UNIVERSIDADE DO VALE DO PARAÍBA
FACULDADE DE ENGENHARIAS, ARQUITETURA E URBANISMO
CURSO DE ENGENHARIA CIVIL

Guilherme Palmanhani Valli

TRABALHO DE CONCLUSÃO I

Sistema IoT Seguro para Rastreabilidade e Monitoramento no Transporte de Vacinas

Trabalho de Graduação apresentado no Curso de Bacharel em Engenharia da Computação da Faculdade de Engenharias, Arquitetura e Urbanismo - Univap como parte dos requisitos para obtenção do título de Engenheiro da Computação.

Orientador: Wagner dos Santos Clementino de Jesus

SÃO JOSÉ DOS CAMPOS
2025

RESUMO

Neste trabalho apresenta-se o desenvolvimento de um sistema IoT seguro destinado à gestão do transporte de vacinas, motivado pela necessidade de garantir condições ambientais adequadas, rastreabilidade contínua e proteção dos dados envolvidos nesse processo crítico. A metodologia prevê a construção de um protótipo baseado em ESP32, responsável por coletar temperatura, umidade e localização por meio do sensor DHT22 e de um módulo GPS, estruturado segundo os pilares de Percepção, Conectividade, Análise e Ação, e integrando comunicação via MQTT com aplicação de autenticação mútua, TLS, HMAC-SHA256, controle de acesso, criptografia e hardening do broker. Os procedimentos metodológicos incluem ainda a implementação de mecanismos de continuidade e recuperação, como failover do broker, redundância de energia, backups criptografados e reconexão automática, além da execução de testes de segurança e resiliência, incluindo sniffing, MITM, DDoS e tentativas de acesso não autorizado, para comparar o comportamento do sistema antes e depois das medidas de proteção. Espera-se como resultado a validação da arquitetura proposta, demonstrando maior integridade, disponibilidade e confiabilidade na transmissão e armazenamento dos dados, bem como a eficácia operacional de um dashboard seguro para monitoramento em tempo real. Conclui-se que a aplicação integrada de IoT e práticas robustas de cibersegurança pode elevar substancialmente o nível de proteção e rastreabilidade do transporte de vacinas, contribuindo para maior segurança sanitária e conformidade regulatória.

Palavras-chave: IoT; transporte de vacinas; cibersegurança; MQTT; ESP32; continuidade de negócios.

ABSTRACT

This work presents the development of a secure IoT system designed for the management of vaccine transportation, motivated by the need to ensure adequate environmental conditions, continuous traceability, and the protection of data involved in this critical process. The methodology involves the construction of a prototype based on an ESP32, responsible for collecting temperature, humidity, and location using a DHT22 sensor and a GPS module, structured according to the pillars of Perception, Connectivity, Analysis, and Action, and integrating MQTT communication with mutual authentication, TLS, HMAC-SHA256, access control, encryption, and broker hardening. The methodological procedures also include the implementation of continuity and recovery mechanisms, such as broker failover, power redundancy, encrypted backups, and automatic reconnection, as well as the execution of security and resilience tests, including sniffing, MITM, DDoS, and unauthorized access attempts, to compare the system's behavior before and after applying the protection measures. The expected results include validation of the proposed architecture, demonstrating greater integrity, availability, and reliability in data transmission and storage, as well as the operational effectiveness of a secure dashboard for real-time monitoring. It is concluded that the integrated application of IoT and robust cybersecurity practices can substantially increase the level of protection and traceability in vaccine transportation, contributing to improved sanitary safety and regulatory compliance.

Keywords: IoT; vaccine transportation; cybersecurity; MQTT; ESP32; business continuity.

SUMÁRIO

1. INTRODUÇÃO

A distribuição de vacinas representa uma das etapas mais sensíveis e críticas dentro das cadeias de suprimentos do setor da saúde. Por se tratarem de produtos biológicos altamente sensíveis a variações de temperatura, pequenas falhas no armazenamento ou transporte podem comprometer sua eficácia, segurança e validade, afetando diretamente a saúde pública e a confiança populacional nos programas de imunização (WHO, 2022). Estima-se que até 25% das vacinas em países em desenvolvimento sejam degradadas devido a falhas na cadeia de frio, principalmente durante o transporte e manuseio inadequado (UNICEF, 2021).

