

Uma imagem com alimentação

Descrição gerada automaticamente

**Disaster Recovery Plan**

**ASIST – Sprint 3 (Sprint D)**

**Turma 3DJ \_ Grupo 57**

1190903 \_ Miguel Gonçalves

1191018 \_ Rúben Rodrigues

1191042 \_ Rui Pinto

1191106 \_ Tomás Limbado

**Data: 23/1/2022**

Índice

[Declaração de Informação Tecnológica 3](#_Toc93589432)

[Equipa de Suporte 3](#_Toc93589433)

[Serviços e Prioridades 3](#_Toc93589434)

[Mitigação de Riscos 4](#_Toc93589435)

[Matriz de Risco 4](#_Toc93589436)

[Avaliação de Riscos 5](#_Toc93589437)

[Estratégia de Backup 6](#_Toc93589438)

[Processos de Recuperação 6](#_Toc93589439)

[Conclusão 6](#_Toc93589440)

# Declaração de Informação Tecnológica

Este documento planeia as políticas para os sistemas considerados críticos da infraestrutura, identificando e quantificando os riscos e os procedimentos para assegurar a continuidade de negócio. Na eventualidade de uma situação de emergência, modificações deste documento poderão ser feitas para garantir a segurança física das pessoas, equipamentos e informação.

# Equipa de Suporte

|  |  |
| --- | --- |
| Nome | Endereço de Correio Eletrónico |
| Miguel Gonçalves | **1190903@isep.ipp.pt** |
| Rúben Rodrigues | **1191018@isep.ipp.pt** |
| Rui Pinto | **1191042@isep.ipp.pt** |
| Tomás Limbado | **1191106@isep.ipp.pt** |

# Serviços e Prioridades

Quanto menor o valor, maior a prioridade.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Módulo | Localização | Prioridade (1-3) | TMD | Serviços Dependentes | RTO | RPO |
| MDR | Microsoft SQL Server 2017 – DEI Cloud | 2 | 12 horas | SPA  Planeamento | 24 horas | 24 horas |
| MDP | MongoDB Server – DEI Cloud | 2 | 12 horas | SPA  Planeamento | 24 horas | 24 horas |
| Planeamento | SWI-Prolog – DEI Cloud | 3 | 24 horas | MDR  MDP | 36 horas | 36 horas |
| SPA | Apache and others on Ubuntu – DEI Cloud | 1 | 6 horas | Todos | 12 horas | 12 horas |

**TMD** – Tempo Máximo de Disrupção – Tempo considerado aceitável para o sistema estar sem serviço correspondente.

**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.

# Mitigação de Riscos

Analisando os serviços utilizados verificamos que a maior vulnerabilidade no nosso projeto é a utilização de VM’s do DEI.

Para se mitigar este risco a transição para serviços de Cloud pagos seria a melhor solução. Porém, tendo sempre em conta a qualidade/preço e se é viável essa opção.

# Matriz de Risco

A matriz de risco tem por objetivo fazer uma avaliação tendo em conta a avaliação do impacto e a probabilidade de ocorrência de uma falha nos sistemas.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Intolerável | Indesejável | Tolerável | Aceitável |
| 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 |

# Avaliação de Riscos

|  |  |  |  |
| --- | --- | --- | --- |
| Módulo | Risco | Classificação | Justificação |
| SPA | Falha da VM do DEI | 16 | Há múltiplas razões para que ocorra falha na VM do DEI, e tem esta classificação por ser um serviço com prioridade e será intolerável que a falha aconteça. |
| MDR | Falha da VM do DEI | 12 | Há múltiplas razões para que ocorra falha na VM do DEI, e tem esta classificação por ser um serviço com alguma prioridade e será indesejável que a falha aconteça. |
| MDP | Falha da VM do DEI | 12 | Igual à do MDR |
| Planeamento | Falha da VM do DEI | 8 | Há múltiplas razões para que ocorra falha na VM do DEI, e tem esta classificação por ser um serviço com alguma prioridade, mas será tolerável que a falha aconteça. |
| Todos | Ataques DDoS e DoS | 6 | Possíveis ataques à VM devem ser considerados. |
| Todos | Falha na conexão à Internet | 4 | A falha na conexão à Internet pode impedir a conectividade com os restantes módulos do Produto. |
| Todos | Falha no fornecimento de eletricidade | 4 | Este acontecimento, embora improvável, será responsável pela inativação dos módulos. |

# Estratégia de Backup

Relativamente aos backups, as suas estratégias vão ser dependentes dos sistemas que estamos a ponderar, por exemplo, tanto poderão ser backups diários como poderão ter de ser backups incrementais diários no caso de o serviço ser mais crítico, como é o caso do SPA.

Para os serviços com maior prioridade (MDR e MDP) o ideal seria um backup integral em 2 dias da semana (por exemplo ao domingo e o outro num dia útil) e ainda backups incrementais a cada 12 horas.

Para os serviços com prioridade inferior aos acima mencionados o ideal seria um backup integral semanal (por exemplo ao domingo) e ainda um backup incremental diário.

# Processos de Recuperação

* Em caso de falha numa das VM’s do DEI, deve ser efetuado o restauro do sistema a partir do último backup, assegurando a rápida reparação e disponibilização dos módulos hospedados nas máquinas.
* Em caso de falha na conexão à Internet ou no fornecimento de eletricidade, deve ser efetuado um processo idêntico.

# Conclusão

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.