a probabilidade de não ocorrerem falhar, destacam-se as seguintes medidas:

- Monitorização rigorosa dos serviços;
- Teste continua e frequento do software;
- Adoção de boas práticas de desenvolvimento e modularidade;
- Controlo de competências dos recursos.

Fault Tolerance

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

Caso o serviço se mantenha em funcionamento normal, estamos perante um *Full Fault Tolerant*. Caso ocorra uma degradação temporária, é uma *Graceful Degradation*. No entanto, caso a degradação seja significativa, é considerado um *Fail Soft*.

Por fim, se a falha torna o serviço inativo, mas mantém a integridade, considera-se um *Fail Safe*.

Risk Assessment (RA)

Constituição dos cenários que podem afetar a continuidade de negócio assim como a probabilidade de ocorrerem e qual o seu impacto.

Análise de Riscos

Riscos	**Descrição**
Falha de hardware	Falhas relacionadas com o hardware dos servidores
Falha de rede / ISP	Problemas / avarias com a LAN e / ou WAN
Falha elétrica	Corte de fornecimento da rede, falhas técnicas
Ataques maliciosos	Ciberataques, sabotagem, vírus
Catástrofe	Incêndios, inundações, explosões, terrorismo
Falhas de Software	Erros nos módulos aplicacionais ou em bases de dados

Análise de Ameaças

Ameaça	**Descrição**
Perda de dados	Perda de qualquer tipo de dados relacionados com a aplicação
Roubo de informação	Exposição de dados sensíveis de utilizadores
Perturbação de negócio	Impossibilidade de serem efetuados novos registos de utilizadores, criação de relações e visualização da rede
Credibilidade e reputação	Possível perda de credibilidade e reputação da empresa

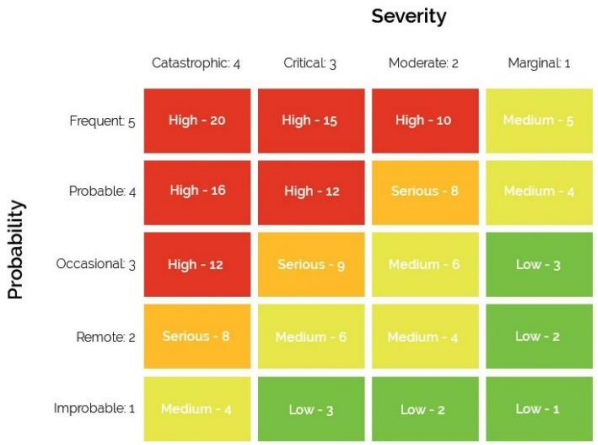

Figura 1 – Matriz de risco

Classificação do risco com base nos níveis de impacto e probabilidade da matriz de risco. O resultado é obtido em função do produto do impacto pela probabilidade:

Cenário	Severidade	Probabilidade	Resultado
Falha de hardware	4	2	8
Falha de rede / ISP	4	2	8
Falha elétrica	4	2	8
Ataques maliciosos	4	3	12
Desastres Naturais	4	1	4
Falha nas aplicações *Master Data Rede Social* e *SPA*	4	2	8
Falha na aplicação *Master Data Posts*	3	2	5
Falha na aplicação *Planeamento*	2	2	4

Business Continuity Plan (BCP)

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

Risco	Procedimento
Falha de hardware	Substituição de hardware
Falha de rede / ISP	Caso seja possível, intervenção rápida, senão contactar a operadora
Falha elétrica	Caso seja possível, intervenção rápida, senão utilizar outra fonte de energia elétrica e contactar operadora
Ataques maliciosos	Reunir/Contratar equipa especializada de forma a reduzir e eliminar intruso;
Desastres Naturais	Ativar uma equipa especializada em recuperação após desastres naturais
Falhas de Software	Reparar o erro, e melhorar a instrução dos profissionais.

Planos de recuperação em caso de falha

Falha de hardware

Após falhas de hardware:

- Verificar a existência de hardware de substituição e proceder à sua reparação;
- Em caso de impossibilidade de reparação/substituição, proceder à sua compra de um novo imediatamente;
- Efetuar testes de acesso a aplicação.

