Uma imagem com texto, Tipo de letra, logótipo, Gráficos

Descrição gerada automaticamenteUma imagem com Tipo de letra, texto, Gráficos, logótipo

Descrição gerada automaticamente

**ASIST**

**SPRINT 3**

**Realizado por:**

**Diogo Ferreira, 1220829**

**Francisco Osório, 1220846**

**Sérgio Moreira, 1220890**

**Rafael Ferraz, 1221104**

**01/2025**

**ÍNDICE**

[Divisão Tarefas 3](#_Toc183523809)

[User Stories 4](#_Toc183523810)

[User Story 1 4](#_Toc183523811)

[User Story 2 6](#_Toc183523812)

[User Story 3 7](#_Toc183523813)

[User Story 4 8](#_Toc183523814)

[User Story 5 9](#_Toc183523815)

[User Story 6 10](#_Toc183523816)

[User Story 7 11](#_Toc183523817)

[User Story 8 12](#_Toc183523818)

[User Story 9 13](#_Toc183523819)

[User Story 10 14](#_Toc183523820)

[User Story 11 15](#_Toc183523821)

[User Story 12 16](#_Toc183523822)

# Divisão Tarefas

Tabela 1- Divisão das Tarefas

|  |  |
| --- | --- |
| User Stories | Aluno |
| 1 | Francisco Osório |
| 2 | Sérgio Moreira |
| 3 | Rafael Ferraz |
| 4 | Sérgio Moreira |
| 5 | Diogo Ferreira |
| 6 | Rafael Ferraz |
| 7 | Sérgio Moreira |
| 8 | Francisco Osório |
| 9 | Francisco Osório |
| 10 | Sérgio Moreira |
| 11 | Diogo Ferreira |
| 12 | Rafael Ferraz |

# User Stories

## User Story 1

Nesta *user story* pretendia-se que desenvolvêssemos um plano de recuperação de desastre que satisfaça o *MBCO* definido no *sprint B*.

O *Disaster Recovery Plan (DRP)* é um documento detalhado que descreve as estratégias e procedimentos de como a organização deve responder a um incidente não planeado, de forma eficaz, e retomar as suas operações diárias.

Desta forma, para satisfazer o *MBCO* que foi definido no *Sprint B*, elaborou-se o seguinte *Disaster Recovery Plan* para a nossa organização.

O plano visa cobrir a recuperação dos módulos que foram definidos no *MBCO*: o *backend,* o  *frontend ,* o *3D visualization* eo *planning.* Sendo assim, este plano tem como objetivo:

* Assegurar que as funcionalidades mínimas sejam mantidas (*MBCO*) durante uma disrupção.
* Recuperar completamente as funcionalidades de todos os módulos dentro do *MTPD* definido.
* Minimizar impactos para a organização e seus clientes.

Para isso temos uma equipa de resposta, que é essencial para garantir rapidez na resolução de problemas e coordenação.

|  |  |  |
| --- | --- | --- |
| Nome | Responsabilidade | Contacto |
| Francisco Osório | Coordenação do *DRP* e comunicação externa e interna | [1220846@isep.ipp.pt](mailto:1220846@isep.ipp.pt) |
| Sérgio Moreira | Recuperação dos módulos | [1220890@isep.ipp.pt](mailto:1220890@isep.ipp.pt) |
| Diogo Ferreira | Recuperação dos módulos | [1220829@isep.ipp.pt](mailto:1220829@isep.ipp.pt) |
| Rafael Ferraz | Gestão dos backups | [12221104@isep.ipp.pt](mailto:12221104@isep.ipp.pt) |

Para garantir a recuperação rápida e segura dos módulos, foi definida uma estratégia robusta de backups que cobre os seguintes aspetos:

* Backups incrementais diariamente;
* Backups completos ao domingo;

Desta forma, com esta estratégia de backups, é possível oferecer um equilíbrio entre eficácia e eficiência.

Os procedimentos para recuperação foram desenvolvidos com foco em garantir que os módulos sejam restaurados dentro do *MTPD*. A sequência de recuperação é estabelecida para priorizar os módulos mais críticos, assim a prioridade será dada ao *backend*, seguido do *frontend*, posteriormente o *planning* e por fim o *3D* *Visualization*. Desta forma, temos os seguintes procedimentos:

* Identificação do escopo e do impacto do incidente;
* Ativação da equipa de resposta;
* Recuperação dos dados, através dos backups recentes;
* Recuperação dos módulos;
* Verificação da operacionalidade dos módulos;
* Elaboração de um relatório detalhado para documentar o incidente e as ações tomadas;

É essencial garantir a eficácia do plano, e não apenas desenvolver, desta forma serão realizados testes periódicos, simulando alguns cenários de disrupção que podem acontecer. Sendo assim, é possível identificar falhas no plano desenvolvido, preparar a equipa de resposta e validar a capacidade da recuperação dos módulos.

Concluindo, este plano será revisado frequentemente e estará sujeito a alterações sempre que necessário, para garantir a sua eficácia frente a mudanças na infraestrutura ou na organização.

