

Relatório de ASIST

Sprint C

Licenciatura em Engenharia Informática

**Turma 3DA\_Grupo03**

1171060\_André Silva

1200750\_Vasco Silva

1200774\_Cláudia Freitas

121001\_Carlos Rodrigues

**Data: 08/01/2023**

Conteúdo

[Parte I – Introdução e estrutura do Trabalho 3](#_Toc123999926)

[I. User Stories – Sprint C 3](#_Toc123999927)

[Parte II – Desenvolvimento 5](#_Toc123999928)

[I. Implementação User Stories 5](#_Toc123999929)

[I.I. US01 5](#_Toc123999930)

[Finalidade do DRP 5](#_Toc123999931)

[Objetivos 5](#_Toc123999932)

[Equipa responsável pelo DRP 5](#_Toc123999933)

[Armazenamento do DRP 5](#_Toc123999934)

[Procedimentos de Backup 5](#_Toc123999935)

[Casos de Desastre 6](#_Toc123999936)

[Ativação do Plano 6](#_Toc123999937)

[Documentação do Desastre 7](#_Toc123999938)

[Testes ao DRP 7](#_Toc123999939)

[Melhorias ao DRP 7](#_Toc123999940)

[Webgrafia 7](#_Toc123999941)

[I.III. US03 9](#_Toc123999942)

[I.IV. US04 10](#_Toc123999943)

[I.V. US05 12](#_Toc123999944)

[I.VI. US06 14](#_Toc123999945)

[I.VII. US07 14](#_Toc123999946)

[I.VIII. US08 15](#_Toc123999947)

[Tabela 1- Business Impact Analysis 15](#_Toc124008446)

# Parte I – Introdução e estrutura do Trabalho

Este relatório visa a expor o processo de administração de sistemas no modulo Infraestrutura, parte do Projeto Integrador do 5º semestre de Licenciatura de Engenharia Informática, no ano 2022/2023.

### User Stories – Sprint C

* US01 - Como administrador da organização quero um plano de recuperação de desastre que satisfaça o MBCO definido na US B5.
* US02 - Como administrador da organização quero que me seja apresentada de forma justificada a ou as alterações a realizar na infraestrutura por forma a assegurar um MTD (Maximum Tolerable Downtime) de 20 minutos.
* US03 - 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.
* US04 - Como administrador de sistemas quero que utilizando o Backup elaborado na USC3, seja criado um script quer 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.
* US05 - 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.
* US06 - Como administrador de sistemas quero que a cópia de segurança da US C3 tenha um tempo de vida não superior a 7 (sete) dias exceto no indicado na US C4.
* US07 - Como administrador da organização quero que me seja apresentado um BIA (Business Impact Analysis) da solução final, adaptando se e onde aplicável o(s) risco(s) da US B4.
* US08- Como administrador da organização quero que seja implementada uma gestão de acessos que satisfaça os critérios apropriados de segurança.

# Parte II – Desenvolvimento

## Implementação User Stories

### I.I. US01

#### Finalidade do DRP

Um plano de recuperação de desastre (DRP) é um documento que contém um conjunto de regras e procedimentos que uma empresa segue para garantir que as funções vitais do negócio continuam ativas no evento de um desastre ou incidente grave (ataques informáticos, desastres naturais, …).

O plano tem como objetivo minimizar os efeitos de um desastre para a organização poder continuar a operar ou, rapidamente, resumir os serviços críticos do negócio.

#### Objetivos

* Minimizar tempo de paragem e perda de dados em caso de desastre;
* Criar planos de emergência;
* Recuperar os serviços afetados o mais rápido possível;
* Definir cenários de desastre e respetivos procedimentos de recuperação.

#### Equipa responsável pelo DRP

|  |  |
| --- | --- |
| Nome | Contacto |
| André Silva | [1171060@isep.ipp.pt](mailto:1171060@isep.ipp.pt) |
| Carlos Rodrigues | [1201001@isep.ipp.pt](mailto:1201001@isep.ipp.pt) |
| Cláudia Freitas | [1200774@isep.ipp.pt](mailto:1200774@isep.ipp.pt) |
| Vasco Silva | [1200750@isep.ipp.pt](mailto:1200750@isep.ipp.pt) |

#### Armazenamento do DRP

Todos os membros da equipa terão acesso a uma cópia do DRP. A empresa irá definir lugares seguros para armazenar cópias em formato físico (papel) e formato digital (*USB pen drive)* do DRP.

