**Apresentação**

**Introdução -M**

Um sistema de armazenamento necessita de ser seguro, eficiente e em conformidade com as regulamentações atuais. Num mundo em que a quantidade de dados tem crescido exponencialmente, a necessidade de proteger e gerir essas informações tornou-se mais necessário que nunca.

Vamos agora mostrar todas as fases da construção do nosso sistema.

**Camada de Aquisição de Dados -G**

Na nossa camada de aquisição de dados usamos HTTPS para garantir que todas as transferências de dados sejam criptografadas, impedindo qualquer tentativa de interceção ou adulteração.

Usamos assinaturas digitais para verificar a autenticidade dos dados, garantindo que cada fonte os assine antes de enviá-los. Além disso, usamos checksums para detetar qualquer alteração nos dados durante a transferência.

Utilizamos o TLS/SSL para criptografar os dados durante a transmissão entre o cliente e o servidor, e garantimos que os algoritmos de criptografia sejam fortes e atualizados.

Esta abordagem robusta, fortalece a nossa defesa contra ameaças cibernéticas e aumenta a confiança dos utilizadores e partes interessadas na nossa capacidade de gerir dados.

**Armazenamento de Dados - M**

O sistema de armazenamento desenvolvido é um sistema distribuído e escalável.

Quanto à sua **segmentação e distribuição** os dados são armazenados como objetos em buckets no sistema. Cada objeto pode ser de qualquer tamanho, permitindo flexibilidade no armazenamento de dados.

A segmentação é automática, ou seja, os dados são segmentados conforme forem carregados, dividindo-se em partes menores, se necessário. Desta forma teremos uma distribuição eficiente dos dados em vários nós de armazenamento.

Os buckets podem ser distribuídos em várias regiões geográficas para garantir alta disponibilidade e recuperação de desastres. Assim, é possível que os utilizadores acedam aos dados de qualquer localidade reduzindo a latência.

É importante garantir a **Tolerância a Falhas e a Redundância**. O sistema oferece duas diferentes classes de armazenamento com níveis diferentes de redundância:  
**- Vault Standart:** dados encontram-se replicados automaticamente em múltiplas zonas de disponibilidade para garantir a alta disponibilidade e durabilidade.

**- One Vault:** dados armazenados em apenas uma zona de disponibilidade

A zona de disponibilidade fica isolada dentro de uma região da “SecureVault “ composta por diversos data centres. Cada uma destas zonas é independente de qualquer outra para prevenir problemas por dependência.

“One Vault” tem um custo menor devido à redução dos custos de armazenamento em comparação com a classe “Vault Standart” que replica os dados por múltiplas zonas.

Os dados que se encontram armazenados são automaticamente **criptografados** antes de serem armazenados no sistema, garantindo segurança adicional.

As chaves criptográficas são geridas pelo próprio sistema, garantindo a segurança e integridade dos dados. Os utilizadores podem optar por usar as suas próprias chaves criptográficas.

O sistema suporta práticas de **versionamento**, ou seja, permite rastrear alterações nos objetos ao longo de um determinado tempo. Isto permite que utilizadores restaurem versões anteriores dos objetos, caso necessário.

Os dados armazenados no sistema podem ser exportados para sistemas de **backup** **externos**.

O nosso sistema oferece uma solução robusta e confiável para armazenar dados de forma distribuída e escalável, com foco na segmentação, distribuição, redundância, segurança e backups.

**Controlo de acesso -G**

Com a implementação do Controlo de Acesso Baseado em Funções (RBAC), cada utilizador é atribuído a funções específicas que correspondem às suas responsabilidades e autorizações.

As principais componentes do RBAC são as Funções, as Atribuição de Funções e as Permissões.

Como funções temos:

O Administrador que pode criar, ler, atualizar e excluir dados, o Utilizador Comum que pode apenas ler dados, e o Analista que Pode executar consultas e gerar relatórios.

Em suma, o RBAC é uma abordagem eficaz para gerir o acesso aos recursos do sistema, garantindo que cada utilizador tenha as permissões adequadas para desempenhar as suas funções, sem comprometer a segurança ou a integridade dos dados.