A gestão do transporte de vacinas é, portanto, um sistema crítico, pois envolve a integridade de um insumo estratégico de saúde pública, cuja falha pode gerar impactos epidemiológicos, econômicos e sociais significativos. Além da preservação da temperatura adequada (geralmente entre +2 °C e +8 °C), a rastreabilidade, a auditoria e a conformidade regulatória tornaram-se exigências legais em diversos países. No Brasil, a Agência Nacional de Vigilância Sanitária (Anvisa), por meio da Resolução RDC nº 430/2020, determina que fabricantes, distribuidores e transportadores de medicamentos e imunobiológicos devem garantir o monitoramento contínuo de temperatura, registros auditáveis e rastreabilidade completa durante o transporte e armazenamento, de forma a possibilitar ações corretivas e investigações em caso de desvios de qualidade (ANVISA, 2020).

A ausência de sistemas confiáveis de monitoramento e registro acarreta problemas sérios de auditoria e conformidade. Em situações de recall ou suspeita de defeitos em determinados lotes, é fundamental identificar rapidamente quando, onde e sob quais condições as vacinas foram expostas a possíveis falhas. Sem um sistema de gestão digital e automatizado, esse processo é lento, sujeito a erros humanos e frequentemente inviabiliza a rastreabilidade completa exigida por normas internacionais, como o Good Distribution Practice (GDP) da União Europeia e o WHO Model Guidance for Vaccine Management (WHO, 2023).

Nesse contexto, a aplicação de tecnologias digitais e conectadas surge como uma resposta estratégica aos desafios de rastreabilidade e confiabilidade do transporte de vacinas. Soluções baseadas em Internet das Coisas (IoT) possibilitam o monitoramento em tempo real de parâmetros ambientais, geográficos e logísticos, permitindo maior visibilidade e controle da cadeia de frio. No entanto, a adoção dessas tecnologias também traz novas responsabilidades, especialmente no que se refere à segurança e integridade das informações coletadas e transmitidas por dispositivos conectados.

A Internet das Coisas (IoT) tem se consolidado como um dos pilares centrais da transformação digital global, integrando sensores, atuadores e sistemas inteligentes a praticamente todos os setores produtivos. Segundo estimativas da Statista (STATISTA, 2024), espera-se que o número de dispositivos IoT conectados ultrapasse 30 bilhões até 2030, impulsionando uma nova era de automação e análise de dados em tempo real. No entanto, essa rápida expansão traz consigo novos desafios de cibersegurança e privacidade, especialmente em setores críticos, como o de saúde, onde a confiabilidade e a integridade das informações são vitais.

O aumento exponencial de dispositivos conectados ampliou significativamente a superfície de ataque das infraestruturas digitais. Relatórios recentes da ENISA (European Union Agency for Cybersecurity, 2023) indicam que ataques direcionados a dispositivos IoT cresceram mais de 400% entre 2020 e 2023, com destaque para tentativas de sequestro de dados (ransomware), interceptação de comunicações (MITM) e exploração de falhas em protocolos inseguros. Esses ataques demonstram que, apesar do potencial transformador da IoT, sua adoção sem mecanismos adequados de proteção pode comprometer a disponibilidade e a confiabilidade de serviços essenciais.

Na área da saúde, o risco é ainda maior. Sistemas hospitalares e logísticos baseados em IoT frequentemente lidam com dados sensíveis e operações críticas, desde o monitoramento de pacientes até o transporte de insumos biológicos. Um incidente de segurança pode resultar não apenas em perdas financeiras, mas também em danos à saúde pública e à confiança institucional. Por isso, organismos internacionais, como o NIST (National Institute of Standards and Technology) e a Organização Mundial da Saúde (WHO), têm reforçado diretrizes para o desenvolvimento de soluções IoT seguras, destacando a importância da autenticação mútua, criptografia ponta a ponta, monitoramento contínuo e planos de continuidade operacional.

Nesse contexto, torna-se evidente que a evolução da IoT deve caminhar junto com o fortalecimento da ciber-resiliência — a capacidade de resistir, responder e se recuperar de incidentes digitais. Essa integração entre conectividade e segurança é o que permite que soluções IoT sejam confiáveis em ambientes de missão crítica, como cadeias de suprimento de vacinas, sistemas hospitalares e dispositivos médicos conectados, como mostrado na Figura 1.

