



IoT avançada na cadeia de valor agroalimentar

Capacitação para PME portuguesas do setor agroalimentar

Julho/2026

Sobre esta publicação

Um guia de decisão para usar dados de dispositivos conectados no reforço da rastreabilidade, da gestão da qualidade, da conservação e do desempenho operacional ao longo da cadeia agroalimentar.

Finalidade

Esta publicação apoia empresários, gestores e técnicos de pequenas e médias empresas na conceção, contratação, implementação e melhoria de soluções de Internet das Coisas. A tecnologia é tratada como parte de um sistema de trabalho: é suscetível de criar valor de forma consistente quando os dados são fiáveis, compreendidos e associados a decisões, responsabilidades e evidências.

O guia combina fundamentos técnicos, critérios de seleção, modelos de processo e instrumentos de verificação. Não substitui a avaliação de perigos, os programas de pré-requisitos, o plano HACCP, a validação de processos, a legislação aplicável ao produto ou o aconselhamento especializado. Os Princípios Gerais de Higiene Alimentar do Codex constituem uma referência enquadadora para a abordagem preventiva ^[4].

Âmbito

- dispositivos conectados, sensores, atuadores, gateways e computação periférica;
- identificação, eventos de rastreabilidade e integração entre sistemas;
- monitorização em tempo real, alertas, controlo de qualidade e conservação;
- logística inteligente, governação de dados, cibersegurança e adoção pelas PME.

Princípio editorial

As recomendações são tecnicamente neutras. Protocolos, produtos e arquiteturas devem ser escolhidos a partir dos requisitos do processo, do risco, do ambiente de utilização e da capacidade de manutenção.

Critérios de utilização responsável

Digitalizar não transfere a responsabilidade sobre a segurança dos alimentos, a conformidade, a qualidade nem a continuidade operacional.

Leitura técnica e regulamentar

Nos termos do artigo 18.º do Regulamento (CE) n.º 178/2002, os operadores devem dispor de sistemas e procedimentos que permitam identificar, pelo menos, os fornecedores e os operadores a quem forneceram os produtos abrangidos, facultando essa informação às autoridades competentes, a pedido ^[25]. Os registos IoT podem apoiar a organização, consulta e robustez desta evidência, mas não substituem a obrigação legal, a avaliação do produto nem os procedimentos de segurança alimentar.

Os requisitos de higiene e segurança aplicáveis dependem do setor, do produto, da atividade e do mercado. Os Regulamentos (CE) n.º 852/2004 e n.º 853/2004, quando aplicável, devem ser lidos em conjunto com a legislação setorial, as orientações das autoridades competentes e o sistema de segurança alimentar da organização ^{[26] [27]}.

Limites e validação

- um sensor não demonstra, por si só, que um produto é seguro ou conforme;
- um alerta é uma indicação para avaliar; a decisão exige critérios previamente aprovados;
- a ausência de dados pode resultar de uma falha de comunicação e não de condições estáveis;
- os valores-limite devem provir do processo validado, da especificação ou do requisito legal aplicável;
- qualquer automatização com impacto no produto deve admitir supervisão e tratamento de exceções.

Data de fecho editorial

A legislação e as referências foram verificadas para esta edição em julho de 2026. Antes de contratar ou implementar, confirme a versão em vigor e a aplicabilidade ao caso concreto.

Como utilizar o guia

A sequência dos módulos acompanha a passagem do problema operacional para uma solução implementada e controlada.

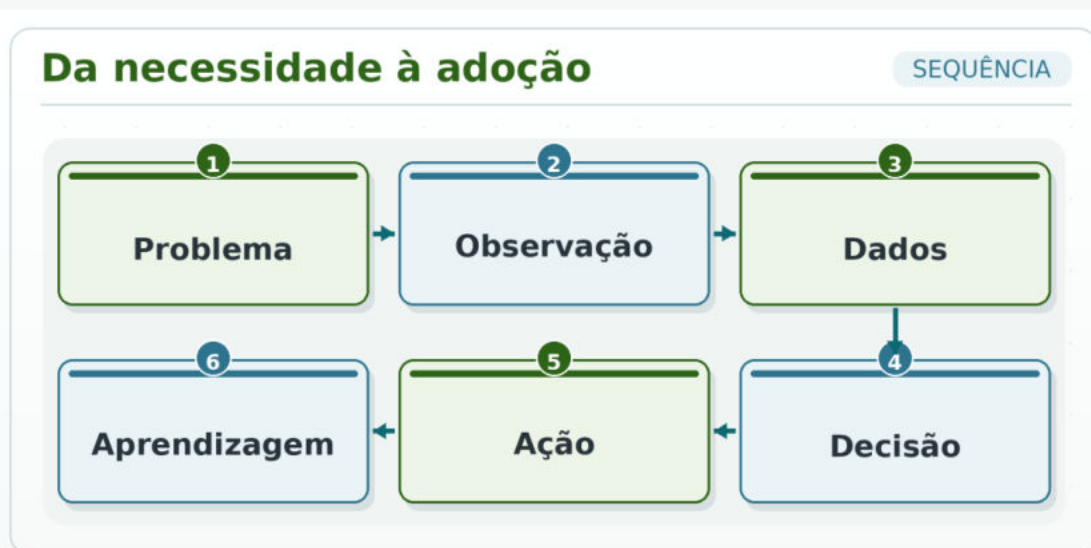


Figura 1 - Percurso de leitura e de decisão recomendado.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Percurso principal

Comece pelo processo e pelo evento que precisa de conhecer. Em seguida, defina a variável, a identificação ou o estado a observar; escolha a forma de recolha; estabeleça o percurso do dado; relacione-o com uma decisão; e determine quem responde. Esta ordem reduz compras prematuras e integrações frágeis.

1. Compreender a cadeia, os atores e os resultados pretendidos.
2. Selecionar dispositivos, sensores, identificação e conectividade.
3. Estruturar dados, interfaces, interoperabilidade e segurança.
4. Automatizar eventos de rastreabilidade e evidências de qualidade.
5. Controlar conservação, armazenamento, transporte e expedição.
6. Converter dados em alertas, fluxos de trabalho e indicadores.
7. Preparar requisitos, piloto, contratação, adoção e expansão.

Elementos recorrentes

- diagramas para compreender sistemas e processos;
- quadros de decisão para comparar alternativas;
- caixas técnicas para riscos, dependências e critérios;
- cenários ilustrativos para ligar conceitos sem atribuir resultados reais;
- listas de verificação para preparar a aplicação na empresa.

Percursos de leitura por responsabilidade

Nem todos os leitores necessitam do mesmo nível de pormenor. Os percursos seguintes ajudam a localizar as decisões mais relevantes.

Responsabilidade	Questões prioritárias	Módulos
Administração / gerência	valor, risco, investimento, dependências, escala	1 · 6 · 7
Qualidade e segurança alimentar	evidência, desvios, rastreabilidade, calibração	2 · 4 · 5 · 6
Produção e manutenção	instalação, fiabilidade, integração, atuação	2 · 3 · 6
Logística e armazém	identificação, estado, conservação, incidentes	4 · 5 · 6
Informática / fornecedor tecnológico	arquitetura, interfaces, segurança, operação	2 · 3 · 6 · 7
Compras e projeto	requisitos, contratação, aceitação, ciclo de vida	3 · 7

Tabela 1 – Percorso de leitura por responsabilidade.

Regra de leitura cruzada

Uma decisão técnica deve ser verificada por, pelo menos, três perspetivas: adequação ao processo, qualidade da evidência e capacidade de operação. Por exemplo, uma tecnologia de

comunicação pode cumprir a cobertura prevista, mas ser inadequada se não houver procedimento para detetar mensagens em falta ou se o fornecedor impedir a exportação dos dados.

Reunião recomendada

Use os quadros do guia numa sessão conjunta entre operação, qualidade, informática, manutenção e gestão. As divergências detetadas antes da compra são geralmente mais fáceis de resolver.

Mapa do guia

Sete módulos ligam tecnologia, dados, processo e capacidade organizacional.



Figura 2 - Mapa pedagógico do guia e relações entre módulos.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Lógica de progressão

Os módulos 1 e 2 estabelecem o problema e a camada física. O módulo 3 assegura que os dados podem circular com significado e proteção. Os módulos 4 e 5 aplicam essa base à rastreabilidade, qualidade, logística e conservação. O módulo 6 organiza a resposta em tempo útil. O módulo 7 transforma a arquitetura em projeto, contrato e adoção sustentável.

Dependência essencial

A qualidade e a credibilidade do resultado ficam limitadas pela qualidade combinada da medição, da identificação, do contexto, da integração e da resposta operacional.

NAVEGAÇÃO

Índice

Sobre esta publicação	2
Finalidade	2
Âmbito.....	2
Critérios de utilização responsável	3
Leitura técnica e regulamentar	3
Limites e validação	3
Como utilizar o guia	4
Percurso principal	4
Elementos recorrentes.....	5
Percursos de leitura por responsabilidade	5
Regra de leitura cruzada	5
Mapa do guia	6
Lógica de progressão.....	6
Módulo 1 - IoT ao longo da cadeia agroalimentar	20
1.1 Da conectividade à capacidade operacional.....	21
O que torna uma solução «IoT».....	21
Cinco perguntas de partida	21
1.2 Do dispositivo ao valor para a empresa.....	22
Uma cadeia com seis elos	22
Critérios por elo	22
1.3 Atores, objetos e eventos da cadeia	23
Três classes de elementos.....	23
Mapear antes de instrumentar	23

1.4 Casos de utilização com valor verificável	24
Formulação recomendada	25
Priorização.....	25
1.5 Maturidade e condições de prontidão	26
Níveis acumulativos	26
Sinais de prontidão	26
1.6 Cenário ilustrativo — receção conectada	27
Situação.....	27
Desenho do caso.....	27
Aprendizagem	27
1.7 Síntese e decisões do módulo	28
Saída para o módulo seguinte.....	28
Módulo 2 - Dispositivos, sensores e conectividade	30
2.1 Componentes e fronteiras do sistema	31
Camada física.....	31
Fronteiras que devem constar do projeto.....	31
2.2 Da variável ao requisito de medição	32
Especificação mínima	32
Adequação ao uso.....	33
2.3 Famílias de sensores e identificação	33
Três distinções	34
Identificação automática	34
2.4 Edge, gateways e atuação	34
Funções adequadas à periferia.....	35
Atuadores e comandos	35
2.5 Selecionar conectividade	35
Tecnologias e papéis.....	36

Critérios de decisão.....	36
2.6 Instalação, cobertura e continuidade.....	37
Plano de implementação:	37
Condições agroalimentares	37
2.7 Fiabilidade, verificação e calibração.....	38
Controlos complementares.....	39
Da falha do sensor ao produto	39
2.8 Cenário ilustrativo — câmara de conservação.....	39
Decisões de desenho	39
Teste de aceitação	40
Resultado esperado	40
2.9 Lista de verificação técnica.....	40
Saída para o módulo seguinte.....	40
Módulo 3 - Dados, integração e interoperabilidade	42
3.1 Do dispositivo aos sistemas de negócio	43
Camadas com contratos explícitos.....	43
Perguntas por fronteira.....	43
3.2 Arquitetura modular e desacoplada.....	44
Princípios de desenho	44
Tempo real como requisito graduado	44
3.3 Protocolos, interfaces e modelos de dados	45
Papéis diferentes	46
Conteúdo do contrato de dados.....	46
3.4 Integração com ERP, MES, WMS, QMS e manutenção.....	46
Escolher o sistema de registo.....	47
Integração por eventos	47
3.5 Identidade, contexto e qualidade dos dados	47

Dimensões essenciais	48
Controlos no percurso.....	48
3.6 Governação, responsabilidade e direitos de acesso	49
Decisões de governação	49
Regulamento dos Dados	49
3.7 Cibersegurança, continuidade e ciclo de vida	50
Capacidades de base.....	50
Aplicabilidade legal.....	51
3.8 Cenário ilustrativo — integração de eventos	51
Fluxo proposto	51
Exceções previstas	52
Critério de sucesso	52
3.9 Lista de verificação de interoperabilidade.....	52
Saída para o módulo seguinte.....	52
Módulo 4 - Rastreabilidade automatizada e controlo da qualidade	54
4.1 Unidade rastreável, lote, local e ator.....	55
Entidades fundamentais	55
Atributos mínimos controlados.....	55
4.2 Eventos críticos e pontos de captura	56
Eventos frequentes	56
Ponto crítico de captura.....	57
4.3 Captura automática com controlo de exceções	57
Controlos no ponto de captura	57
Supervisão humana no circuito	58
4.4 Ligar medição, especificação e decisão	58
Contexto antes de cálculo	59
4.5 Desvios, alertas e evidência	59

Fluxo controlado	59
Qualidade da trilha de auditoria.....	60
4.6 Rastreabilidade de extremo a extremo	60
Teste de rastreabilidade.....	61
Critérios a observar	61
4.7 Investigação, retirada e comunicação	61
Preparação	61
Contribuição dos dados IoT.....	62
4.8 Cenário ilustrativo — transformação de lotes	62
Modelo	62
Ensaio	62
Aprendizagem	63
4.9 Lista de verificação de rastreabilidade	64
Saída para o módulo seguinte.....	64
Módulo 5- Logística inteligente e conservação	65
5.1 Observar armazenamento e transporte	66
Quatro dimensões	66
Continuidade entre organizações	66
5.2 Cadeia de frio: medir e interpretar	67
O que o sensor representa	67
Interpretação de uma excursão.....	68
5.3 Localização, estado e integridade.....	68
Precisão adequada.....	69
Integridade e cadeia de custódia.....	69
5.4 Alertas e gestão de incidentes logísticos.....	70
Desenho do escalamento.....	70
Evitar fadiga de alarmes.....	70

5.5 Integrar inventário, expedição e transporte	71
Estados coerentes.....	71
Eventos de ligação	71
5.6 Conservação, perdas e eficiência	72
Hipóteses que podem ser testadas	72
Método de avaliação.....	72
5.7 Qualidade de serviço e gestão de parceiros.....	74
Partilha de dados	74
Evidência de serviço.....	74
5.8 Cenário ilustrativo — distribuição refrigerada	75
Preparação	75
Durante e após o percurso	75
Critérios de aceitação	75
5.9 Lista de verificação logística	76
Saída para o módulo seguinte.....	76
Módulo 6 - Monitorização em tempo útil, automatização e decisão	77
6.1 Painéis orientados à ação	78
Três níveis.....	78
Princípios de experiência de utilização	78
6.2 Regras, limiares e qualidade do alerta	79
Componentes da regra	79
Tipos de regra	79
6.3 Fluxos de trabalho e resposta fechada	80
Elementos do fluxo	80
Integração com trabalho existente	81
6.4 Graduação da automatização.....	81
Escada de autonomia.....	81
	13

Condições para subir.....	82
6.5 Análise de dados e apoio à decisão	82
Do descritivo ao prescritivo.....	82
Validação	82
6.6 Indicadores e revisão de desempenho	83
Três famílias.....	84
Ficha de indicador	84
6.7 Cenário e síntese — alerta com ação	85
Configuração ilustrativa	85
Lista de decisão	85
Saída para o módulo seguinte.....	85
Módulo 7 - Adoção pelas PME: do requisito à expansão.....	87
7.1 Necessidade, alternativa e prontidão	88
Diagnóstico inicial.....	88
Escolher o primeiro caso	88
7.2 Requisitos funcionais e técnicos.....	89
Forma verificável	89
Matriz de rastreabilidade de requisitos	89
7.3 Avaliar propostas e contratar	90
Diligência técnica.....	90
Cláusulas que protegem a continuidade	90
7.4 Desenhar um piloto que produza evidência	91
Protocolo do piloto	91
Representatividade.....	92
7.5 Aceitação, indicadores e decisão.....	92
Regra de decisão.....	92
Custo total	93
	14

7.6 Implementação e mudança organizacional.....	93
Plano de transição	93
Competências internas mínimas	93
Adoção	94
7.7 Riscos, dependências e expansão.....	94
Riscos a acompanhar	94
Padrão de escala	95
7.8 Cenário ilustrativo — piloto numa PME.....	95
Preparação	95
Execução	95
Decisão	95
7.9 Roteiro e lista final de adoção	96
Princípio de fecho	97
Lista consolidada de adoção	98
Processo e valor	98
Medição e dispositivo	98
Dados e integração	98
Operação e segurança	98
Fornecedor e ciclo de vida.....	98
Glossário A–C.....	100
Glossário D–I	101
Siglas e acrónimos.....	103
Bibliografia.....	105
Ficha técnica.....	109

Índice de Figuras

Figura 1 - Percorso de leitura e de decisão recomendado.	4
Figura 2 - Mapa pedagógico do guia e relações entre módulos.	6
Figura 3 - Do sinal à decisão: síntese editorial do guia.	22
Figura 4 - Atores, objetos e eventos que estruturam uma cadeia de valor conectada.	23
Figura 5 - Escada de maturidade para utilização de dados IoT.	26
Figura 6 - Componentes funcionais de uma solução IoT agroalimentar.	31
Figura 7 - Distribuição de funções entre dispositivo, edge, plataforma e operação.	34
Figura 8 - Perfis típicos de tecnologias de conectividade; a adequação deve ser validada no local.	36
Figura 9 - Controlos que contribuem para a fiabilidade da medição e do dado ao longo do ciclo de vida.	38
Figura 10 - Arquitetura em camadas do dispositivo ao processo empresarial.	43
Figura 11 - Camadas de interoperabilidade: transporte, estrutura, significado e operação.	45
Figura 12 - Dimensões da qualidade de dados avaliadas em relação ao uso.	48
Figura 13 - Papéis mínimos de governação, responsabilidade e acesso aos dados.	49
Figura 14 - Cinco dimensões de um evento EPCIS e informação complementar de responsabilidade operacional.	56
Figura 15 - Da captura automática à evidência aceite.	57
Figura 16 - Ciclo de tratamento de um desvio suportado por dados IoT.	59
Figura 17 - Relações de rastreabilidade através de receção, transformação, agregação e expedição.	60
Figura 18 - Dimensões de visibilidade na logística agroalimentar.	66
Figura 19 - Relação entre equipamento, ar, superfície, embalagem e produto.	67
Figura 20 - Fluxo de resposta a uma ocorrência logística conectada.	70
Figura 21 - Fluxo integrado entre armazém, expedição, transporte e receção.	71
Figura 22 - Hierarquia de informação de um painel operacional.	78
Figura 23 - Fluxo fechado entre deteção, decisão, execução e aprendizagem.	80
Figura 24 - Níveis de automatização e condições de passagem.	81
Figura 25 - Árvore de indicadores técnicos, operacionais e de resultado.	84
Figura 26 - Matriz de prontidão: importância do caso e capacidade de execução.	88
Figura 27 - Dimensões de avaliação de uma proposta IoT.	90

