

Relatório de ASIST

Sprint 3

Turma 3DA _ Grupo 2

1190624 - Gonçalo Monteiro

1190797 - Lara Domingos

1190818 - Luís Pinto

1190825 - Luís Costa

Data: 08/01/2023

Índice

| | |
|--|---|
| User Stories | 3 |
| US 1: Luís Costa (1190825) | 3 |
| US 3: Lara Domingos (1190797) | 4 |
| US 4: Lara Domingos (1190797) | 6 |
| US 7: Gonçalo Monteiro (1190624) | 7 |
| US 10: Luís Pinto (1190818) | 8 |

User Stories

US 1: Luís Costa (1190825)

Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO definido na US B5

Podemos começar por descrever em que consiste um plano de recuperação de desastres. Este consiste num documento formal que descreve um conjunto de procedimentos e medidas tomadas com o objetivo de garantir a continuidade de atividades ou negócios em caso de falhas técnicas, ataques informáticos ou desastres naturais, diminuindo o impacto que estas causam no conjunto e procedimento normal de atividades, mesmo em condições adversas.

Assim sendo podemos começar por listar diversas possibilidades que obrigam a existência de um plano de recuperação de dados (PRD):

- Desastres naturais (Terramotos, inundações, incêndios florestais, deslizamentos de terras, tsunamis etc.);
- Falhas de hardware ou software;
- Ataques informáticos (DDoS, Malware, etc.);
- Danificação de hardware por 3os;

Os pontos chave para a construção e cumprimento de um PRD consistem na avaliação de risco, análise do impacto empresarial, estratégias de recuperação, testes e formação e manutenção.

Avaliar o risco da organização consiste em listar as possíveis causas de adversidade, como listado acima. Analisar o impacto empresarial implica avaliar o nível de impacto que um desastre venha a causar na perda de dados, lucros ou investidores.

Quanto as estratégias de recuperação, são necessárias as implementações de planos de backup regular, possivelmente por diversos meios (backup do backup), e capacidade de alteração de espaço de trabalho. Deve, portanto, ser regular a realização de testes as estruturas e meios de recuperação de dados e formar os membros da organização com os procedimentos adequados aquando de um acontecimento de carácter catastrófico. A prática de simulações de catástrofe é também ideal na maioria dos casos, permitindo uma melhor sensibilização numa situação dita real. Uma manutenção adequada dos meios e do PRD em si permite minimizar o impacto causado e ajuda a organização a sofrer o mínimo de repercussões possível.

US 3: Lara Domingos (1190797)

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.

Para ser possível realizar uma copia de segurança da DB para um ambiente de Cloud, no meu caso usei a google drive pessoal, foi criado um script que faz conexão com a base de dados do projeto da Logística, designado por mongodb, e também foram instaladas as dependências necessárias para a execução do mesmo, como por exemplo, wget https://fastdl.mongodb.org/tools/db/mongodb-database-tools-debian11-x86_64-100.6.1.tgz.

```
#!/bin/bash

DIA="/gdrive/diario/"
SEM="/gdrive/semanalmente/"
MES="/gdrive/mensalmente/"

root@vs262:~# gdrive about
Authentication needed
Go to the following url in your browser:
https://accounts.google.com/o/oauth2/auth?access_type=offline&client_id=367116221053-7n0vf5akeru7on6o2fjinrecpdoe99eg.apps.googleusercontent.com&redirect_uri=http%3A%2F%2Flocalhost%3A1&response_type=code&scope=https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fdrive&state=state
Enter verification code: 4/0AMgavdFw816_zBzvg1-HjEa5L0LHiCI_d91Cg75K7krsojooks1nBx1YgWlPwDV2Sg3joA
User: I am Yellow, larocasalmeyda9999@gmail.com
Used: 310.8 MB
Free: 15.8 GB
Total: 16.1 GB
Max upload size: 5.2 TB
root@vs262:~# gdrive list
Id                                     Name                                     Type   Size   Created
1GufwrX3H5E9sKEHB5VCxY_L-jx104-rzDpEVpe22u8 message-2                             doc    1.0 KB 2022-01-01 10:23:16
1yPPjNwvy7-MizKquT6Ts_zwb53GeVQKcs5KqdD5s06M message (3)                           doc    1.0 KB 2021-11-29 02:42:53
11ZqN8r3ZKzGq008hLHntrZjpiiu-UibMf9uQ99njk message (3)                           doc    1.0 KB 2021-11-29 02:33:04
1yOXf9w99XUURIV0dr1Ztr13HUIKkAHikD08-z0ZV1M message (3)                           doc    1.0 KB 2021-11-29 02:27:07
1odmiyhtVPZs5xTXo-DnyAXvhXGVUNZhw5u-BVIV1JhA message (2)                           doc    1.0 KB 2021-11-29 02:16:25
17aD9MyqeaG0eVZyx22uF6A1jId1CxZz9430U5I40rsQ message                             doc    1.0 KB 2021-11-07 21:48:20
160Mf6ptE27M9nL_0yhdUQ-BXv42VfeLA5XHPFgT2FB8 .archivetempmain.c                   doc    1.0 KB 2021-10-08 21:48:51
16n6ipza6rj9SUOP82IIXDlv6Inig114oh9RYErnHgzQ .archivetempmain.c                   doc    1.0 KB 2021-10-06 14:57:08
1-LD4XoufqtT35mgsYgkFmLc5ZQtgczLmQXDFwEkAbM .archivetempmain.c                   doc    1.0 KB 2021-10-06 14:27:22
1m1dj2lwm2SD4S-7iLUa06dfcwR03yv4duxRGXN2rjw .archivetempmain.c                   doc    1.0 KB 2021-10-06 14:17:48
14GIE06Voh3G6nUxwrrDPvsqObTr01yQk39B7hhuMas .archivetempmain.c                   doc    1.0 KB 2021-10-06 14:08:36
1Uf...
```

