Disaster Recovery Plan

Turma 3DI

1190424 - Beatriz Seixas

1190682 - Jéssica Alves

1190967 - Pedro Santos

1191460- Tiago Costa

Professor Responsável

Rui Filipe Marques, RFM

Unidade Curricular

ASIST

Data de Entrega: 23/01/2022

Índice

Conteúdo

Equipa de Suporte

Nome	Email
Beatriz Seixas	1190424@isep.ipp.pt
Jéssica Alves	1190682@isep.ipp.pt
Pedro Santos	1190967@isep.ipp.pt
Tiago Costa	1191460@isep.ipp.pt

Historial de Revisão

No momento em que acontece um desastre, todo o negócio sofre. Um dos objetivos do planeamento de negócio é então mitigar as consequências da disrupção do produto e entrega de serviços de melhor forma no caso de desastre.
Um dos eixos na estratégia de continuidade de um negócio é então o DRP (Disaster Recovery Plan), de modo a garantir que o negócio mantém o nível mínimo de serviço enquanto é restaurada a organização de negócio.
No caso de o DRP falhar, no caso de um desastre, a empresa corre um risco altíssimo de perda de clientes para empresas rivais, como consequência perdem financiamento e também um maior risco dos seus produtos e serviços serem reavaliados sem motivo.

Declaração da Informação Tecnológica

Com este documento temos o objetivo de delinear todas as nossas políticas e procedimentos de modo a recuperar a informação tecnológica em caso de desastre, e também delinear os planos a nível de processamento de modo a recuperar plataformas tecnológicas.
Este Documento sintetiza os nossos procedimentos recomendados. Na eventualidade de uma emergência. Modificações deste documento poderão ser feitas para garantir a segurança física das pessoas, equipamentos e informação. A nossa missão é assegurar o sistema de informação, integridade e disponibilidade de informação e continuidade do negócio.

Declaração de políticas

- O Disaster Recovery Plan deve ser mantido atualizado para a possibilidade de serem efetuadas mudanças circunstanciais.

- O Disaster Recovery Plan deve abranger todos os aspetos essenciais como elementos de infraestrutura, sistemas e redes, de acordo com as principais atividades de negócio.

- A avaliação de risco formal deve ser realizada para determinar os requisitos para o Disaster Recovery Plan.

- O Disaster Recovery Plan deve ser testado periodicamente com base numa simulação para garantir que possa ser implementado em emergências e que todos os colaboradores da empresa entendam como deve ser executado

- Todos os funcionários devem ser informados sobre o Disaster Recovery Plan e as respetivas funções.

Objetivos

O objetivo preliminar de um plano de recuperação de desastre (DRP) é permitir que uma organização sobreviva a um desastre e que possa restabelecer as operações dos negócios. 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 objetivos o DRP deve atender os seguintes requisitos:

- Prover 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;
- Facilitar a coordenação eficaz de tarefas da recuperação;
- Reduzir a complexidade do esforço de recuperação.

Serviços e prioridades

TMD – Tempo Máximo de Disrupção

RPO - Recovery Point Objective - Método de controlo para calcular a quantidade limite de dados que uma organização toleraria perder em caso de paralisação. O objetivo é não atingir esse limiar de tolerância de forma a proteger a empresa de ter os seus produtos comprometidos.

RTO - Recovery Time Objective - Método de controlo para calcular o período máximo que o sistema necessita para voltar a operar após uma paralisação. Isto inclui download de dados, reinstalações, atualizações, etc.

Componente	Localização	TMD	Componentes dependentes	Prioridade De Serviços	RTO	RPO
MDS	Cloud-Azure	12H	gateway	2	24H	24H
MDF	Cloud-Azure	12H	gateway	2	24H	24H
Planeamento	VM Windows azure	12H		2	24H	24H
SPA	Firebase	6H	gateway	1	12H	12H
Gateway	Cloud-Azure	12H	spa,plan	1	12H	12H
Base de dados azure	Cloud-Azure	12H	gateway	1	12H	12H
Base de dados Mongo DB	Cloud-Azure	12H	gateway	1	12H	12H

No caso dos backups, e a forma como estes seriam implementados, dependendo do sistema, serão backups diários, ou até mesmo, nos serviços mais críticos, como por exemplo o SPA, dois backups incrementais diários, de forma a possibilitar o RPO de 12 horas.

Para serviços que estão alojados na Cloud, seriam optados por outros servidores da Cloud para alojarem os ficheiros de backup, uma vez que isto reduz os custos operacionais da empresa, deixando os funcionários focados em tarefas mais importantes.