Figura 28 - Etapas e portas de decisão de um piloto IoT.	91
Figura 29 - Mapa de dependências a rever antes da expansão.	94
Figura 30 - Roteiro de adoção da necessidade à melhoria contínua.	96

Índice de Ilustrações

Ilustração 1 - Imagem de abertura - contexto do módulo 1: decisão e aplicação.	20
Ilustração 2 - Receção conectada de matéria-prima: associação entre fornecedor, lote, doca, operador e evidência de verificação operacional.	25
Ilustração 3 - Continuidade entre observação no campo e receção ou transformação agroalimentar.....	28
Ilustração 4 - Imagem de abertura - contexto do módulo 2: dispositivos, sensores e conectividade.	30
Ilustração 5 - Instalação representativa de sensores e gateway em ambiente protegido; a cobertura deve ser ensaiada no local.	38
Ilustração 6 - Imagem de abertura - contexto do módulo 3: dados, integração e segurança. ..	42
Ilustração 7 - Imagem editorial — Processamento periférico e integração: o percurso do dado liga a operação local aos sistemas autorizados.	45
Ilustração 8 - Imagem de abertura - contexto do módulo 4: rastreabilidade e qualidade.	54
Ilustração 9 - Rasto digital de um lote entre transformação, embalagem e expedição.....	63
Ilustração 10 - Imagem de abertura - contexto do módulo 5: logística, conservação e transporte.	65
Ilustração 11 - Continuidade da monitorização entre palete, cais e transporte refrigerado. ...	69
Ilustração 12 - Verificação de um dispositivo de monitorização numa operação refrigerada. A imagem ilustra o contexto; não define o ponto de medição nem substitui a validação da instalação.	73
Ilustração 13 - Imagem de abertura — contexto do módulo 6: alertas, fluxos de trabalho e indicadores.....	77
Ilustração 14 - Análise conjunta de dados por produção, qualidade e manutenção, com supervisão humana e decisão documentada.	83
Ilustração 15 – Resposta coordenada a um alerta, com verificação física e fecho documentado.	86
Ilustração 16 - Imagem de abertura — contexto do módulo 7: requisitos, piloto e adoção.	87
Ilustração 17 - Desenho de um piloto com representação digital da linha e pontos de decisão.	96

Índice de Tabelas

Tabela 1 – Percurso de leitura por responsabilidade.	5
Tabela 2 - Casos de utilização e evidência de valor.	24
Tabela 3 - Perguntas para definir o requisito de medição.	32
Tabela 4 - Variáveis observáveis, aplicações e pontos críticos de instalação.	34
Tabela 5 – Sistemas de registo, contexto fornecido e informação recebida.	47
Tabela 6 - Elementos de controlo para ligar medição, especificação e decisão.	59
Tabela 7 - Necessidades de localização, tecnologias possíveis e limites operacionais.	68
Tabela 8 - Evidência de serviço e questões contratuais por objeto.	74
Tabela 9 - Estados do dado e comportamento recomendado.	79
Tabela 10 – Indicadores de desempenho e perguntas de gestão.	84
Tabela 11 – Classes de requisitos e conteúdo mínimo.	89
Tabela 12 - Matriz de avaliação de soluções IoT na cadeia agroalimentar.	92

Módulo 1 - IoT ao longo da cadeia agroalimentar

Compreender onde a IoT cria informação útil, como essa informação atravessa a cadeia e que condições devem existir antes de investir.

RESULTADOS DE APRENDIZAGEM

- distinguir dispositivo, dado, informação, decisão e valor;
- mapear atores, objetos, locais e eventos relevantes;
- selecionar casos de utilização a partir do problema operacional;
- avaliar a maturidade e as dependências da organização.



Ilustração 1 - Imagem de abertura - contexto do módulo 1: decisão e aplicação.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 1 · DECISÃO E APLICAÇÃO

1.1 Da conectividade à capacidade operacional

A Internet das Coisas é uma arquitetura sociotécnica: liga objetos e ambientes ao sistema de decisão da empresa.

O que torna uma solução «IoT»

Um sistema IoT observa ou identifica uma entidade física, transmite dados, conserva o contexto necessário e disponibiliza a informação a uma aplicação ou processo; pode ainda emitir comandos para um atuador. A Recommendation ITU-T Y.4000/Y.2060 enquadra a Internet das Coisas como ligação entre entidades físicas, redes, aplicações e processos, evitando que a solução seja reduzida ao sensor ^[14].

Na cadeia agroalimentar, a entidade observada pode ser um lote, uma palete, um equipamento, uma câmara, um veículo, uma matéria-prima ou uma condição ambiental. Para apoiar uma decisão operacional, o dado deve estar ligado a identidade, tempo, local, estado, contexto e responsabilidade definidos.

Cinco perguntas de partida

- Que decisão não pode hoje ser tomada com confiança ou em tempo útil?
- Que objeto, evento ou condição precisa de ser conhecido?
- Que evidência é necessária e durante quanto tempo deve ser conservada?
- Que pessoa ou sistema deve agir quando o estado se altera?
- Como será detetada uma falha do próprio sistema de monitorização?

Erro recorrente

Começar pela lista de dispositivos disponíveis tende a produzir dados sem finalidade definida. O ponto de partida é o processo e a decisão.

MÓDULO 1 · DECISÃO E APLICAÇÃO

1.2 Do dispositivo ao valor para a empresa

Entre medir e criar valor existem várias transformações, cada uma com critérios e responsáveis.



Figura 3 - Do sinal à decisão: síntese editorial do guia.

Fonte: elaboração própria, com base nas normas GS1 de rastreabilidade e eventos de visibilidade [9] [10].

Uma cadeia com seis elos

O dispositivo produz uma observação ou leitura. A comunicação transporta-a. A plataforma valida, contextualiza e conserva. A aplicação apresenta ou combina a informação. Uma regra ou uma pessoa toma a decisão. A operação executa e regista a resposta. Se um elo estiver ausente, a monitorização pode ser visualmente convincente e operacionalmente ineficaz.

Critérios por elo

- medição: adequação, instalação, incerteza e estado de calibração;
- contexto: identidade, tempo, local, unidade, lote e estado;
- transporte: cobertura, disponibilidade, segurança e deteção de perdas;
- interpretação: regra aprovada, dados suficientes e exceções conhecidas;
- resposta: responsável, prazo, autoridade e registo de fecho;
- valor: efeito verificável no risco, qualidade, tempo, perdas ou serviço.

1.3 Atores, objetos e eventos da cadeia

A cadeia digital deve representar a cadeia física sem apagar transformações, agregações, divisões ou mudanças de custódia.



Figura 4 - Atores, objetos e eventos que estruturam uma cadeia de valor conectada.

Fonte: elaboração própria com base nos conceitos da GS1 de rastreabilidade e eventos de visibilidade [9] [10].

Três classes de elementos

- atores: produtores, transformadores, armazenistas, transportadores, distribuidores, laboratórios, clientes e autoridades;
- objetos: unidades logísticas, lotes, matérias-primas, embalagens, equipamentos, locais e documentos;
- acontecimentos empresariais a representar: receção, transformação, agregação, expedição, transferência, inspeção, medição, bloqueio e libertação. Estes exemplos não correspondem, por si só, às classes formais de evento EPCIS.

Mapear antes de instrumentar

O mapa deve mostrar quem cria a identificação, quem a lê, quando muda a relação entre unidades e que sistema conserva a ligação. Uma medição de temperatura sem referência ao contentor ou lote pode ser útil para manutenção ambiental, mas insuficiente para demonstrar o percurso de um produto.

Questão de controlo

Se uma unidade for dividida, reembalada ou combinada, o sistema consegue preservar a relação entre entradas e saídas?

1.4 Casos de utilização com valor verificável

Um caso de utilização descreve uma mudança operacional concreta, não uma funcionalidade isolada.

Necessidade	Observação / evento	Resposta possível	Evidência de valor
rastrear um lote	identificação e movimentos	localizar, bloquear, retirar	tempo, completude e precisão da reconstrução, com âmbito delimitado
proteger conservação	condição e duração	avaliar, corrigir, segregar	percentagem de ocorrências detetadas, avaliadas e fechadas dentro do prazo, e completude dos registos
reduzir paragens	estado e comportamento do ativo	inspecionar, planear intervenção	disponibilidade, horas de paragem não planeada, tempo médio de reparação e intervenções planeadas
controlar expedição	identidade, destino, condição	validar carga e documentação	taxa de erros e exceções detetados e corrigidos antes da expedição, e reconciliações pendentes
melhorar processo	variáveis e sequência	ajustar parâmetros autorizados	estabilidade, conformidade, desperdício e retrabalho, comparados com uma linha de base

Tabela 2 - Casos de utilização e evidência de valor.

Formulação recomendada

Descreva o caso com a estrutura: «quando ocorrer ou for observado X, o responsável Y deve poder decidir Z, usando a evidência E e respeitando a restrição R». Esta frase obriga a explicitar o gatilho, o utilizador, a decisão, a prova e o limite.

Priorização

- relevância para segurança, qualidade ou compromisso comercial;
- frequência e consequência do problema;
- capacidade de intervir após receber a informação;
- viabilidade de medir e contextualizar com confiança; possibilidade de confirmar o benefício sem depender de suposições.

Do lote ao dado operacional

A utilidade resulta da ligação entre identidade, medição, contexto e decisão.



Ilustração 2 - Receção conectada de matéria-prima: associação entre fornecedor, lote, doca, operador e evidência de verificação operacional.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 1 · DECISÃO E APLICAÇÃO

1.5 Maturidade e condições de prontidão

A sofisticação tecnológica deve acompanhar a capacidade de definir, operar e melhorar o processo.

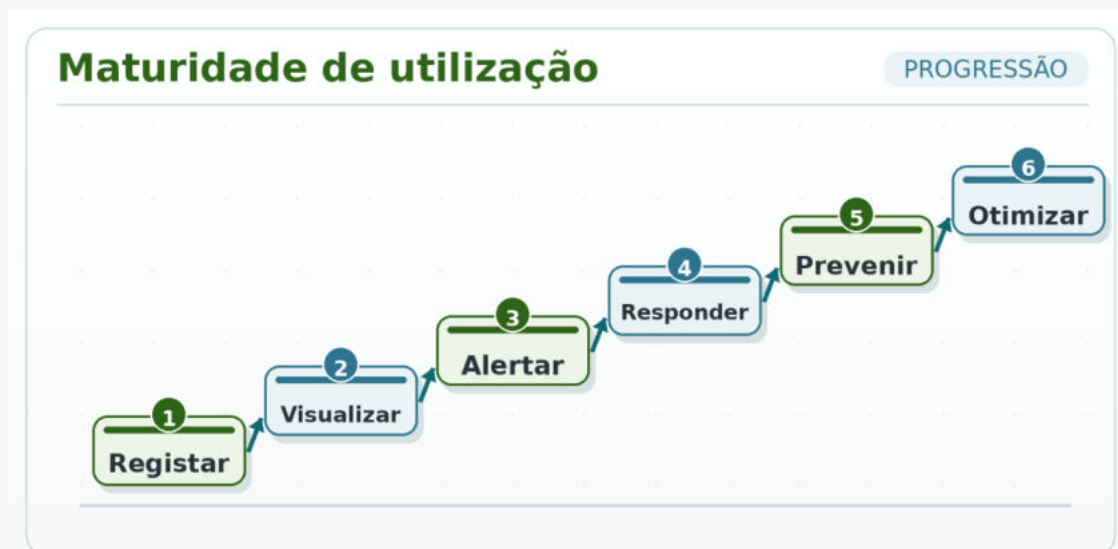


Figura 5 - Escada de maturidade para utilização de dados IoT.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Níveis acumulativos

Neste modelo, os níveis são acumulativos: registrar digitalmente não equivale a monitorizar; monitorizar não equivale a responder; responder não equivale a prevenir. Cada nível pressupõe capacidades dos anteriores. Uma empresa pode ter maturidades diferentes por caso de utilização; por isso, a avaliação deve ser feita por caso e não apenas para a organização no seu conjunto.

Sinais de prontidão

- processo e responsabilidades descritos;
- identificadores e nomenclaturas controlados;
- critérios de aceitação e de desvio aprovados;
- equipamentos e infraestrutura com manutenção definida;
- acesso aos dados e às interfaces contratualmente assegurado;

- pessoas disponíveis para receber, avaliar e fechar ocorrências.

Limite prático

Se a organização não consegue decidir o que fazer perante um desvio confirmado, a automatização do alerta apenas acelera a chegada de um problema sem resposta.

1.6 Cenário ilustrativo — receção conectada

Uma PME transformadora pretende reduzir dúvidas na receção de matérias-primas refrigeradas e acelerar a decisão de aceitação.

Situação

A receção combina a identificação do fornecedor e do lote, a documentação, a inspeção visual e medições definidas pelo sistema de qualidade. Os dados estão dispersos entre papel, mensagens e aplicações. Quando surge uma dúvida posterior, a reconstrução é demorada.

Desenho do caso

1. Ler ou introduzir a identificação do lote e da unidade logística.
2. Associar a doca, o instante, o operador e o veículo ao evento de receção.
3. Recolher apenas as medições previstas no procedimento aprovado.
4. Validar unidade, plausibilidade, estado do instrumento e completude.
5. Apresentar a informação ao responsável pela decisão, sem substituir a inspeção.
6. Registar aceitação, retenção ou rejeição, respetivo fundamento e ações.

Aprendizagem

O valor não está na leitura automática isolada, mas na ligação entre identidade, evidência, decisão e registo. A solução deve continuar a funcionar através de um procedimento alternativo quando a rede ou a integração estiver indisponível.

Natureza do exemplo

Cenário pedagógico, sem empresa identificada nem resultados quantitativos atribuídos.

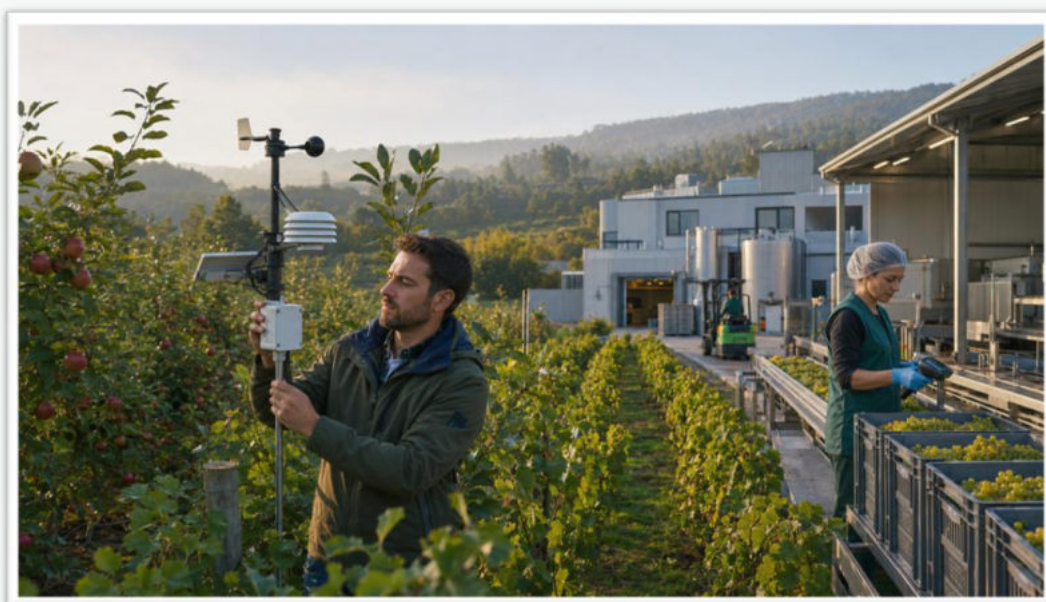


Ilustração 3 - Continuidade entre observação no campo e receção ou transformação agroalimentar.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

1.7 Síntese e decisões do módulo

Antes de selecionar tecnologia, a empresa deve conseguir responder de forma consistente às questões seguintes.

Saída para o módulo seguinte

A empresa deve terminar este módulo com um caso de utilização priorizado, um mapa simplificado do processo e uma primeira lista de requisitos de informação. O módulo 2 converte essa necessidade em escolhas de sensores, identificação, edge, gateways e conectividade.

- ☐ O problema operacional está descrito sem referência a uma marca ou equipamento?
- ☐ A entidade física, o evento e a variável a conhecer estão identificados?
- ☐ A decisão e o respetivo responsável estão definidos?
- ☐ Existe uma ação possível e proporcionada quando o estado se altera?
- ☐ Os critérios provêm de requisito legal, especificação, avaliação de risco ou processo validado?

- ☐ É possível relacionar cada dado com identidade, tempo, local e unidade?
- ☐ O modo degradado foi previsto para falha de energia, rede, dispositivo ou integração?
- ☐ O acesso, a exportação e a conservação dos dados podem ser contratados?
- ☐ O benefício pode ser verificado através de um indicador adequado?

Decisão de passagem

Não avance para a aquisição enquanto não estiver claro o que será observado, para que decisão, com que evidência e por quem.

Módulo 2 - Dispositivos, sensores e conectividade

Traduzir requisitos do processo em escolhas técnicas instaláveis, mantíveis e capazes de produzir dados fiáveis.

RESULTADOS DE APRENDIZAGEM

- reconhecer os componentes de uma solução conectada;
- seleccionar sensores e identificação segundo a finalidade;
- comparar conectividade sem confundir alcance com adequação;
- planear instalação, verificação, calibração e manutenção.



