| 1ª Apresentação para o orientador | | |
| --- | --- | --- |
| **Critérios** | **Classificações** | **Pts** |
| **Dedicação: amplitude e profundidade do trabalho do aluno até o momento**  **Comentários do instrutor**  **A mudança do projeto após os feedbacks ocorreu um pequeno atraso, em minha opnião, em relação a pesquisa. Digo isso por não ter visto na apresentação um pouco mais sobre os requisitos e possíveis soluções. O foco ficou em apresentar o negócio e problema. No entanto é compreensível e consideraria um bônus.** | 2,5 pts  Satisfatório  1,25 pts  Razoável  0 pts  Ausente | 2,5 / 2,5 pts |
| **Envolvimento: qualidade do diálogo entre orientador e orientando** | 2,5 pts  Satisfatório  1,25 pts  Razoável  0 pts  Ausente | 2,5 / 2,5 pts |
| Total de pontos: 5 | | |

**Adicionar um comentário:**

[Conteúdo de mídiaAnexar Arquivo](https://igti.instructure.com/courses/1384/assignments/31993/submissions/7487)

Salvar

Olá,

Conforme conversado lhe indico alguns pontos para argumentar os levantamentos feitos pelo corpo da Unesco.

[https://aws.amazon.com/compliance/data-privacy-faq/ (Links para um site externo)Links para um site externo](https://aws.amazon.com/compliance/data-privacy-faq/)

Especialmente as partes que falam sobre a propriedade do conteúdo nos servidores, e sobre conformidade com segurança. Acredito também que não precise apenas confiar na palavra deles, pois há leis que garantem que a propriedade dos dados é da pessoa que hospeda e não do provedor.

Com relação a criptografia dos dados, existem várias soluções:

A criptografia dos discos e a manutenção de chaves sob responsabilidade da equipe unesco. [https://aws.amazon.com/kms/ (Links para um site externo)Links para um site externo](https://aws.amazon.com/kms/)

Acredito que a azure fornece um serviço equivalente, mas acho não estar tão integrado quando o da Amazon. [https://azure.microsoft.com/en-us/services/key-vault/ (Links para um site externo)Links para um site externo](https://azure.microsoft.com/en-us/services/key-vault/)

Porém antes de usá-los veja isso: [https://info.townsendsecurity.com/who-owns-my-encryption-key-in-the-amazon-aws-cloud (Links para um site externo)Links para um site externo](https://info.townsendsecurity.com/who-owns-my-encryption-key-in-the-amazon-aws-cloud)

Um projeto realmente seguro é: [https://www.vaultproject.io/ (Links para um site externo)Links para um site externo](https://www.vaultproject.io/)

O vault é um recurso mais avançado e seria mais interessante em conjunto com a aplicação, isto é, seria interessante com programação na aplicação para receber segredos e chaves e utilizá-los para acessar informações, embora possa fazer algumas coisas fora dela (ssh keys, cryptografia de dados, etc...)

Precisamos definir o requisito de confidencialidade. Se quisermos migrar para núvem e manter acesso exclusivo ao conteúdo, de forma que nem uma ordem judicial de um pais possa obrigar fornecedores a entregar os dados. Isso é bem mais complicado, mas possível.

Uma forma de fazê-lo é gravar dados de forma irreversível e manter a chave de descriptografia segura (no vault) de forma que o acesso a esses dados seja feito apenas por pessoas autorizadas.

Isso só será possível com alterações na aplicação, mas acredito ser estratégico a longo prazo, dado que seria interessante para  a organização garantir independência de qualquer governo, claro que ainda sim a unesco cumpriria com mandatos judiciais, a questão não é se não, mas o faria conhecendo o processo e seria notificada do mesmo.

Interessante notar que manter os dados onpromise ajuda mas não garante isso. O servidor ainda pode ser confiscado ou atacado.