Figura 2- Conexão com o Google Drive

Fig. 2- Conexão com o Google Drive

Na imagem em baixo está apresentado a conexão com a google drive na VM do DEI.

Para que os ficheiros fossem guardados na google drive foram acrescentados os seguintes comandos no script.

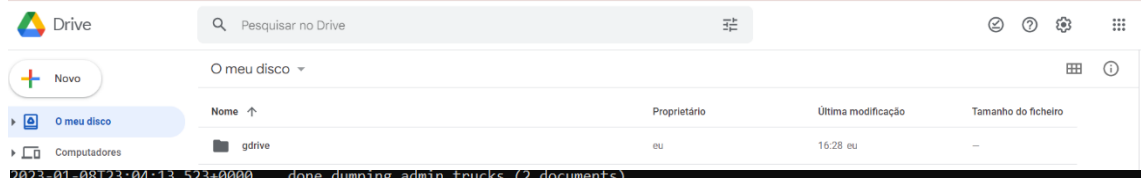
```
#Guardar na cloud(google drive)
SYNC_DIR=$(gdrive list --query "name = 'gdrive'" --no-header | awk '{print $1}')
gdrive delete -r $SYNC_DIR

gdrive mkdir gdrive
gdrive sync upload gdrive/ $SYNC_DIR
```

Figura 3- Conexão ao Google drive

Por fim, foi testado a conexão com a base de dados, se era possível aceder e posteriormente guardar na cloud em questão, e verificou-se o mesmo.

```
lara@Carry:~/sprintC$ sudo ./main_backup.sh
-----Extrair a Base de Dados -----
2023-01-08T23:04:12.998+0000    writing admin.system.users to /gdrive/diario/admin/system.users.bson
2023-01-08T23:04:13.086+0000    done dumping admin.system.users (1 document)
```



The screenshot shows the Google Drive web interface. At the top, there's a search bar and navigation icons. Below, under 'O meu disco', there's a folder named 'gdrive' owned by 'eu' (me), last modified on '16/28 eu'.

Figura 6- Pasta do backup no google drive.

```
updating: admin/system.users.bson (deflated 23%)
updating: admin/users.bson (deflated 52%)
updating: admin/system.version.bson (deflated 19%)
updating: admin/trucks.metadata.json (deflated 74%)
updating: admin/plannings.bson (deflated 57%)
updating: admin/routes.bson (deflated 68%)
updating: admin/routes.metadata.json (deflated 77%)
updating: admin/system.users.metadata.json (deflated 45%)
updating: admin/plannings.metadata.json (deflated 72%)
updating: admin/users.metadata.json (deflated 74%)
updating: admin/trucks.bson (deflated 37%)
```

Figura 4- Execução do script para retirar da base de dados e guardar na pasta dos backup diários.

```
lara@Carry:~/sprintC$ ls
gdrive  main_backup.sh
lara@Carry:~/sprintC$ cd gdrive/diario
lara@Carry:~/sprintC/gdrive/diario$ ls
'<Logistica>_20230108.zip'
lara@Carry:~/sprintC/gdrive/diario$
```

Figura 5- Localização dos Backups

Como administrador de sistemas quero que utilizando o Backup elaborado na US C3, seja criado um script que 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.

Depois de ser realizado o script para conectar a base de dados a uma cloud, foi necessário desenvolver um script para a realização de backup, diário, semanais e mensais como é pedido, e por isso foi aproveitado o script anterior para acrescentar o necessário.

