Políticas de segurança sistema CATE

1. **Recebimento dos dados**
    a. O controlador dos dados deverá realizar o upload das bases de dados através de um repositório criado no **Proton Drive**, onde somente os e-mails autorizados terão acesso.
2. **Armazenamento local dos dados**
    a. Será realizado o download das bases de dados através do **Proton Drive**.
    b. As bases de dados serão armazenadas em uma pasta segura criada pelo **VeraCrypt**.
    c. As bases de dados armazenadas localmente devem obrigatoriamente estar criptografadas pelo **VeraCrypt**.
    d. Os desenvolvedores do sistema CATE devem acessar somente as bases de dados armazenados pelo **VeraCrypt**.
3. **Extração dos dados**
    a. Os dados extraídos da planilha serão armazenados no banco de dados **MongoDB** através de uma conexão segura TLS/SSL.
4. **Armazenamento externo dos dados**
    a. Os dados serão armazenados em um banco de dados **MongoDB** gerenciado pelo sistema CATE.
    b. Somente os usuários autorizados poderão acessar o banco de dados.
5. **Exclusão dos dados**
    a. Após a utilização da base de dados a mesma será armazenada dentro de um container VeraCrypt e este será excluído.
6. **Armazenamento local dos LOGs**
    a. Os LOGs gerados pelo sistema CATE serão armazenados em pastas criptografadas criadas pelo **VeraCrypt**.
7. **Armazenamento externo dos LOGs**
    a. Será feito o upload no **Proton Drive** das pastas criptografadas contendo os LOGs.
8. **Solicitação dos LOGs**
    a. A solicitação dos LOGs deverá ser documentada, assinada pelo solicitante e encaminhada para a empresa **The Velopers** através dos controladores de dados.
    b. O acesso aos LOGs será permitido somente à empresa controladora dos dados. O link para acesso aos arquivos solicitados funcionará de forma somente leitura durante período constante na solicitação.
    c. As solicitações serão avaliadas pela equipe **The Velopers** conforme necessidade apresentada.