#### Procedimentos de Backup

O sistema representa a junção de vários módulos e a relação entre eles (SPA, Gestão de Armazéns, Logística e Planeamento). Portanto, é essencial que existam *backups* para todos os componentes do sistema.

Foi decidido que existirão 3 cópias para cada um dos módulos seguindo a estratégia 3-2-1 que defende que devem existir 3 cópias dos dados usando 2 métodos diferentes de armazenamento e 1 das cópias guardada *off-site*.

1 das cópias encontra-se num servidor remoto, outra é um *backup* na *cloud* e a última uma cópia num disco externo, guardada em local seguro.

#### Casos de Desastre

* Ataque informático - Tentar entender se as informações foram adulteradas ou apenas copiadas. No primeiro caso, usando *backups* da base de dados, tentar entender quando as informações foram adulteradas e restaurar os dados originais e, no segundo, entender quais dados foram copiados e qual o impacto que essa cópia pode ter. Também é necessário saber como o atacante entrou no sistema e lidar com essa vulnerabilidade o mais rápido possível. Por fim, recorrer às autoridades e tentar perceber quem foi o responsável pelo ataque para prevenir futuros ataques desta entidade.
* Incêndio - Alertar os bombeiros. Evacuar o edifício pelas devidas saídas e se possível remover e evacuar os discos rígidos do servidor para evitar a perda dos dados críticos da empresa.
* Inundação - Desligar todos os equipamentos para evitar curto-circuitos, e proteger quaisquer dados que sejam crucias e que possam ser afetados pela água, sejam documentos impressos, ou os disco rígidos do servidor. Deve-se também contactar imediatamente os bombeiros.
* Falha do sistema - Contactar a equipa de recuperação de desastre para resolver o problema o quanto antes.
* Ataque vindo de dentro da empresa - Identificar o responsável ​​e acionar todos os mecanismos legais necessários. Questionar o responsável sobre como ele executou o seu plano, e descobrir se ele tinha credenciais para usar os mecanismos que utilizou. Caso não tenha, verificar como proteger esses mecanismos para evitar incidentes futuros.

#### Ativação do Plano

Quando ocorre um incidente a equipa de resposta de emergência deve ser ativada (ERT). Esta equipa tem como objetivos:

* Definir quais dos elementos do DRP a ser invocados, consoante o tipo de desastre;
* Contactar as autoridades de emergência;
* Estabelecer e gerir a equipa de recuperação de desastre (DRT) para recuperar e manter os serviços vitais;
* Notificar os funcionários e alocar responsabilidades e atividades se necessário.

|  |  |
| --- | --- |
| Nome | Equipa |
| André Silva | ERT |
| Carlos Rodrigues | ERT |
| Cláudia Freitas | DRT |
| Vasco Silva | DRT |

A DRT será contactada pela ERT. As suas responsabilidades passam por ter os serviços vitais a funcionar no tempo definido no RTO e reportar à equipa de resposta de emergência.

#### Documentação do Desastre

Depois da recuperado do desastre, deve ser realizado um relatório descrevendo as atividades exercidas durante a execução do DRP.

Este relatório deve conter:

* Descrição da emergência, pessoas notificadas e quando foram notificadas e ações realizadas pela ERT;
* Ações realizadas pelos membros da DRT e consequências dessas ações;
* Possíveis aprendizagens com os eventos.

#### Testes ao DRP

Testar o DRP frequentemente é essencial para o seu desenvolvimento. Através dos testes descobre-se o que precisa de ser melhorado e como essas melhorias podem ser implementadas.

Planear testes garante que as equipas de emergência estão familiarizadas com os procedimentos e confiantes nas suas capacidades.

#### Melhorias ao DRP

Baseando-se em desastres anteriores e testes realizados, o DRP deve ser atualizado regularmente podendo, desta forma, ser o mais eficaz possível a combater os diversos desastres que podem acontecer.