Ilustração 4 - Imagem de abertura - contexto do módulo 2: dispositivos, sensores e conectividade.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 2 · DECISÃO E APLICAÇÃO

2.1 Componentes e fronteiras do sistema

Uma solução robusta explicita o que pertence ao dispositivo, à rede, à plataforma, à aplicação e ao processo humano.

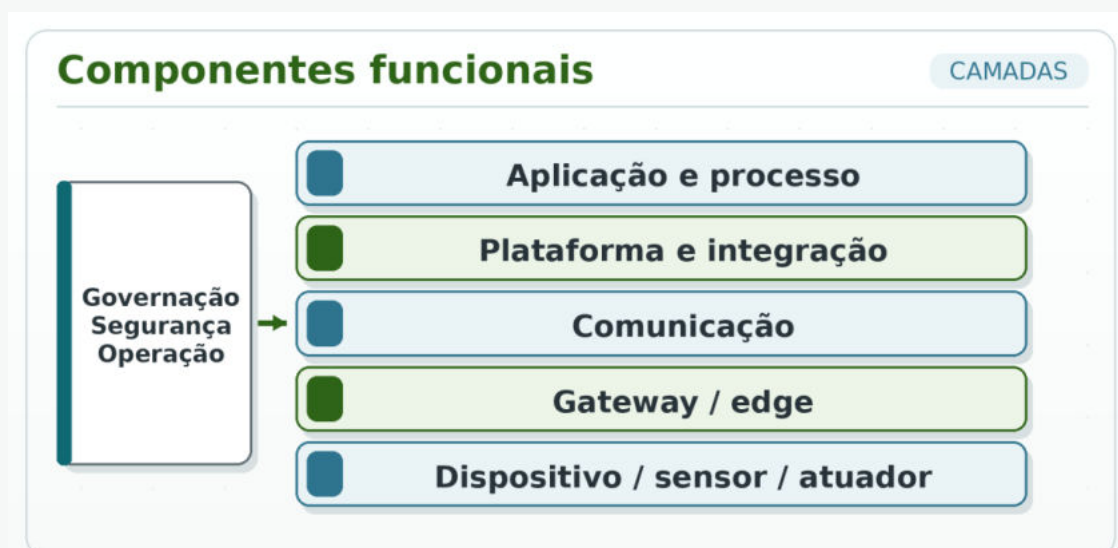


Figura 6 - Componentes funcionais de uma solução IoT agroalimentar.

Fonte: elaboração própria com base na Recommendation ITU-T Y.4000/Y.2060 ^[14].

Camada física

O elemento sensor converte uma grandeza física ou química num sinal. O dispositivo condiciona, processa e regista esse sinal; pode associar tempo, identidade e diagnóstico. Um gateway agrega dispositivos, converte protocolos ou mantém funções locais. A computação periférica pode executar regras junto do processo e reduzir a dependência de uma ligação externa, desde que as funções locais, o armazenamento e o modo degradado sejam projetados e ensaiados ^[20].

Fronteiras que devem constar do projeto

- responsável pelo dispositivo, firmware, credenciais e configuração;
- origem do relógio e comportamento quando perde sincronização;
- local de armazenamento temporário e política de reenvio;
- ponto em que termina a responsabilidade de cada fornecedor;

- interfaces entregues à empresa e formatos de exportação;
- processo de substituição, atualização e desativação segura.

Regra de arquitetura

Cada componente deve ter uma função clara e um mecanismo observável para indicar falha, degradação ou perda de comunicação.

2.2 Da variável ao requisito de medição

Selecionar um sensor começa por definir a grandeza, o local, o intervalo de utilização e a decisão associada.

Pergunta	Exemplo de resposta bem definida
O quê?	temperatura do ar no ponto representativo definido
Onde?	zona crítica identificada no estudo de distribuição
Quando?	durante armazenamento e abertura de porta
Para quê?	triagem e investigação de desvio
Com que prova?	registo, diagnóstico e estado de verificação

Tabela 3 - Perguntas para definir o requisito de medição.

Especificação mínima

- mensuranda: grandeza que se pretende medir;
- matriz ou ambiente: ar, produto, superfície, fluido, equipamento ou embalagem;
- intervalo de utilização e condições ambientais;
- exatidão, resolução, repetibilidade e tempo de resposta necessários;
- frequência de amostragem e latência admitida pela decisão;
- requisitos de higienização, contacto alimentar, proteção e montagem;
- método de verificação, calibração, substituição e rastreabilidade metrológica.

Adequação ao uso

A melhor exatidão declarada não garante a melhor medição no processo. A posição, a resposta térmica, a circulação de ar, a condensação, a sujidade, o contacto, a vibração e o método de fixação podem constituir contribuições relevantes para o erro e a incerteza de medição. O requisito deve ser suficientemente exigente para a decisão, mas compatível com manutenção e custo.

Quando a calibração externa for necessária, a empresa deve confirmar se o laboratório tem âmbito acreditado adequado à calibração em causa e se o método, a incerteza declarada e a adequação ao uso são compatíveis com a decisão. A ILAC P14 enquadra a declaração da incerteza de medição em calibração ^[12]; um certificado, por si só, não substitui essa análise.

2.3 Famílias de sensores e identificação

As tecnologias devem ser escolhidas pela grandeza e pelo evento; identificação e medição resolvem problemas diferentes.

Família	Aplicações possíveis	Cuidados principais
temperatura / humidade	câmaras, armazéns, transporte, processo	posição, resposta, condensação, deriva
pressão / caudal / nível	linhas, depósitos, utilidades	compatibilidade, obstrução, instalação
massa / força	silos, doseamento, inventário	estrutura, tara, vibração, calibração
gases e qualidade do ar	atmosferas, maturação, processo	seletividade, interferências, manutenção
pH / condutividade / grandezas químicas	processo e limpeza	matriz, sujidade, referência, frequência de calibração
vibração / corrente / estado	manutenção de ativos	linha de base, modo de funcionamento

Família	Aplicações possíveis	Cuidados principais
código de barras / RFID / NFC	identidade e eventos	portador, leitura, associação, unicidade

Tabela 4 - Variáveis observáveis, aplicações e pontos críticos de instalação.

Três distinções

- medição direta versus indicador indireto: a relação deve ser demonstrada;
- condição do ambiente versus condição do produto: não são automaticamente equivalentes;
- identidade lida versus identidade correta: a associação ao objeto precisa de controlo.

Identificação automática

Códigos óticos, RFID e NFC variam em distância, orientação, ambiente, custo e possibilidade de escrita. A escolha deve considerar o ponto de leitura, o material da embalagem, a presença de metal ou líquidos, a velocidade do processo e o procedimento para leituras duplicadas, ausentes ou indevidas.

2.4 Edge, gateways e atuação

Processar junto do processo pode preservar continuidade e tempo de resposta, mas aumenta a necessidade de gestão local.



Figura 7 - Distribuição de funções entre dispositivo, edge, plataforma e operação.

Fonte: elaboração própria com base no NIST SP 500-325 [20].

Funções adequadas à periferia

- filtrar ruído e validar formatos antes de transmitir;
- associar instante, identidade e estado do dispositivo;
- conservar dados durante indisponibilidade da rede;
- executar regras locais aprovadas quando a latência é crítica;
- interligar protocolos de equipamentos legados;
- expor diagnósticos de saúde e capacidade de armazenamento.

Atuadores e comandos

Um atuador altera o processo: válvula, relé, variador, sinalização ou mecanismo de separação. A autorização, os interbloqueios, o estado seguro e a confirmação do efeito devem ser definidos. Uma mensagem enviada não prova que a ação física ocorreu.

Quando a atuação pode afetar segurança, produto, equipamento ou pessoas, a lógica deve ser sujeita a análise de risco, teste, gestão de alterações e possibilidade de intervenção manual. O registo deve distinguir comando, receção, execução e resultado.

Pergunta crítica

Que decisão deve continuar localmente se a ligação à plataforma externa falhar?

2.5 Selecionar conectividade

Não existe uma tecnologia universal: alcance, energia, capacidade, ambiente, mobilidade e operação formam um compromisso.

Conectividade: perfis típicos, não garantias					
A adequação depende do ambiente, da implementação, do contrato e da operação.					
Tecnologia	Cobertura típica	Energia	Capacidade	Mobilidade	Condição crítica
Ethernet / industrial	local, cablada	alimentação	elevada	baixa	tempo previsível só com tecnologia própria
Wi-Fi	local	média	média-elevada	média	cobertura, canais e gestão
BLE	muito local	muito baixa	baixa-média	média	distância e perfil de aplicação
LoRaWAN	alargada	muito baixa	baixa	baixa	cobertura, duty cycle e operador
NB-IoT	rede alargada	baixa	baixa	baixa	rede e perfil do operador
LTE-M	rede alargada	baixa-média	média	média-elevada	rede, cobertura e mobilidade

Validar sempre no local: cobertura, latência, perdas, consumo, segurança e recuperação.

Figura 8 - Perfis típicos de tecnologias de conectividade; a adequação deve ser validada no local.

Fonte: elaboração própria com base em fontes institucionais sobre MQTT, OPC UA, LoRaWAN, Bluetooth LE, NB-IoT, LTE-M e TSN ^{[1] [2] [3] [11] [16] [22] [23]}.

Tecnologias e papéis

Ethernet cablada é adequada a instalações fixas que valorizem capacidade, estabilidade e gestão da infraestrutura. O comportamento determinístico não é uma propriedade de qualquer rede Ethernet: depende da tecnologia industrial adotada, da arquitetura, da configuração e dos mecanismos de tempo real. Redes industriais específicas podem oferecer tempos de comunicação limitados e previsíveis quando corretamente projetadas e validadas ^[11]. Wi-Fi oferece capacidade em áreas com infraestrutura gerida. Bluetooth Low Energy é comum em ligações de proximidade e dispositivos de baixo consumo ^[3]. LoRaWAN organiza redes de grande área e baixo débito para dispositivos alimentados por bateria ^[16]. NB-IoT e LTE-M devem ser avaliadas separadamente segundo cobertura, energia, capacidade e mobilidade disponibilizadas pela rede e pelo operador ^{[1] [2]}.

MQTT é um protocolo de mensagens publish/subscribe e não uma tecnologia de rádio ^[22]. RFID e NFC identificam ou trocam dados em interações de leitura; também não substituem, por si, uma rede contínua de telemetria.

CrITÉrios de decisão

- cobertura demonstrada no local e nos percursos reais;
- energia disponível e autonomia no perfil de utilização;

- volume, frequência, prioridade e tolerância a atrasos;
- mobilidade, roaming, interiores, metal, líquidos e obstáculos;
- gestão de credenciais, atualizações, operação e fornecedores;
- custo total: infraestrutura, serviço, instalação, apoio e substituição.

2.6 Instalação, cobertura e continuidade

A instalação transforma uma especificação em desempenho real; deve ser tratada como uma etapa de engenharia e aceitação.

Plano de implementação:

1. Confirmar pontos de medição, leitura, alimentação e montagem.
2. Realizar ensaios de cobertura nas condições e percursos representativos.
3. Definir identificação física, inventário e configuração de cada ativo.
4. Proteger cabos, caixas, antenas e interfaces contra ambiente e intervenção indevida.
5. Testar perda de ligação, energia, sincronização e recuperação.
6. Registrar o estado inicial e aceitar contra requisitos documentados.

Condições agroalimentares

Lavagem, condensação, poeiras, frio, calor, agentes químicos, pressão mecânica e higienização podem comprometer conectores, invólucros e adesivos. O grau de proteção declarado deve corresponder à montagem real; uma caixa adequada perde proteção se o prensa-cabos, a tampa ou a passagem não forem igualmente adequados.

A cobertura deve ser ensaiada com portas, produto, paletes, veículos e rotinas reais. Mapas teóricos ou ensaios num espaço vazio não demonstram o comportamento durante a operação.

Modo degradado

Defina como o dispositivo guarda dados, como sinaliza a falha, quando reenvia e como evita duplicação ou alteração da ordem dos eventos.

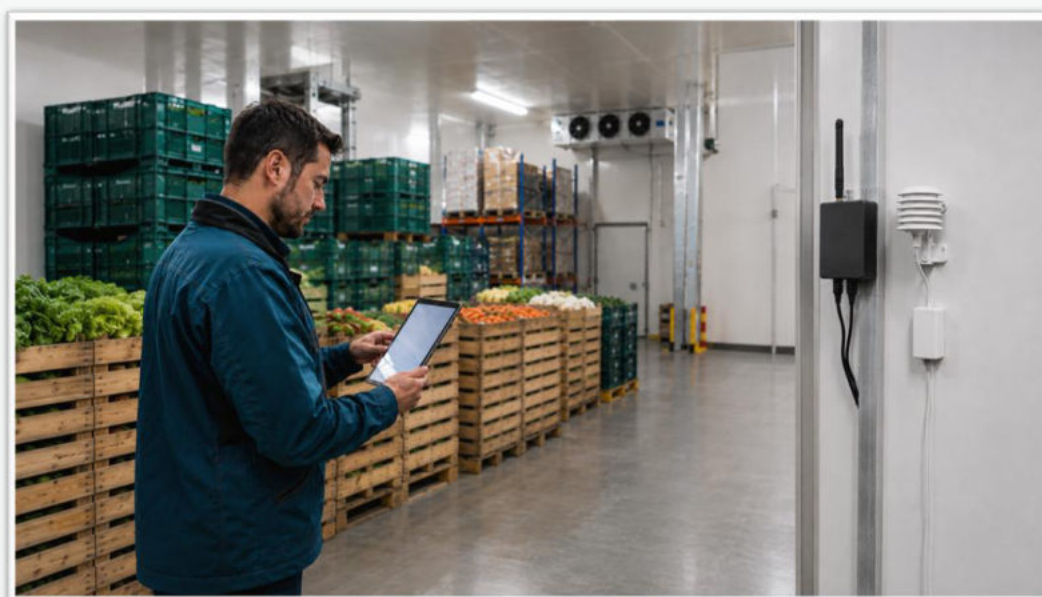


Ilustração 5 - Instalação representativa de sensores e gateway em ambiente protegido; a cobertura deve ser ensaiada no local.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

2.7 Fiabilidade, verificação e calibração

A confiança resulta de controlos ao longo do ciclo de vida e não apenas da especificação de compra.



Figura 9 - Controlos que contribuem para a fiabilidade da medição e do dado ao longo do ciclo de vida.

Fonte: elaboração própria; referência metrológica ao JCGM 200:2012 ^[15] e à ILAC P14 ^[12].

Controlos complementares

- verificação de receção e identificação do equipamento;
- instalação e comparação inicial em condições representativas;
- verificações intermédias com método e critérios definidos;
- calibração quando necessária à rastreabilidade metrológica;
- monitorização de deriva, dados constantes, saltos e valores impossíveis;
- gestão do impacto quando se deteta medição fora de critério.

Da falha do sensor ao produto

Quando um instrumento é considerado inadequado, a empresa deve avaliar o intervalo afetado, os lotes potencialmente relacionados, a existência de evidência alternativa e a necessidade de retenção ou investigação. Substituir o sensor resolve a causa técnica, mas não encerra automaticamente a avaliação do produto.

Distinção útil

Calibração — operação que, em condições especificadas, estabelece primeiro uma relação entre os valores e incertezas fornecidos por padrões e as indicações correspondentes do instrumento e usa depois essa informação para obter um resultado de medição a partir de uma indicação. Ajuste — conjunto de operações efetuadas num sistema de medição para que este forneça indicações prescritas. Verificação — apresentação de evidência objetiva de que requisitos especificados foram cumpridos. Os três conceitos não são equivalentes

[15].

2.8 Cenário ilustrativo — câmara de conservação

Uma PME pretende passar de verificações pontuais para monitorização contínua de uma câmara, mantendo o procedimento de qualidade.

Decisões de desenho

- o estudo do espaço define zonas e situações críticas, em vez de escolher posições por conveniência;

- os sensores são identificados, instalados e verificados no local;
- o intervalo de registo e o atraso de alerta decorrem do processo e da capacidade de resposta;
- o sistema distingue porta aberta, descongelação, manutenção e desvio não explicado;
- a plataforma mostra mensagens em falta e estado dos dispositivos;
- o procedimento descreve confirmação, avaliação de produto e encerramento.

Teste de aceitação

A equipa simula, de forma controlada, perda de comunicação, falta de energia, leitura fora de critério e restabelecimento. Confirma receção, escalamento, armazenamento local, sincronização, registo da ação e produção de evidência. O ensaio não deve comprometer produto nem equipamento.

Resultado esperado

A solução fornece maior continuidade de observação e melhor contexto para a decisão. Não se presume uma equivalência automática entre ar e produto, nem se eliminam inspeções definidas pelo sistema de segurança alimentar.

Natureza do exemplo

Cenário pedagógico, sem resultados quantitativos nem limiares universais.

2.9 Lista de verificação técnica

Utilize esta lista antes da encomenda, na instalação e na aceitação.

Saída para o módulo seguinte

Com a camada física definida, é necessário garantir que sistemas diferentes trocam dados com estrutura, significado, identidade e proteção. O módulo 3 apresenta a arquitetura de integração e a governação necessária.

☐ A mensuranda, o local, o intervalo e a finalidade estão documentados?

☐ A adequação ao ambiente, higienização e eventual contacto alimentar foi verificada?

- ☐ O tempo de resposta e a frequência de amostragem correspondem à decisão?
- ☐ A identificação do dispositivo e a associação ao ativo ou local são inequívocas?
- ☐ A alimentação, autonomia e substituição foram calculadas para o perfil real?
- ☐ A cobertura foi ensaiada com obstáculos, produto e movimentos representativos?
- ☐ O comportamento offline, o armazenamento e o reenvio estão definidos?
- ☐ Existem diagnósticos para bateria, comunicação, relógio, memória e sensor?
- ☐ A verificação, calibração, limpeza e manutenção têm periodicidade e responsável?
- ☐ O acesso às configurações, firmware, dados brutos e registos está assegurado?
- ☐ Foram testados falha, recuperação, duplicação, atraso e ordem de mensagens?
- ☐ A aceitação inclui critérios técnicos e operacionais assinados?

Módulo 3 - Dados, integração e interoperabilidade

Fazer com que dados provenientes de dispositivos diferentes circulem, sejam interpretados de forma consistente e permaneçam controlados ao longo do ciclo de vida.