Desta forma, o plano de backups para os serviços fornecidos seguiria o seguinte formato:

Prioridade De Serviço	Estratégia adotada
1	Backup integral em dois dias da semana (Domingo e Quinta), e dois backups incrementais diários (A cada 12 horas de serviço). Isto porque o RPO é baixo, o que significa que precisamos de backups mais frequentes de forma a conseguir atingi-lo.
2	Backup integral em apenas um dia da semana, com um backup incremental diário. A justificação é porque o RPO e RTO é mais alto que a dos serviços de prioridade 1, então temos mais tempo para poder fazer a recuperação dos dados.

Proteções oferecidas pela Cloud

Os serviços que hospedam aplicações na Cloud fornecem vários métodos de segurança que reduzem riscos.

- Prevenção de desastres
- Testes de Penetração e Avaliações de Vulnerabilidades;
- Sistemas de Deteção e Supressão de fogo nas instalações;
- Redundância nas fontes elétricas para suprimento 24/7;
- Controlo de clima e temperatura;
- Monitorização de eventos elétricos, mecânicos e de "vida" dos equipamentos nos Centros de Dados;
- Firewalls;
- Mitigação de DDoS através da utilização de cookies e limite de conexões;
- Proteção contra Spoofing e Sniffing;
- Backups;
- Entre outros;
- Para garantir tolerância a possíveis ataques e/ou desastres naturais, atos humanos ou de cariz tecnológico as aplicações adotam as seguintes medidas:

Visão Geral do Plano

Atualização do plano

É necessário que o processo de atualização do DRP seja devidamente estruturado e controlado. Sempre que forem efetuadas mudanças no plano, estas devem ser totalmente testadas e os dispositivos de treino deverão sofrer alterações.

Plano de armazenamento de documentação

Cópias deste Plano, CDs e cópias impressas serão armazenadas em locais seguros a serem definidos pela empresa.
Cada membro da administração receberá um CD e uma cópia deste plano para arquivar em casa.

Cada membro da equipa de recuperação de desastres e a equipa de recuperação de negócios receberá um CD e uma cópia impressa deste plano.
Uma cópia protegida será armazenada em infraestruturas específicas para este propósito.

Gestão de Riscos

Existem muitas potenciais ameaças de interrupção que podem ocorrer a qualquer momento e afetar o processo normal de negócios.
Cada potencial desastre ambiental ou situação de emergência foi examinada. O foco aqui é o nível de interrupção que poderiam ocorrer nos negócios por cada tipo de desastre.
Os potenciais desastres foram avaliados da seguinte forma:

Desastre	Probabilidade	Impacto
Incêndio	3	4
Inundação	3	4
Tornado	5	*
Falha no sistema elétrico	3	3
Terrorismo	5	*
Perda de Comunicações	3	4

Impacto	
1	Destruição total
2	Destruição parcial
3	Danos significativos
4	Danos consideráveis
5	Danos pequenos
*	Depende do nível

Probabilidade	
1	Muito alta
2	Alta
3	Media
4	Baixa
5	Muito baixa

Matriz de riscos

A matriz de riscos tem por objetivo fazer uma avaliação tendo em conta a avaliação do impacto e a probabilidade de ocorrência de uma falha nos sistemas.
Como grande parte dos serviços estão hospedados por serviços aplicacionais na Cloud, estes fornecem, à partida, uma maior segurança em termos de falhas e ataques.
Com isto, garante ao produto da ROAD, uma diminuição dos fatores de risco das aplicações hospedadas nas diversas Clouds.

Em seguida, está representada a Matriz de Risco responsável por classificar os riscos possivelmente identificados.

	Catastrófico	Crítico	Moderado	Ligeiro
Frequente	20	15	10	5
Provável	16	12	8	4
Ocasional	12	9	6	3
Isolado	8	6	4	2
Improvável	4	3	2	1

SERVIÇO	RISCO	CLASSIFICAÇÃO	JUSTIFICAÇÃO
SPA	Paragem dos Serviços Firebase (Manutenções e afins)	6	A plataforma Firebase providência aos seus clientes múltiplos mecanismos que possibilitam uma rápida recuperação/segurança das aplicações hospedadas (Backups frequentes, geradores alternados, deteção de fogo nas instalações, etc). .
MDS	Paragem nos Serviços Azure (Manutenções e afins)	6	A plataforma Azure disponibiliza múltiplos mecanismos que possibilitam uma rápida recuperação dos componentes hospedados.
MDF	Paragem nos Serviços Azure (Manutenções e afins)	6	A plataforma Azure disponibiliza múltiplos mecanismos que possibilitam uma rápida recuperação dos componentes hospedados.
Base de Dados Azure	Paragem nos Serviços (Manutenções e afins)	6	A plataforma Azure disponibiliza múltiplos mecanismos que possibilitam uma rápida recuperação dos componentes hospedados.

