| **ID** | **Nome** | **Descrição** |
| --- | --- | --- |
| BR01 | Normas de utilização | O administrador deve estabelecer um conjunto de normas de utilização responsável do serviço para garantir um bom entendimento entre os membros da comunidade. |
| BR02 | Responder a perguntas fechadas | Os utilizadores autenticados não podem responder a uma pergunta que tenha sido fechada pelo respetivo autor. |
| BR03 | Alterar voto | Os utilizadores autenticados podem alterar a votação previamente atribuída a uma pergunta ou resposta. |
| BR04 | Anular voto | Os utilizadores autenticados podem retirar a votação previamente atribuída a uma pergunta ou resposta. |
| BR05 | Cálculo da pontuação | A pontuação de uma determinada pergunta é dada pela soma aritmética dos “gostos” (classificação positiva, +1 ponto) e “não gostos” (classificação negativa, -1 ponto) atribuídos pelos utilizadores. |
| BR06 | Melhor pergunta / resposta | No caso de existirem várias perguntas / respostas com a mesma pontuação, terá prioridade aquela que apresentar maior número de votos no geral (quer positivos, quer negativos); será ainda considerada para desempate a data de publicação, ou seja, de duas perguntas / respostas com a mesma popularidade, será escolhida a mais recente. |
| BR07 | Associação de categorias | A uma categoria podem estar associadas uma ou várias instituições de ensino da Universidade do Porto. A uma instituição de ensino podem estar associadas várias categorias. |
| BR08 | Múltiplas respostas | Um utilizador autenticado pode responder mais do que uma vez à mesma pergunta. |
| BR09 | Múltiplos comentários | Um utilizador autenticado pode comentar mais do que uma vez a mesma pergunta / resposta. |
| BR10 | Multiplos votos | Um utilizador autenticado não pode atribuir mais do que um voto à mesma pergunta / resposta. |
| BR11 | Votar nas próprias publicações | Um utilizador autenticado não pode atribuir votos às suas perguntas nem às suas respostas. |
| BR12 | Mensagens privadas | Um utilizador autenticado não pode enviar mensagens para ele próprio. |
| BR13 | Contas de utilizador | Não podem existir utilizadores com a mesma alcunha nem mais do que uma conta de utilizador associada a determinado endereço de e-mail. |
| BR14 | Informações pessoais | A introdução de informações pessoais (endereço de *e-mail* de contato, localização) deve ser facultativa para todos os utilizadores, à exceção do primeiro e último nome e da instituição de ensino. |

| **ID** | **Nome** | **Descrição** |
| --- | --- | --- |
| TR01 | Tecnologias *Web* | A interface *web* do sistema deve ser implementada com páginas dinâmicas recorrendo a diversas tecnologias como HTML5, CSS3, JavaScript, jQuery e PHP. |
| TR02 | *Responsive Design* | A *interface* *web* deve aplicar alguns princípios de *responsive design* para adaptar-se aos diferentes dispositivos móveis e tamanhos de ecrã. |
| TR03 | *Frameworks* | A *interface* *web* deve tirar máximo partido da linguagem de *design* gráfico e das funcionalidades oferecidas pela *framework* “SAPO Ink”. |
| TR04 | *SGBD* | A aplicação *web* deve utilizar um sistema de gestão de bases de dados *PostgreSQL*. |
| TR05 | Usabilidade | A *interface web* deve ser simples, intuitiva e apelativa aos utilizadores; deve ser possivel aceder ás funcionalidades de pesquisa em qualquer página |
| TR06 | Robustez | O sistema deverá estar preparado para permanecer em funcionamento mesmo quando ocorrem erros de execução. Estes devem ser comunicados ao utilizador quando este tenta realizar uma operação crítica (publicar uma pergunta, registar conta, autenticar-se) sem sucesso. |
| TR07 | Privacidade | Deve ser implementado um sistema de autenticação e verificação de privilégios de forma a proteger os dados pessoais dos utilizadores e outras informações sensíveis de acessos não autorizados. |
| TR08 | Segurança | O sistema deve impedir que os utilizadores ou terceiros tentem aceder a páginas ou realizem operações para os quais não estão autorizados, através da verificação de privilégios e prevenção de ataques externos como *bruteforce*, SQL *Injection*s ou *Cross Site Scripting* (XSS). |
| TR09 | *CAPTCHA* | Para evitar ataques de *bruteforce* sobre as *passwords* dos utilizadores deve ser pedido ao utilizador para resolver um CAPTCHA ao fim de cinco tentativas de autenticação falhadas. |
| TR10 | Ética | O sistema deve respeitar os princípios éticos que se aplicam ao desenvolvimento de serviços e aplicações *web*. As *passwords* devem ser encriptadas segundo um algoritmo de *hashing* seguro, de preferência com utilização de *salts*, para garantir que estas são conhecidas apenas pelo dono. |