Relatório ASIST

Sprint 3

Instituto Superior de Engenharia do Porto – Janeiro 2025

Grupo 51

Gonçalo Costa – 1220897

Gonçalo Ribeiro- 1220702

Guilherme Pinto – 1221074

José Sá - 1220612

Índice

[Atribuição User Stories 4](#_Toc187003559)

[Introdução 4](#_Toc187003560)

[User Story 1 5](#_Toc187003561)

[Plano de Recuperação de Desastres (DRP) 5](#_Toc187003562)

[User Story 2 7](#_Toc187003563)

[Implementação de Sistemas de Monitorização e Alerta 7](#_Toc187003564)

[Mecanismos de cópia de segurança e recuperação: 7](#_Toc187003565)

[Clustering e balanceamento de carga: 7](#_Toc187003566)

[Formação de funcionários: 7](#_Toc187003567)

[Testes de esforço: 7](#_Toc187003568)

[Simulações de recuperação de desastres: 8](#_Toc187003569)

[Consequências das alterações 8](#_Toc187003570)

[Alinhamento com o MBCO 8](#_Toc187003571)

[Avaliação e Mitigação de Riscos 8](#_Toc187003572)

[Viabilidade e relação custo-benefício 9](#_Toc187003573)

[Conhecimento Técnico 9](#_Toc187003574)

[Plano de Teste e Validação 9](#_Toc187003575)

[User Story 3 10](#_Toc187003576)

[User Story 4 13](#_Toc187003577)

[User Story 5 16](#_Toc187003578)

[User Story 6 17](#_Toc187003579)

[User Story 7 18](#_Toc187003580)

[Identificação 18](#_Toc187003581)

[Quantificação de Potenciais Impactos 19](#_Toc187003582)

[Impactos Financeiros 19](#_Toc187003583)

[Impactos Operacionais 19](#_Toc187003584)

[Impactos Legais e Regulatórios 19](#_Toc187003585)

[Identificação de Dependências 19](#_Toc187003586)

[Adaptação ao Risco 20](#_Toc187003587)

[Recomendações 21](#_Toc187003588)

[User Story 8 22](#_Toc187003589)

[User Story 9 23](#_Toc187003590)

[User Story 10 25](#_Toc187003591)

[User Story 11 29](#_Toc187003592)

[User Story 12 30](#_Toc187003593)

# Atribuição User Stories

|  |  |
| --- | --- |
| User Story | Aluno |
| 1 | José Sá - 1220612 |
| 2 | Gonçalo Ribeiro - 1220702 |
| 3 | Gonçalo Costa – 1220897 |
| 4 | Guilherme Pinto – 1221074 |
| 5 | Gonçalo Costa – 1220897 |
| 6 | Guilherme Pinto – 1221074 |
| 7 | Gonçalo Ribeiro - 1220702 |
| 8 | José Sá - 1220612 |
| 9 | Gonçalo Ribeiro - 1220702 |
| 10 | Gonçalo Costa – 1220897 |
| 11 | Guilherme Pinto - 1221074 |
| 12 | José Sá - 1220612 |

# Introdução

Este projeto está a ser desenvolvido no âmbito da Unidade Curricular de Administração de Sistemas Informáticos (ASIST), no ano letivo de 2024/2025.

Ao longo deste projeto, serão abordadas várias tecnologias e ferramentas bastante presentes no contexto de administração de sistemas, tais como servidores Windows e Linux. Este trabalho prático dá a oportunidade aos membros do grupo de consolidarem as competências essenciais abordadas na UC.

# User Story 1

## Plano de Recuperação de Desastres (DRP)

Este plano visa garantir que o nosso sistema de marcação de cirurgias e gestão de informação hospitalar retoma as suas operações mínimas necessárias no menor tempo possível, priorizando a segurança dos pacientes e das operações em curso.

Com base no MBCO, as funcionalidades críticas que têm de ser mantidas durante uma falha incluem:

* **Registo de pacientes:** Permitir o registo e acesso às informações dos pacientes.
* **Pedidos e Gestão de Cirurgias**: Garantir o agendamento de cirurgias e o acesso às informações de procedimentos já agendados.
* **Marcação de Cirurgias de Emergência**: Priorizar e viabilizar a marcação de procedimentos de emergência.
* **Backup e Recuperação de Informação**: Assegurar a integridade e disponibilidade dos dados através de backups regulares e mecanismos de recuperação.

A equipa de resposta é a equipa técnica responsável pela administração do sistema e do banco de dados. Os maiores riscos que possam vir a acionar este plano são:

* Falhas de hardware ou software.
* Ataques cibernéticos.
* Interrupções elétricas prolongadas.
* Desastres naturais.