Base de dados mongo db	Paragem nos Serviços (Manutenções e afins)	6	A plataforma Azure disponibiliza múltiplos mecanismos que possibilitam uma rápida recuperação dos componentes hospedados.
Planeamento	Falha na conexão à Internet	4	A falha na conexão à Internet impediria a conectividade com os restantes módulos do Produto.
Planeamento	Ataques DDoS e DoS	8	Possíveis ataques devem ser considerados.
Planeamento	Falha na VM	6	Há múltiplas razões para que ocorra falha na VM, contudo, o serviço afetado não é dos mais prioritários.
Gateway	Paragem nos Serviços (Manutenções e afins)	4	A plataforma Azure disponibiliza múltiplos mecanismos que possibilitam uma rápida recuperação dos componentes hospedados.

Visão geral do plano de emergência

Estruturação da execução

É previsto que no caso de algum destes acontecimentos, a liderança e o processo de recuperação seja entregue a um dos responsáveis da equipa de recuperação em caso de desastre. No final de todo o processo, o retorno às operações normais deve ser orientado pelos superiores responsáveis. Assim, para cada um dos casos vistos no tópico anterior, as medidas de prevenção criadas são:

• Catástrofes naturais

1. Aceder aos backups nos servidores;
2. A partir dos servidores, efetuar o “deployment” da aplicação;
3. Permitir o acesso à mesma através do mesmo endereço aos utilizadores;
4. Avisar os utilizadores (email) do acontecimento.

• Ataque Informático

1. Desligar todo o acesso à aplicação;
2. Verificar a integridade dos backups existentes (Possíveis falhas de segurança existentes no código, existência de ataques aos servidores onde se encontram os bakups, etc…);

3. Resolução do problema (A probabilidade de este ponto ter de ser resolvido em contacto com as plataformas cloud utilizadas é elevada);
4. Avisar os utilizadores (email) do acontecimento.

• Erro humano

1. Aceder aos backups existentes nos servidores;
2. Utilizar os dados existentes nos backups para reverter para o período mais próximo do acontecimento, de maneira a minimizar a perda de informação / corrigir erros;
3. Avisar os utilizadores (email) do acontecimento.

• Perda de Comunicação entre Componentes

1. Aceder aos backups presentes nos servidores;
2. Efetuar o deployment da aplicação, a partir dos servidores;
3. Permitir acesso à mesma através do mesmo endereço aos utilizadores;
4. Avisar os utilizadores (mail) do acontecimento.

Solução mais eficiente

Após pesquisa e análise extensa dos possíveis serviços que o mercado propõe, concluímos que a solução adotada pela equipa da é a menos dispendiosa tendo em conta o produto desenvolvido.

Assim sendo segue a descrição dos pacotes e serviços utilizados pela empresa.
Para hospedar o serviço mais importante, **SPA**, foi utilizado o plano gratuito do **Google Firebase** que conta com:

- **Realtime Database** com espaço para **1GB** de dados armazenados e **1GB** de dados transferidos
- **Storage** com espaço de **5GB**
- **Cloud Functions** com disponibilidade de **2 000 000 invocações** para funções, **120 minutos** de Build, **200 000 segundos** de CPU com velocidade de **1GHz**
- **Hospedagem** com **10GB de armazenamento** com capacidade para **5000 páginas** de conteúdo estático

Para hospedar o serviço **MDS** foi utilizado o plano do **azure web app B1 tear,** que tem o custo de 0,075$/hora que conta com:

- 10 GB de armazenamento
- 1 núcleo
- 1,75 GB de Ram

Para hospedar o serviço **MDF** foi utilizado o plano **Azure web app F1 tear,** gratuito que conta com:

- Núcleos partilhado (60 minutos CPU/dia)
- 1GB Ram
- 1GB armazenamento

Para hospedar o serviço de **Planeamento** foi utilizado o plano windows Server B1s, que tem o custo de 0,0104$/hora e conta com:

- 1 núcleo
- 4GiB de armazenamento temporário
- 1 GiB de Ram

Conclusão do processo de Recuperação

No caso de desastre, após a recuperação deve ser elaborado um relatório detalhado do processo na sua totalidade. Este deve incluir a altura em que aconteceu, o seu local, o problema em questão, pessoas/plataformas envolvidas, componentes afetados e por fim uma descrição da resolução efetuada. Este deve ser incluído como um anexo deste documento para em posteriores revisões o plano ser adaptado às circunstâncias desse problema.