**ASIST**

**Administração de Sistemas**

Sprint 2 – G033

A picture containing shape

Description automatically generated

1210816 - João Castro

1210913 - Pedro Mendes

1211523 - Martim Botelho

1191831 - Rui Gonçalves

ÍNDICE

[Alínea 1 3](#_Toc149511452)

[Alínea 2 4](#_Toc149511453)

[Alínea 3 6](#_Toc149511454)

[Alínea 4 8](#_Toc149511455)

[Alínea 5 13](#_Toc149511456)

[Alínea 6 16](#_Toc149511457)

[Alínea 7 18](#_Toc149511458)

[Alínea 8 20](#_Toc149511459)

# **Divisão - User Stories**

|  |  |
| --- | --- |
| **Alínea 1** | Ficou responsável pelo Pedro Mendes - 1210913 |
| **Alínea 2** | Ficou responsável pelo Martim Botelho - 1211523 |
| **Alínea 3** | Ficou responsável pelo Martim Botelho - 1211523 |
| **Alínea 4** | Ficou responsável pelo João Castro - 1210816 |
| **Alínea 5** | Ficou responsável pelo Rui Gonçalo - 1191831 |
| **Alínea 6** | Ficou responsável pelo Rui Gonçalo - 1191831 |
| **Alínea 7** | Ficou responsável pelo Pedro Mendes - 1210913 |
| **Alínea 8** | Ficou responsável pelo João Castro - 1210816 |

# **Alínea 1**

Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO definido no sprint B

O plano de recuperação de desastres é um procedimento para reaver o trabalho após uma perda. Este plano está dividido em várias fases:

* Métricas relativas ao tempo – Recovery Point Objective (RPO) e Recovery Time Objective (RTO)
* Assinalar as pessoas responsáveis por cada ação
* Listar todos os aplicativos/equipamentos que são usados para o bom funcionamento da organização
* Backups
* Recuperações de serviços
* Local específico para ser efetuada a recuperação dos desastres
* Restauro

RPO e RTO são métricas essenciais para a elaboração de um plano de recuperação de desastres.

* RPO é a quantidade de dados que se pode perder de maneira que as suas operações vitais não sejam afetadas.
* RTO define o limite de tempo que uma aplicação pode ficar inativa até que se consiga restabelecer o sistema ou o ambiente afetado pelo desastre.

A organização em questão definiu os seguintes valores para RPO e RTO:

RPO: 3 horas - A organização garante que não perderá mais do que 3 horas de dados em caso de desastre.

RTO: 2 horas - A organização garante que suas aplicações estarão operacionais novamente dentro de 2 horas após um desastre.

Essas definições refletem a necessidade da organização de minimizar o impacto de um desastre em suas operações.

A definição desses valores deve ser feita com base na análise dos riscos da organização e dos impactos que um desastre pode causar em suas operações.

O um plano de recuperação de desastres precisa de ser bem definido e bem implementado daí conter alguns elementos necessários para a realização do mesmo.

O plano inclui os seguintes elementos:

* Testagem dos métodos de recuperação: O plano é testado pelo menos duas vezes por ano para assegurar o seu funcionamento.
* Lista de ativos essenciais: A organização possui uma lista dos hardwares, softwares e serviços de nuvem necessários para o dia a dia.
* Procedimentos de backup: A organização faz backups regulares de todos os dados e aplicativos essenciais para evitar a perda de dados.
* Procedimentos de recuperação de serviços: A organização implementou um sistema de failover para garantir que seus serviços essenciais continuem ativos mesmo caso aconteça algum tipo de desastre.
* Local de recuperação de desastres: A organização utiliza o Azure como seu local de recuperação de desastres.
* Procedimentos de restauro: O plano de recuperação tem procedimentos bastante específicos caso aconteça um desastre. Pois caso aconteça é necessários restaurar os dados e aplicativos.

Os procedimentos de restauro são deferentes com base no contexto do desastre.

* Contexto 1: Avaria na base de dados principal: Neste contexto, aplica-se uma restauração da base de dados a partir de um backup.
* Contexto 2: Avaria num dos serviços da aplicação: Neste contexto, usa-se o serviço de failover para substituir o serviço que falhou.

O plano de recuperação de desastres da organização é um exemplo de como as empresas podem se preparar para lidar com desastres.