Falha de rede / ISP

Após falhas de rede:

- Caso seja possível, intervenção rápida para corrigir falha de rede;
- Em caso de impossibilidade, contactar operadora de imediato;

- Efetuar testes de acesso a aplicação.

Nota: Resolução terá de ser concluída dentro do tempo contratado após uma falha. Caso não aconteça, será necessário verificar indemnização estipulada.

Falha elétrica

Após falha elétrica:

- Será ativada de imediato fontes de energia alternativas (UPSs);
- Caso seja possível, intervenção rápida para corrigir falha de rede;
- Em caso de impossibilidade, contactar operadora de imediato;
- Efetuar testes de acesso a aplicação.

Ataques maliciosos

Após cyber ataque:

- Desligar equipamento infetado imediatamente da rede;
- Reunir/Contratar equipa especializada de forma a reduzir e eliminar intruso;
- Avaliar danos e possíveis perdas;
- Efetuar testes de acesso a aplicação.

Desastres Naturais

Após desastres naturais:

- Estabelecer novas ligações com as infraestruturas de backup dentro do tempo calculado;
- Reunir equipa especializada para recuperação após desastres naturais.
- Efetuar testes de acesso a aplicação.

Falhas de Software

Após falha de software:

- Reunir equipa especializada para avaliar e desenvolver procedimento sanar problema;
- Avaliar o motivo do erro e se possível aplicar mudanças de modo a evitar problemas idênticos no futuro.

Estratégia de Backup

Em relação aos *backups*, foram projetadas as estratégias abaixo.

Para os serviços considerados críticos (Módulo Master Data Rede Social, Master Data Posts, Módulo SPA), foi implementado um *Mirroring* para local remoto. Com isto, facilita a recuperação em caso de desastre e é possível ter o RPO e o WRT nulos ou muito próximo disso. No entanto, todos os domingos é realizada uma cópia de segurança completa.

No que diz respeito aos serviços considerados não críticos, como é o caso do Módulo de Planeamento, é efetuado uma cópia de segurança Integral/Completa ao domingo para copiar todos os dados. Nos restantes dias, é efetuada uma cópia de segurança diferencial a cada 2 horas e com isto apesar de necessitar sempre de uma cópia integral/completa prévia, faz uma cópia apenas de todos os dados que foram alterados desde a cópia integral anterior.

Para além destas estratégias, as cópias de segurança são sempre realizadas em duplicado e os dispositivos de armazenamento das cópias são guardadas em local remoto.

A cada duas semanas são verificados os tamanhos das cópias e a respetiva capacidade de reposição dos dados.

As cópias mensais de informação serão mantidas durante um período de 10 anos.

Plano de testes

Para atestar o plano descrito, é necessário fazer algumas validações e testes. Para isso, é necessário simular algo semelhante a um ataque ou situação de desastre.

Teste de simulação simples

É efetuado mensalmente e não compromete o normal funcionamento da atividade da empresa. Por exemplo, verificar se o *backup* do dia anterior reflete exatamente as transações efetuadas.

Teste de simulação integrais

É efetuado anualmente e simula o pior cenário possível. Este tipo de testes é programado fora do horário de funcionamento da empresa e contempla, por exemplo, testes de resistência dos sistemas alternativos de energia, as UPS (*Uninterruptible Power Supply*).

Contactos

Abaixo encontra-se os contactos das pessoas com responsabilidade e permissões para aconselhar ou ativar medidas traçadas no plano de recuperação de desastre.

Contactos Internos

Nome	**Contacto**
Carlos Moutinho	1140858@isep.ipp.pt
Rui Marinho	1171602@isep.ipp.pt
Rafael Soares	1181882@isep.ipp.pt
Sara Silva	1181892@isep.ipp.pt
Fábio Silva	1181895@isep.ipp.pt

Contactos Externos

Nome	**Organização**	**Contacto**
Jorge P. Leite	ISEP	jpl@isep.ipp.pt