RESULTADOS DE APRENDIZAGEM

- desenhar o percurso do dado até aos sistemas de negócio;
- distinguir protocolo, interface, modelo de dados e semântica;
- definir identidade, qualidade, governação e direitos de acesso;
- incorporar cibersegurança e continuidade desde os requisitos.



Ilustração 6 - Imagem de abertura - contexto do módulo 3: dados, integração e segurança.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 3 · DECISÃO E APLICAÇÃO

3.1 Do dispositivo aos sistemas de negócio

A integração liga o acontecimento físico ao registo operacional, evitando ilhas de informação.



Figura 10 - Arquitetura em camadas do dispositivo ao processo empresarial.

Fonte: elaboração própria com base na Recommendation ITU-T Y.4000/Y.2060 ^[14] e na W3C WoT Architecture 1.1 ^[32].

Camadas com contratos explícitos

Dispositivo, gateway, comunicação, plataforma, integração, aplicação e sistema empresarial devem trocar dados através de contratos técnicos conhecidos. Cada fronteira precisa de definir formato, identidade, tempo, unidade, confirmação, erro, segurança e responsabilidade.

A plataforma IoT não deve tornar-se automaticamente o registo mestre de lotes, fornecedores ou artigos. A empresa deve decidir que sistema é autoridade para cada dado e como são tratadas divergências.

Perguntas por fronteira

- quem cria e quem valida o identificador?
- que sistema atribui o instante e em que fuso horário?
- como se distingue leitura original, corrigida e calculada?

- o que acontece a mensagens atrasadas, duplicadas ou fora de ordem?
- como é comunicada uma indisponibilidade ou rejeição?
- onde se conserva o registo necessário para auditoria?

3.2 Arquitetura modular e desacoplada

Separar aquisição, transporte, processamento e utilização pode reduzir dependências e facilitar a substituição controlada, desde que as interfaces, responsabilidades, versões e testes de integração sejam governados.

Princípios de desenho

- interfaces documentadas em vez de acessos diretos e informais;
- identificadores estáveis e independentes do fornecedor;
- dados brutos preservados quando necessários à investigação;
- regras e configurações versionadas;
- componentes substituíveis sem perder histórico ou contexto;
- observabilidade sobre filas, erros, atrasos e capacidade.

Tempo real como requisito graduado

«Tempo real» não é uma propriedade única. O requisito deve indicar o intervalo máximo admissível entre observação, disponibilidade, interpretação e ação. O NIST SP 1500-203 enquadra a relevância dos requisitos temporais em sistemas ciberfísicos ^[21]. Em muitos processos, o importante é garantir uma latência máxima compatível com a resposta, e não atualizar o ecrã continuamente.

A arquitetura deve priorizar mensagens com impacto distinto. Um alarme de processo, um registo de tendência e um relatório histórico podem admitir tempos e percursos diferentes.

Teste de independência

Se a plataforma for substituída, a empresa consegue exportar dados, significados, configurações, históricos de alarme e relações de identidade num formato utilizável?



Ilustração 7 - Imagem editorial — Processamento periférico e integração: o percurso do dado liga a operação local aos sistemas autorizados.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

3.3 Protocolos, interfaces e modelos de dados

A interoperabilidade exige mais do que usar um protocolo conhecido.

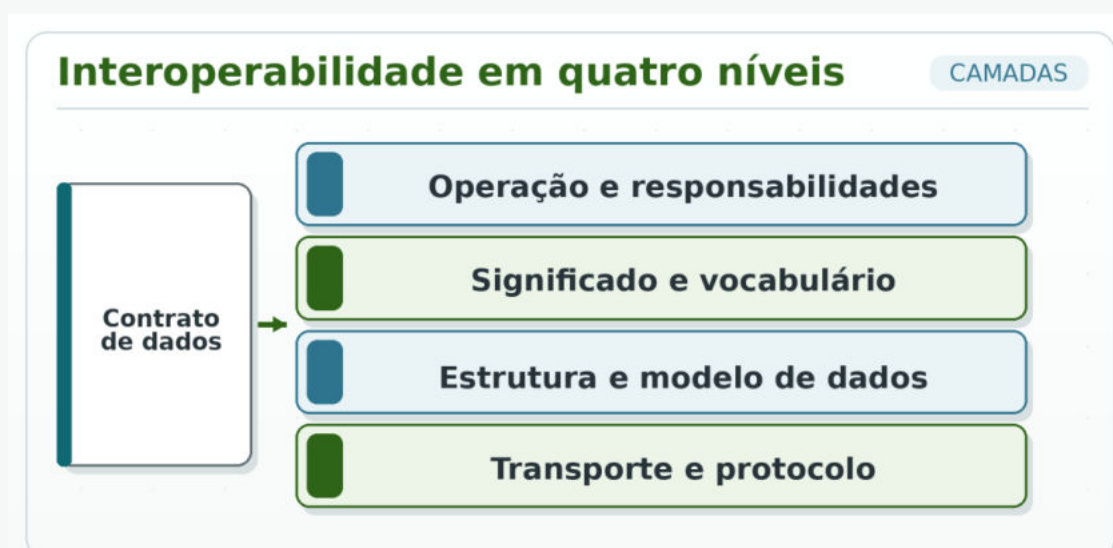


Figura 11 - Camadas de interoperabilidade: transporte, estrutura, significado e operação.

Fonte: elaboração própria com referência a MQTT, OPC UA, W3C WoT, EPCIS e CBV [9] [22] [23] [32] [33].

Papéis diferentes

MQTT define um mecanismo leve de publicação/subscrição (publish/subscribe) de mensagens [22]. HTTP e APIs REST são comuns em integrações de aplicações. OPC UA combina serviços e modelos de informação para interoperabilidade industrial [23]. A Web of Things do W3C define uma arquitetura abstrata para interoperabilidade entre plataformas e domínios IoT. As Thing Descriptions, especificadas numa recomendação própria, descrevem metadados e interfaces de interação de entidades físicas ou virtuais [32] [33]. EPCIS estrutura eventos de visibilidade da cadeia [9]. Nenhuma destas opções resolve isoladamente todas as camadas.

Conteúdo do contrato de dados

- nome e definição inequívoca do campo;
- tipo, formato, unidade e escala;
- identificador do objeto, dispositivo e local;
- instante da observação e instante de receção;
- qualidade, estado, origem e método;
- versão do esquema e regra de compatibilidade;
- códigos de erro, valores ausentes e comportamento perante alteração.

3.4 Integração com ERP, MES, WMS, QMS e manutenção

A utilidade aumenta quando o evento IoT encontra o contexto operacional certo.

Sistema	Contexto que pode fornecer	Informação que pode receber
ERP	artigo, fornecedor, ordem, cliente	quantidade, estado, confirmação
MES / produção	operação, linha, receita, turno	medição, evento, paragem
WMS / armazém	local, unidade logística, movimento	leitura, condição, exceção

Sistema	Contexto que pode fornecer	Informação que pode receber
QMS / qualidade	plano, especificação, não conformidade	evidência, desvio, ação
CMMS / manutenção	ativo, plano, intervenção	estado, alarme, diagnóstico
TMS / transporte	viagem, veículo, rota, entrega	posição, condição, ocorrência

Tabela 5 – Sistemas de registo, contexto fornecido e informação recebida.

Escolher o sistema de registo

A integração deve evitar duplicar autoridades. Por exemplo, o ERP pode gerir o artigo, o WMS a localização atual e o QMS a decisão de libertação. A plataforma IoT conserva observações e diagnósticos. As relações e precedências devem ser aprovadas pela organização.

Integração por eventos

- emitir um evento quando ocorre uma mudança relevante;
- incluir chave de idempotência para tratar repetição;
- confirmar processamento e encaminhar rejeições;
- reconciliar periodicamente totais e estados entre sistemas;
- manter fila de exceções com responsável e prazo.

3.5 Identidade, contexto e qualidade dos dados

A qualidade deve ser avaliada em relação ao uso: correto, completo e pontual para uma decisão definida.



Figura 12 - Dimensões da qualidade de dados avaliadas em relação ao uso.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Dimensões essenciais

- validade: formato, unidade e domínio permitidos;
- exatidão do dado: grau em que o dado representa corretamente o objeto, acontecimento ou valor a que se refere; quando o dado é um resultado de medição, considerar também a incerteza e a rastreabilidade metrológica;
- completude: observações e campos esperados presentes;
- consistência: ausência de contradições entre fontes e estados;
- pontualidade: disponibilidade dentro do tempo necessário;
- unicidade: ausência de eventos indevidamente duplicados;
- rastreabilidade: origem, transformação, versão e responsável conhecidos.

Controlos no percurso

A validação deve ocorrer tão cedo quanto possível, sem apagar o valor original. Uma leitura impossível pode ser sinalizada, mas não deve ser substituída silenciosamente. Dados calculados devem conservar a fórmula ou versão do algoritmo e as entradas usadas.

Relógios dessincronizados alteram sequências, durações e relações com lotes. A fonte de tempo, o fuso, a mudança de hora e o comportamento offline devem fazer parte da especificação.

3.6 Governação, responsabilidade e direitos de acesso

A empresa precisa de saber quem pode usar, alterar, partilhar e conservar os dados, quais os direitos aplicáveis e quem assume a responsabilidade empresarial — também depois do contrato.



Figura 13 - Papéis mínimos de governação, responsabilidade e acesso aos dados.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Decisões de governação

- responsável empresarial por cada conjunto de dados;
- gestor da definição, qualidade e catálogo;
- administrador técnico de acessos e integrações;
- utilizadores autorizados e finalidades permitidas;
- prazo de conservação, arquivamento e eliminação;
- regras de partilha com clientes, fornecedores e autoridades;
- procedimento para correção, disputa e investigação.

Regulamento dos Dados

O Regulamento (UE) 2023/2854 aplica-se, de forma geral, desde 12 de setembro de 2025 e estabelece regras sobre acesso e utilização de dados, incluindo dados de produtos conectados e serviços relacionados; algumas obrigações têm datas e condições específicas ^[30]. Na contratação, a PME deve clarificar papéis de utilizador, detentor de dados, destinatário dos

dados e prestador de serviço, bem como direitos de acesso, formato, frequência, custos, portabilidade, segredos comerciais, segurança e mudança de prestador. Dados inferidos ou derivados, dados pessoais e dados protegidos por segredo comercial podem exigir análise própria.

Se os dados permitirem identificar uma pessoa, direta ou indiretamente, o RGPD pode ser aplicável ^[28]. A presença de dados de localização de condutores ou registos associados a trabalhadores exige uma avaliação própria; «dados industriais» não significa automaticamente «dados não pessoais».

3.7 Cibersegurança, continuidade e ciclo de vida

A segurança deve proteger disponibilidade, integridade, confidencialidade e capacidade de recuperação sem impedir a operação.

Capacidades de base

O NIST IR 8259 Rev. 1 (2026) descreve atividades fundacionais dirigidas a fabricantes de produtos IoT; não constitui, por si só, uma lista de controlos para a PME utilizadora ^[17]. Para requisitos de aquisição, o NIST IR 8259A oferece uma linha de base de capacidades técnicas do dispositivo — identificação, configuração, proteção de dados, controlo de acesso às interfaces, atualização de software e comunicação do estado de cibersegurança — e o NIST IR 8259B acrescenta capacidades não técnicas de apoio do fabricante ou de terceiros ^{[18] [19]}. As recomendações da ENISA enquadram a segurança IoT ao longo do ciclo de vida, incluindo cadeias de fornecimento, governação, requisitos de segurança, operação e gestão de vulnerabilidades ^{[7] [8]}.

- inventário de ativos, versões, dependências e responsáveis;
- credenciais únicas, menor privilégio e desativação de contas não usadas;
- segmentação entre operação, dispositivos, visitantes e serviços externos;
- encriptação e autenticação adequadas ao risco e à capacidade do dispositivo;
- atualizações verificadas, janela de manutenção e possibilidade de recuperação;
- registos, deteção, cópias de segurança e ensaios de restauro;
- gestão de vulnerabilidades, incidentes, fornecedor e fim de suporte.

Aplicabilidade legal

Em Portugal, o Decreto-Lei n.º 125/2025, de 4 de dezembro, aprovou o Regime Jurídico da Cibersegurança e transpôs a Diretiva SRI 2. No setor alimentar, o regime pode abranger empresas que se dediquem à distribuição por grosso e à produção e transformação industriais, desde que preencham os critérios de dimensão, âmbito territorial e qualificação previstos no diploma, sem prejuízo das situações especiais de inclusão. Por isso, não se deve presumir que todas as PME agroalimentares estão abrangidas; a qualificação deve ser verificada caso a caso [24] [29].

O Regulamento Ciber-Resiliência entrou em vigor em 10 de dezembro de 2024. As obrigações de reporte aplicam-se a partir de 11 de setembro de 2026; as principais obrigações aplicam-se a partir de 11 de dezembro de 2027. A PME deve distinguir as obrigações legais que lhe possam caber enquanto fabricante, importador ou distribuidor e, quando seja apenas utilizadora, as responsabilidades operacionais e contratuais associadas à aquisição, configuração, atualização e utilização segura de produtos com elementos digitais [31]. Mesmo fora de um âmbito obrigatório, os princípios de gestão de risco são úteis na contratação.

Cláusula essencial

O contrato deve indicar período de suporte, processo de notificação de vulnerabilidades, disponibilização de atualizações e opções quando o suporte termina.

3.8 Cenário ilustrativo — integração de eventos

Uma PME liga leitores de identificação, plataforma IoT e sistema de armazém para registar movimentos de unidades logísticas.

Fluxo proposto

1. O WMS cria ou recebe a unidade logística e o movimento esperado.
2. O leitor envia identidade, ponto, instante e diagnóstico à camada de integração.
3. A integração valida estrutura, autorização e correspondência com o movimento.
4. O WMS confirma o movimento ou devolve uma exceção tratável.
5. A plataforma conserva o evento original e o estado de processamento.

6. Uma reconciliação procura leituras sem movimento e movimentos sem leitura.

Exceções previstas

- leitura duplicada dentro do mesmo contexto;
- unidade desconhecida ou desativada;
- leitura no ponto errado ou fora da sequência;
- mensagem atrasada após restabelecimento;
- identidade correta associada ao objeto físico errado;
- indisponibilidade do WMS ou da ligação.

Critério de sucesso

Não basta receber mensagens. O processo deve demonstrar que cada movimento é aceite ou encaminhado para exceção, sem perda silenciosa e com possibilidade de reconstruir a sequência.

Natureza do exemplo

Cenário pedagógico, independente de fornecedor e sem resultados atribuídos.

3.9 Lista de verificação de interoperabilidade

A solução está pronta para integrar quando tecnologia, significado, operação e contrato são coerentes.

Saída para o módulo seguinte

Com identidades, eventos e interfaces controlados, a empresa pode automatizar a rastreabilidade e reforçar evidências de qualidade. O módulo 4 aplica a arquitetura a lotes, transformações e desvios.

☐ As fontes, destinos e sistemas de registo estão identificados?

☐ Cada interface tem responsável, documentação, versão e ambiente de teste?

☐ Campos, unidades, códigos, tempo e identidade têm definições comuns?

- ☐ Valores ausentes, inválidos, atrasados e duplicados têm tratamento definido?
- ☐ Existe confirmação de processamento e fila de exceções?
- ☐ A empresa consegue exportar dados, configurações e histórico em formato utilizável?
- ☐ Os acessos seguem menor privilégio e são revistos?
- ☐ Dispositivos, versões, dependências e fim de suporte estão inventariados?
- ☐ Atualização, cópia de segurança, restauro e resposta a incidente foram ensaiados?
- ☐ Dados pessoais e segredos comerciais foram identificados?
- ☐ As responsabilidades do fornecedor durante e após o contrato estão escritas?
- ☐ A reconciliação entre sistemas foi testada com falhas reais simuladas?

Módulo 4 - Rastreabilidade automatizada e controlo da qualidade

Estruturar identidades, eventos e evidências para reconstruir percursos, tratar desvios e apoiar decisões de qualidade.

RESULTADOS DE APRENDIZAGEM

- modelar unidades rastreáveis, lotes, locais e relações;
- automatizar recolha sem ocultar exceções;
- ligar medição, especificação, decisão e ação;
- testar a rastreabilidade de extremo a extremo.

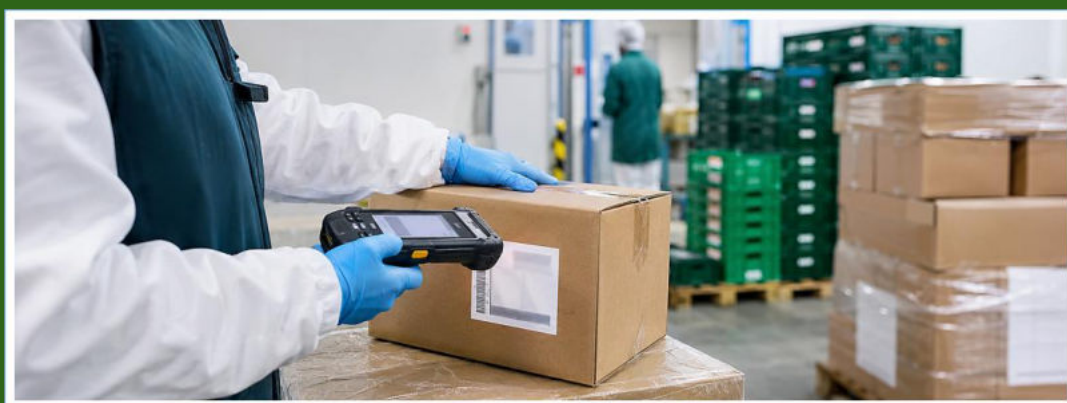


Ilustração 8 - Imagem de abertura - contexto do módulo 4: rastreabilidade e qualidade.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 4 · DECISÃO E APLICAÇÃO

4.1 Unidade rastreável, lote, local e ator

A rastreabilidade começa por definir o que deve ser seguido e em que nível de granularidade.

Entidades fundamentais

Uma unidade rastreável pode ser um lote, uma unidade comercial, uma unidade logística ou outra entidade definida pelo processo. A granularidade influencia o esforço de identificação, o volume de dados e a extensão potencial de uma retenção ou retirada. Deve ser escolhida segundo o risco, o processo, os requisitos legais e comerciais e a capacidade de manter relações corretas.