Cada funcionalidade crítica tem um Recovery Time Objective (RTO):

* **Registo de Pacientes:** 15 minutos.
* **Pedidos e Gestão de Cirurgias:** 30 minutos.
* **Marcação de Cirurgias de Emergência:** 10 minutos.
* **Backup e Recuperação:** 1 hora.

Para evitar danos significativos, devem ser implementadas várias estratégias de recuperação, como:

* Backup automático de dados em intervalos regulares.
* Redundância no armazenamento de dados e no sistema em si.
* Realizar testes trimestrais do plano de recuperação.

Em caso de uma falha, os procedimentos a seguir são:

* Notificar a equipa responsável imediatamente após ser detetada uma falha.
* Redirecionar operações críticas para sistemas de backup
* Informar os funcionários da clínica sobre a falha.
* Restaurar backups para o sistema principal.
* Verificar integridade dos dados e realizar testes de funcionalidade antes de retornar à operação completa.

No caso de uma falha, as funções secundárias que podem ser desativadas são:

* Gestão de Perfis.
* Módulo de Visualização 3D do Hospital.
* Algoritmos Avançados de Marcação (substituído por processos manuais).

É importante realizar treinamentos anuais para a equipa de resposta familiarizar-se com os procedimentos do DRP. Também é preciso atualizar o plano em caso de houver alterações no sistema.

Em caso de emergência, é preciso manter uma lista atualizada de contatos essenciais, como os coordenadores da equipa técnica.

# User Story 2

Esta User Story visa justificar as alterações necessárias à infraestrutura da organização para garantir um tempo máximo de inatividade tolerável (MTD - Maximum Tolerable Downtime) de 20 minutos. O MTD representa o limite máximo de tempo em que um sistema pode estar indisponível sem causar impacto significativo às operações críticas da organização.

Para atingir um MTD de 20 minutos, são propostas as seguintes alterações de infraestrutura:

Implementação de Sistemas de Monitorização e Alerta:

Implementar sistemas capazes de detetar falhas e notificar os administradores de imediato para minimizar o tempo de reação e garantir uma resolução rápida.

## Mecanismos de cópia de segurança e recuperação:

Backups automatizados regulares de sistemas e bases de dados críticos.

## Clustering e balanceamento de carga:

Implementar clusters de alta disponibilidade e balanceadores de carga (por exemplo, HAProxy) para distribuir o tráfego por vários servidores e garantir a tolerância a falhas.

## Formação de funcionários:

Formação da equipa em resposta a incidentes, procedimentos de cópia de segurança e resolução de problemas básicos para reduzir a dependência de suporte externo durante emergências.

## Testes de esforço:

Testes de esforço regulares para validar a capacidade do sistema sob cargas elevadas e identificar estrangulamentos.

## Simulações de recuperação de desastres:

Realização de exercícios simulados de recuperação de desastres para garantir que todas as partes interessadas estão preparadas para reagir prontamente durante uma interrupção.

## Consequências das alterações

Cada alteração proposta contribui diretamente para atingir o MTD de 20 minutos:

* Os sistemas de monitorização detetam problemas em tempo real, permitindo uma ação imediata.
* Os backups e a recuperação garantem a perda mínima de dados e a rápida restauração de serviços.
* O clustering e o balanceamento de carga mantêm a disponibilidade operacional mesmo durante falhas de hardware ou software.
* A formação dos colaboradores reduz o tempo de resolução de questões menores.

## Alinhamento com o MBCO

O Objetivo Mínimo de Continuidade de Negócio (MBCO) exige uma capacidade operacional mínima aceitável durante uma interrupção. As alterações propostas alinham-se com:

* Garantir o funcionamento ininterrupto de serviços essenciais como bases de dados e servidores.
* Garantir que os sistemas críticos cumprem os requisitos de SLA predefinidos.

## Avaliação e Mitigação de Riscos

Com base na Avaliação de Risco (RA), os principais riscos incluem o tempo de inatividade do sistema, a perda de dados e os ataques cibernéticos. As estratégias de mitigação incluem:

* Backups automatizados para proteger a integridade dos dados.
* Sistemas de firewall e prevenção de intrusão para proteção contra ameaças externas.
* Configurações de alta disponibilidade para solucionar falhas de hardware.

## Viabilidade e relação custo-benefício

* Análise Custo-Benefício:
  + O investimento em clustering, ferramentas de monitorização e backups garante custos mais baixos a longo prazo, evitando tempos de inatividade prolongados e possíveis violações de dados.
  + As soluções de código aberto (por exemplo, HAProxy baseado em Linux, ferramentas de monitorização) reduzem os custos iniciais de implementação.
* Viabilidade: As tecnologias propostas (por exemplo, HAProxy, scripts de cópia de segurança) são padrão da indústria e bem documentadas, garantindo uma implementação sem problemas.