#### Webgrafia

<https://cloudian.com/guides/disaster-recovery/4-disaster-recovery-plan-examples-and-10-essential-plan-items/>

<https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan>

<https://www.ibm.com/uk-en/services/business-continuity/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20(DR)%20plan%20is%20a%20formal%20document%20created,and%20any%20other%20disruptive%20events>.

<https://www.druva.com/glossary/what-is-a-disaster-recovery-plan-definition-and-related-faqs/>

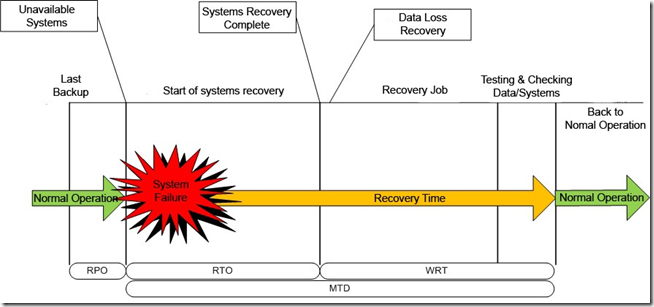
<https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf>

I.II. US02

MTD representa o tempo máximo de inoperacionalidade da infraestrutura informática. Ultrapassando este tempo podem existir consequências irreversíveis das quais resultam danos severos para a viabilidade do negócio.

Para respeitar o MTD de 20 minutos, optamos por fazer *mirroring* síncrono dos nossos servidores para servidores de *backup* remotos. *Server mirroring* é um processo em que uma réplica exata do servidor é criada em tempo real. Assim, caso um dos servidores falhe, é possível restaurar os dados através do *backup server*.

Ao realizar este processo criamos redundância no nosso sistema. Caso um servidor falhe, temos outro funcional, criando assim tolerância a falhas. Desta forma o WRT (*Work Recovery Time*) - tempo necessário para repor os dados e aplicações é praticamente nulo respeitando assim o MTD definido.



### I.III. US03

Nesta US é pedido que seja feito um Backup da base de dados utilizadas para um ambiente cloud, logo decidimos utilizar as máquinas virtuais da cloud do DEI. A máquina utilizada tem a distribuição Ubuntu 20.04.

Primeiramente, para que o nome ficasse com a data atual utilizei a variavél now, que vai buscar a data da forma mostrada na iamgem abaixo.

A explicação da forma como é feito oBackup vai dividir-se em 2, já que temos 2 bases de dados a utilizar diferentes tecnologias e abordagens.

**MONGODB:**

Para fazer o Backup desta Base de dados utilizo o comando mongodump, para que o dump funcione utilizamos o uri da BD e especificamos o local do output, que é especificado pelo comando --out.

As verificações serão explicadas na US05.

**SQLSERVER:**

Para este tipo de base de dados optei pelo comando sqlcmd, e para que este funcione especificamos qual a BD e a porta (-S), o username (-U), a password (-P), o catalogo (-d), confiamos no certificado (-C) e o -Q é utilizado para especificar o local do Backup.

Mais uma vez as verificações serão explicadas na US05.

Uma imagem com texto

Descrição gerada automaticamente

### I.IV. US04

Nesta US é pedido para o administrador de sistema gerir os ficheiros resultantes do backup elaborado na US03.

A gestão deve ser feita de forma agendada:

1 Backup por mês no último ano;

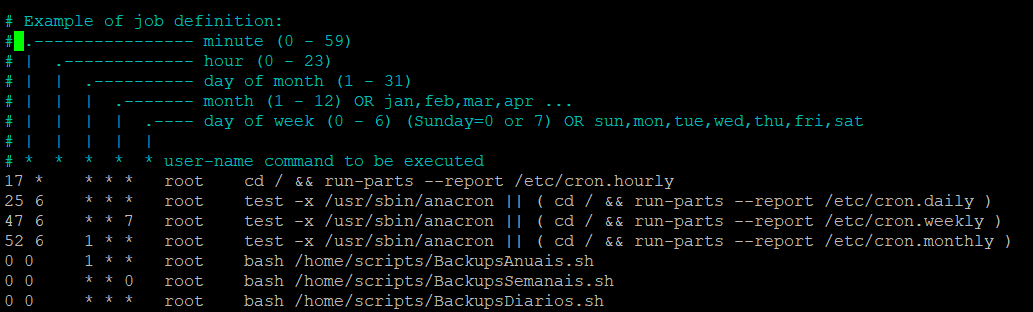
1 Backup por semana no último mês;

1 Backup por dia na última semana.

**1º - Backup agendado**

Começamos por agendar os backups de forma a que haja backups todos os dias, todas as semanas e todos os meses.