Assim, a necessidade de um sistema inteligente e seguro de gestão de transporte de vacinas emerge não apenas pela eficiência operacional, mas pela obrigação de garantir rastreabilidade, confiabilidade e conformidade regulatória. A integração de tecnologias IoT ao processo permite monitorar em tempo real variáveis ambientais, localização e status de entrega das câmaras térmicas, viabilizando respostas imediatas a anomalias. Contudo, o valor real do sistema está em sua capacidade de assegurar integridade, autenticidade e disponibilidade das informações, pilares que definem a criticidade desse tipo de solução em ambientes de missão crítica como o setor da saúde.

Figura 1: Arquitetura geral do sistema desenvolvido

Fonte: O autor

2. METODOLOGIA

A metodologia deste trabalho será estruturada de forma a descrever o processo de concepção, desenvolvimento e validação de um sistema de Internet das Coisas (IoT) voltado para o monitoramento seguro do transporte de vacinas. O sistema será projetado com base em uma arquitetura distribuída que integra hardware, software e protocolos de comunicação para garantir a coleta, transmissão, armazenamento e análise de dados sensíveis em tempo real. Para isso, será desenvolvido um protótipo composto por um microcontrolador ESP32, sensores DHT22 para medição de temperatura e umidade, módulo GPS para rastreamento de localização, além de um sistema de alimentação híbrido baseado em fonte de energia e bateria, assegurando a operação contínua durante o deslocamento. A comunicação entre o dispositivo e o servidor será realizada por meio do protocolo MQTT, enquanto os dados coletados serão armazenados em um banco de dados relacional para posterior análise e visualização.

A estrutura metodológica seguirá os princípios fundamentais de um sistema IoT, sendo organizada de acordo com os quatro pilares que o sustentam: Percepção, Conectividade, Análise e Ação. Essa divisão permitirá compreender, de forma sistemática, como cada etapa contribui para o funcionamento e a segurança do sistema. Assim, as subseções seguintes detalharão o papel de cada pilar dentro do contexto do projeto, abordando desde a captação dos dados ambientais até os processos que asseguram a integridade, autenticidade e disponibilidade das informações monitoradas durante o transporte das vacinas.

O pilar da Percepção constitui a base fundamental do sistema IoT proposto, responsável por coletar, quantificar e pré-processar os dados provenientes do ambiente físico, transformando variáveis analógicas em informações digitais significativas que serão utilizadas nas etapas posteriores. No contexto deste trabalho, essa camada será responsável por monitorar temperatura, umidade e localização geográfica durante o transporte de vacinas, permitindo rastreabilidade contínua e avaliação das condições ambientais ao longo do deslocamento.

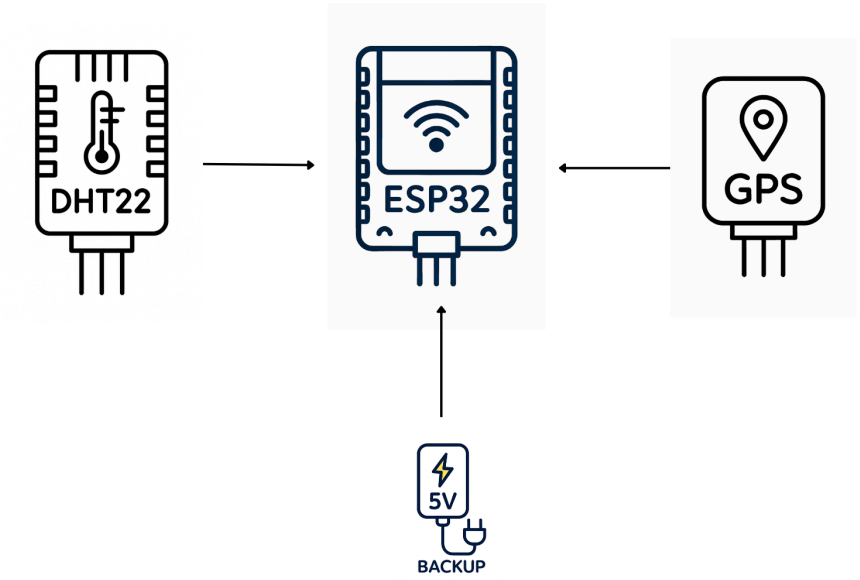
O sistema será implementado com base no microcontrolador ESP32, que foi selecionado por oferecer um conjunto robusto de recursos para aplicações IoT, como conectividade Wi-Fi e Bluetooth integradas, processador dual-core de 32 bits e suporte a múltiplas interfaces de comunicação digital. O ESP32 atuará como unidade central de aquisição e coordenação, gerenciando a leitura dos sensores, o pré-processamento dos dados e a transmissão ao servidor via MQTT.