## Conhecimento Técnico

O conhecimento técnico necessário inclui o conhecimento de:

* Configuração de cluster (por exemplo, HAProxy).
* Scripts de automatização de backup.
* Ferramentas de teste de esforço. As equipas internas ou os especialistas externos contratados atenderão a essas necessidades conforme necessário.

### Plano de Teste e Validação

* Testes de stress sob condições simuladas de pico de carga.
* Exercícios regulares de recuperação de desastres, incluindo cenários como falhas de servidores e falhas de rede.
* Monitorização contínua e auditorias periódicas para garantir que os sistemas cumprem os padrões de desempenho e disponibilidade.

Garantir um MTD (Maximum Tolerable Downtime) de 20 minutos é um objetivo essencial para a continuidade das operações críticas da organização. As alterações propostas à infraestrutura são fundamentais para alcançar este objetivo, assegurando a disponibilidade dos serviços, a resiliência contra falhas e a capacidade de recuperação rápida em caso de incidentes.

Estas mudanças não apenas minimizam os riscos e impactos operacionais, como também reforçam a confiança nos sistemas da organização, promovendo uma experiência contínua e eficiente para os utilizadores e contribuindo para a sustentabilidade e competitividade da organização a longo prazo.

# User Story 3

Na User Story 3, foi-nos pedido o seguinte: “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 \_yyyymmdd sendo 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 tal, vamos seguir os seguintes passos:

1. Criar um script
2. Adaptar o ficheiro para haver execução diária
3. Verificar os logs

O primeiro passo é, então, criar o script com o seguinte comando:

A screenshot of a computer program

Description automatically generatedO script é o seguinte:

Para o explicar devidamente, vamos decompô-lo:

A computer screen shot of text

Description automatically generatedNas primeiras linhas estamos a definir os caminhos para os diretórios e a associá-los a variáveis para mais facilitar eventuais mudanças no futuro.

De seguida, criamos o diretório para os logs, caso ele não exista.

A black background with yellow and blue text

Description automatically generatedAs duas linhas seguintes guardam a data atual e criam o os logs com essa data.

Nas próximas linhas, criamos o diretório para dar “dump” (também, caso ele não exista) e atribui permissões totais para o proprietário.

 Nesta linha é realizado o backup da base de dados da MongoDB (“dump”), que será feito no diretório definido “mongodb\_dump\_dir”. As mensagens de saída tanto de sucesso como de erro serão enviadas para o ficheiro de logs “mongodb\_log\_file”.

A screenshot of a computer

Description automatically generatedNestas condições, primeiramente é verificado se o comando anterior foi bem executado e, se sucedido, cria um diretório para backups (se não existir) e atribui as permissões totais para o proprietário. De seguida, compacta os dados em um ficheiro “.tar.gz”. Por fim, com a segunda condição, é verificado se o comando anterior teve sucesso ou não, e regista as mensagens de sucesso ou erro no log.

A computer screen shot of a black screen

Description automatically generated No segundo passo, vamos alterar o ficheiro “/etc/crontab” para executar o script anteriormente explicado.

Para tal, foi acrescentada a última linha para ser realizada, todos os dias, uma cópia à meia-noite.

A screen shot of a computer

Description automatically generated Por fim, para não ter de esperar pelas 00:00, foi alterado o ficheiro ser realizada uma cópia de teste às 17:50 da tarde, onde verificamos o ficheiro de logs. Como podemos ver, o script funciona.

# User Story 4

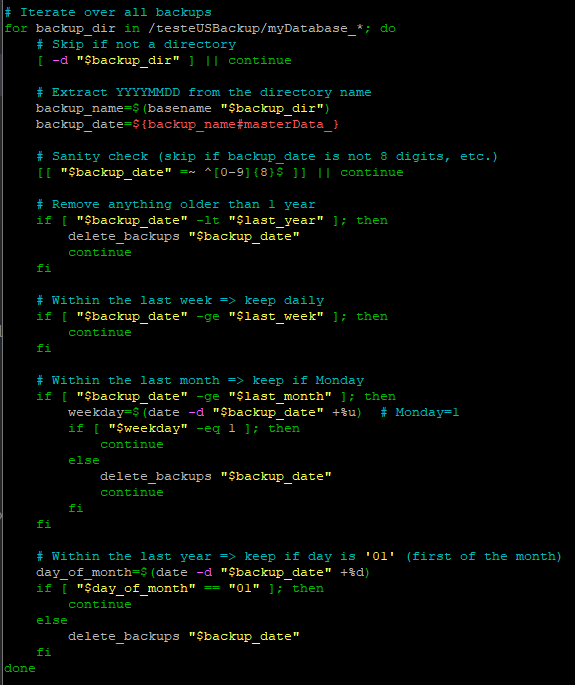
Na User Story 4 é pedido que façamos um script para gerir os backups feitos pela US anterior resultando no seguinte:

