ASIST - Sprint 2

Grupo 33

**Realizado por:**

Pedro Sousa -1201428

Gonçalo Boa-Nova -

José Silva -

Diogo Carvalho -

Diogo Ribeiro –

**Índice**

**User story 1 3**

**User story 2 3**

**User story 3 3**

**User story 4 4**

**User story 5 5**

**User story 6 6**

**User Stories**

**User story 1**

**US – 1** – Como administrador do sistema quero que o deployment de um dos módulos do RFP numa VM do DEI seja sistemático, validando de forma agendada com o plano de testes.

**User story 2**

**US – 2** – Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução.

**User story 3**

**US – 3** – Como administrador do sistema quero que os clientes indicados na user story 2 possam ser definidos pela simples alteração de um ficheiro de texto.

**User story 4**

**US – 4** – Como administrador quero identificar e quantificar os riscos envolvidos na solução preconizada, Plan-Do-Check-Act (PDCA).

**Matriz de Riscos**

|  |  |  |  |
| --- | --- | --- | --- |
| Probabilidade\Gravidade | **Tolerável** | **Moderado** | **Catastrófico** |
| **Improvável** | 1 | 4 | 7 |
| **Ocasional** | 2 | 5 | 8 |
| **Provável** | 3 | 6 | 9 |

A tabela seguinte representa riscos específicos e ocorrentes com a sua devida justificação, avaliados através da matriz de riscos:

|  |  |  |  |
| --- | --- | --- | --- |
| **Componente** | **Desastre** | **Nível de Risco** | **Justificação** |
| SPA | Serviço DEI inacessível | 8 | Devido a um grande congestionamento na utilização da Cloud do DEI, os serviços podem por vezes tornarem-se lentos ou mesmo inacessíveis. |
| SPA | Interrupção do serviço | 3 | Devido a manutenções semanais à infraestrutura da Cloud do DEI, os serviços encontram-se indisponíveis, requerendo a reiniciação dos mesmos. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**User story 5**

**US – 5** – Como administrador quero que seja definido o **Mininum Business Continuity Objective (MBCO)** (Especifica o nível mínimo de operacionalidade que deve ser mantida durante uma disrupção na infraestrutura) a propor aos stakeholders.

**Servidor de Front-End (Angular)** - É categorizada com prioridade nível 1 pois, em caso de desastre, a aplicação torna-se 100% inutilizável já que o utilizador do sistema não tem acesso a um site funcional para usar as funcionalidades da aplicação.

**Servidor de Back-End (.NET CORE)** - É categorizada com prioridade nível 2 pois, em caso de desastre, não existe a possibilidade de conectar o “Servidor de Front-End (Angular)” com a “Base de Dados”, logo, a aplicação torna-se aproximadamente 100% inutilizável já que o utilizador tem apenas acesso à página de login e registo.

**Servidor de Back-End (Node.js)** - É categorizada com prioridade nível 3 pois, em caso de desastre, não existe a possibilidade de conectar o “Servidor de Front-End (Angular)” com a “Base de Dados”, logo, as funcionalidades da aplicação tornam se reduzidas já que não se mostra possível apresentar as publicações dos utilizadores tal como os seus comentários.

**Base de Dados (Mongo)** - É categorizada com prioridade nível 3 pois, em caso de desastre, a aplicação tem a sua funcionalidade extremamente reduzida, já que não se torna possível o armazenamento de dados respetivamente às publicações e comentários.

**User story 6**

**US – 6** – Como administrador quero que seja proposta e implementada uma estratégia de segurança para minimizar o **Recovery Point Objective (RPO)** (tempo máximo de perda de dados aceite) e o **Work Recovery Time (WRT)** (tempo necessário para repor os dados e aplicações e testá-los).

**Estratégia de cópia de segurança**

**Backups**

Foi definido pelo Grupo 33 que os servidores de armazenamento de dados devem ter prioridade sobre os servidores API. Isto devido ao seu baixo RPO, requerendo backups recorrentes para a menor perda de dados possível e visto que os servidores API, que apresentam raras alterações, satisfazem-se com novos backups apenas em momentos de alteração de código. Assim, cada servidor deve ter um servidor de “backup” para Load Balancing, implementado na Cloud do DEI de modo a manter a consistência da infraestrutura. Para servidores de armazenamento de dados, deve existir adicionalmente uma Base de Dados e mais um servidor de backup para o anterior.

**Base de Dados** - Backup integral em dois dias da semana (Segunda e Sexta) e três backups incrementais diários (8 em 8 horas).

**API** - Backup Integral sempre que exista uma alteração.

**Processo de mitigação de dados**

Numa situação de desastre, deve existir, para além dos servidores de backup para Load Balancing, um servidor responsável pelo Load balancing do tráfego recebido. Este servidor tem a responsabilidade de garantir que o tráfego recebido seja enviado apenas para servidores que estão operacionais ou com menos conexões. Cada servidor de armazenamento de dados, deverá ter a função de enviar recorrentemente as suas alterações para a Base de Dados que irá agregar e registar as alterações. Finalmente, é usada a estratégia de backup para a Base de Dados.