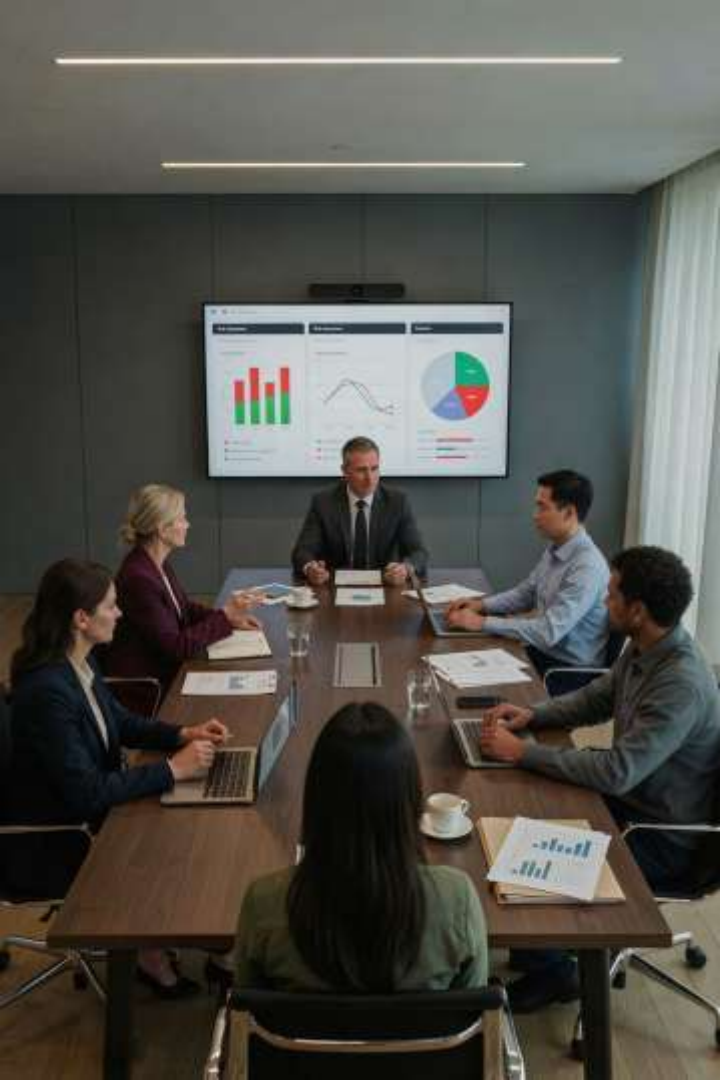


CAPÍTULO 5 — RISCO E FLEXIBILIDADE

Do "Ação Preventiva" ao Pensamento Baseado em Risco

A ISO/IEC 17020:2026 realizou uma **transição filosófica profunda**: o conceito clássico de "ação preventiva" foi completamente retirado. Um sistema reativo — que aguarda o surgimento de potenciais desvios para então propor ações — foi substituído por uma mentalidade sistemática e integrada de **gestão de riscos e oportunidades** sob a nova **Cláusula 8.4**. O organismo é agora formalmente obrigado a planejar e implementar ações estruturadas de forma proativa, com duplo objetivo: mitigar falhas na validade técnica dos relatórios e capturar oportunidades de melhoria e expansão de escopo.

CAPÍTULO 5 — RISCO E FLEXIBILIDADE

O "Risk Loop" Integrado da ISO/IEC 17020:2026

Identificação na Base

Monitoramento contínuo de ameaças à imparcialidade e conflitos de interesse (Cláusula 4.1.3)

Aprovação Executiva

Resultados e registro de riscos aprovados formalmente na Análise Crítica pela Administração (Cláusula 8.7)

Consolidação e Planejamento

Ameaças mapeadas são registradas, avaliadas e convertidas em ações práticas de mitigação (Cláusula 8.4)

Auditoria Baseada em Risco

Eficácia das ações mitigadoras verificada no programa de auditorias internas (Cláusula 8.6)

CAPÍTULO 5 — RISCO E FLEXIBILIDADE

Análise de Impacto em Inspeções Anteriores (Cláusula 8.5)

Este é um dos requisitos de maior impacto operacional introduzidos pela ISO/IEC 17020:2026. Ignorá-lo configura não-conformidade maior.