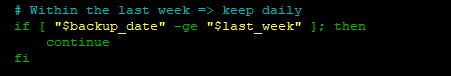
-1 backup por dia nos últimos 7 dias

-1 backup por semana nas últimas 4 semanas

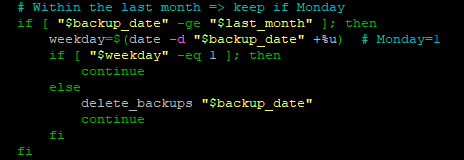
-1 backup por mês nos últimos 12 meses

Para cumprir com estes requisitos, temos de corretamente filtrar os backups. Isto é atingido através de um for loop que elimina os backups adequadamente.

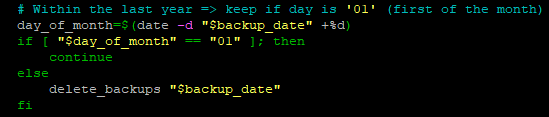


Para cumprir corretamente o primeiro requisito passa pelo seguinte ‘if’:  


Para cumprir corretamente o segundo requisito passa pelo seguinte ‘if’:



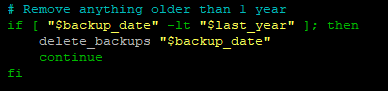
Para cumprir corretamente o terceiro requisito passa pelo seguinte ‘if’:



Se o backup não corresponder a nenhum destes três filtros ele é apagado da diretoria



Se o backup for mais velho que um ano este também é apagado



# User Story 5

Na user story 5, foi-nos pedido o seguinte: “Como administrador de sistemas quero que o processo da US C3 seja mantido no log do Linux, num contexto adequado, e alertado o administrador no acesso à consola se ocorrer uma falha grave neste processo.”.

Para realizar esta US, seguimos os seguintes passos:

1. Configurar o RSYSLOG
2. Alterar o ficheiro para garantir execução automática
3. Configurar os alertas

Para configurar o RSYSLOG, primeiro temos de instalar o mesmo com o seguinte comando:

A black screen with white text

Description automatically generatedDe seguida, abrimos o ficheiro de configuração com o comando “*sudo nano /etc/rsyslog.conf*” e adicionamos as seguintes linhas no fim do ficheiro:

Depois, foram executados os seguintes comandos para criar os ficheiros de logs com as permissões corretas:

Para terminar o primeiro ponto, executamos o comando “*sudo systemctl restart rsyslog”* para reiniciar o serviço RSYSLOG.

A screen shot of a computer error

Description automatically generatedNo segundo passo, vamos começar por alterar o script da US3 para que a verificação do backup seja feita para os novos diretórios. Para isso, vamos acrescentar as seguintes linhas:

De seguida, vamos abrir o ficheiro “cron” e adicionar uma linha para que o script seja executado diariamente. No entanto, esta linha já foi executada na US3 e decidimos manter o horário para a meia-noite.

Por fim, no último passo vamo-nos certificar que as mensagens de severidade “emerg” são mostradas na consola, ao adicionar a seguinte linha no ficheiro “*sudo nano /etc/rsyslog.conf*”:

# User Story 6

A screen shot of a computer

Description automatically generatedNa User Story 6 é pedido que o backup da DB tem um tempo de vida não superior a 7 dias. Para cumprirmos com esse requisito incluímos no script que faz o backup o seguinte:

# User Story 7

O Business Impact Analysis (BIA) tem como objetivo analisar os potenciais impactos de interrupções no sistema de marcação de cirurgias e gestão de recursos, identificando processos críticos e suas dependências, bem como quantificando as consequências financeiras, operacionais e regulatórias de possíveis falhas. Esta análise considera os riscos previamente identificados e adapta-se a eles, garantindo que a organização esteja preparada para minimizar o impacto de interrupções e assegurar a continuidade dos serviços essenciais.

Através deste documento, serão identificados os principais processos de negócio suportados pelo sistema, avaliados os riscos e impactos das disrupções, e recomendadas ações para mitigar esses riscos e melhorar a resiliência da infraestrutura. O objetivo final é fortalecer a capacidade da organização em lidar com desafios inesperados, garantindo a recuperação dentro do tempo máximo tolerável de inatividade (MTD) de 20 minutos, alinhando-se ao Mínimo Objetivo de Continuidade de Negócio (MBCO) definido.