Para o monitoramento ambiental, será utilizado o sensor DHT22, responsável por medir temperatura e umidade com resolução de 0,1°C e 0,1% de umidade relativa. A comunicação entre o DHT22 e o ESP32 ocorrerá por um barramento digital único, com taxa de amostragem entre 2 e 5 segundos.

Para rastreamento geográfico será utilizado o módulo GPS. Os dados de localização serão agregados às medições ambientais e estruturados em mensagens padronizadas, facilitando sua interoperabilidade com o broker MQTT e o banco de dados.

O sistema de alimentação utilizará redundância energética, combinando uma fonte regulada de 5 V e uma bateria, assegurando operação contínua durante interrupções externas, como mostrado na Figura 2. Essa redundância é essencial para sistemas críticos e contribui diretamente para disponibilidade, um dos requisitos centrais do monitoramento de vacinas.

Figura 2: Coleta de dados pelos sensores e GPS no dispositivo IoT



Fonte: O autor

O Pilar da Conectividade é responsável por garantir a transmissão confiável e segura dos dados coletados até a infraestrutura de processamento. Em sistemas sensíveis como o transporte de vacinas, a comunicação deve priorizar segurança, disponibilidade e tolerância a falhas.

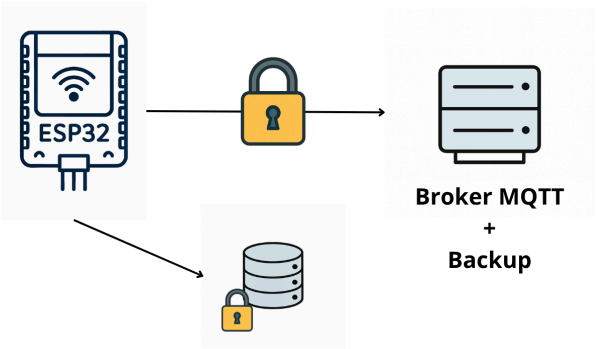
Neste projeto, a conectividade será implementada por meio do protocolo MQTT sobre TLS, assegurando confidencialidade, integridade e autenticação mútua entre o dispositivo e o servidor central. O MQTT, por ser leve e baseado no padrão publish/subscribe, é amplamente recomendado para IoT, especialmente em contextos com restrições de energia e banda.

O ESP32 atuará como cliente MQTT, publicando periodicamente mensagens em tópicos predefinidos. O broker, hospedado em servidor seguro, empregará autenticação baseada em certificados X.509, reforçando a proteção contra ataques de impersonação e interceptação.

Para aumentar a resiliência da comunicação, o sistema utilizará QoS 1, garantindo entrega ao menos uma vez, além de mecanismos automáticos de reconexão e failover para um broker secundário caso o principal se torne indisponível. Esses mecanismos atendem às recomendações para sistemas distribuídos tolerantes a falhas em ambientes IoT críticos.

Adicionalmente, mensagens transmitidas incluirão assinaturas HMAC-SHA256, timestamps e nonces, prevenindo ataques de repetição e adulteração. Em caso de perda temporária de conectividade, o ESP32 armazenará leituras em buffer local, retransmitindo-as assim que a conexão for reestabelecida, como mostrado na figura 3.

Figura 3: Transmissão segura das informações via MQTT com TLS



Fonte: O autor

O Pilar da Análise é responsável pelo processamento, validação, armazenamento e interpretação dos dados recebidos, transformando medições brutas em informações relevantes para auditoria, rastreabilidade e avaliação de conformidade, como mostrado na figura 4. Esse pilar garante que os dados de temperatura, umidade e localização sejam avaliados continuamente segundo normas sanitárias e diretrizes de transporte de insumos termossensíveis (ANVISA, 2020).