A Cláusula 8.5.5 exige que, sempre que uma falha ou desvio operacional for identificado, o organismo execute uma **análise de impacto técnica abrangente sobre resultados de inspeções anteriores**. Se um equipamento foi usado com calibração vencida ou um inspetor não seguiu o método prescrito, **não é suficiente registrar apenas uma ação corretiva isolada** — é necessário rastrear e reavaliar sistematicamente todas as inspeções executadas anteriormente com aquele recurso.

1

Notificar o Cliente

Comunicado formal detalhando o desvio e seu impacto técnico no laudo emitido

2

Recall de Trabalho

Recall físico para re-inspeção imediata ou invalidação formal da declaração de conformidade

3

Notificar Autoridades

Comunicar proativamente à autoridade reguladora e ao organismo de acreditação

CAPÍTULO 6 — DADOS E TECNOLOGIA

A Nova Cláusula 7.5 — Controle de Dados e Informações

A digitalização acelerada dos organismos de inspeção — com relatórios eletrônicos, bases de dados em nuvem e assinaturas digitais — exigiu a criação de requisito robusto e inédito. A **Cláusula 7.5** é uma seção inteiramente nova, sem equivalente nas edições anteriores da norma, dedicada exclusivamente ao controle de dados e informações relevantes para as atividades de inspeção.

CAPÍTULO 6 — DADOS E TECNOLOGIA

Requisitos Técnicos da Cláusula 7.5

Validação Prévia Mandatória

Todo software ou sistema computacional — incluindo apps móveis, bancos de dados, planilhas e sistemas integrados — deve ser **formalmente validado** antes da implementação operacional.

Controle de Mudanças

Atualizações de sistemas, configurações de rede e modificações de código exigem processos formais de **autorização, documentação e revalidação** de conformidade.

Integridade e Cibersegurança

Dados técnicos devem ser protegidos contra acesso não autorizado, adulteração, sabotagem e perda física, exigindo implementação de **logs de auditoria intransferíveis**.

Registro de Falhas

Todas as falhas de sistema devem ser **documentadas e analisadas**, com especificação das ações de contenção e corretivas para restabelecer integridade dos dados.

CAPÍTULO 6 — DADOS E TECNOLOGIA

Inspeção Remota e Inteligência Artificial

Tecnologias Reconhecidas pela Norma

A ISO/IEC 17020:2026 reconhece explicitamente o uso de técnicas de inspeção remota, realidade aumentada (AR) e inteligência artificial (IA) para processamento de dados e classificação visual de falhas. Entretanto, exige validação criteriosa de parâmetros adicionais.

Inspeções Remotas com Câmera/Vídeo

O organismo deve demonstrar que resolução de imagem, controle de iluminação, latência de rede e largura de banda são tecnicamente adequados, sem introduzir "pontos cegos" que prejudiquem a acuidade da avaliação versus avaliações presenciais.

Validação de Algoritmos de IA

Se o organismo utiliza IA ou visão computacional para identificação automatizada de defeitos:

- O **modelo de IA** deve ser formalmente validado
- O **conjunto de dados de treinamento** deve ser documentado
- Exige-se **rastreabilidade metrológica** e transparência sobre decisões automatizadas

CAPÍTULO 6 — DADOS E TECNOLOGIA

O Problema da Confiança Multipartidária

Em processos que envolvem fabricante (Parte A), organismo de inspeção de terceira parte (Parte B) e cliente/proprietário (Parte C), a guarda de registros em sistemas de TI centralizados de uma única parte introduz o **"problema da confiança multipartidária"**. Arquivos em SharePoint ou servidores gerenciados por uma única organização estão vulneráveis a adulterações indetectáveis — logs de auditoria podem ser editados, datas retroagidas — comprometendo força probatória em disputas comerciais e exames judiciais de responsabilidade técnica.