A Autenticação Multifatorial (MFA) e a Monitorização de Acessos são essenciais para a nossa segurança. Com a MFA, exigimos uma segunda forma de autenticação além das credenciais usuais, como um código enviado por SMS ou uma autenticação biométrica, o que torna mais difícil o acesso não autorizado, mesmo em caso de comprometimento das credenciais.

A Monitorização de Acessos mantém registos detalhados de todas as atividades dos utilizadores, permitindo-nos identificar rapidamente qualquer atividade suspeita e manter a conformidade com regulamentos de privacidade.

**Camada de Privacidade dos Dados – M**

Na camada de privacidade dos Dados o nosso foco é garantir a proteção e a confidencialidade das informações pessoais dos utilizadores, especialmente em conformidade com regulamentações rigorosas, como o RGPD (Regulamentação Geral de Proteção de Dados).

Vamos abordar agora cada aspeto detalhadamente:

**- Mascaras de Dados, Anonimização e Pseudonimização:**

Implementámos técnicas de Máscaras de Dados, Anonimização e Pseudonimização para proteger as informações pessoais, garantindo que os dados sensíveis sejam ocultados ou substituídos por valores fictícios.

**- Privacidade Diferencial**

Adotámos técnicas de privacidade diferencial para proteger contra-ataques de identificação, preservando a privacidade dos utilizadores mesmo quando os dados são compartilhados ou analisados. É adicionado ruído aos dados de forma controlada, garantindo que consultas ou analises não revelem informações especificas.

**Camada Legal e Judicial – M**

Na camada Legal e Judicial, a conformidade regulatória é essencial para garantir que o sistema de armazenamento de dados esteja alinhado com as leis e regulamentações aplicáveis. Vamos explorar os principais aspetos dessa camada:

**- Conformidade Regulatória: -G**

Comprometemo-nos com a conformidade regulatória, especialmente com o RGPD para dados pessoais da UE e o HIPAA para dados de saúde nos EUA. Sob o RGPD, garantimos transparência, consentimento explícito e direito ao esquecimento.

No contexto do HIPAA, protegemos a privacidade dos pacientes com acesso restrito e criptografia de dados sensíveis. Essas medidas demonstram o nosso compromisso com a segurança e privacidade dos dados.

**- Armazenamento de Metadados: - M**

Os metadados são informações sobre os dados (por exemplo, data de criação, autor, histórico de alterações). O armazenamento destes dados para rastreamento e uma auditoria permite que posteriormente saibamos quem acedeu aos dados e quando.

**- Acesso Judicial Controlado: -M**

Para conformidade com as leis, em casos legais em que as autoridades judiciais solicitem acesso aos dados foi implementado um processo rigoroso para conceder acesso controlado, através de uma revisão legal, documentação detalhada e restrições especificas.

**- Notificação e Validação: -G**

Em conformidade com as exigências legais, comprometemo-nos a notificar prontamente as partes afetadas em caso de violação de dados. Esta notificação é crucial para garantir que os indivíduos afetados sejam informados sobre a violação e possam tomar medidas adequadas para se protegerem.

Implementamos processos de validação rigorosos, verificando a extensão da violação, identificando as partes afetadas e avaliando os potenciais impactos antes de proceder com as notificações.

**- Considerações Éticas e Sociais: -M**

Além das obrigações legais, consideramos sempre o impacto social e ético do sistema, garantindo sempre transparência com os utilizadores sobre como os dados são tratados.

**- Importância da Conformidade Legal e Judicial: -G**

A conformidade legal e judicial é crucial para proteger os direitos dos utilizadores e garantir a transparência e integridade das nossas operações. Ao cumprir as regulamentações de privacidade de dados e permitir um acesso judicial controlado, demonstramos o nosso compromisso com a proteção da privacidade e a conformidade legal. Essas medidas fortalecem a confiança dos utilizadores e protegem a empresa contra riscos legais e financeiros.