Aqui estão algumas dicas para ajudar as empresas a desenvolver um plano de recuperação de desastres:

* Defina seus objetivos e metas: O que você espera alcançar com seu plano de recuperação de desastres? Você quer restaurar seus sistemas e dados em um determinado período?
* Identifique seus ativos essenciais: Quais sistemas e dados são essenciais para o seu negócio?
* Avalie seus riscos: Quais são os tipos de desastres que podem afetar sua empresa?
* Desenvolva um plano de ação: Quais são os passos que você tomará para restaurar seus sistemas e dados em caso de desastre?
* Teste seu plano: Teste seu plano regularmente para garantir que está atualizado e funcionando corretamente.

# **Alínea 2**

Como administrador da organização quero que me seja apresentada de forma justificada a ou as alterações a realizar na infraestrutura por forma a assegurar um MTD (Maximum Tolerable Downtime) de 20 minutos

Antes de explicar esta alínea vamos apresentar alguns conceitos teóricos para facilitar a compreensão desta questão. Iremos começar por explicar o que é o RTO, WRT e por fim o MTD.

RTO, WRT e MTD são métricas essenciais para a elaboração de um plano de recuperação de desastres.

* RTO (**Recovery Time Objective)** define o limite de tempo que uma aplicação pode ficar inativa até que se consiga restabelecer o sistema ou o ambiente afetado pelo desastre.
* WRT (Work Recovery Time) define o tempo máximo que é necessário para testar e verificar a operacionalidade de todos os sistemas, aplicativos, banco de dados e outros.
* MTD (Maximum Tolerable Downtime) define o tempo máximo de inatividade tolerável dos sistemas.

O cálculo de MTD é dado pela soma de RTO e WRT.

Exemplo:

* RTO: 2 horas
* WRT: 1 hora
* MTD: 3 horas

Significa que a organização pode tolerar que os sistemas fiquem inativos por até 3 horas em caso de desastre.

A definição desses valores deve ser feita com base na análise dos riscos da organização e dos impactos que um desastre pode causar em suas operações.

O WRT deve ser automatizado para que não seja necessário o envolvimento humano pois automatizar esse processo pode ajudar a reduzir o tempo de recuperação e aumentar a confiabilidade do plano de recuperação de desastres.

Aqui estão algumas dicas para automatizar o WRT:

* Utilize um sistema de automação de testes.
* Crie scripts de teste automatizados.
* Utilize ferramentas de monitoramento de desempenho.

A automatização do WRT pode ser uma tarefa complexa, mas é um investimento que vale a pena para qualquer organização que deseja ter um plano de recuperação de desastres eficaz.

Alterações necessárias:

A virtualização de servidores é uma estratégia para melhorar a recuperação de desastres. A virtualização permite que vários servidores sejam executados em um único hardware, o que pode ajudar a reduzir custos e melhorar o desempenho.

Além disso, cada conjunto de serviços deve ter pelo menos uma dupla de servidores virtuais. Isso permite que os pedidos sejam redirecionados para um servidor alternativo caso um servidor principal falhe. O servidor reserva deve ser usado como um espelho do servidor principal, para que os dados sejam mantidos atualizados.

O RTO para a recuperação de um servidor virtual com falha deve ser no máximo 15 minutos. O WRT para a recuperação de dados deve ser no máximo 2 a 3 minutos. Isso significa que o MTD total para a recuperação de um desastre deve ser no máximo 18 minutos.

Conclusão:

A virtualização de servidores pode ser uma estratégia eficaz para melhorar a recuperação de desastres. Ao reduzir custos, melhorar o desempenho e fornecer redundância, a virtualização pode ajudar as organizações a se recuperarem mais rapidamente de desastres.

Aqui estão algumas dicas adicionais para melhorar a recuperação de desastres com virtualização:

* Use um sistema de gerenciamento de virtualização (VMM) que ofereça recursos de alta disponibilidade e recuperação de desastres.
* Crie um plano de recuperação de desastres que inclua procedimentos para a recuperação de servidores virtuais.
* Teste regularmente seu plano de recuperação de desastres para garantir que ele funcione conforme o esperado.