O Regulamento (CE) n.º 178/2002 exige que os operadores disponham de sistemas e procedimentos que permitam identificar os fornecedores e os outros operadores a quem forneceram géneros alimentícios, alimentos para animais, animais produtores de géneros alimentícios e substâncias abrangidas pelo artigo 18.º, facultando essa informação às autoridades competentes, a pedido ^[25]. A granularidade interna necessária para reconstruir transformações deve ser adequada à atividade e aos restantes requisitos aplicáveis.

Atributos mínimos controlados

- identificador e tipo de unidade;
- produto, lote e quantidade, quando aplicável;
- local e estado atual;
- origem, destino e intervenientes;
- relações com unidades de entrada, saída e agregação;
- datas e eventos relevantes;
- estado de qualidade: disponível, retido, libertado ou outro definido.

Granularidade

Mais detalhe só cria valor se a identidade física permanecer legível, aplicada ao objeto certo e registada em todos os pontos necessários.

MÓDULO 4 · DECISÃO E APLICAÇÃO

4.2 Eventos críticos e pontos de captura

Um evento de rastreabilidade deve responder, de forma controlada, ao que aconteceu, quando e onde, por que motivo ou etapa empresarial e, quando aplicável, em que condições. No EPCIS 2.0, estas dimensões são sintetizadas como What, When, Where, Why e How; a dimensão How pode incluir dados de sensores ^[9].



Figura 14 - Cinco dimensões de um evento EPCIS e informação complementar de responsabilidade operacional.

Fonte: elaboração própria com base no GS1 EPCIS 2.0.1 e no Core Business Vocabulary 2.0.0 ^[9].

Eventos frequentes

- receção e expedição;
- criação, transformação e consumo de lote;
- agregação, desagregação e reembalagem;
- movimento e mudança de custódia;
- inspeção, amostragem, medição e decisão de qualidade;
- retenção, libertação, bloqueio, devolução e destruição.

Ponto crítico de captura

Nem todos os passos precisam do mesmo detalhe. A análise deve localizar mudanças de identidade, propriedade, custódia, localização, estado e composição. Nesses pontos, a captura deve ser suficientemente controlada para preservar a relação entre o acontecimento físico e o registo digital.

O EPCIS organiza dados de eventos de visibilidade e um vocabulário associado ^[9]. A adoção deve ser avaliada segundo o ecossistema e a necessidade de partilha; usar o nome do padrão sem implementar identificadores e semântica consistentes não garante interoperabilidade.

4.3 Captura automática com controlo de exceções

Automatizar pode reduzir a transcrição manual, mas introduz ou desloca modos de falha: leituras indevidas, associações erradas, eventos silenciosamente perdidos e erros propagados entre sistemas.



Figura 15 - Da captura automática à evidência aceite.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Controlos no ponto de captura

- confirmar que o identificador corresponde ao objeto físico;
- restringir a zona e o instante de leitura ao evento esperado;
- distinguir leitura técnica de evento empresarial confirmado;

- detetar repetição, ausência, conflito e sequência inválida;
- dar feedback imediato ao operador quando é necessária correção;
- conservar o registo original e o resultado da validação.

Supervisão humana no circuito

O operador não deve ser transformado num mero confirmador. A interface deve explicar a exceção, apresentar opções autorizadas e impedir correções sem rasto. Em situações ambíguas, a unidade deve ser encaminhada para retenção ou revisão segundo procedimento.

Regra de evidência

Uma leitura demonstra que um identificador foi detetado; o evento aceite demonstra que a operação prevista foi validada.

4.4 Ligar medição, especificação e decisão

O controlo de qualidade digital precisa de conservar o contexto que permite interpretar cada resultado.

Elemento	Pergunta de controlo	Registo necessário
plano	o que medir e quando?	versão e aplicabilidade
método	como obter o resultado?	procedimento e instrumento
especificação	qual o critério?	fonte, versão e unidade
amostra / objeto	a que se refere?	identidade e relação com lote
resultado	o que foi observado?	valor, estado e qualidade do dado
decisão	qual o efeito no produto?	responsável, fundamento e instante
ação	como foi tratado?	contenção, correção e fecho

Tabela 6 - Elementos de controlo para ligar medição, especificação e decisão.

Contexto antes de cálculo

Um resultado pode cumprir o formato e estar associado à amostra errada, ao método errado ou a uma especificação obsoleta. A integração deve validar a aplicabilidade da regra e conservar a versão usada na decisão.

Quando adotados ou usados como enquadramento, os sistemas de gestão da segurança alimentar, incluindo a família ISO 22000, articulam comunicação, controlo operacional, avaliação do desempenho e melhoria ^[13]. A ferramenta digital deve apoiar esses processos sem criar uma via paralela não controlada.

4.5 Desvios, alertas e evidência

O objetivo de um alerta não é gerar notificações; é conduzir uma ocorrência até uma decisão documentada.



Figura 16 - Ciclo de tratamento de um desvio suportado por dados IoT.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Fluxo controlado

1. Detetar o sinal e verificar a integridade mínima do dado.
2. Notificar o papel responsável segundo prioridade e horário.

3. Confirmar a condição por fonte adequada ou inspeção.
4. Conter o produto, processo ou equipamento quando previsto.
5. Avaliar impacto com base em tempo, exposição, lote e evidência.
6. Executar correção e ação corretiva quando aplicável.
7. Registar decisão, fundamento, anexos, responsável e fecho.

Qualidade da trilha de auditoria

- registos cronológicos e protegidos contra alteração não autorizada;
- distinção entre informação automática e introdução manual;
- motivo obrigatório para correção ou anulação;
- versão da regra que gerou o alerta;
- ligação entre alerta, ocorrência, lote, ação e decisão.

4.6 Rastreabilidade de extremo a extremo

A cadeia deve conseguir reconstruir relações para montante e jusante, atravessando transformações e sistemas.

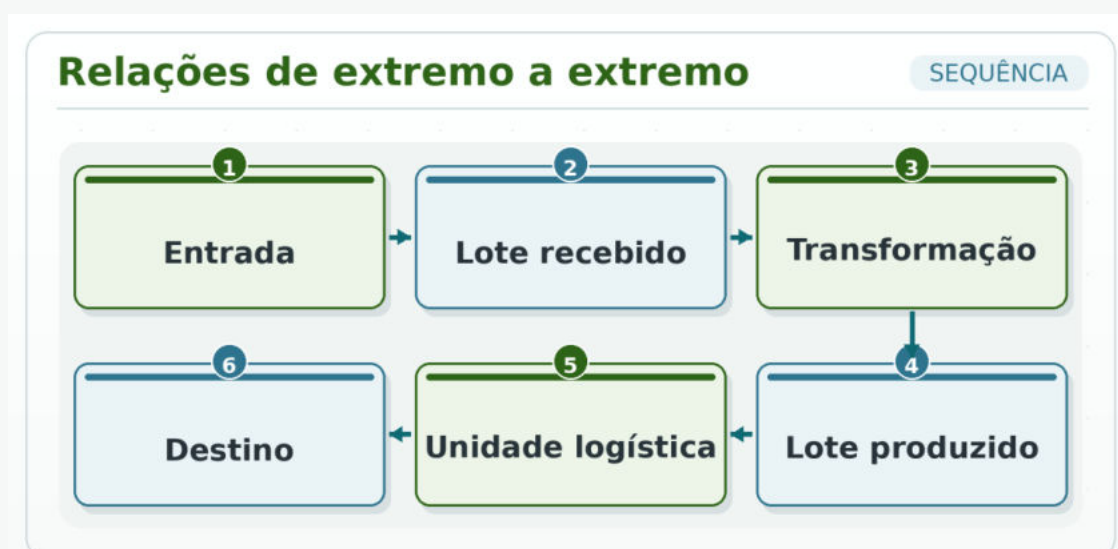


Figura 17 - Relações de rastreabilidade através de receção, transformação, agregação e expedição.

Fonte: elaboração própria com base em GS1 Global Traceability Standard ^[10].

Teste de rastreabilidade

Selecione uma unidade de saída e percorra as matérias-primas, lotes intermédios, operações, controlos, localizações e destinos. Em sentido inverso, selecione uma entrada e identifique todos os produtos e clientes potencialmente relacionados. O teste deve incluir relações de agregação e períodos de indisponibilidade.

CrITÉrios a observar

- completude de ligações e campos obrigatórios;
- coerência entre quantidades e estados, quando pertinente;
- tempo necessário para obter e validar a informação;
- capacidade de explicar lacunas e correções;
- identificação de produto retido, expedido, devolvido ou destruído;
- acesso à documentação e aos responsáveis de decisão.

Teste realista

Inclua um lote com reembalagem, divisão, retrabalho ou agregação; percursos excessivamente simples podem não revelar falhas importantes.

4.7 Investigação, retirada e comunicação

Uma arquitetura de dados deve apoiar a investigação sem substituir o plano de gestão de incidentes.

Preparação

- papéis, contactos, suplentes e autoridade para bloquear ou libertar;
- fontes de dados e procedimento de extração;
- critérios para determinar o âmbito potencial;
- modelos de registo e comunicação aprovados;
- preservação de evidência e controlo de acesso;
- ensaio periódico e revisão de lições aprendidas.

Contribuição dos dados IoT

Os dados podem ajudar a localizar unidades, ordenar eventos, identificar condições e delimitar hipóteses. A sua interpretação deve considerar falhas do sensor, lacunas de comunicação, posição, representatividade e alterações de configuração. A investigação deve, sempre que possível, combinar fontes independentes e registar as limitações quando a confirmação cruzada não esteja disponível.

A comunicação externa, incluindo com autoridades, clientes ou consumidores, segue o plano da organização e os requisitos aplicáveis. Um painel de controlo não deve emitir conclusões automáticas sobre segurança ou responsabilidade.

Preservação

Num incidente, preserve dados originais, registos de acesso, configurações, versões e evidência de sincronização temporal antes de efetuar alterações.

4.8 Cenário ilustrativo — transformação de lotes

Uma PME combina várias entradas numa operação e divide a saída por diferentes unidades logísticas.

Modelo

1. Cada entrada é confirmada no ponto de consumo e associada à ordem.
2. A operação regista linha, intervalo temporal, versão de processo e estado.
3. O sistema cria o lote de saída e liga todas as entradas efetivamente usadas.
4. As unidades logísticas de saída são agregadas ao lote e ao destino.
5. A decisão de qualidade altera o estado das unidades relacionadas.
6. Exceções — substituição, retrabalho ou correção — requerem motivo e aprovação.

Ensaio

A equipa seleciona uma entrada e confirma todas as saídas relacionadas; depois escolhe uma unidade expedida e reconstrói entradas, operação e controlos. As diferenças são classificadas como falha de identificação, processo, integração, dados mestres ou procedimento.

Aprendizagem

A automatização é eficaz quando reduz a digitação sem retirar visibilidade às substituições reais. Forçar o processo digital a assumir uma sequência ideal cria registos coerentes, mas falsos.

Natureza do exemplo

Cenário pedagógico; a definição de lote e os registos obrigatórios dependem do produto e do processo.



Ilustração 9 - Rasto digital de um lote entre transformação, embalagem e expedição.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 4 · DECISÃO E APLICAÇÃO

4.9 Lista de verificação de rastreabilidade

Confirme se identidade, evento, decisão e evidência permanecem ligados.

Saída para o módulo seguinte

A mesma combinação de identidade, tempo e condição permite controlar armazenamento, transporte e conservação. O módulo 5 aprofunda a logística conectada e a interpretação responsável da cadeia de frio.

- ☐ As unidades rastreáveis e a granularidade estão definidas?
- ☐ Os identificadores são únicos, controlados e aplicados ao objeto correto?
- ☐ Transformação, divisão, agregação, retrabalho e reembalagem preservam relações?
- ☐ Os eventos críticos têm local, instante, ator, motivo e estado?
- ☐ A leitura automática é validada antes de se tornar evento empresarial?
- ☐ As exceções são visíveis e não podem ser apagadas sem rasto?
- ☐ Medições estão ligadas ao lote, amostra, método, instrumento e especificação?
- ☐ Retenção, libertação e bloqueio propagam-se aos sistemas necessários?
- ☐ É possível reconstruir para montante e jusante através de todos os sistemas?
- ☐ O teste inclui falhas, dados em falta e operações não lineares?
- ☐ Os registos podem ser exportados e apresentados de forma inteligível?
- ☐ O plano de incidente define preservação, decisão e comunicação?

Módulo 5- Logística inteligente e conservação

Usar identidade, localização e condição para prevenir perdas, responder a incidentes e manter a continuidade entre armazém, transporte e entrega.

RESULTADOS DE APRENDIZAGEM

- desenhar monitorização representativa de armazenamento e transporte;
- interpretar excursões sem confundir ar, equipamento e produto;
- integrar alertas com inventário, expedição e decisão de qualidade;
- avaliar conservação e perdas com evidência adequada.



Ilustração 10 - Imagem de abertura - contexto do módulo 5: logística, conservação e transporte.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 5 · DECISÃO E APLICAÇÃO

5.1 Observar armazenamento e transporte

Uma cadeia logística conectada combina o «onde», o «quando», o «quê» e o «em que condição».



Figura 18 - Dimensões de visibilidade na logística agroalimentar.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Quatro dimensões

- identidade: lote, unidade logística, contentor, ativo ou remessa;
- localização: zona, doca, veículo, percurso ou ponto de entrega;
- condição: variável ambiental, estado do equipamento ou integridade;
- evento: carga, partida, chegada, transferência, abertura ou incidente.

Continuidade entre organizações

A mudança de custódia é um ponto frequente de perda de contexto. O contrato e o procedimento devem indicar quem instala, ativa, lê, devolve e mantém o dispositivo; quem recebe alertas; e como os dados são partilhados e associados à remessa.

O CXC 47-2001 constitui uma referência técnica para o transporte de alimentos a granel e semienvasados; o CXC 44-1995 pode ser pertinente para embalagem e transporte de frutas e produtos hortícolas frescos. Ambos reforçam condições higiénicas e adequadas ao produto,

mas não substituem requisitos legais, setoriais, contratuais ou orientações da autoridade competente [5] [6].

5.2 Cadeia de frio: medir e interpretar

A temperatura é uma grandeza local e temporal. O resultado de medição depende do ponto, do método e da resposta do sensor; a evolução térmica do produto depende, entre outros fatores, da massa térmica e das condições de transferência de calor.

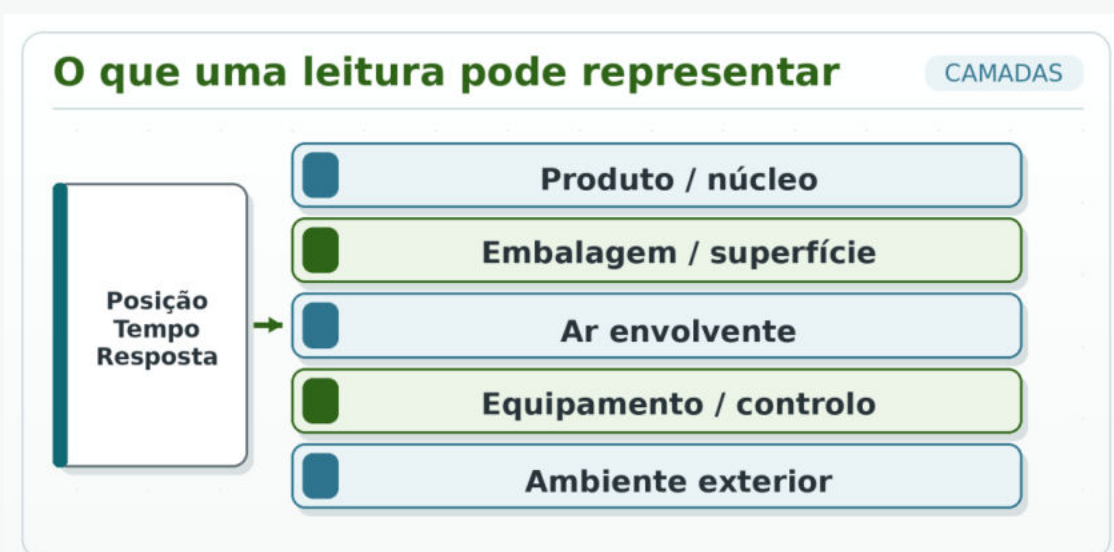


Figura 19 - Relação entre equipamento, ar, superfície, embalagem e produto.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

O que o sensor representa

Um sensor no ar descreve a condição no seu ponto de instalação e com a sua resposta. Não mede automaticamente a temperatura do núcleo do produto. Sensores junto da saída de ar, porta, evaporador ou teto podem responder de forma muito diferente. A posição deve resultar da finalidade e, quando necessário, de um estudo de distribuição.

Durante o transporte, a proximidade de paredes, teto, portas, retorno de ar, produto e fontes de calor altera a leitura. O registo deve conservar a posição e o método, especialmente quando a informação sustenta uma decisão sobre produto.

Interpretação de uma excursão

- confirmar integridade do sensor, posição e relógio;
- avaliar duração, padrão, contexto operacional e evidência independente;
- distinguir evento transitório previsto de condição não explicada;
- relacionar unidades e lotes potencialmente expostos;
- aplicar critérios aprovados e decisão competente;
- conservar fundamento, ação e incertezas.

Não há limiar universal

Os limites e tempos admissíveis devem provir da legislação, especificação, estudo de vida útil, processo validado ou avaliação de risco aplicável ao produto.

5.3 Localização, estado e integridade

A localização é útil quando a precisão e a frequência correspondem à decisão logística.

Necessidade	Abordagem possível	Limitação a testar
presença num ponto	código ótico, RFID, leitura de doca	leitura em falta ou indevida
zona interior	beacons, Wi-Fi, RFID ou infraestrutura local	reflexões, densidade, bateria
percurso exterior	posicionamento do veículo ou dispositivo celular	cobertura, energia, associação
abertura / impacto	sensor de estado ou evento	montagem, falsos positivos
estado do ativo	telemetria do equipamento	interface, interpretação, suporte

Tabela 7 - Necessidades de localização, tecnologias possíveis e limites operacionais.