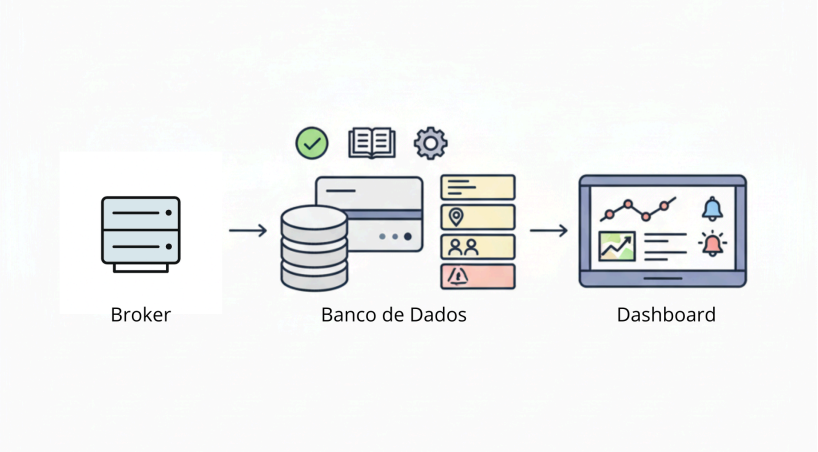
Os dados recebidos do broker MQTT serão encaminhados a um servidor de aplicação que realizará validação de integridade (HMAC/SHA256), registro de logs e persistência em banco de dados MySQL. A escolha do MySQL se justifica pela robustez, integridade transacional e aderência a ambientes industriais e acadêmicos.

O banco de dados será estruturado com tabelas específicas para leituras ambientais, localização, eventos, usuários e dispositivos IoT, permitindo rastreabilidade completa do histórico de transporte. Um módulo de auditoria registrará eventos críticos, como falhas de autenticação, desconexões inesperadas e variações abruptas de leitura, apoiando investigações forenses e atendendo às exigências de conformidade (ISO, 2022).

Uma interface de visualização (dashboard) permitirá acompanhamento em tempo real de dados ambientais e trajetos, além de emissão de alertas em caso de violações de parâmetros críticos. O dashboard implementará autenticação RBAC, assegurando níveis de acesso distintos conforme o perfil do usuário.

Para garantir continuidade operacional, serão implementadas rotinas automáticas de backup criptografado e replicação assíncrona para servidor secundário, alinhadas às recomendações de continuidade de negócios e recuperação de desastres descritas no NIST SP 800-34 (NIST, 2023).

Figura 4: Processamento e visualização dos dados no servidor e dashboard



Fonte: O autor

O Pilar da Ação abrange os mecanismos que garantem a continuidade do funcionamento seguro do sistema, a preservação do fluxo de dados e a supervisão operacional durante o transporte de vacinas. Embora o sistema não execute ações sobre o ambiente físico, este pilar assegura que o processo de monitoramento permaneça ativo mesmo sob condições adversas, preservando integridade e rastreabilidade.

Um dos elementos essenciais neste pilar é a redundância energética: o ESP32 realiza monitoramento contínuo da alimentação e, em caso de falha da fonte principal, migra automaticamente para a bateria sem interromper seu funcionamento. Essa estratégia segue boas práticas de resiliência operacional recomendadas pelo NIST (NIST, 2023).

Outro componente importante é o mecanismo de reconexão e sincronização. Quando ocorre perda momentânea de conectividade, o ESP32 registra leituras na memória não volátil (SPIFFS/EEPROM). Após o restabelecimento da conexão, as mensagens pendentes são retransmitidas com controle de integridade baseado em timestamps e identificadores únicos, evitando duplicações e garantindo ordenação, conforme diretrizes do NIST SP 800-183 (NIST, 2020).

O dashboard também desempenha papel relevante neste pilar, oferecendo supervisão, registro de incidentes, visualização de rotas e geração de relatórios. Esses elementos contribuem para rastreabilidade e conformidade com RDC nº 430/2020 e normas GDP de cadeia fria

As comunicações entre broker, servidor e dashboard utilizarão TLS 1.3, reforçando a segurança dos dados em trânsito. Além disso, mecanismos de backup criptografado, failover e verificação pós-recuperação garantirão integridade e continuidade mesmo em caso de falhas severas ou ataques de negação de serviço.

3. RESULTADOS ESPERADOS

A implementação do sistema IoT seguro para o transporte de vacinas deverá resultar em um protótipo funcional capaz de realizar medições contínuas de temperatura, umidade e localização durante o deslocamento, além de registrar eventos de confirmação de recebimento. Espera-se que o dispositivo baseado em ESP32 seja capaz de coletar esses dados de forma consistente e enviá-los periodicamente ao servidor utilizando o protocolo MQTT, permitindo o acompanhamento completo de cada viagem e a associação automática das leituras ao lote transportado.

