A picture containing shape

Description automatically generated

**Relatório Sprint 2**

**Turma 3DG-Grupo 37**

1161274- Artur Muiria

1190827- Luís Araújo

1191240- Danilton Lopes

1201183- João Oliveira

**Professor:**

André Moreira, ASC

**Unidade Curricular:**

Administração de Sistemas

**Data: 04/12/2022**

**Índice**

[**Introdução** 3](#_Toc121083183)

[**User Story 2** 4](#_Toc121083184)

[**User Story 4** 5](#_Toc121083185)

[**User Story 5** 7](#_Toc121083186)

[**User Story 6** 8](#_Toc121083187)

[***WebGrafia*** 10](#_Toc121083188)

# 

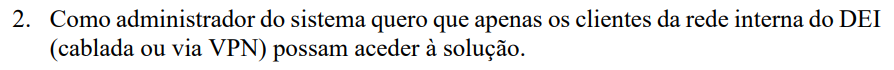
# **Introdução**

O presente relatório foi escrito no âmbito do *Sprint* 2 da unidade curricular **Administração de Sistemas.**

No presente relatório iremos apresentar as *User Stories* que foram pedidas servindo como apoio e explicação da execução destas últimas.

Visto que o grupo é constituído apenas por 4 elementos, realizamos somente 4 *User Stories*.

# **User Story 2**



Text

Description automatically generatedNesta user story foi pretendido dar acesso à solução apenas a clientes da rede interna do DEI portanto foi necessário filtrar os endereços IP com o uso do **“iptables”**.

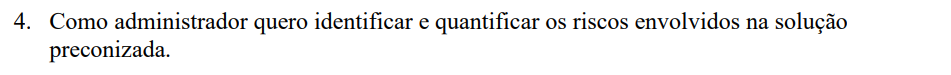
O comando **“iptables”** é utilizado para filtrar pacotes através de regras. A opção **“-A”** é usado para adicionar uma regra quando a ordem da regra na cadeia não importa. A opção **“INPUT”** é uma sequência de regras ACCEPT/DROP aplicadas aos pacotes quando chegam da rede e se destinam ao nó. A opção **“-p”** define o protocolo IP para a regra que pode ser icmp, tcp, udp ou todos, para corresponder a todos os protocolos suportados. O **“tcp”** é o protocolo escolhido.O **“-m**” serve para carregar o módulo pelo nome, **“iprange”** é o módulo, **“--src-range”** permite especificar o IP de origem num intervalo definidosendoeste o intervalo **“10.9.1.1-10.9.255.255”**.A opção **“--dport 22”** define a porta de destino para o pacote, sendo **22** o número da porta que é utilizada para comunicação Secure Shell (SSH) e permite acesso de administração remota à VM. A opção **“-j”** salta para o destino especificado quando um pacote corresponde a uma regra específica e pode ser do tipo (ACCEPT, DROP, QUEUE e RETURN). O **“ACCEPT”** permite que o pacote se mova com sucesso para o seu destino ou outra cadeira enquanto que o **“DROP”** descarta o pacote sem responder ao solicitante e não notifica ao sistema que enviou o pacote da falha.  
Portanto a primeira linha na linha de comandos permite que o intervalo de IP’s (que é neste caso a rede interna do DEI) especificado em cima tenha acesso à solução e a segunda linha bloqueia todos os outros fora desse mesmo intervalo.

O **“iptables”** não persiste as regras definidas após os reboots portanto será necessário guardar essas configurações para os próximos boots. Isso torna-se possível com a instalação do pacote **“iptables-persistent”** e de seguida com a execução de **“iptables-save > /etc/iptables/rules.v4”** onde permite persistir as configurações no ficheiro **“rules.v4”**.

Text

Description automatically generated

# **User Story 4**



De forma a haver uma boa compreensão dos riscos existentes na solução preconizada, o grupo decidiu fazer uma matriz de risco para, consoante a probabilidade e o impacto, identificar os riscos que devem receber mais atenção.

**Matriz de riscos**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | |  | | --- | | Impacto | |  |  |
| |  | | --- | | Probabilidade | | **1** | **2** | **3** |
|  |  |  | **-Falha de internet nos servidores do DEI**  **-Ataques informáticos aos servidores** |
| **1** | **– 1 –** | **– 2 –** | **– 3 –** |
|  | **-Pequenos bugs no programa** | **-Mau planeamento do projeto** |  |
| **2** | **– 2 –** | **– 4 –** | **– 6 –** |
|  |  |  |  |
| **3** | **– 3 –** | **– 6 –** | **– 9 –** |

Os valores de probabilidade que o grupo definiu para a matriz de risco foram os seguintes:

-Probabilidade baixa: 0%-30%

-Probabilidade media:31%-50%

-Probabilidade alta: 51%-70%

O valor de risco é dado pela multiplicação do valor da probabilidade com o valor do impacto.