Para isto acrescentamos no ficheiro /etc/crontab as seguintes linhas:

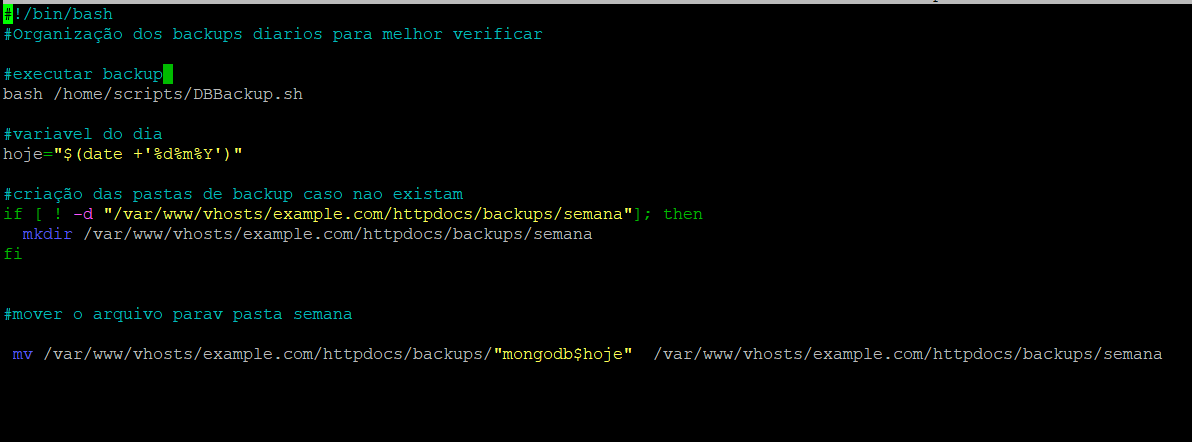


As últimas três linhas dizem respeito, respetivamente, a executar o backup todos os meses, executar o backup todas as semanas e executar o backup todos os dias.

Será executado o script correspondente.

Estes Scripts são constituídos pelo comando de execução de backup e da organização do ficheiro resultante do backup numa pasta especifica. Ou seja, cada backup irá para uma pasta que corresponde ao backup feito.

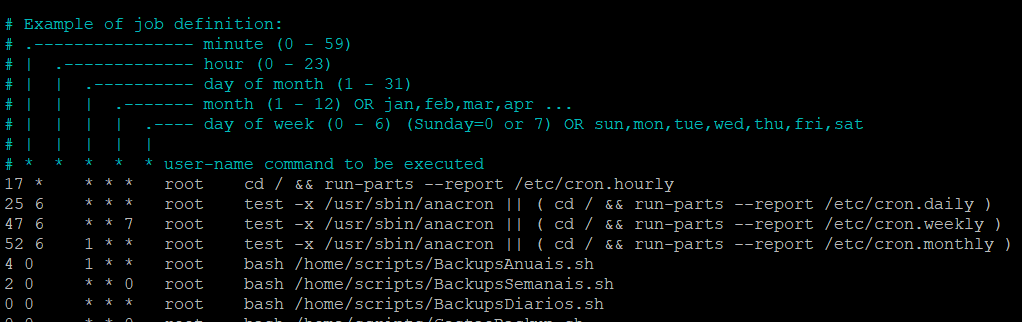
Exemplo, script **BackupsDiarios.sh**:



Será executado o backup e depois o ficheiro resultante do backup será movido para a pasta **semana**, onde se encontram todos os backups diários.

O mesmo processo acontece para os backups semanais e mensais, mas iram para pastas, respetivamente, **Mes e Ano**.