Com a aplicação das medidas de segurança propostas, o sistema deverá demonstrar capacidade de proteger a confidencialidade e a integridade das informações transmitidas. O uso de MQTT sobre TLS com autenticação mútua, aliado a mecanismos como timestamp, nonce e assinaturas HMAC, deverá dificultar ataques de interceptação, adulteração de mensagens ou reutilização de pacotes. A autenticação forte no dashboard e o controle de acesso baseado em papéis deverão permitir que somente usuários autorizados consultem ou modifiquem informações, reduzindo a probabilidade de acessos indevidos. A criptografia de dados armazenados e as restrições no broker MQTT também deverão contribuir para uma redução mensurável dos riscos.

O sistema também deverá apresentar continuidade operacional adequada. Os mecanismos de failover do broker, juntamente com as rotinas de backup e recuperação, deverão permitir que o ambiente se restabeleça após falhas ou interrupções de serviços sem perda significativa de dados. A reconexão automática dos dispositivos e a redundância na alimentação do protótipo deverão contribuir para a manutenção do funcionamento mesmo em situações adversas.

Espera-se ainda que os testes realizados mostrem melhora concreta na segurança e na estabilidade do sistema após a implementação das medidas propostas. A comparação entre o ambiente inicial (sem proteção) e o ambiente final deverá evidenciar redução de falhas, menor exposição a ataques comuns, maior resiliência frente a indisponibilidades e diminuição de perdas ou inconsistências nas leituras coletadas.

O dashboard desenvolvido deverá permitir a visualização clara das leituras em tempo real e dos dados históricos, além de exibir alertas e eventos relevantes. A expectativa é que o painel ofereça usabilidade, organização e segurança adequadas para acompanhamento da operação, incluindo latência, uptime, perda de pacotes e demais indicadores relacionados ao transporte.

De forma geral, espera-se que o sistema demonstre a viabilidade técnica de integrar IoT, segurança da informação e rastreabilidade aplicada ao transporte de vacinas, apresentando dados completos, protegidos e acessíveis de maneira confiável durante todo o ciclo da operação.

4. CONSIDERAÇÕES FINAIS

O desenvolvimento realizado até esta etapa permitiu estabelecer a base conceitual, técnica e estrutural necessária para a construção de um sistema IoT seguro aplicado ao transporte de vacinas. Foram definidas a arquitetura geral, os requisitos de segurança, os mecanismos de proteção da comunicação e dos dados, além da modelagem do banco de dados e do fluxo operacional do sistema.

As análises e estudos conduzidos mostraram que a integração de sensores, protocolos seguros, autenticação robusta e mecanismos de continuidade é essencial para garantir confiabilidade em ambientes críticos como a cadeia de frio da saúde. Esta etapa consolidou o entendimento teórico e os fundamentos tecnológicos que nortearão as próximas fases de implementação e validação prática da solução.

Assim, o trabalho desenvolvido até aqui fornece um alicerce sólido para a continuidade do projeto, permitindo avançar com clareza e segurança para as etapas subsequentes.

REFERÊNCIAS

WORLD HEALTH ORGANIZATION (WHO). WHO‑IVB‑15.04. Disponível em: https://www.who.int/publications/i/item/WHO-IVB-15.04. Acesso em: 02 dez. 2025.

UNICEF. What cold chain. Disponível em: https://www.unicef.org/supply/what-cold-chain. Acesso em: 02 dez. 2025.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). Resolução de Diretoria Colegiada RDC n. 430, de 8 de outubro de 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-de-diretoria-colegiada-rdc-n-430-de-8-de-outubro-de-2020-282070593. Acesso em: 02 dez. 2025.

WORLD HEALTH ORGANIZATION (WHO). Publicação 9789240109544. Disponível em: https://www.who.int/publications/i/item/9789240109544. Acesso em: 02 dez. 2025.

STATISTA. IoT connected devices worldwide. Disponível em: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/. Acesso em: 02 dez. 2025.

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). Threat landscape. Disponível em: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape. Acesso em: 02 dez. 2025.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA / AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). Resolução de Diretoria Colegiada RDC n. 430, de 8 de outubro de 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-de-diretoria-colegiada-rdc-n-430-de-8-de-outubro-de-2020-282070593. Acesso em: 02 dez. 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). ISO/IEC 27001. Disponível em: https://www.iso.org/standard/27001. Acesso em: 02 dez. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). NIST Privacy Framework; NIST SP 800‑34. Disponível em: https://www.nist.gov/privacy-framework/nist-sp-800-34. Acesso em: 02 dez. 2025.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). SP 800‑183 (final). Disponível em: https://csrc.nist.gov/pubs/sp/800/183/final. Acesso em: 02 dez. 2025.