## User Story 2

## User Story 3

## User Story 4

Nesta US é pedido que os backups realizados pela US 3 sejam guardados 1 por dia da última semana, 1 por semana do último mês, 1 por mês do último ano. Para tal, precisamos de mover os backups diários para um outro diretório, visto que a US 6 apaga automaticamente os backups diários com tempo de vida superior a 1 semana:

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

Descrição gerada automaticamente

Figura - db\_backup\_save.sh

Depois, precisamos de escalonar o *script* para correr semanalmente (por exemplo, todas as terças de madrugada) e mensalmente (por exemplo, todos os dias 2, de madrugada), para isso, adicionamos o seguinte ao *cron* (**crontab -e**):

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

Descrição gerada automaticamente

Figura - crontab parcial

Como mencionado antes, a US 6 apaga os ficheiros diários com tempo de vida superior a 1 semana, mas também temos de apagar os semanais e mensais que perdem relevância:

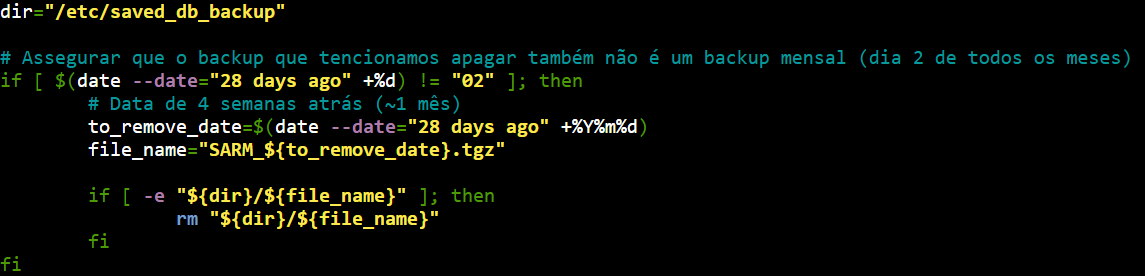


Figura - db\_remove\_old\_weeklies.sh

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

Descrição gerada automaticamente

Figura - db\_remove\_old\_monthlies.sh

Estes dois scripts apagam backups feitos 1 mês e 1 ano atrás, respetivamente, não esquecer que pode acontecer que haja um backup semanal exatamente 4 semanas após um backup mensal, nesse caso não o podemos apagar). Só precisamos agora de correr os dois scripts em simultâneo com os outros, fazendo as alterações finais ao *cron* (os de remover irão correr 5 minutos depois da hora):

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

Descrição gerada automaticamente

Figura - crontab final

## User Story 5

## User Story 6

## User Story 7

## User Story 8

Nesta *user story* foi solicitado que implementássemos uma gestão de acessos que satisfaça os critérios apropriados de segurança.

Desta forma, para termos uma gestão de acessos robusta e segura aplicaram-se as seguintes práticas:

* **Controlo de Acesso Baseado em *Roles* (*RBAC*)**: Foram definidas *roles* (*Admin, Patient, Doctor, Nurse, Technician*), atribuindo a cada uma, um conjunto de permissões que determina o acesso aos recursos ou funcionalidades. Desta forma, quando um utilizador dá login na aplicação, o *backend* retornará o *token* e a sua role, sendo estes armazenados no *localstorage* do *browser*. Sempre que o utilizador faz um pedido ao *backend*, este *token* será enviado sempre no *header* dos *requests*, sendo verificado assim no *backend* se o utilizador tem permissões para tal funcionalidade, através de políticas de autorização. Já no *frontend*, cada *role* tem a sua *dashboard* personalizada e para além disso, todas as rotas são protegidas por um *Guard* (neste caso *Role* *Guard*), garantindo assim maior segurança no acesso às funcionalidades do sistema.
* **Armazenamento das Passwords:** Na nossa aplicação estamos a usar um provedor externo, para facilitar a parte da autenticação e autorização, o *Auth0*. Desta forma, o *Auth0* armazena as passwords dos utilizadores de forma segura, utilizando práticas de segurança como o *hashing*,
* **Política de Password**: Foi definida uma política de password robusta que seguem os seguintes critérios:
  + Conter pelo menos 8 caracteres;
  + Incluir uma letra maiúscula, um número e um caractere especial
* **Bloqueio após exceder as tentativas de *Login*:** Para proteger as contas dos utilizadores contra ataques *Brute-Force* e acessos não autorizados, caso um utilizador falhe o login após 5 tentativas a conta do mesmo será bloqueado e enviada uma notificação por email.
* **Expiração do *Token*:** O *token* emitido pelo *backend* após o login foi definido para ter uma expiração de 3600 segundos, ou seja, 1 hora, independentemente da atividade do utilizador.
* ***Single Sign-On* (*SSO*)**: Para simplificar a experiência do utilizador e aumentar a segurança, utilizou-se um *SSO* que já vem definido por *default* no *Auth0*, sendo assim possível aceder a várias aplicações da organização uma única credencial de login, não havendo credenciais duplicadas.
* ***Logs* de Auditoria:** Foi implementado um sistema de *logs* de auditoria, também fornecido já pelo *Auth0*, que regista todas as atividades relevantes de autenticação e autorização. Esses *logs* incluem eventos como tentativas de login (bem-sucedidas ou não), alterações nas credenciais dos utilizadores, mudanças nas permissões de acesso e ações administrativas (como a criação, atualização e deleção de utilizadores e roles).

Concluindo, através das práticas anteriormente descritas, é possível estabelecer uma gestão de acessos segura, desde a proteção das contas dos utilizadores contra os ataques e acessos não autorizados, mas também oferecer uma experiência confiável e eficiente para todos os utilizadores da aplicação.

## User Story 9

## User Story 10

## User Story 11

## User Story 12