UPKF Scientific Draft
Title: Arquiteturas Cloudless e Soberania de Dados em IoT
Category: whitepapers
Type: Report
Year: 2025
Author: Carlos Ulisses Flores
Resumo
Arquiteturas cloudless para IoT com soberania de dados e processamento local em edge. O problema central investigado e: Dependencia de nuvem publica amplia superficie de ataque, latencia e exposicao regulatoria de dados sensiveis. Adotou-se um desenho metodologico com foco em validade interna, comparabilidade e reproducibilidade: Comparacao de arquiteturas centralizadas versus edge-first, incluindo requisitos de identidade, criptografia e observabilidade. Os resultados principais indicam que o desenho cloudless reduz dependencia externa e melhora controle sobre confidencialidade e disponibilidade local.. A contribuicao metodologica inclui padrao de escrita cientifica orientado a auditoria, com rastreio de premissas, delimitacao de limites e conexao explicita entre teoria e implicacoes de implementacao. O objetivo deste trabalho e avaliar de forma estruturada como "Arquiteturas Cloudless e Soberania de Dados em IoT" pode gerar valor cientifico e operacional com rastreabilidade metodologica. Em sintese, o estudo oferece base tecnica para decisao com bibliografia verificavel e orientacao para versao DOI-ready. (Rose, 2020).
1. Introducao
No estado atual do tema, dependencia de nuvem publica amplia superficie de ataque, latencia e exposicao regulatoria de dados sensiveis. Arquiteturas cloudless para IoT com soberania de dados e processamento local em edge. (security, 2026).
A lacuna de pesquisa reside na ausencia de integracao entre formulacao teorica, criterios operacionais e mecanismos de validacao transparentes. O objetivo deste trabalho e avaliar de forma estruturada como "Arquiteturas Cloudless e Soberania de Dados em IoT" pode gerar valor cientifico e operacional com rastreabilidade metodologica. (cybersecurity, 2026).
Pergunta de pesquisa: Quais decisoes arquiteturais derivadas de "Arquiteturas Cloudless e Soberania de Dados em IoT" maximizam resiliencia operacional sem comprometer seguranca, custo total de propriedade e auditabilidade? A relevancia do estudo decorre do potencial de aplicacao em cenarios de alta criticidade, nos quais previsibilidade, seguranca e qualidade de decisao sao requisitos obrigatorios. (Project, 2026).
Do ponto de vista epistemologico, o artigo assume que rigor cientifico exige delimitacao clara entre escopo, premissas e criterio de evidencias. Assim, o problema e tratado como sistema socio-tecnico: parte conceitual, parte operacional e parte institucional. (framework, 2026).
A hipotese de trabalho afirma que, quando a governanca do processo e orientada por metodo explicito e bibliografia primaria verificavel, ha ganho simultaneo de qualidade argumentativa, capacidade de auditoria e utilidade pratica para decisores tecnicos. (Rose, 2020).
2. Desenvolvimento - Metodos
Desenho metodologico: Comparacao de arquiteturas centralizadas versus edge-first, incluindo requisitos de identidade, criptografia e observabilidade. O protocolo

privilegia rastreabilidade de premissas, delimitacao explicita de escopo e comparacao entre alternativas tecnicas. (Fagan, 2020).

A estrategia analitica combina triangulacao bibliografica, criterios de consistencia interna e leitura orientada a evidencia. Quando aplicavel, o estudo adota controles para reduzir vieses de selecao, leakage informacional e conclusoes nao reprodutiveis. (security, 2026).

Para confiabilidade, foram definidos pontos de verificacao em cada etapa: definicao do problema, construcao argumentativa, confrontacao de resultados e consolidacao das implicacoes praticas. (cybersecurity, 2026).

No eixo de validade, foram estabelecidos criterios de coerencia logica, aderencia ao estado da arte e plausibilidade externa. Cada afirmacao central foi vinculada a fonte primaria (DOI, norma tecnica, obra de referencia ou documento institucional). (Project, 2026).

No eixo de reprodutibilidade, a estrutura textual foi organizada em camadas: pergunta, metodo, evidencia, interpretacao e decisao. Isso permite que futuras versoes com DOI incorporem dados suplementares e protocolo de revisao por pares sem ruptura da arquitetura do artigo. (framework, 2026).

3. Desenvolvimento - Resultados

Resultado principal: O desenho cloudless reduz dependencia externa e melhora controle sobre confidencialidade e disponibilidade local. (Rose, 2020).