Identificação de processos críticos de negócio

Os processos críticos de negócio apoiados pelo sistema de agendamento cirúrgico e gestão de recursos incluem:

* Agendamento de procedimentos cirúrgicos: Garante a alocação das salas de cirurgia, equipa médica e equipamento necessário.
* Gestão de dados do paciente: mantém informações confidenciais sobre os pacientes e os seus planos de tratamento.
* Alocação de Recursos: Gere a disponibilidade de pessoal médico, equipamento e instalações para operações hospitalares ideais.
* Monitorização da conformidade: Garante que o hospital cumpre os padrões legais e regulamentares de segurança do doente e de dados.

## Quantificação de Potenciais Impactos

### Impactos Financeiros

Custos de inatividade: Cada hora de inatividade do sistema pode levar ao cancelamento de cirurgias, gerando perda de receitas e ineficiências operacionais.

Penalidades regulamentares: O não cumprimento do RGPD ou dos regulamentos de saúde pode resultar em multas até 20 milhões de euros ou 4% da receita anual do hospital.

### Impactos Operacionais

Interrupção do serviço: As interrupções podem atrasar ou cancelar as cirurgias, afetando os resultados dos pacientes e causando danos à reputação.

Pessoal sobrecarregado: A realocação manual de recursos e nomeações aumentaria a carga de trabalho do pessoal e reduziria a eficiência.

### Impactos Legais e Regulatórios

Violações de dados: as violações do RGPD devido à exposição de dados podem levar a ações legais significativas e à perda de confiança do público.

Prazos de comunicação não cumpridos: O não cumprimento das obrigações de comunicação pode resultar em multas ou suspensão de operações.

### Identificação de Dependências

Sistemas de gestão médica e de pacientes: O sistema de agendamento cirúrgico depende de outros sistemas para gerir os registos de pacientes e os históricos médicos. A falha nestes sistemas impactaria diretamente as operações cirúrgicas.

Infraestrutura de Rede e Comunicação: A conectividade é fundamental para a integração de vários sistemas e atualizações em tempo real.

Formação e Preparação do Pessoal: O erro humano nas operações do sistema pode agravar o impacto das falhas técnicas.

### Adaptação ao Risco

Os riscos identificados no sprint anterior foram integrados nesta análise:

* Violações de dados: implemente encriptação, autenticação multifatorial e auditorias de segurança frequentes para mitigar este risco.
* Tempo de inatividade do sistema: O clustering de alta disponibilidade, os sistemas de backup e os balanceadores de carga são propostos para resolver este risco.
* Ataques DoS/DDoS: Implemente firewalls, sistemas de deteção/prevenção de intrusão (IDS/IPS) e ferramentas de monitorização de tráfego.
* Ameaças internas: introduza controlos de acesso mais rigorosos, formação dos colaboradores e monitorização para detetar atividades incomuns.
* Erros de eliminação de dados: automatize cópias de segurança e implemente processos de validação de dados antes das eliminações.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Impacto Potencial | Dependências | Mitigações Propostas |
| Marcação Cirúrgica | Perda de receitas; cirurgias atrasadas/canceladas | Network, disponibilidade de pessoal, software de agendamento | Balanceadores de carga, clustering e formação de pessoal |
| Gestão da informação do paciente | Coimas legais; perda de confiança; ineficiências operacionais | Sistemas de armazenamento de dados, conformidade com o RGPD | Encriptação, backups regulares e monitorização |
| Alocação de Recursos | Má gestão de pessoal e equipamentos; atrasos nas cirurgias | Sistemas integrados de gestão de recursos | Automação e monitorização do sistema em tempo real |
| Monitorização de Conformidade | Multas por incumprimento; danos à reputação | Ferramentas regulamentares e sistemas de reporting | Auditorias frequentes e software de monitorização da conformidade |

## Recomendações

Com base na BIA, são recomendadas as seguintes ações:

* Melhore os planos de recuperação de desastres:
  + Incorpore exercícios frequentes de recuperação de desastres para se preparar para os piores cenários.
  + Mantenha a documentação atualizada de todas as dependências e etapas de recuperação.
* Mitigar riscos identificados:
  + Implemente ferramentas de segurança avançadas para evitar violações e ataques de dados.
  + Formar a equipa para reduzir a probabilidade de erros e ameaças internas.
* Melhore a resiliência do sistema:
  + Expanda as capacidades de clustering e balanceamento de carga para processos críticos.
  + Aumente a redundância para armazenamento e infraestrutura de rede.
* Adote testes e monitorização regulares:
  + Realize testes de stress mensais para avaliar a capacidade do sistema sob carga.
  + Audite regularmente as definições do sistema para garantir o alinhamento com as melhores práticas.