# **Alínea 3**

Como administrador de sistemas quero que seja realizada uma cópia de segurança da(s) DB(s) para um ambiente de Cloud através de um script que a renomeie para o formato <nome\_da\_db>\_yyyymmdd sendo <nome\_da\_db> o nome da base de dados, yyyy o ano de realização da cópia, mm o mês de realização da cópia e dd o dia da realização da cópia

# **Alínea 4**

Como administrador de sistemas quero que utilizando o Backup elaborado na US 840, seja criado um script quer faça a gestão dos ficheiros resultantes desse backup, no seguinte calendário. 1 Backup por mês no último ano, 1 backup por semana no último mês, 1 backup por dia na última semana

# **Alínea 5**

Como administrador de sistemas quero que o processo da US da cópia de segurança da DB seja mantido no log do Linux, num contexto adequado, e alertado o administrador no acesso à consola se ocorrer uma falha grave neste processo

Nesta user storie pretende se que o utilizador seja informado de qualquer falha em relação a realização do backup, para isso foi necessária editar o ficheiro /etc/rsyslog.conf e descomentar o facility cron.\* acrescentando o facility cron.err e o seu devidamente ficheiro de log –/var/log/cron.err.

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

De seguida, fomos ao ficheiro /etc/profile onde acrescentou-se uma variável com o uso de wc -l com o objetivo de imprimir o numero de linhas presentes no ficheiro que antes foi adicionado.

Para acabar, adicionamos também uma condição para imprimir o conteúdo do ficheiro cron.err.

Uma imagem com texto, captura de ecrã, software, ecrã

Descrição gerada automaticamente

# **Alínea 6**

Como administrador de sistemas quero que a cópia de segurança da US da cópia de segurança da DB tenha um tempo de vida não superior a 7 (sete) dias exceto no indicado na US de retenção das cópias mensais e anuais

Para começar esta user storie em primeiro criamos o arquivo de backup\_and\_retention.sh e colocamos este conteúdo para excluir os backups com mais de 7 dias… e damos permissão a este ficheiro através do comando chmod +x backup\_and\_retention.sh

Uma imagem com texto, eletrónica, captura de ecrã, software

Descrição gerada automaticamente

Por fim testamos a eliminação de backups que foram feitos há mais de 7 dias através do comando /backup\_and\_retention.sh

Uma imagem com texto, captura de ecrã, Tipo de letra, preto

Descrição gerada automaticamente

# **Alínea 7**

Como administrador da organização quero que me seja apresentado um BIA (Business Impact Analysis) da solução final, adaptando se e onde aplicável o(s) risco(s) identificados no sprint anterior

Para fazermos o Bussiness Impact Analysis (BIA) do nosso projeto, abordamos essencialmente dois tópicos sendo estes os valores de risco dos módulos e o nível de criticidade

Iremos começar por abordar os valores de risco dos módulos.

Neste capítulo, tendo em conta o nosso projeto, conseguimos afirmar que alguns não são 100% essenciais para o funcionamento ideal do sistema como por exemplo, o modulo SPA. Este módulo é responsável pela interface do utilizador do sistema. Se o módulo SPA não estiver 100% funcional, os utilizadores não irão conseguir usar o sistema, logo podemos concluir que o valor de risco é 9

Os valores de risco são uma medida da importância do módulo para o negócio. Um valor de risco mais alto significa que o módulo é mais crítico para o negócio.

Conclusão: Os resultados da BIA indicam que o módulo SPA é um dos mais críticos para o funcionamento do sistema. As empresas devem priorizar a proteção desses módulos para garantir que o sistema esteja disponível para os utilizadores quando necessário.

Por fim vamos abordar o nível de criticidade:

|  |  |  |  |
| --- | --- | --- | --- |
| RTO | RPO | MPTD | Nível de Criticidade |
| <4h | <4h | >0h e <1h | Muito alto |
| >4h e <1d | >4h e <1,5d | >1h e <1d | Alto |
| >1d e <3d | >1,5d e <4d | >1d e <3d | Moderado |
| >3d e <14d | >4d e <15d | >3d e <7d | Baixo |
| >14d e <30d | >15d e <37d | >7d e <14d | Muito baixo |

-Segundo o impacto da reputação:

|  |  |
| --- | --- |
| Impacto no Negocio | Nível de criticidade |
| Falha no negócio, provocando várias implicações, como por exemplo o cliente ficar insatisfeito, perdas de rendimento comprometendo-o de forma irreversível a médio/grande-prazo | Muito alto |
| Falha no negócio, provocando várias implicações, como por exemplo o cliente ficar insatisfeito, perdas de rendimento comprometendo-o de forma irreversível a curto-prazo. | Alto |
| Falha no âmbito de determinadas operações de negócio, que originam alertas ou reclamações, mas que não impedem o negócio na sua totalidade | Moderado |
| Falhas com impacto residual no negócio com pouca relevância para o negócio | Baixo |
| Falhas internas sem interação com comunicações externas, sem qualquer impacto na continuação do negócio | Muito Baixo |