Precisão adequada

Saber que uma unidade está no armazém pode ser suficiente para inventário; localizar uma paleta específica numa zona pode exigir infraestrutura e procedimentos adicionais. A empresa deve evitar prometer uma precisão que não foi demonstrada no ambiente real.

Integridade e cadeia de custódia

- associação controlada entre dispositivo e remessa;
- selo ou estado de abertura com contexto e autorização;
- registo de transferência entre responsáveis;
- deteção de remoção, troca ou reutilização indevida;
- procedimento para dispositivo perdido, danificado ou não devolvido.

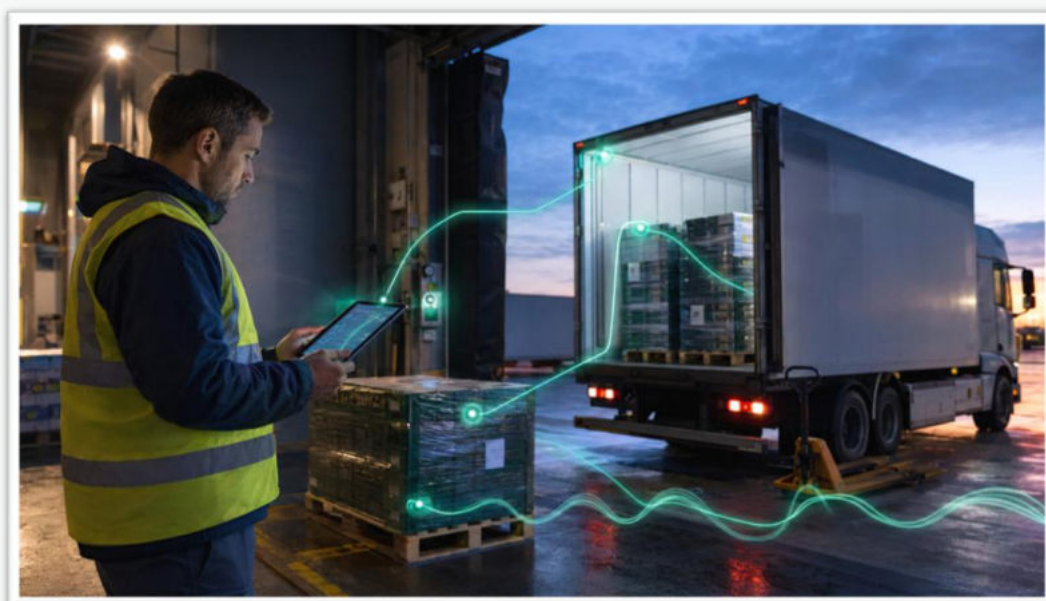


Ilustração 11 - Continuidade da monitorização entre paleta, cais e transporte refrigerado.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

5.4 Alertas e gestão de incidentes logísticos

O alerta deve chegar à pessoa que ainda consegue intervir, com o contexto necessário para decidir.



Figura 20 - Fluxo de resposta a uma ocorrência logística conectada.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Desenho do escalamento

- prioridade segundo consequência e reversibilidade;
- papel primário, suplente e horário de cobertura;
- canal principal e confirmação de receção;
- escalamento quando não há reconhecimento ou resolução;
- instruções seguras para transportador, armazém e qualidade;
- fecho apenas após decisão e registo.

Evitar fadiga de alarmes

Alarmes repetidos, transitórios ou sem ação possível levam à dessensibilização. A equipa deve analisar frequência, causa, utilidade e tempo de resposta. Ajustar uma regra exige aprovação e registo; não se deve aumentar um limite apenas para reduzir notificações.

A interface deve agrupar eventos relacionados sem ocultar o primeiro instante, o pior estado e a duração. O responsável precisa de ver dados em falta e falhas do dispositivo com prioridade própria.

5.5 Integrar inventário, expedição e transporte

A visibilidade logística cria valor quando altera estados nos sistemas que executam o processo.

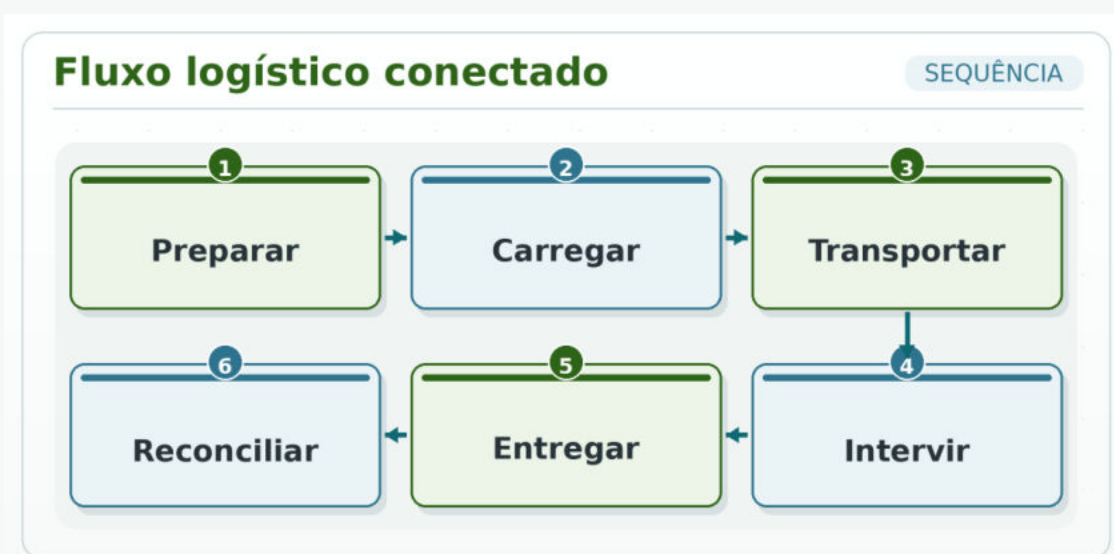


Figura 21 - Fluxo integrado entre armazém, expedição, transporte e receção.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Estados coerentes

O WMS pode conhecer a localização e disponibilidade; o TMS, a viagem; o ERP, a encomenda; a plataforma IoT, a condição e o dispositivo; o QMS, a decisão de qualidade. A integração deve implementar controlos para que o estado de uma unidade retida bloqueie ou sinalize movimentos incompatíveis e para que uma ocorrência no transporte seja encaminhada, confirmada e reconciliada com o processo de qualidade.

Eventos de ligação

- unidade preparada e atribuída à encomenda;
- carga confirmada no veículo e dispositivo associado;

- partida e início da janela de monitorização;
- ocorrência, intervenção e alteração de estado;
- chegada, prova de entrega e transferência de custódia;
- encerramento da viagem e desassociação do dispositivo.

Reconciliação

Compare remessas expedidas com viagens iniciadas, dispositivos ativos, entregas confirmadas e monitorizações encerradas. As diferenças revelam falhas que painéis isolados não mostram.

5.6 Conservação, perdas e eficiência

Os dados ajudam a localizar causas e oportunidades, mas a atribuição de benefício exige comparação e contexto.

Hipóteses que podem ser testadas

- aberturas de porta e práticas de carga associadas a instabilidade;
- zonas do armazém com comportamento sistematicamente diferente;
- atrasos entre preparação, carga e partida;
- percursos ou transferências com maior incidência de ocorrências;
- equipamentos com sinais de degradação antes de falhar;
- devoluções ou perdas relacionadas com condições observadas.

Método de avaliação

1. Definir o resultado e a origem dos dados antes da intervenção.
2. Distinguir variação sazonal, produto, cliente, rota e operação.
3. Registar alterações simultâneas que possam explicar o efeito.
4. Comparar períodos ou grupos de forma adequada ao processo.
5. Rever efeitos indesejados, custos de operação e carga de trabalho.
6. Decidir manter, corrigir ou retirar a solução segundo evidência.

Causalidade

Uma correlação entre condição e perda é um ponto de investigação. Não demonstra, isoladamente, causa nem justifica alterar critérios de segurança.



Ilustração 12 - Verificação de um dispositivo de monitorização numa operação refrigerada. A imagem ilustra o contexto; não define o ponto de medição nem substitui a validação da instalação.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

5.7 Qualidade de serviço e gestão de parceiros

A operação atravessa fornecedores, transportadores, clientes e plataformas; os níveis de serviço precisam de refletir essa cadeia.

Objeto de serviço	Evidência	Questão contratual
dispositivo	estado, bateria, verificação, substituição	quem mantém e em que prazo?
conectividade	cobertura, mensagens, indisponibilidade	como é medida e comunicada?
plataforma	acesso, latência, retenção, exportação	que dados e formatos são entregues?
alerta	emissão, entrega, reconhecimento, escalamento	quem responde fora do horário?
integração	sucesso, rejeição, reconciliação	quem corrige cada fronteira?
fim de serviço	migração, eliminação, devolução	como se evita perda de histórico?

Tabela 8 - Evidência de serviço e questões contratuais por objeto.

Partilha de dados

Defina finalidade, detalhe, frequência, utilizadores, conservação e responsabilidade por interpretação. O acesso deve ser proporcional: um parceiro pode necessitar de uma ocorrência e respetivo contexto, mas não de todo o histórico operacional da empresa.

Evidência de serviço

A disponibilidade global não revela períodos críticos nem mensagens perdidas. As métricas devem corresponder ao processo: dados completos por viagem, tempo até alerta, ocorrências sem responsável, dispositivos não associados e integrações por reconciliar.

5.8 Cenário ilustrativo — distribuição refrigerada

Uma PME expede várias encomendas num percurso com transferências de custódia e pretende melhorar a resposta a ocorrências.

Preparação

1. Atribuir unidades e lotes à viagem no sistema logístico.
2. Associar o dispositivo correto e confirmar estado antes da carga.
3. Registar posição do sensor e condição de início.
4. Ativar regras aprovadas para o produto e o percurso.
5. Disponibilizar instruções de resposta ao responsável de serviço.

Durante e após o percurso

Uma ocorrência é confirmada com o transportador e avaliada pela qualidade; a intervenção e o efeito são registados. Na entrega, a custódia, os dados e eventuais reservas são transferidos. O encerramento verifica completude, mensagens em falta e devolução do dispositivo.

Critérios de aceitação

- associação inequívoca entre viagem, carga e dispositivo;
- alerta recebido e reconhecido por papel autorizado;
- dados disponíveis apesar de interrupção de rede prevista;
- decisão ligada às unidades potencialmente afetadas;
- histórico exportável e inteligível para investigação.

Natureza do exemplo

Cenário pedagógico; as condições e decisões dependem do produto, contrato e requisitos aplicáveis.

5.9 Lista de verificação logística

Verifique a continuidade entre preparação, transporte, receção e encerramento.

Saída para o módulo seguinte

Depois de recolher eventos e condições, a empresa precisa de apresentar, priorizar e encaminhar a informação. O módulo 6 organiza monitorização em tempo útil, automatização e indicadores.

- ☐ Remessa, unidades, lotes, veículo e dispositivo estão associados?
- ☐ A posição do sensor e o que a leitura representa estão documentados?
- ☐ Os critérios de alerta provêm de fonte aprovada para o produto?
- ☐ Cobertura, autonomia e armazenamento offline foram ensaiados no percurso?
- ☐ Aberturas, transferências e mudanças de custódia são registadas?
- ☐ O alerta inclui contexto, prioridade, responsável e escalamento?
- ☐ Existe procedimento para confirmar, conter, avaliar e fechar a ocorrência?
- ☐ O estado de qualidade impede movimentos incompatíveis nos outros sistemas?
- ☐ Viagens e monitorizações são reconciliadas no encerramento?
- ☐ Parceiros conhecem responsabilidades, dados partilhados e modo degradado?
- ☐ A exportação e retenção dos dados estão contratadas?
- ☐ A avaliação de benefício separa correlação, causa e efeitos sazonais?

Módulo 6 - Monitorização em tempo útil, automatização e decisão

Converter fluxos de dados em conhecimento da situação operacional, resposta controlada e aprendizagem, preservando a supervisão humana.

RESULTADOS DE APRENDIZAGEM

- desenhar painéis orientados a decisões;
- definir regras, alertas e fluxos de trabalho;
- graduar a automatização segundo risco e reversibilidade;
- seleccionar indicadores úteis e interpretáveis.



Ilustração 13 - Imagem de abertura — contexto do módulo 6: alertas, fluxos de trabalho e indicadores.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

MÓDULO 6 · DECISÃO E APLICAÇÃO

6.1 Painéis orientados à ação

Um painel deve reduzir o tempo para reconhecer uma situação e escolher a próxima ação autorizada.

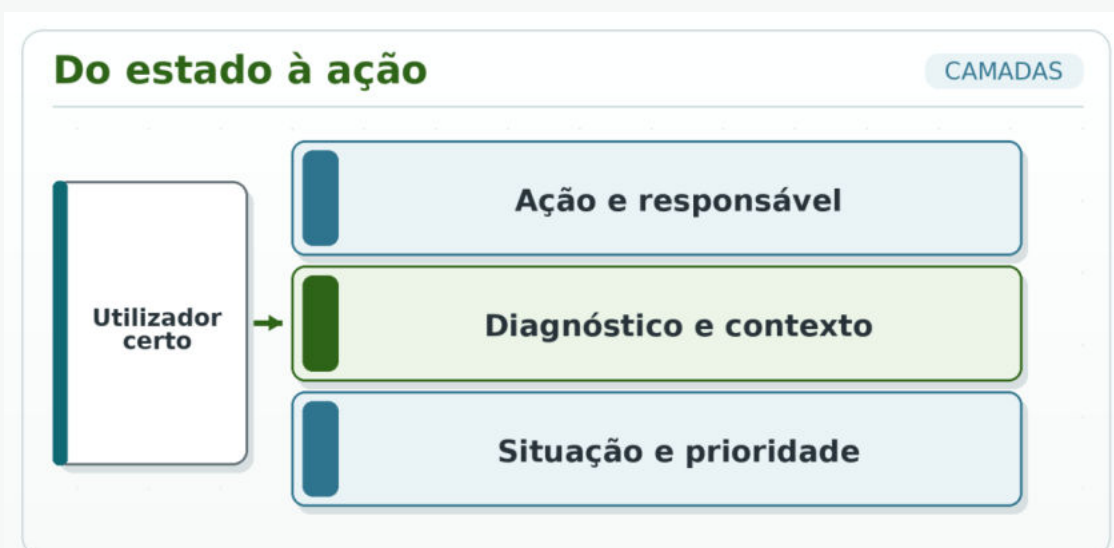


Figura 22 - Hierarquia de informação de um painel operacional.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Três níveis

- situação: o que está normal, degradado, em alerta ou sem dados;
- diagnóstico: tendência, contexto, eventos relacionados e saúde do sistema;
- ação: responsável, instrução, prazo, confirmação e fecho.

Princípios de experiência de utilização

A cor deve reforçar texto e símbolo, nunca ser o único código. Unidades, fuso horário, atualização e período devem estar visíveis. Gráficos precisam de escala coerente e indicação de lacunas; unir pontos separados por ausência de dados cria uma continuidade falsa.

O painel executivo agrega resultados e riscos; o painel operacional mostra tarefas e exceções; o painel técnico mostra dispositivos, filas, cobertura e integrações. Misturar estes níveis aumenta ruído e dificulta a responsabilização.

Pergunta de teste

Um utilizador autorizado consegue perceber, sem explicação externa, o que aconteceu, que dados faltam e qual é a ação seguinte?

6.2 Regras, limiares e qualidade do alerta

Uma regra traduz conhecimento aprovado num mecanismo repetível; deve ter responsável, versão e justificação.

Estado do dado	Comportamento recomendado
válido e atual	avaliar regra operacional
atrasado	sinalizar atraso e limitar decisão
ausente	abrir falha de monitorização
inválido	preservar original e encaminhar verificação
origem desconhecida	não usar para decisão automática

Tabela 9 - Estados do dado e comportamento recomendado.

Componentes da regra

- população ou ativos a que se aplica;
- variável, unidade e estado de qualidade exigido;
- condição, duração, histerese e dependências;
- eventos que suspendem ou alteram a interpretação;
- prioridade, destinatário, instrução e escalamento;
- versão, aprovador, data de entrada e teste realizado.

Tipos de regra

Uma regra pode verificar um limite, uma duração, uma ausência de mensagem, uma sequência inválida, uma divergência entre fontes ou uma tendência. Regras simples são mais

fáceis de explicar e testar. Modelos analíticos exigem dados adequados, validação, monitorização do desempenho e tratamento de mudança do processo.

A qualidade do alerta pode ser revista através de ocorrências confirmadas, alertas sem ação, falhas não detetadas, tempo até reconhecimento e capacidade de fechar. Os termos «falso positivo» e «falso negativo» só são úteis quando existe uma referência de confirmação clara.

6.3 Fluxos de trabalho e resposta fechada

A ocorrência só termina quando a condição, o impacto e a ação estão registados e revistos.

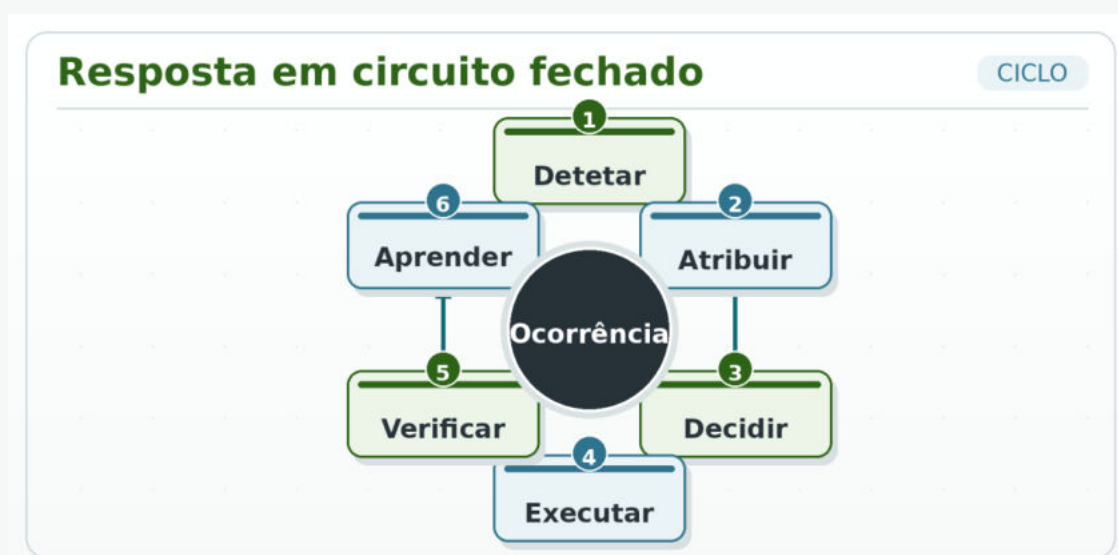


Figura 23 - Fluxo fechado entre deteção, decisão, execução e aprendizagem.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Elementos do fluxo

- criação automática com dados e contexto preservados;
- atribuição a papel e não apenas a pessoa individual;
- prazo e escalamento segundo prioridade;
- campos obrigatórios proporcionados à decisão;
- ligação a produto, ativo, lote, ordem ou viagem;
- verificação da eficácia e encerramento autorizado;
- classificação para análise posterior.