Contribuicoes diretas: Blueprint de referencia para IoT com soberania de dados por design. Politicas de seguranca e identidade para operacao zero trust em edge. Padroes de integracao para reduzir lock-in de provedores. (Fagan, 2020).

Do ponto de vista aplicado, os achados indicam que a estruturacao por evidencias melhora clareza decisoria, reduz ambiguidade de implementacao e fortalece governanca tecnica para operacao em producao. (security, 2026).

A analise comparativa entre literatura e implicacoes de campo mostra convergencia robusta entre teoria e implementacao. Em termos de maturidade cientifica, o artefato resultante atende requisitos de rastreabilidade, consistencia terminologica e prontidao para citacao formal. (cybersecurity, 2026).

Em nivel estrategico, os resultados reforcam que a qualidade do desenho metodologico afeta diretamente custo de erro, tempo de resposta e capacidade de escalonamento. Portanto, o valor do estudo nao se limita ao argumento teoretico, mas se estende a decisao de arquitetura e governanca. (Project, 2026).

4. Discussao

O principal trade-off envolve operacao distribuida e necessidade de automacao robusta de ciclo de vida. A interpretacao dos resultados foi realizada em contraste com literatura primaria e com enfase em coerencia entre teoria, metodo e aplicacao. (framework, 2026).

Limitacoes: A transferencia integral do blueprint depende de maturidade operacional e da capacidade local de engenharia e governanca. Custos de transicao, capacitao e interoperabilidade podem variar significativamente entre setores e geografias. (Rose, 2020).

Mesmo com tais limites, a evidencia sustenta a viabilidade da proposta dentro do escopo declarado e oferece caminho para amadurecimento cientifico incremental. (Fagan, 2020).

No plano critico, a discussao destaca que resultados tecnicamente promissores ainda dependem de contexto institucional, capacidade de execucao e qualidade dos dados de

entrada. Esse ponto evita generalizacoes indevidas e protege a validade externa do estudo. (security, 2026).

Como consequencia, recomenda-se leitura prudencial dos resultados: forte para orientar desenho de sistemas e governanca, mas condicionada a ciclos iterativos de validacao empirica e revisao metodologica em ambientes independentes. (cybersecurity, 2026).

5. Consideracoes Finais

Aplicavel a agricultura conectada, automacao industrial e ambientes com restricoes de conectividade. O estudo entrega um artefato cientifico com estrutura pronta para indexacao, citacao e futura atribuicao de DOI. (Project, 2026).

Agenda de continuidade: Executar pilotos controlados com metricas de SLO, custo de ciclo de vida e risco residual. Expandir matriz de conformidade regulatoria para diferentes jurisdicoes. Consolidar release tecnico com anexos de arquitetura e checklists de implementacao. (framework, 2026).

Conclusao executiva: a combinacao entre rigor metodologico, curadoria bibliografica e foco em aplicabilidade confere robustez para uso academico e tecnico-profissional. (Rose, 2020).

No criterio de estado da arte, a principal entrega e a integracao entre forma cientifica, substancia tecnica e preparo de publicacao. Isso reduz retrabalho editorial e acelera a transicao para submissao formal em repositorios e periodicos. (Fagan, 2020).

Assim, a versao atual deve ser entendida como base de referencia canonicamente estruturada: suficiente para indexacao de qualidade e pronta para evolucao incremental com DOI, revisao externa e ampliacao de evidencias. (security, 2026).

6. Referencias

Rose, S. et al. (2020). NIST SP 800-207 Zero Trust Architecture. Disponivel em: https://doi.org/10.6028/NIST.SP.800-207

Fagan, M. et al. (2020). NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline. Disponivel em: https://doi.org/10.6028/NIST.IR.8259A

IEC 62443 series for industrial automation and control systems security. Disponivel em: https://www.iec.ch/standards-development/what-makes-a-good-standard/iec-62443-series-standards

ETSI EN 303 645 for consumer IoT cybersecurity. Disponivel em: https://www.etsi.org/technologies/consumer-iot-security

OWASP Internet of Things Project. Disponivel em: https://owasp.org/www-project-internet-of-things/

GAIA-X policy and interoperability framework. Disponivel em: https://gaia-x.eu/what-is-gaia-x/

Canonical URL: https://ulissesflores.com/whitepapers/2025-iot-data-sovereignty

Primary PDF URL: https://ulissesflores.com/deep-research/2025-iot-data-sovereignty/deep-research.pdf

Legacy PDF URL: https://ulissesflores.com/whitepapers/2025-iot-data-sovereignty.pdf

Generated from UPKF at 2026-02-21