O Business Impact Analysis (BIA) demonstra de forma clara a importância de preparar a organização para lidar com possíveis interrupções nos sistemas críticos, como o de marcação de cirurgias e gestão de recursos. Ao identificar os processos essenciais, quantificar os impactos financeiros, operacionais e regulatórios, e mapear as principais dependências, esta análise fornece um panorama abrangente dos riscos e vulnerabilidades existentes.

Além disso, a integração dos riscos identificados previamente assegura que as soluções propostas são eficazes e adaptadas à realidade da organização. As recomendações apresentadas, incluindo o reforço das medidas de segurança, a implementação de backups robustos, a capacitação de colaboradores e a realização de testes regulares, são essenciais para minimizar o impacto de falhas e maximizar a resiliência.

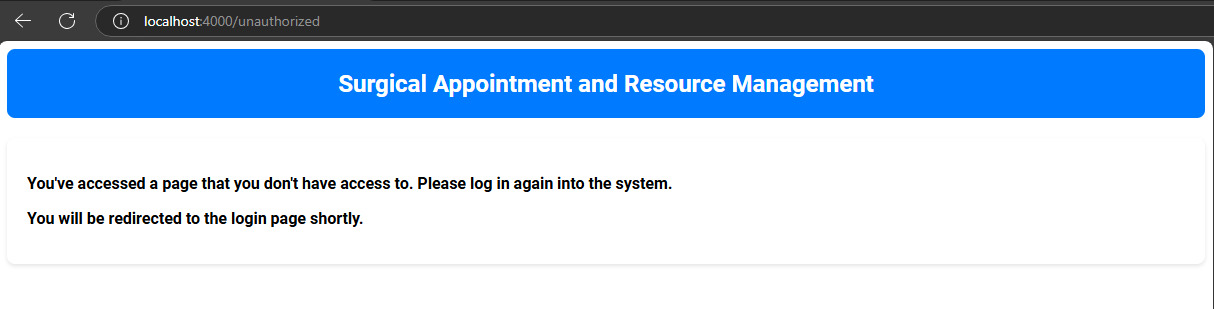
Ao adotar estas estratégias, a organização estará mais bem preparada para garantir a continuidade dos seus serviços dentro do MTD (Maximum Tolerable Downtime) de 20 minutos, assegurando a confiança dos seus utilizadores e cumprindo com os requisitos legais e operacionais. Assim, a abordagem proposta não só reduz os riscos, como também fortalece a eficiência e a credibilidade da organização a longo prazo.

# User Story 8

Na user story 8, foi-nos pedido o seguinte: “Como o administrador da organização, eu quero que a gestão de acesso a ser implementada segue os critérios de segurança apropriados.”

Para isso, enquanto desenvolvemos o sistema, tivemos o cuidado de ter uma enfase em segurança.

Para aceder à base de dados, primeiro é preciso estar conectado à rede do DEI. E quando se ussa a frontend, o sistema só deixa o usuário aceder as partes do sistema no qual ele tem permissão, dependendo da função que este tiver (Admin, Doutor, Enfermeira, Paciente).

A autenticação é feita através dos serviços da Google, onde cada conta está associada a uma função. Tentar aceder a uma página de uma função pela qual não tem autorização para aceder resulta em erro. Quando um usuário tenta aceder a conteúdo a que não tem acesso, o sistema não permite: 

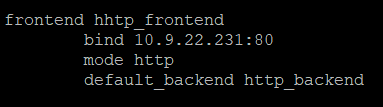
# User Story 9

Na User Story 9, propõe-se a implementação de um sistema de clustering entre os servidores que suportam o SPA. Para cumprir esse objetivo, é necessário que a aplicação SPA seja executada em múltiplas máquinas. Neste sprint, a execução do projeto foi estendida para mais dois servidores (vs758 e vs550).