Integração com trabalho existente

Sempre que possível, a ocorrência deve ser encaminhada para o sistema onde a equipa já gere não conformidades, manutenção ou tarefas. Uma aplicação paralela cria filas concorrentes e perda de responsabilidade. A integração deve conservar a ligação ao evento original.

Antipadrão

Enviar correio eletrónico ou mensagem sem confirmação, responsável, escalamento e fecho não constitui um processo controlado de resposta.

6.4 Graduação da automatização

A autonomia deve aumentar apenas quando dados, regras, efeitos e recuperação são suficientemente controlados.



Figura 24 - Níveis de automatização e condições de passagem.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Escada de autonomia

1. Observar e registrar.
2. Notificar e apresentar contexto.
3. Recomendar uma ação a uma pessoa autorizada.
4. Executar após confirmação.

5. Executar automaticamente dentro de limites e interbloqueios.
6. Otimizar parâmetros dentro de espaço validado e sob supervisão.

Condições para subir

- dados e diagnósticos demonstram desempenho adequado;
- regra é explicável, testada e versionada;
- efeito é reversível ou existe estado seguro;
- exceções e limites de autoridade estão definidos;
- intervenção manual e recuperação foram ensaiadas;
- alteração é aprovada e monitorizada após entrada em serviço.

6.5 Análise de dados e apoio à decisão

A análise deve responder a uma pergunta operacional e declarar os limites da inferência.

Do descritivo ao prescritivo

- descritivo: o que aconteceu e em que contexto;
- diagnóstico: que fatores são compatíveis com o padrão observado;
- preditivo: que estado pode ocorrer, com que incerteza;
- prescritivo: que ação é recomendada dentro de restrições definidas.

Validação

Separe dados de desenvolvimento e avaliação, evite usar informação que só estaria disponível depois da decisão e compare com uma referência simples. Avalie desempenho por produto, período, equipamento e condição relevante. Uma média global pode ocultar falhas em situações raras, mas críticas.

O modelo deve indicar versão, entradas, saída, confiança ou limitação aplicável e caminho de substituição quando está indisponível. Mudanças de sensor, processo, produto ou política podem degradar o desempenho; por isso, a monitorização continua após a entrada em serviço.

Rigor na linguagem

«Prevê», «indica» e «está associado» não significam «demonstra a causa». A decisão deve respeitar o nível de evidência disponível.

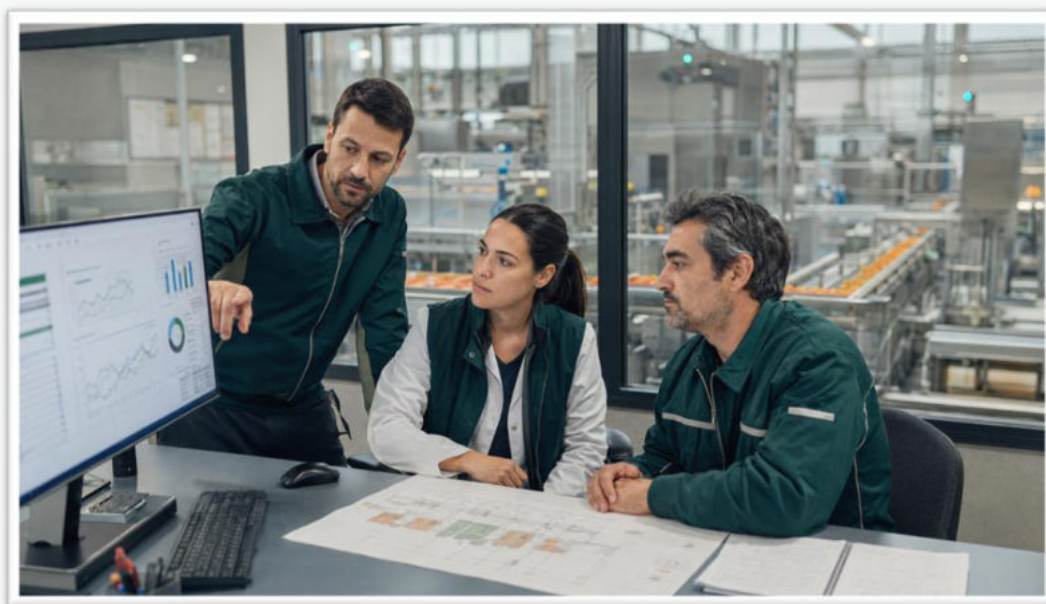


Ilustração 14 - Análise conjunta de dados por produção, qualidade e manutenção, com supervisão humana e decisão documentada.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica

6.6 Indicadores e revisão de desempenho

Indicadores eficazes ligam o funcionamento técnico ao resultado operacional sem incentivar comportamentos errados.



Figura 25 - Árvore de indicadores técnicos, operacionais e de resultado.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Indicador	Pergunta que responde
completude por ativo	recebemos o que esperávamos?
tempo até reconhecimento	a informação chegou a quem podia agir?
ocorrências sem fecho	o processo terminou com decisão?
reconciliações pendentes	os sistemas concordam?
benefício verificado	a mudança produziu o efeito pretendido, considerando linha de base, contexto, custos e outros fatores explicativos?

Tabela 10 – Indicadores de desempenho e perguntas de gestão.

Três famílias

- saúde técnica: dispositivos ativos, dados completos, atraso, erros e recuperação;
- processo: alertas reconhecidos, ocorrências fechadas, reconciliação e cumprimento do fluxo;
- resultado: desvios, perdas, tempo de decisão, serviço e risco residual.

Ficha de indicador

Para cada indicador, defina objetivo, fórmula, fonte, população, exclusões, periodicidade, responsável e ação associada. Apresente numerador e denominador quando a percentagem puder ocultar volume. Conserve a definição ao comparar períodos.

Indicadores de disponibilidade podem parecer favoráveis enquanto faltam dados no momento crítico. A revisão deve cruzar o desempenho médio com ocorrências, períodos de maior risco e modos degradados.

6.7 Cenário e síntese — alerta com ação

Uma PME deteta condições anómalas num equipamento e pretende evitar notificações sem seguimento.

Configuração ilustrativa

1. A regra avalia leitura, qualidade do dado e estado operacional.
2. O alerta cria uma ocorrência no sistema de manutenção.
3. O técnico confirma condição, regista diagnóstico e ação.
4. Se houver possível impacto no produto, a qualidade recebe uma tarefa ligada.
5. O fecho exige verificação e classificação da causa.
6. A revisão periódica analisa utilidade, falhas e necessidade de alteração.

Lista de decisão

- o painel distingue condição normal, alerta e ausência de dados;
- cada regra tem versão, responsável e critério documentado;
- a ocorrência tem papel, prazo, escalamento e fecho;
- a automação respeita estado seguro e possibilidade de intervenção;
- modelos analíticos são validados e monitorizados;
- indicadores ligam saúde técnica, processo e resultado.

Saída para o módulo seguinte

A empresa dispõe agora de uma arquitetura de informação e resposta. O módulo 7 converte-a em requisitos, piloto, contratação, implementação e expansão.

Natureza do exemplo

Cenário pedagógico, sem alegação de prevenção de falhas ou benefício quantitativo.

CONTEXTO VISUAL

Do alerta à resposta verificada

Uma ocorrência torna-se controlada quando há confirmação, intervenção, registo e fecho autorizado.



Ilustração 15 – Resposta coordenada a um alerta, com verificação física e fecho documentado.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

Módulo 7 - Adoção pelas PME: do requisito à expansão

Preparar um projeto executável, contratar com controlo, produzir evidência sobre valor e viabilidade num piloto e expandir sem perder segurança, dados ou capacidade interna.

RESULTADOS DE APRENDIZAGEM

- avaliar necessidade, prontidão e alternativas;
- escrever requisitos funcionais, técnicos e de serviço;
- desenhar piloto, aceitação e indicadores;
- organizar adoção, ciclo de vida e roteiro de expansão.



Ilustração 16 - Imagem de abertura — contexto do módulo 7: requisitos, piloto e adoção.

Fonte: imagem editorial produzida com apoio de IA; validação pela equipa técnica

MÓDULO 7 · DECISÃO E APLICAÇÃO

7.1 Necessidade, alternativa e prontidão

O projeto começa com uma decisão de negócio: resolver, reduzir, controlar ou aprender sobre um problema específico.

Importância e prontidão			MATRIZ DE DECISÃO
	Prontidão baixa	Prontidão alta	
Importância alta	Preparar condições	Priorizar piloto	
Importância baixa	Reavaliar	Executar se útil	

Figura 26 - Matriz de prontidão: importância do caso e capacidade de execução.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Diagnóstico inicial

- problema, frequência, consequência e processo afetado;
- evidência disponível e limitações do método atual;
- alternativas não tecnológicas ou de menor complexidade;
- capacidade de intervir quando a informação chegar;
- dados mestres, infraestrutura e integrações existentes;
- patrocínio, responsável de processo e disponibilidade da equipa.

Escolher o primeiro caso

Um bom primeiro caso é relevante, delimitado, mensurável e executável. Evite começar por uma cadeia inteira, vários produtos e integrações críticas simultâneas. A delimitação deve permitir aprender sobre instalação, dados, resposta e operação sem criar uma demonstração artificial sem relação com o trabalho real.

Critério de não avanço

Se não existe responsável pelo processo nem ação possível perante a informação, adie a tecnologia e resolva primeiro a governação.

7.2 Requisitos funcionais e técnicos

Um requisito deve ser verificável e independente da solução proposta pelo fornecedor.

Classe	Exemplos de conteúdo
funcional	evento, utilizador, decisão, fluxo e evidência
medição	grandeza, local, desempenho, verificação e calibração
dados	campos, identidade, unidade, tempo, qualidade e retenção
integração	interfaces, confirmação, erro, volume e reconciliação
segurança	identidade, acesso, atualização, registo e incidente
serviço	instalação, suporte, substituição, formação e níveis de serviço
ciclo de vida	escalabilidade, exportação, migração e fim de suporte

Tabela 11 – Classes de requisitos e conteúdo mínimo.

Forma verificável

Prefira «o sistema deve sinalizar dados em falta por dispositivo e intervalo» a «o sistema deve ter elevada fiabilidade». Associe cada requisito a um método de aceitação: inspeção, demonstração, teste, análise documental ou ensaio operacional.

Matriz de rastreabilidade de requisitos

- identificador e origem do requisito;
- prioridade e responsável pela aprovação;
- componente ou fornecedor que o satisfaz;
- método, ambiente e evidência de teste;
- resultado, desvio e decisão de aceitação.

MÓDULO 7 · DECISÃO E APLICAÇÃO

7.3 Avaliar propostas e contratar

A proposta mais convincente deve ser transformada em arquitetura, responsabilidades, custos e evidências comparáveis.



Figura 27 - Dimensões de avaliação de uma proposta IoT.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Diligência técnica

- demonstração contra casos e dados representativos;
- arquitetura, dependências, limites e componentes de terceiros;
- referências verificáveis em ambientes comparáveis;
- modelo de suporte, atualização, vulnerabilidades e fim de vida;
- interfaces, formatos, direitos de acesso e portabilidade;
- recursos necessários à empresa e ao integrador.

Cláusulas que protegem a continuidade

O contrato deve cobrir direitos de acesso, utilização, disponibilização, exportação e portabilidade dos dados; formatos, frequência, conservação, confidencialidade, subcontratantes, local de tratamento, níveis de serviço, segurança, notificação de incidentes,

atualização, substituição, reversibilidade e assistência à saída. O Regulamento dos Dados deve ser considerado segundo a aplicabilidade ao produto e ao serviço ^[30].

A aceitação não deve depender apenas de o sistema «estar online». Deve exigir dados corretos, integrações confirmadas, falhas ensaiadas, documentação entregue e utilizadores capazes de executar o processo.

7.4 Desenhar um piloto que produza evidência

O piloto deve testar as incertezas decisivas e aproximar-se do ambiente de operação.



Figura 28 - Etapas e portas de decisão de um piloto IoT.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Protocolo do piloto

- hipótese, âmbito, população e exclusões;
- linha de base e fontes de comparação;
- requisitos e critérios de aceitação;
- papéis, formação e modo degradado;
- plano de instalação, teste e recolha de evidência;
- riscos, alterações permitidas e controlo de versões;
- decisão final: parar, corrigir, repetir ou expandir.

Representatividade

Inclua condições normais e exceções relevantes: carga, higienização, mudança de turno, perda de rede, dispositivo com bateria baixa, integração indisponível e operação manual. Não comprometa segurança nem produto para provocar falhas; use simulações controladas e ambientes adequados.

Separar demonstração de piloto

Uma demonstração prova que uma função pode ser apresentada. Um piloto testa se o sistema e a organização conseguem operar nas condições definidas.

7.5 Aceitação, indicadores e decisão

A decisão de avançar deve combinar desempenho técnico, integração, utilização, risco e resultado.

Dimensão	Exemplos de critérios
técnica	completude, atraso, autonomia, recuperação, diagnósticos
medição	adequação, verificação, deriva, rastreabilidade
integração	sucesso, exceções, reconciliação, exportação
operacional	reconhecimento, ação, fecho, modo degradado
segurança	acesso, atualização, registos, restauro, incidentes
utilização	compreensão, carga de trabalho, formação, acessibilidade
resultado	efeito observado, custo total, risco residual

Tabela 12 - Matriz de avaliação de soluções IoT na cadeia agroalimentar.

Regra de decisão

Defina previamente quais os requisitos eliminatórios e quais admitem correção. Um resultado médio não deve compensar uma falha crítica. Registe desvios, ação proposta, responsável, prazo, necessidade de novo teste e risco aceite.

Custo total

- dispositivos, instalação, infraestrutura e integração;
- licenças, comunicações, armazenamento e suporte;
- calibração, bateria, limpeza, substituição e deslocação;
- cibersegurança, cópias, auditoria e atualização;
- formação, administração, tratamento de alertas e exceções;
- migração, exportação e desativação no fim do ciclo.

7.6 Implementação e mudança organizacional

A entrada em produção altera tarefas, autoridade, informação e dependências; precisa de gestão explícita.

Plano de transição

1. Aprovar processo futuro, papéis e documentação.
2. Preparar dados mestres, infraestrutura e acessos.
3. Formar por tarefa e ensaiar situações de exceção.
4. Executar instalação e qualificação contra critério
5. Operar em paralelo quando o risco justificar.
6. Transferir suporte, inventário e conhecimento.
7. Rever após entrada em serviço e corrigir lacunas.

Competências internas mínimas

- responsável pelo processo e pela decisão;
- responsável pelos dados e respetivas definições;
- administração de utilizadores e configuração;
- manutenção de dispositivos e instalação;
- triagem de alertas e coordenação de incidentes;
- gestão de fornecedor, contrato e ciclo de vida.

Adoção

A formação deve usar tarefas reais, não apenas menus. Registe dúvidas, atalhos, alertas ignorados, trabalho duplicado e dependências de uma pessoa. A solução deve reduzir ambiguidade sem retirar capacidade de questionar o dado.

Continuidade

Mantenha procedimentos para operação segura quando o sistema, a integração ou o fornecedor estiver indisponível.

7.7 Riscos, dependências e expansão

Escalar multiplica dispositivos, dados, utilizadores, integrações e consequências; não é apenas repetir a instalação.



Figura 29 - Mapa de dependências a rever antes da expansão.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Riscos a acompanhar

- dependência de fornecedor, plataforma, rede ou componente sem alternativa;
- fim de suporte, credenciais partilhadas e versões divergentes;
- crescimento de alertas sem capacidade de resposta;
- dados mestres inconsistentes entre locais;

- custos de comunicação, armazenamento e manutenção subestimados;
- alterações locais que quebram comparabilidade e validação;
- expansão de acesso a dados pessoais ou comercialmente sensíveis.

Padrão de escala

Crie um pacote replicável: arquitetura aprovada, catálogo de dispositivos, configuração de referência, contrato de dados, procedimento de instalação, testes, formação, indicadores e critérios de aceitação. Permita variações locais apenas através de gestão de alterações.

7.8 Cenário ilustrativo — piloto numa PME

Uma PME escolhe um processo de conservação delimitado para testar monitorização, integração e resposta.

Preparação

A equipa documenta a decisão, o procedimento atual e a linha de base. Qualidade define o critério e a avaliação; operação define a resposta; manutenção define instalação; informática define integração e segurança; compras transforma requisitos e saída em contrato.

Execução

1. Instalar e verificar dispositivos segundo o plano.
2. Confirmar identidade, tempo, unidade, lacunas e exportação.
3. Ensaiai alertas, escalamento, modo degradado e restauro.
4. Operar com utilizadores e condições representativas.
5. Registar carga de trabalho, desvios e alterações.
6. Avaliar critérios técnicos, operacionais e de resultado.

Decisão

A administração recebe uma síntese com evidência, riscos residuais, custos de ciclo de vida e condições para expansão. A decisão pode ser corrigir e repetir; não avançar também é um resultado válido quando evita dependência ou risco não justificado.

Natureza do exemplo

Cenário pedagógico; não representa um projeto, fornecedor ou resultado real.



Ilustração 17 - Desenho de um piloto com representação digital da linha e pontos de decisão.

Fonte: imagem editorial produzida com apoio de IA e validada pela equipa técnica.