A primeira conclusão deduzida da avaliação de riscos é que estamos muito dependentes de máquinas do DEI. Uma solução seria investir num serviço de *cloud* com uma melhor qualidade.

A segunda conclusão é existir uma segurança de má qualidade na máquina virtual, logo deverão ser investidos recursos num aumento da qualidade de segurança.

# **User Story 5**

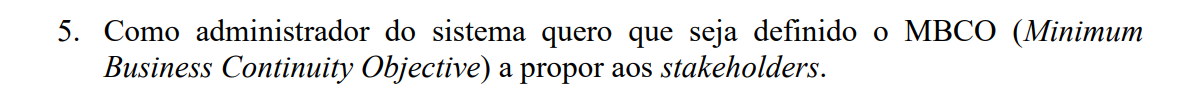


Figura 1 - Enunciado US 5

O **MBCO** (Minimum Business Continuity Objective), ou Objetivo Mínimo de Continuidade de Negócios, é o nível **mínimo** de serviços e/ou produtos que é aceitável para a organização, para **atingir** os seus **objetivos** de negócios durante um **desastre**. Por outras palavras, o MBCO **orienta** a organização sobre o que deve ser **recuperado** e qual deve ser a **extensão** da recuperação.

De facto, a estruturação do MBCO pode-se dividir em quatro fases:

* Identificação da **missão** da organização;
* Identificação dos **produtos** e **serviços** essenciais;
* Identificação de possíveis **disrupções** em cada **área**/**serviço** da organização;
* Identificação do **tempo** de **funcionamento** após a disrupção e do tempo levado a **restaurar** os danos.

Relativamente ao primeiro ponto, a **missão** da nossa organização é a **distribuição** de **entregas** entre armazéns utilizando uma **frota** de **veículos** **elétricos,** tentando **otimizar** todas as viagens entre armazéns.

Relativamente ao segundo ponto, a aplicação divide-se em **três módulos**- gestão de armazéns, logística e planeamento de distribuição- sendo estes os **serviços** **essenciais** para o **bom** e **correto** **funcionamento** da organização. Resumidamente, esta última tem como objetivo a **criação** **otimizada** de **rotas** entre os seus armazéns com as entregas que vão sendo feitas, tendo em conta as **distâncias** mas também as **baterias** dos veículos elétricos.

Relativamente ao terceiro ponto, as **disrupções** podem **influenciar** o **funcionamento** da organização tanto a nível **físico**/**material** como a nível dos **programas**. Em relação ao primeiro, desastres naturais como **sismos** podem **destruir** os **equipamentos** utilizados pela organização e **impossibilitar** o **funcionamento** desta mesma. Em relação às disrupções a nível dos programas, a aplicação da organização tanto pode sofrer **ataques informáticos** como **avarias** na **base de dados** ou mesmo no ***core*** da aplicação.

Por fim, e relativamente ao quarto ponto, como **administrador** do **sistema** abordarei apenas as disrupções ao **nível da aplicação**. Para estas disrupções, e perante a **impossibilidade** de se **selecionarem** novas **entregas** e, consequentemente, **carregar** **totalmente** os seus veículos, a organização distribuirá **20%** destas nos armazéns em **24 horas**. O mesmo se aplica à **impossibilidade** de se conseguirem **criar** **rotas** de forma **eficiente**, pelo que a empresa distribuirá os mesmos **20%** de entregas em **24 horas** num raio de **40km** relativamente ao armazém **principal**. Quanto às **avarias** na **base de dados**, a nossa organização possui uma base de dados de **suporte** que contém as **cópias de segurança** feitas a partir da base de dados **principal**. Assim, a organização utilizará **90%** dos dados totais.

# **User Story 6**

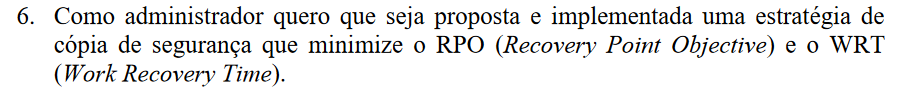


Figura 2 - Enunciado US 6

Antes de falar sobre a estratégia que será proposta primeiro iremos explicar quais são os conceitos de **RPO (Recovery Point Objetive)** e **WRT** **(Work Recovery Time)** e ainda mais conceitos relacionados, como **RTO (Recovery Time Objetive)**, **MTD (Maximum Tolerable Downtime)**, retenção e arquivamento, que fazem parte de planeamento para recuperação de desastres. Estes 2 conceitos pedidos em si separados não farão efeito pois fazem parte de uma sequência de etapas para a recuperação de operacionalidade da produção de uma organização, e que entre **RPO** e **WRT**, têm-se o **RTO**.

