**Planejamento de Arquitetura do Sistema (22 a 28 de agosto)**

* Criptografia: Utilizar TLS/SSL para proteger a comunicação entre o ESP32 e o Google Cloud IoT Core, e entre a plataforma de nuvem e a interface de monitoramento.
* Autenticação: Implementar autenticação robusta para assegurar que apenas dispositivos e usuários autorizados possam acessar os dados e APIs.
* Criptografia: Utilizar a criptografia nativa do Google Cloud Storage para proteger os dados armazenados.
* Controle de Acesso: Configurar políticas de acesso e permissões no Google Cloud para garantir que somente usuários e sistemas autorizados possam acessar e manipular os dados.

MQTT

* Uso: Protocolo leve ideal para comunicação de dados entre dispositivos IoT e a nuvem, suportando transmissão eficiente e em tempo real.
* Vantagens: Reduzido consumo de largura de banda e latência, ideal para redes com limitações.