Estes scripts encontram se no diretório **/home/scripts/**.

Para que não haja erro nos backups, alteramos os minutos de cada backup, dando espaço de tempo, uma vez que haverá dias onde ocorrerá os três ou dois backups ao mesmo tempo.

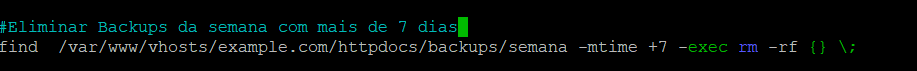
Desta forma, os ficheiros estão organizados em pastas correspondentes e podemos passar à segunda fase.

**2º - Eliminação de backups antigos**

* Começaremos pela eliminação dos backups **passado a semana**.

Os backups diários de uma semana serão guardados e quando mudar de semana e após haver novos backups da semana atual, os backups com +7 dias serão eliminados.

Isto permite que haja sempre backups de uma semana completa.

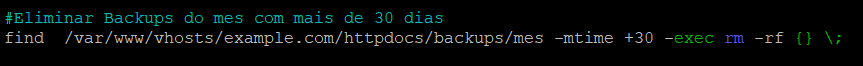


Este comando irá à pasta semana onde se encontram os ficheiros resultantes dos backups feitos diariamente e irá eliminar todos os backups que foram feitos há **+ 7 dias**.

* **Passando o mês**, o processo será o mesmo.

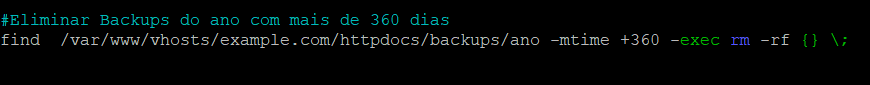
Um mês terá um backup todas as semanas e mudando de mês e com novos backups do novo mês, os backups do mês anterior serão eliminados.

Existindo sempre os backups de um mês completo.



Este comando irá à pasta mes onde se encontram os ficheiros resultantes dos backups feitos semanalmente e irá eliminar todos os backups que foram feitos há +30 dias (1 mes). Por exemplo, no início do mês de agosto terá os backups de julho e irá eliminar os backups de junho.

* **Passando o ano**, também terá o mesmo processo.

Haverá sempre um ano completo de backups feitos mensalmente. Por exemplo, no início do ano de 2023 terá os backups completos de 2022 e irá eliminar os backups de 2021.

Este comando irá à pasta ano onde se encontram os ficheiros resultantes dos backups mensais e irá eliminar todos os backups que foram feitos há + 360 dias (1 ano).

### I.V. US05

O objetivo desta US resumidamente é gravar no log do sistema os processos de Backup, e decidiu-se guardar tanto os casos de sucesso como os de insucesso.

Numa segunda parte era necessário também mostrar ao utilizador os erros ocorridos aquando do login.

Para gravar no syslog os logs foi utilizado o comando logger, com a gravidade alert, e para saber se passou um não verificávamos o estado do último comando feito na consola que era sempre o dump da BD.

**MONDODB:**

Uma imagem com texto, ecrã, captura de ecrã

Descrição gerada automaticamente

**SQLSERVER:**

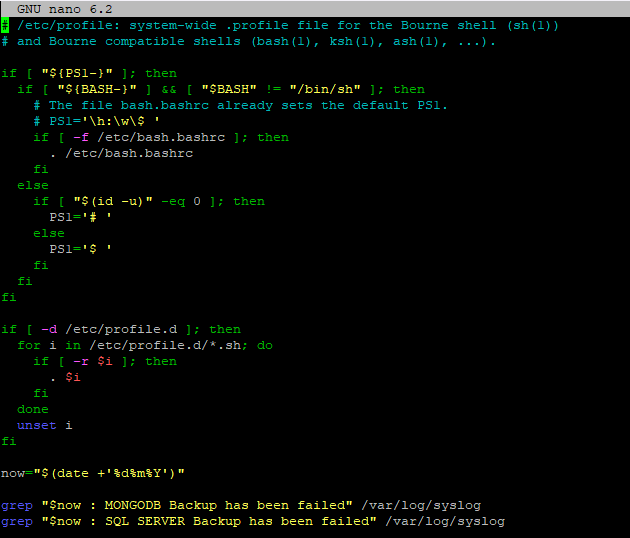
Uma imagem com texto

Descrição gerada automaticamente

Após este processo ainda falta mostrar ao utilizador os erros neste processo aquando do login. Deste modo, e tal como já feito em sprints anteriores, alteramos o ficheiro /etc/profile.