Os backups foram divididos em pastas diferentes de acordo com o seu propósito. A primeira pasta criada foi a dos backups diários, onde eram guardados os que são feitos diariamente, como mostra na US anterior.

De seguida foi desenvolvido um conjunto de comando para os backups por semana, onde é retirado da pasta dos diários o último a ser realizado e este é movido para a pasta semanal, como mostra o print em baixo.

```
#Backup por semana
#verifica se é domingo
if [ $(date +%u) == 7 ]
then
echo -e "-----Backup no ultimo dia para a pasta relacionada com pasta do backup por semana-----"
#ls -t -> ordena a lista ascendente
#head -1 -> vai buscar o primeiro elemento da lista
cd $DIA
mv $(ls -t $DIA | head -1) $SEM
fi
```

Figura 7-Script para realizar o backup por semana.

Por fim, através da pasta semanal, foi retirado os backups mais recente para ser movido para a pasta do backup por mês.

```
#Backup por mês
#verifica se é o primeiro dia do mês
if [ $(date +%d) == 01 ]
then
echo -e "\n Backup da ultima semana para a pasta relacionada com o backup por mes \n"
cd $SEM
mv $(ls -t $SEM | head -1) $MES
fi
```

Figura 8- Script para realizar o backup por mês.

Para verificar se estava a guardar corretamente foram alteradas as permissões do ficheiro para que este fosse executável (chmod +x {PASTA}) e por fim foi executado. Não foi possível obter resultados, devido a certos erros apresentados no terminal do Linux.

US 7: Gonalo Monteiro (1190624)

Como administrador da organizao quero que me seja apresentado um BIA (Business Impact Analysis) da soluo final, adaptando se e onde aplicvel o(s) risco(s) da US B4

Um BIA existe com o propsito de apresentar um prazo de recuperao, desta forma compreendendo o impacto que cada desastre tenha na organizao. Utilizando os dados da US B4 podemos realizar uma anlise representada na seguinte tabela

| | Ataque DDoS / Malware | Inundaes / Sismos / Incndios | Disrupes de conectividade ou energticas | Falhas de Hardware / Software | Covid / Outros problemas de sade |
|--|---|---|---|--|--|
| Atividade Afetada | Servios informticos | Sistemas estruturais e possvel hardware | Sistemas informticos | Sistemas hardware/ software | Membros de trabalho |
| Potencial Perdas Operacionais | Sistema de coordenao de entregas no funcional | Impossibilidade de atividade normal | Impossibilidade de trabalho | Impossibilidade de trabalho | Mo de obra ou possvel perda estrutural |
| Potenciais Perdas Financeiras | Graves perdas | Perdas baixas a altas dependendo do grau de dano | Baixas a Altas dependendo do downtime | Baixas a Altas dependendo do tipo de falha | Mnimas devido a trabalho a distncia |
| Tempo Mnimo de Recuperao | 30min – 50h | 24h-1semana (dependendo dos danos) | 1h-24h | 30min-1semana | 24h-48h para realocao remota |

US 10: Luís Pinto (1190818)

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

Sendo o objetivo um acesso apenas por certificado, começamos pela criação do mesmo. Para tal utilizamos o comando `ssh-keygen`, criando uma chave par publica que permite uma autenticação automática com a máquina virtual, não sendo necessário autenticar manualmente. Este certificado ficará guardado no ficheiro `~/.ssh/authorized_keys` permitindo assim ser realizada a autenticação automática pretendida.

```
root@vs262:~/.ssh# cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDIjeGF9lZx4UE4qNMtx5wmChjk/8axH2FMf37/dk4y6o0SseosudtiRkWEJyctLWXM0rVec45TebBHw/nJA2SNsCZPJQL4FxyPhy523Iw7KM0efhJ6y3lDmS27j1o6t8lPHK3TFYGiHw6nc0zB9C0qYNhm6r140Givjy2QUL0/CcArcz9JAeNvthhsVSRCKpwcDfDwmRZ9T3lImumdDTPZtD81Jw6lG25wxs9wKUCm2Y3pfqzbQhafR/vJqzIrp1h1yIH19jT6V4sBgjEnQ4Nw79QD6ZhrQfBWeHfgLY8FqvzCaQJLNhJ9/eMDeH9pXrsvn15SmMV3IhzTRjPt/b0VhAnn+RAiERuhe657vLJImW3A37zMK4GXurxzU3tWztwnoH6m2HYa63QS+bz9K3AaFTGinP7omn0E0VDo06skL8hRK4/R8bzPveBHx58KIQXm/kB4WZa5WlYd/pUjkuWhCPgEoMbFTUMfhYoShPQsTFPxYlckbgz1jWSrWE7buE= lara.domingos@Carry
```