7.9 Roteiro e lista final de adoção

A expansão responsável preserva propósito, requisitos, evidência e capacidade de operação.



Figura 30 - Roteiro de adoção da necessidade à melhoria contínua.

Fonte: elaboração própria com apoio de ferramenta de IA generativa.

Princípio de fecho

A passagem para uma operação controlada só deve considerar-se concluída quando a empresa consegue operar, explicar, manter, auditar e, se necessário, substituir a solução. A melhoria e a revisão do risco prosseguem ao longo do ciclo de vida. O objetivo não é acumular dispositivos; é melhorar decisões e evidências ao longo da cadeia de valor.

☐ O problema, o processo e a alternativa foram avaliados?

☐ Existe responsável pelo processo, patrocinador e equipa multidisciplinar?

☐ Requisitos são verificáveis e ligados a métodos de aceitação?

☐ Dados, interfaces, segurança, suporte e saída constam do contrato?

☐ O piloto testa incertezas reais e condições representativas?

☐ Indicadores e critérios de decisão foram definidos antes da execução?

☐ Falhas, recuperação, modo degradado e intervenção manual foram ensaiados?

☐ Documentação, formação, inventário e conhecimento foram transferidos?

☐ Custos de ciclo de vida e riscos residuais são conhecidos?

☐ A expansão usa configuração de referência e gestão de alterações?

INSTRUMENTO TRANSVERSAL

Lista consolidada de adoção

Uma verificação transversal antes de autorizar a entrada em produção ou a expansão.

Processo e valor

- ☐ problema, decisão, ação e benefício verificável estão definidos;
- ☐ critérios provêm de fontes aprovadas e adequadas ao produto;
- ☐ papéis e modo degradado estão documentados.

Medição e dispositivo

- ☐ sensor, posição, resposta e ambiente são adequados ao uso;
- ☐ identidade, relógio, diagnóstico, energia e armazenamento são controlados;
- ☐ verificação, calibração, manutenção e impacto de falha estão previstos.

Dados e integração

- ☐ campos, unidades, tempo, identidade e qualidade têm definições comuns;
- ☐ atraso, ausência, duplicação, erro e reconciliação foram testados;
- ☐ exportação, retenção, portabilidade e sistemas de registo estão definidos.

Operação e segurança

- ☐ acessos, atualizações, registos, cópias e resposta a incidente são geridos;
- ☐ alertas têm responsável, escalamento, ação e fecho;
- ☐ intervenção manual, estado seguro e recuperação foram ensaiados.

Fornecedor e ciclo de vida

- ☐ arquitetura, dependências, suporte e fim de vida são conhecidos;
- ☐ contrato cobre dados, serviço, segurança, vulnerabilidades e saída;
- ☐ equipa interna consegue operar, auditar, manter e melhorar.

Critério de autorização

Qualquer resposta negativa deve originar uma ação, um responsável, um prazo e uma decisão explícita sobre o risco antes da entrada em produção.

REFERÊNCIA RÁPIDA

Glossário A–C

Ação corretiva — Ação para eliminar a causa de uma não conformidade e prevenir a recorrência; não se confunde com a correção imediata.

Agregação — Relação entre uma unidade que contém ou agrupa outras unidades, preservando a identidade destas quando necessário.

Alarme / alerta — Indicação de uma condição que requer atenção. A prioridade, o destinatário e a ação devem estar definidos.

Amostragem — Seleção e recolha de observações segundo um plano. Em IoT, inclui frequência temporal e posição espacial.

API — Interface de programação que permite a sistemas trocar pedidos, respostas ou eventos segundo regras documentadas.

Atuador — Componente que produz uma alteração física, como comutar, regular, abrir, fechar ou sinalizar.

Autonomia energética — Período durante o qual um dispositivo opera com a energia armazenada, sob condições de utilização definidas. A continuidade sem comunicação externa deve ser descrita separadamente como modo degradado.

Calibração — Operação que, em condições especificadas, estabelece primeiro uma relação entre os valores e incertezas fornecidos por padrões e as indicações correspondentes do instrumento e usa depois essa informação para obter um resultado de medição a partir de uma indicação ^[15].

Cadeia de custódia — Registo das transferências de responsabilidade ou posse de uma unidade e da evidência associada.

Cibersegurança — Gestão de riscos que podem afetar sistemas, serviços e dados, incluindo disponibilidade, integridade e confidencialidade.

Computação periférica (edge) — Processamento realizado próximo da origem dos dados, do dispositivo ou do processo físico, podendo complementar uma plataforma central e suportar funções locais.

Conectividade — Capacidade e condições através das quais componentes comunicam; inclui meio, cobertura, operação e segurança.

Contexto — Informação necessária para interpretar um dado: identidade, tempo, local, unidade, método, estado e relação com o processo.

REFERÊNCIA RÁPIDA

Glossário D–I

Dado bruto — Registo recebido da fonte antes das transformações de interpretação; pode já conter conversões efetuadas pelo dispositivo.

Dado mestre — Dado de referência partilhado, como artigo, local, fornecedor, ativo ou unidade, gerido por um sistema autorizado.

Deriva instrumental — Alteração contínua ou incremental, ao longo do tempo, da indicação, devida a alterações das propriedades metrológicas de um instrumento de medição.

Deriva de modelo — Alteração do desempenho de um modelo decorrente de mudanças nos dados, na relação entre variáveis ou no processo observado.

Dispositivo conectado — Equipamento com capacidade de observar, identificar, processar, comunicar ou atuar no ambiente físico.

Evento — Registo de algo que aconteceu num instante ou intervalo, associado a entidades e contexto.

EPCIS — Norma GS1 para partilha de dados de eventos de visibilidade entre aplicações e organizações.

Exatidão de medição — Grau de concordância entre um valor medido e um valor verdadeiro da mensuranda. É um conceito qualitativo e não deve ser usado como sinónimo de incerteza, erro ou precisão.

Firmware — Software incorporado num dispositivo, sujeito a configuração, atualização, suporte e controlo de versão.

Gateway — Componente que agrega dispositivos, interliga redes ou protocolos e pode executar processamento local.

Histerese — Diferença deliberada entre condições de ativação e desativação de uma regra para evitar comutações repetidas.

Identificador — Código que distingue uma entidade dentro de um âmbito definido; a unicidade e a associação física precisam de controlo.

Idempotência — Propriedade pela qual processar repetidamente a mesma mensagem não duplica o efeito empresarial.

Incerteza de medição — Parâmetro não negativo que caracteriza a dispersão dos valores atribuídos à mensuranda, com base na informação utilizada.

Interoperabilidade — Capacidade de sistemas trocarem dados e utilizá-los com estrutura, significado e processos compatíveis.

IoT — Internet das Coisas: sistema em que entidades físicas são observadas, identificadas ou atuadas através de componentes digitais e redes.

Latência — Tempo entre um acontecimento e a disponibilidade ou ação resultante; deve ser especificado entre pontos concretos.

Lote — Quantidade definida de produto ou material considerada como uma unidade segundo critérios do processo e requisitos aplicáveis.

Mensuranda — Grandeza que se pretende medir.

Metadado — Dado que descreve outro dado, como origem, unidade, qualidade, versão ou condições de recolha.

Modo degradado — Forma de operação controlada quando uma capacidade está indisponível ou limitada.

Observabilidade — Capacidade de compreender o estado interno de um sistema através de métricas, registos, diagnósticos e eventos.

Pista de auditoria — Sequência protegida de ações e alterações que permite reconstruir quem fez o quê e quando.

Publicação/subscrição (publish/subscribe) — Padrão de comunicação em que produtores publicam mensagens em tópicos e consumidores subscrevem os tópicos necessários.

Plataforma IoT — Conjunto de serviços para gerir dispositivos, receber, processar, conservar e disponibilizar dados IoT.

Reconciliação — Comparação sistemática entre fontes ou estados para identificar e resolver diferenças.

Rastreabilidade — Capacidade de seguir o movimento, a história, a aplicação ou a localização de uma entidade através de registos relacionados. No domínio alimentar e dos alimentos para animais, aplicar também a definição e as obrigações legais específicas do Regulamento (CE) n.º 178/2002.

Resolução — Menor alteração que um sistema de medição consegue indicar nas condições especificadas.

Sensor — Elemento de um sistema de medição diretamente afetado pelo fenómeno, corpo ou substância que transporta a grandeza a medir, fornecendo um sinal relacionado com essa grandeza.

Semântica — Significado partilhado de dados, identificadores, estados e relações.

Sistema de registo — Sistema autorizado a conservar o estado oficial de uma categoria de informação.

Telemetria — Recolha e transmissão remota de medições, estados ou diagnósticos.

Validação — Confirmação, por evidência objetiva, de que requisitos para um uso ou aplicação específicos foram cumpridos.

Verificação — Confirmação, por evidência objetiva, de que requisitos especificados foram cumpridos.

REFERÊNCIA RÁPIDA

Siglas e acrónimos

API	Application Programming Interface — interface de programação de aplicações
BLE	Bluetooth Low Energy
CMMS	Computerized Maintenance Management System — sistema informatizado de gestão da manutenção
EPCIS	Electronic Product Code Information Services
ERP	Enterprise Resource Planning
GS1	Organização internacional, neutra e sem fins lucrativos, que desenvolve e mantém normas globais de identificação, captura e partilha de dados nas cadeias de valor
HACCP	Hazard Analysis and Critical Control Point — análise de perigos e pontos críticos de controlo
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
IoT	Internet of Things — Internet das Coisas
ISO	International Organization for Standardization
LTE-M	Long-Term Evolution for Machines
MES	Manufacturing Execution System
MQTT	Protocolo leve de transporte de mensagens cliente-servidor baseado em publicação/subscrição (designação do protocolo no padrão OASIS MQTT 5.0)
NB-IoT	Narrowband Internet of Things
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OPC UA	Open Platform Communications Unified Architecture
QMS	Quality Management System — sistema de gestão da qualidade
RFID	Radio-Frequency Identification
RGPD	Regulamento Geral sobre a Proteção de Dados
SRI 2	Diretiva (UE) 2022/2555, transposta em Portugal pelo Decreto-Lei n.º 125/2025, de 4 de dezembro
TMS	Transportation Management System
W3C	World Wide Web Consortium
Wi-Fi	Família de tecnologias de rede local sem fios

WMS	Warehouse Management System – sistema de gestão de armazém
------------	--

FONTES VERIFICADAS

Bibliografia

Estado, versão, âmbito e ligação oficial verificados em julho de 2026; normas verificadas pela respetiva ficha institucional.

[1] 3GPP. 3GPP TR 36.802 - Narrowband Internet of Things (NB-IoT). Sophia Antipolis: 3rd Generation Partnership Project.

[Consulte a fonte oficial.](#)

[2] 3GPP. 3GPP TR 36.888 - Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE. Sophia Antipolis: 3rd Generation Partnership Project.

[Consulte a fonte oficial.](#)

[3] BLUETOOTH SIG. Bluetooth Core Specification 6.2 e recursos técnicos de Bluetooth Low Energy. Kirkland: Bluetooth Special Interest Group.

[Consulte a fonte oficial.](#)

[4] CODEX ALIMENTARIUS. CXC 1-1969 - General Principles of Food Hygiene. Roma: FAO/WHO, 2023, revisto em 2022.

[Consulte a fonte oficial.](#)

[5] CODEX ALIMENTARIUS. CXC 44-1995 - Code of Practice for Packaging and Transport of Fresh Fruit and Vegetables. Roma: FAO/WHO, alterado em 2004. Aberta - PDF oficial Codex/FAO.

[Consulte a fonte oficial.](#)

[6] CODEX ALIMENTARIUS. CXC 47-2001 - Code of Hygienic Practice for the Transport of Food in Bulk and Semi-Packed Food. Roma: FAO/WHO, 2001. Aberta - PDF oficial Codex/FAO.

[Consulte a fonte oficial.](#)

[7] ENISA. Baseline Security Recommendations for IoT in the Context of Critical Information Infrastructures. Atenas: European Union Agency for Cybersecurity, 2017.

[Consulte a fonte oficial.](#)

[8] ENISA. Guidelines for Securing the Internet of Things - Secure Supply Chain for IoT. Atenas: European Union Agency for Cybersecurity, 2020.

[Consulte a fonte oficial.](#)

[9] GS1. *EPCIS Standard*, Release 2.0, e *Core Business Vocabulary (CBV) Standard*, Release 2.0. Bruxelas: GS1 AISBL, 2022.

Consulte as fontes oficiais: [EPCIS Standard](#); [Core Business Vocabulary \(CBV\) Standard](#).

[10] GS1. GS1 Global Traceability Standard, versão 2.0. Bruxelas: GS1 AISBL, 2017.

[Consulte a fonte oficial.](#)

[11] IEEE 802.1. Time-Sensitive Networking Task Group - mecanismos de conectividade determinística em redes IEEE 802. Nova Iorque: Institute of Electrical and Electronics Engineers.

[Consulte a fonte oficial.](#)

[12] ILAC. ILAC P14 - ILAC Policy for Measurement Uncertainty in Calibration. International Laboratory Accreditation Cooperation, 2020.

[Consulte a fonte oficial.](#)

[13] ISO. *Food safety management - ISO 22000:2018*. Genebra: International Organization for Standardization, 2018. Aberta - brochura oficial gratuita da ISO; a norma ISO 22000:2018 integral é documento normativo sujeito a aquisição.

[Consulte a fonte oficial.](#)

[14] ITU-T. Recommendation ITU-T Y.4000/Y.2060 - Overview of the Internet of Things. Genebra: International Telecommunication Union, 2012.

[Consulte a fonte oficial.](#)

[15] JCGM. JCGM 200:2012 - International Vocabulary of Metrology - Basic and general concepts and associated terms (VIM), 3.ª edição.

[Consulte a fonte oficial.](#)

[16] LORA ALLIANCE. LoRaWAN Specification, versão 1.1. Fremont: LoRa Alliance, 2017.

[Consulte a fonte oficial.](#)

[17] NIST. NIST IR 8259 Rev. 1 - Foundational Cybersecurity Activities for IoT Product Manufacturers. Gaithersburg: National Institute of Standards and Technology, 2026.

[Consulte a fonte oficial.](#)

[18] NIST. NIST IR 8259A - IoT Device Cybersecurity Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2020.

[Consulte a fonte oficial.](#)

[19] NIST. NIST IR 8259B - IoT Non-Technical Supporting Capability Core Baseline. Gaithersburg: National Institute of Standards and Technology, 2021.

[Consulte a fonte oficial.](#)

[20] NIST. NIST SP 500-325 - Fog Computing Conceptual Model. Gaithersburg: National Institute of Standards and Technology, 2018.

[Consulte a fonte oficial.](#)

[21] NIST. NIST SP 1500-203 - Framework for Cyber-Physical Systems: Timing Annex. Gaithersburg: National Institute of Standards and Technology, 2017.

[Consulte a fonte oficial.](#)

[22] OASIS. MQTT Version 5.0. OASIS Standard, 2019.

[Consulte a fonte oficial.](#)

[23] OPC FOUNDATION. OPC Unified Architecture - série IEC 62541. Scottsdale: OPC Foundation.

[Consulte a fonte oficial.](#)

[24] PORTUGAL. Decreto-Lei n.º 125/2025, de 4 de dezembro, que aprova o Regime Jurídico da Cibersegurança e transpõe a Diretiva (UE) 2022/2555. Diário da República.

[Consulte a fonte oficial.](#)

[25] UNIÃO EUROPEIA. Regulamento (CE) n.º 178/2002, de 28 de janeiro de 2002, que determina os princípios e normas gerais da legislação alimentar, cria a Autoridade Europeia para a Segurança dos Alimentos e estabelece procedimentos em matéria de segurança dos géneros alimentícios. Jornal Oficial das Comunidades Europeias.

[Consulte a fonte oficial.](#)

[26] UNIÃO EUROPEIA. Regulamento (CE) n.º 852/2004, de 29 de abril de 2004, relativo à higiene dos géneros alimentícios. Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[27] UNIÃO EUROPEIA. Regulamento (CE) n.º 853/2004, de 29 de abril de 2004, que estabelece regras específicas de higiene aplicáveis aos géneros alimentícios de origem animal. Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[28] UNIÃO EUROPEIA. Regulamento (UE) 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (RGPD). Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[29] UNIÃO EUROPEIA. Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2). Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[30] UNIÃO EUROPEIA. Regulamento (UE) 2023/2854, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização (Regulamento dos Dados). Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[31] UNIÃO EUROPEIA. Regulamento (UE) 2024/2847, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais (Regulamento Ciber-Resiliência). Jornal Oficial da União Europeia.

[Consulte a fonte oficial.](#)

[32] W3C. Web of Things (WoT) Architecture 1.1. W3C Recommendation, 5 de dezembro de 2023.

[Consulte a fonte oficial.](#)

[33] W3C. Web of Things (WoT) Thing Description 1.1. W3C Recommendation, 5 de dezembro de 2023.

[Consulte a fonte oficial.](#)

Créditos visuais

Identidade gráfica e fundos de página: AgroNet Forward. Diagramas e infografias: elaboração original para este guia. Imagens editoriais: composições visuais produzidas com apoio de ferramentas de inteligência artificial e selecionadas pela equipa técnica; não constituem registos de instalações, empresas ou operações reais. Não foram utilizadas fotografias de terceiros.

Ficha técnica

Designação do Projeto | AgroNet Forward – Digitalizar o agroalimentar do Douro Tâmega

N.º do projeto | 25447

Promotores |

ADCEIDT – Associação de Desenvolvimento, Criatividade, Empreendedorismo e Inovação do Douro Tâmega

UTAD - Universidade de Trás-os-Montes e Alto Douro

Aviso | COMPETE2030-2025-4

Designação do aviso | Ações Coletivas – Digitalização

Tipologia de Ação | Transição Digital das Empresas

Objetivos | Aproveitar as vantagens da digitalização para os cidadãos, as empresas, os organismos de investigação e as autoridades públicas (FEDER)

Edição e conteúdos | ADCEIDT

Guia n.º 2 | versão 1.0 | julho de 2026

A publicação tem finalidade de capacitação. A aplicação a uma empresa exige análise do processo, do produto, do risco, da legislação em vigor e dos requisitos contratuais. As designações de normas e protocolos não constituem recomendação comercial nem certificação.