Com o intuito de viabilizar o sistema de clustering, introduzimos um novo servidor (vs758), responsável pela gestão do cluster. Nesse servidor, realizamos a instalação do HAProxy por meio do comando:

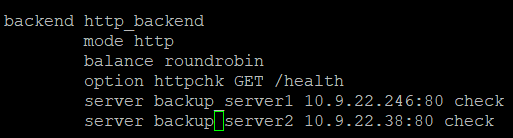
sudo apt-get update && sudo apt-get install haproxy

De seguida, configura-se o HAProxy, atraves do ficheiro /etv/haproxy/haproxy.cfg. Adicionou-se ao ficheiro:



* **frontend hhtp\_frontend**
  + Define uma seção de configuração chamada hhtp\_frontend.
  + “Frontend” é onde o HAProxy “ouve” as conexões de clientes (navegadores, aplicativos, etc.).
* **bind 10.9.22.231:80**
  + Indica que o HAProxy deve **escutar** (listen) no endereço IP 10.9.22.231 na **porta 80** (HTTP).
  + Assim, qualquer requisição que chegue a <http://10.9.22.231:80/> (ou ao hostname que aponte para esse IP) será tratada por este frontend.
* **mode http**
  + Define que o tráfego será tratado como HTTP, permitindo que o HAProxy inspecione cabeçalhos HTTP, faça redirecionamentos e use outras funcionalidades específicas de HTTP.
* **default\_backend http\_backend**
  + Diz ao HAProxy que, **por padrão**, todas as conexões recebidas neste frontend serão encaminhadas para o **backend** chamado http\_backend.
  + Caso não haja nenhuma ACL (regra de encaminhamento) mais específica, este será o destino final do tráfego.

Adicionou-se também:



* **backend http\_backend**
  + Inicia a definição de um **backend** chamado http\_backend.
  + O backend descreve **para onde** (quais servidores) as requisições do frontend serão encaminhadas e **como** serão balanceadas.
* **mode http**
  + Assim como no frontend, define que o tratamento das conexões aqui será em nível HTTP (ao invés de TCP, por exemplo).
  + Permite o uso de verificações HTTP, manipulação de cabeçalhos, etc.
* **balance roundrobin**
  + Define o **algoritmo de balanceamento** de carga.
  + “Round-robin” significa que o HAProxy enviará cada nova requisição para o próximo servidor na lista, de forma cíclica e equilibrada.
* **option httpchk GET /health**
  + Esta opção configura o **health check HTTP**.
  + O HAProxy fará requisições do tipo GET /health em cada servidor listado abaixo.
  + Se a resposta HTTP for considerada válida (geralmente status 2xx ou 3xx), o servidor é marcado como “UP”. Caso contrário, é marcado “DOWN” e removido temporariamente do balanceamento.
* **server backup\_server1 10.9.22.246:80 check**
  + Define um servidor chamado backup\_server1, que está no IP 10.9.22.246 na porta 80.
  + O parâmetro check indica que o HAProxy deve fazer verificações de saúde (health checks) nesse servidor.
  + Se esse servidor falhar na verificação, ele é removido do pool de servidores ativos até ficar saudável novamente.
* **server backup\_server2 10.9.22.38:80 check**
  + Define o segundo servidor, backup\_server2, apontando para 10.9.22.38:80.
  + Assim como o anterior, possui check habilitado, participando do balanceamento no modo “roundrobin”.

Apesar de ainda não ter sido possível implementar todas as funcionalidades de clustering previstas, a configuração atual já possibilita verificar o estado dos servidores através do HAProxy. Isso permite monitorizar cada servidor, identificar problemas antecipadamente e, assim, criar uma base sólida para evoluir futuramente a solução e alcançar a total redundância e alta disponibilidade desejadas.

# User Story 10

Na user story 10, é pedido o seguinte: “Como administrador de sistemas quero que o administrador tenha um acesso SSH à máquina virtual apenas por certificado, sem recurso a password”.

Para tal, seguimos os seguintes passos:

1. Gerar a chave SSH
2. Transferir a chave para o servidor
3. Configurar o servidor SSH

Para começar, vamos gerar a chave SSH ao executar o seguinte comando:

A screenshot of a computer

Description automatically generated“*ssh-keygen*”. Por default, a chave é armazenada “*~/.ssh/id\_rsa*”. Depois, ao carregar duas vezes no ENTER, criámos um acesso sem senha.

A screenshot of a computer

Description automatically generatedNo segundo passo, vamos transferir uma chave pública para o servidor. Vamos, então, começar por executar o seguinte comando: “*ssh-copy-id root@vs211*”.

A computer screen with white letters and numbers

Description automatically generatedPara verificar se a chave foi realmente adicionada ao ficheiro, vamos usar o comando “*cat ~/.ssh/authorized\_keys*”.

Para garantir as permissões no servidor, usámos os seguintes comandos:

A computer screen with blue and white text

Description automatically generatedPor fim, no último passo, vamos configurar o servidor SSH. Para tal, vamos editar o ficheiro de configuração do SSH, com “*sudo nano /etc/ssh/sshd\_config*”. No ficheiro, vamos editar as linhas para ter “PubkeyAuthentication yes” e “PasswordAuthentication no”.

