*Sprint 2*

Administração de Sistemas

*Miguel Oliveira 1211281*

*Rodrigo Castro 1220636*

*Rodrigo Cardoso 1221083*

*Mário Ribeiro 1221019*

*Instituto Superior de Engenharia do Porto*

Table of Contents

[Us01 [] 1](#_Toc181865694)

[Us02 [Mário Ribeiro 1221019] 2](#_Toc181865695)

[Us03 [] 3](#_Toc181865696)

[Us04 [Rodrigo Cardoso 1221083] 4](#_Toc181865697)

[Us05[] 6](#_Toc181865698)

[Us06 [Mário Ribeiro 1221019] 7](#_Toc181865699)

[Us07 [Rodrigo Cardoso 1221083] 8](#_Toc181865700)

[Us08 [] 11](#_Toc181865701)

Table of Figures

# Us01 []

# Us02 [Mário Ribeiro 1221019]

# Us03 []

# Us04 [Rodrigo Cardoso 1221083]

No âmbito desta *User Story*, como Administrador de Sistemas, quero identificar e quantificar os riscos envolvidos na solução recomendada, com base no projeto envolvente.

**1.** **Como avaliar os riscos envolvidos**

As avaliações de riscos envolvidos são normalmente representadas por uma **matriz de risco**, em que cada elemento apresenta dois fatores: a probabilidade e o impacto estimado no sistema. A medida para o risco é dada pela multiplicação dos dois fatores:

**Risco = Impacto x Probabilidade**

É considerado probabilidades numa escala de 1 (menos possível) a 5 (muito possível) e o impacto numa escala de 1 (marginal) a 4 (catastrófico).



Figura - Matriz de risco

No nosso caso, a matriz de risco será usada como um auxílio para a determinação de riscos associados ao dano do sistema. Foi elaborada uma **tabela** com todos as ameaças e a determinação dos seus fatores e o seu risco associado:

|  |  |  |  |
| --- | --- | --- | --- |
| **Ameaça** | **Possibilidade** | **Impacto** | **Risco** |
| Avaria do Sistema | 1 (Improvável) | 4 (Catastrófico) | 4 (Médio) |
| Avaria dos Servidores | 2 (Remoto) | 3 (Crítico) | 6 (Médio) |
| Falhas de autenticação (Acesso indevido) | 3 (Ocasional) | 3 (Crítico) | 9 (Sério) |
| Perda da Base de Dados | 1 (Improvável) | 4 (Catastrófico) | 4 (Médio) |
| *Leak* de Dados Sensíveis | 2 (Remoto) | 3 (Crítico) | 6 (Médio) |
| Vulnerabilidades do Sistema | 2 (Remoto) | 4 (Catastrófico) | 8 (Sério) |

Com base na tabela, pode-se confirmar que a maioria das ameaças apresentadas tem uma baixa possibilidade, mas terá de sempre prevenir com base no impacto envolvido.

A avaliação dos riscos é uma ferramenta necessária na definição da **BCM (Business Continuity Management)**, dado que só será possível uma medida de prevenção para cada risco assegurado com a implementação dessa mesma ferramenta.

# Us05[]

# Us06 [Mário Ribeiro 1221019]

# Us07 [Rodrigo Cardoso 1221083]

No âmbito desta User Story, como Administrador de Sistemas, pretende-se definir uma pasta pública para todos os utilizadores registados no sistema, onde poderão ler o que foi lá colocado.

**1. Criação da pasta pública**

Foi criado uma pasta com o nome “public” no sistema Linux, com o comando:

**mkdir /public**

Para tornar a pasta pública, as permissões do diretório terão de ser alteradas. Poderá ser feito com o seguinte comando:

**chmod 755 /public**

Onde correspondem as seguintes permissões (representadas na forma octal):

* **7 (leitura, escrita e execução)** para o proprietário do diretório (neste caso a *root*)
* **5 (leitura e execução)** para os grupos e utilizadores do sistema

Quando é atribuído as permissões ao diretório, as permissões dos ficheiros e/ou pastas que estão presentes serão as mesmas da pasta principal.

**2. Inserção do ficheiro dentro da pasta**

Foi inserido um ficheiro dentro da pasta pública com os seguintes comandos:

**cd /public**

**nano test.txt**

Foi escrito um texto dentro do ficheiro criado e depois guardado.

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

Descrição gerada automaticamente

Figura - Atribuição de texto ao ficheiro criado

**3. Testes de escrita e leitura do ficheiro pelos utilizadores**

Foi iniciado sessão como um utilizador que não é administrador no sistema (no nosso caso foi o luser1).

O utilizador **conseguiu aceder à pasta pública** e assim conseguiu abrir o ficheiro presente na pasta.

Com a abertura do ficheiro, tentou alterar o conteúdo presente no ficheiro e verificou-se no seguinte erro:

Uma imagem com captura de ecrã, texto, Software de multimédia

Descrição gerada automaticamente

Figura - Tentativa de alteração do ficheiro presente na pasta partilhada

Com esse erro conseguiu-se provar que as permissões atribuídas anteriormente à pasta estão a funcionar e, como dito anteriormente, o utilizador **só irá conseguir ler** o conteúdo presente nos ficheiros/pastas dentro da pasta pública.

A criação de uma pasta pública em que todos os utilizadores poderão ler o conteúdo presente é importante na segurança da pasta, para que permite o **acesso geral** a todos os utilizadores, mas **não poderão escrever** o que está presente dentro do diretório.

# Us08 []