# **Alínea 8**

Como administrador da organização quero que seja implementada uma gestão de acessos que satisfaça os critérios apropriados de segurança

Para ser feita uma gestão de acessos é necessário seguir-se uns determinados critérios de segurança, dos quais:

* Autenticação forte: Este tópico, é para garantir que os utilizadores possuam uma boa password, para que essa seja difícil de ser descoberta. No nosso projeto, uma password é feita com caracteres alfanuméricos e com mais de 8 dígitos
* Autorização de acesso: Este tópico, foca se em limitar o acesso dos utilizadores as funcionalidades que necessitam consoante a sua função. Cada user tem um atributo que define a role do mesmo, condicionando assim as funcionalidades
* Politicas de acesso: Este tópico, é para estabelecer regras de utilização das funcionalidades da aplicação. As regras podem ser:
  + - Não utilizar a conta de outro user
    - Na ocorrência de algum problema técnico, informar um admin
    - Caso algum dos servidores fique inativo, contactar diretamente a equipa de manutenção

# **Alínea 9**

Como administrador da organização quero que seja implementado de forma justificada um sistema de clustering entre os sistemas que implementam o SPA

O primeiro passo é iniciar um processo com a implantação em um servidor adicional, para ser possível ser feitos testes operacionais do cluster

# **Alínea 10**

Como administrador de sistemas quero que o administrador tenha um acesso SSH à maquina virtual, apenas por certificado, sem recurso a password

Para começar esta user storie acedemos ao ficheiro */etc/ssh/sshd\_config onde se alterou o PermitRootLogin como yes para ser possível fazer login do root através de um user remoto.*

Uma imagem com texto, captura de ecrã, Tipo de letra, design

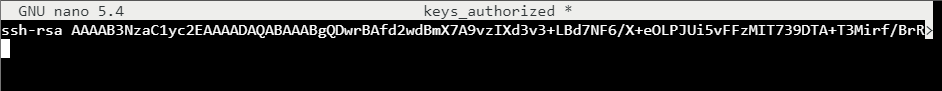
Descrição gerada automaticamente

Após isso, criamos um file keys\_authorized onde estão especificadas as chaves SSH que podem ser usadas pelo root.

Relativamente ao Windows o primeiro passo foi executar o comando ssh-keygen para criar pares de chaves de ssh para dar login.

Após isso acedeu se ao diretório do ssh onde estavam dois ficheiros das chaves, um publico e um privado. Abriu se o ficheiro publico id\_rsa.pub e copiou se a chave.

Apos isso, fomos ao Linux e colocamos a chave que copiamos no ficheiro do ssh.



Por fim demos logout na maquina virtual e ao voltar ao entrar não foi necessário password.

# **Alínea 11**

Como administrador de sistemas quero que para agilização entre as várias equipas seja criada uma partilha pública de ficheiros, formato SMB/CIFS  ou NFS .

Para a realização desta user storie o primeiro passo foi a instalação do samba na maquina virtual através do comando sudo apt-get samba.

De seguida acedemos ao ficheiro smb.conf, através do comando sudo nano /etc/samba/smb.conf e adicionamos uma secção de compartilhamento para isso metemos la estes comandos e reiniciamos o sistema:Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

De seguida instalamos o servidor NFS usando o seguinte comando sudo apt-get install nfs-kernel-server e acedemos ao seu ficheiro de configuração através do comando sudo nano /etc/exports e colocamos uma linha para o compartilhamento publico:

Uma imagem com texto, captura de ecrã, software, Tipo de letra

Descrição gerada automaticamente

E por fim reiniciamos o serviço de NFS

Considerações importantes:

* Permissões:

Certifique-se de que as permissões no diretório compartilhado são configuradas corretamente para garantir que as equipes tenham as permissões adequadas.

* Firewall:

Verifique se a firewall está configurado para permitir o tráfego nos protocolos (SMB ou NFS) e nas portas associadas.

* Segurança:

Considere a implementação de autenticação e autorização adequadas, dependendo dos requisitos de segurança da sua organização.

* Backup:

Implemente um plano de backup regular para garantir a integridade dos dados compartilhados.

# **Alínea 12**

Como administrador de sistemas temos de garantir que em caso de necessidade os backups foram efetuados corretamente. Para isso devemos automatizar a sua reposição, validando no final o funcionamento do sistema (Ex. Base de Dados - executar uma query SQL com sucesso após reposição)

O primeiro passo será criar um script de backup, como mostra a seguinte imagem