Por fim, vamos reiniciar o serviço SSH para aplicar as novas alterações, com o seguinte comando:

# User Story 11

Na User Story 11 é pedido que criassemos uma pasta pública partilha com o formato SMB/CIFS ou NFS. Neste caso, decidimos usar o formato NFS.

Primeiramente antes de conseguirmos fazer esta US temos de instalar o pacote nfs-kernel no servidor:



Depois de instalar os pacotes temos de criar o diretório compartilhado através do comando:



Mudamos as permissões para 777 ():



Por questões de segurança, esta partição é owned pelo utilizador nobody, através do comando ’chown nobody:nogroup /srv/nfs/public’

De seguida abrimos o arquivo /etc/exports onde adicionamos a seguinte linha:  
‘/srv/nfs/public \*(rw,sync,no\_subtree\_check)’ para permitir leitura e escrita com o rw; com o sync garantimos que os arquivos são escritos diretamente no disco; no ‘no\_subtree\_check’ melhoramos o desempenho e no ‘no\_root\_squash’ permitimos que haja privilégios de root.

Por fim temos de alterar a firewall para permitir NFS através do comando:

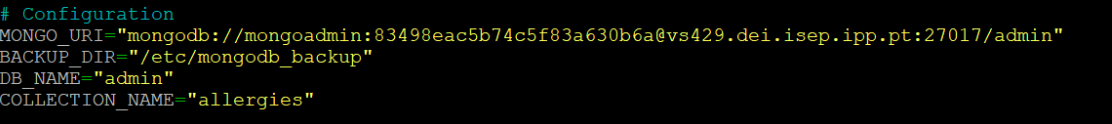


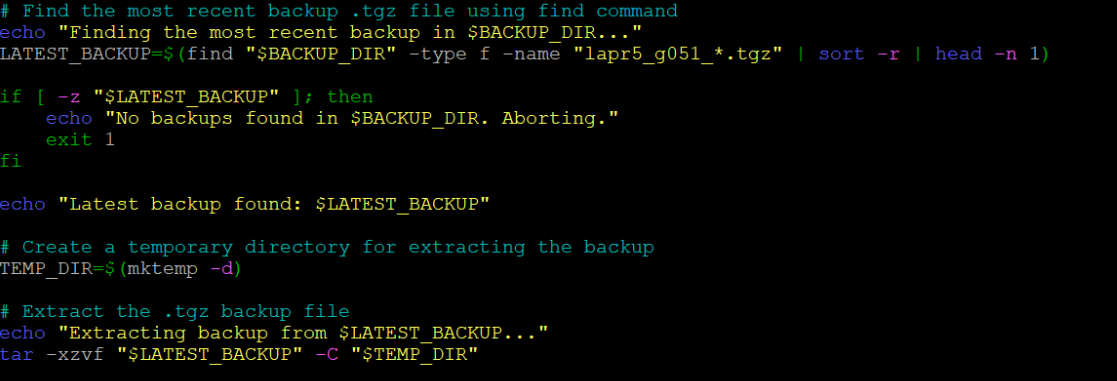
# User Story 12

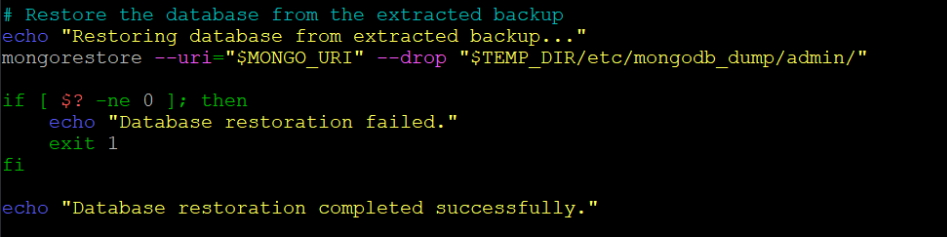
Nesta User Story, é pedido para ser possível restaurar um backup, e verificar se esse backup foi feito de forma certa (através da realização de um query a base de dados).

Para isso, foi criado este script:

Vamos velo por partes.

No início, são definidas as variáveis para uso neste script, como a URL da base de dados, o diretório dos backups, e o nome da base de dados e da coleção para podermos fazer a verificação.

Aqui, o script encontra o backup mais recente para usar neste restauro, e de seguida extrai-o para uma pasta temporária 

Após esta extração, o script envia um comando à base de dados para restaurar-se com os ficheiros acabados de ser extraídos. Por fim, o script faz um query simples à base de dados para verificar se o restauro foi bem-sucedido.