Para não sobrecarregar o utilizador com todos os erros, e como não foi especificada data, decidimos mostrar os erros do próprio dia, o que é facilmente alterável.

Utilizamos o grep para encontrar as mensagens.



Decidi também adicionar a seguinte linha ao ficheiro /etc/syslog.config.



Deste modo todos os utilizadores ativos receberão a mensagem.

### I.VI. US06

Nesta US, iremos limitar o tempo de um backup não agendado no sistema. Ou seja, copias que possam ser feitos manualmente pelo administrador.

Os ficheiros resultantes destes backups irão para o diretório **/var/www/vhosts/example.com/httpdocs/backups** e todas as semanas serão eliminados, fazendo com que não o seu tempo de vida não seja superior a 7 dias.

Para isto, só foi necessário acrescentar uma linha no ficheiro **/etc/crontab** em que todas as semanas são removidos os ficheiros resultantes da copia com +7 dias. Com isto asseguramos sempre a eliminação dos ficheiros, não ultrapassando os 7 dias de vida.

### I.VII. US07

Nesta US, iremos realizar um *Business Impact Analysis* da nossa solução, tendo em conta os problemas e os riscos que foram identificados no sprint anterior.

A *Business Impact Analysis*(BIA) prevê as consequências da interrupção do negocio ou parte dele e também é muito útil para o desenvolvimento de planos de emergência ou de contingência já que reúne e processa informação sobre a interrupção do negocio.

Para realizarmos o BIA iremos apresentar uma tabela que terá os riscos identificados anteriormente e o que tipo de problemas estes riscos poderão causar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Virtual Machine seja restaurada ou eliminada | Demora da resposta da Virtual Machine | Aplicação estar desatualizada durante a atualização | Ataques Spoofing |
| Módulos diretamente afetados | Logística | | | |
| Atividades do negócio afetadas | Afetará todas as atividades do negócios, ou seja, afetará todos os módulos, quer seja de forma impeditiva ou algo mais insignificante. | | | |
| Tempo mínimo necessário para voltar ao normal | Poderá levar algumas horas | O problema poderá desaparecer dentro de minutos | O problema desaparecerá apos alguns momentos | Irá levar muito tempo a resolver dado a sua natureza |
| Perda de reputação | Poderá levar a perda de reputação como uma aplicação confiável | Não deverá impactar a sua reputação | Não deverá impactar a sua reputação | Poderá levar numa grande perda de reputação como uma aplicação confiável |

Tabela 1- Business Impact Analysis

### I.VIII. US08

Nesta secção irmos abordar como estamos a gerir os acessos dos utilizadores no nosso sistema.

Para o utilizador entrar na nossa aplicação e usar as suas funcionalidades irá que realizar o login com a sua conta google e apos o sucesso, iremos verificar se existe um utilizador com esse email no nosso sistema. Apenas quando se confirmam estas duas condições o utilizador consegue entrar na nossa aplicação e será apresentado as funcionalidades a que tem acesso.

Quando o utilizador consegue se autenticar com sucesso na nossa aplicação é gerado um token que é guardado no localStorage do browser e que serve como um passe para usar as funcionalidades da nossa aplicação. Esse token contem ainda alguma informação sobre o utilizador, como o seu role que permite saber que funcionalidades ele terá acesso.

Perante isto, pode-se dizer que a autenticação da nossa aplicação é feita usando o SSO (Single Sign-On), ou seja, usamos uma autenticação centralizada em que o utilizador apenas se autentica uma vez e pode usar todas as funcionalidades que tem acesso. Esta forma de autenticação leva a um maior esforço na verificação de acessos, isto é assegurado com os tokens . Os tokens asseguram a autorização já que em todos a funcionalidade é verificado e validado o token antes de as conseguir usar.