* **RPO**, Recovery Point Objetive, é um método de controle para que possa ser calculado a quantidade de dados que a organização poderia perder em caso de paralisação sem que haja a possibilidade de reversão. Este servirá para que seja feito um plano B para minimizar os problemas ao extremo ou quase exterminá-lo de forma que não cause percas significativas.
* **RTO**, Recovery Time Objetive, é uma métrica para que se calcule o tempo máximo que o que um sistema levaria para que volte a sua operacionalidade normal após um desastre, ou seja, quando para de funcionar por algum motivo que comprometa a operacionalidade da organização. Para o cálculo de RTO deve se ter em conta todas as questões de prioridade do negócio, ou seja, quanto maior a prioridade menor deve ser o tempo para que seja recuperado.
* **WRT**, Work Recovery Time, é usado para determinar o tempo máximo para que se teste e verifique todos os sistemas, podendo ser eles: **sistemas, aplicações, banco de dados** e outros. Mesmo fazendo parte da sequência e sendo uma etapa crucial na recuperação de desastres esta etapa pode a sua ação pode requerer um esforço mínimo, ou até inexistente, uma vez que com a evolução da automação isto acaba por ser incluído nos sistemas de atualmente, ou até mesmo garantido por sistemas internos próprios da organização ou de serviços contratados.
* **MTD,** Maximum Tolerable Downtime, que significa literalmente a sua tradução, o tempo máximo de inatividade/inoperacionalidade tolerável. Ou seja, é o tempo que a empresa deve tolerar a inatividade dos sistemas que estão inativos. Podem existir diferentes MTD para cada parte diferente da organização, dependendo também da sua prioridade e o que afeta a inoperacionalidade daquele sistema. O cálculo de MTD é dado pela soma de RTO e WRT.

A picture containing timeline

Description automatically generated

Figura 3 - Linha de tempo de operação impactada por um desastre

Com a imagem acima apresentar-se-á uma estratégia de cópia de segurança (backups). Alguns pontos a ser considerado são:

* O relatório estará a falar da organização no qual estamos a desenvolver uma aplicação, no âmbito da licenciatura de Engenharia Informática, no primeiro semestre do 3º ano de curso.

Sabendo que o sistema desenvolvido fará um **Mirroring,** dos teus dados para um servidor/base de dados do sistema para um servidor/base de dados exterior, ou pode ser para um local remoto, no qual aconselharíamos ter uma configuração dos servidores para que façam cópias de segurança, num horário onde não se regista utilizadores no sistema, ou o mínimo possivel. Com isso facilitaremos a recuperação de dados no caso de um desastre. Então propõe-se com que seja feito cópias de seguranças com uma estratégia **incremental**, no qual todos os dias numa determinada hora, de preferência quando não há nenhum utilizador do servidor, ou o mínimo, por exemplo de madrugada. Sendo implementado esta estratégia, a organização terá um **RPO** de no máximo **24 horas**, sendo mais ou menos 1 dia de trabalho, ou seja, 8 horas de trabalho.

Por causa do **Mirroring** do sistema o RTO e WRT passam a ser mínimos e quase nulos, uma vez que estão guardados pelo menos 2 lugares diferentes e a chances de isso darem errados são baixas. E o RTO, será o tempo de verificar se houve algum problema, se os dados foram perdidos ou algum foi corrompido, e no caso de confirmar-se vai buscar os dados onde estão no servidor onde estão as cópias de segurança. E o WRT será praticamente nulo uma vez que o sistema logo de início já verifica o funcionamento do sistema e executa testes para que se conforme a totalidade do funcionamento das aplicações.

# ***WebGrafia***

<https://pt.linkedin.com/pulse/mtd-e-wrt-conceitos-para-ir-al%C3%A9m-do-rpo-rto-rodrigo-gazola-?trk=pulse-article_more-articles_related-content-card>

<https://addee.com.br/blog/mtd-e-wrt-conceitos-para-ir-alem-do-rto-e-rpo/>

<https://blog.thiagofmleite.com/2019/06/04/business-continuity-planning/>

<https://defaultreasoning.com/2013/12/10/rpo-rto-wrt-mtd/>

<https://blog.thiagofmleite.com/2019/06/05/plano-de-exercicios-tabletop-para-planos-de-recuperacao-de-desastres/>