A solução técnica de excelência apresentada pela norma é a aplicação de **blockchain permissionada** para governança e custódia segura de dados de inspeção.

CAPÍTULO 6 — DADOS E TECNOLOGIA

Blockchain Permissionada como Solução de Custódia

Geração do Hash SHA-256

No instante de geração do relatório, o arquivo é submetido a algoritmo SHA-256, gerando assinatura digital única — a "impressão digital" inviolável do documento.

Ancoragem no Ledger Distribuído

O hash, a identidade criptograficamente verificada do inspetor e o timestamp inviolável são ancorados em ledger imutável de blockchain permissionada (ex.: Hyperledger Fabric).

Detecção Instantânea de Adulterações

Qualquer alteração no relatório — mesmo de um único caractere — gera hash completamente diferente. Qualquer terceiro autorizado pode validar autenticidade instantaneamente, recalculando o hash e comparando com o ledger.

CAPÍTULO 6 — DADOS E TECNOLOGIA

Benefícios Estratégicos da Arquitetura Blockchain

Proteção Legal

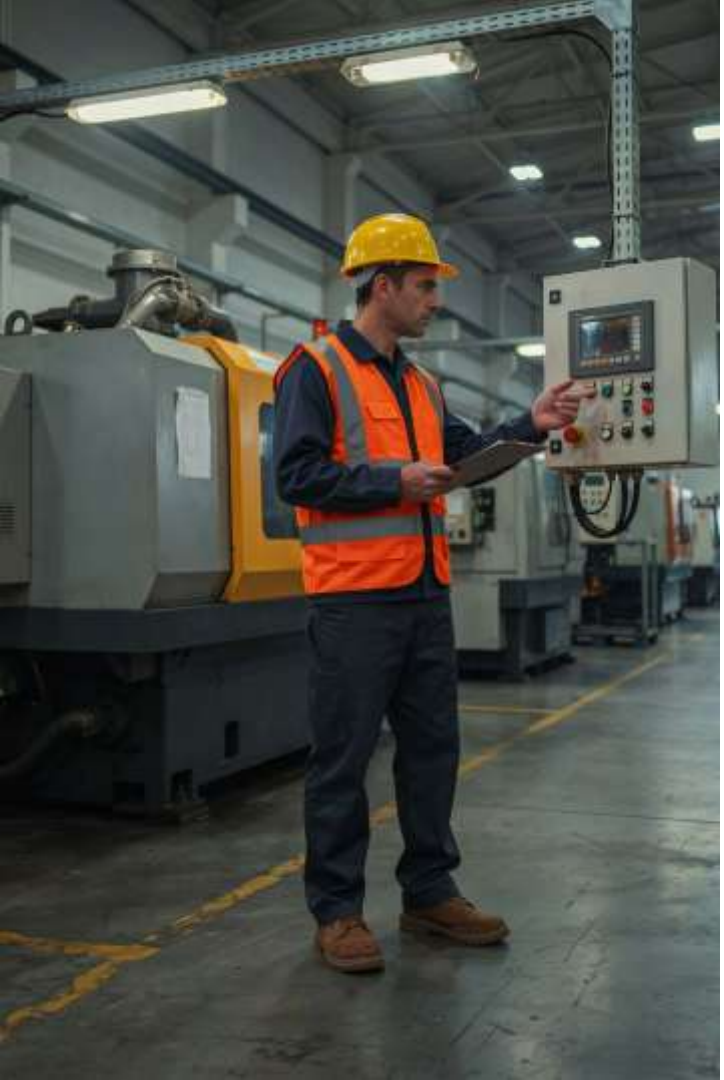
Barreira inviolável contra acusações de falsificação de dados em disputas comerciais e processos judiciais de responsabilidade técnica

Conformidade Avançada

Demonstração técnica de conformidade robusta com as exigências de salvaguarda de dados da Cláusula 7.5 da ISO/IEC 17020:2026

Diferenciação de Mercado

Diferenciação mercadológica relevante em processos competitivos de contratação técnica, por meio da abordagem "verify-it-yourself"



CAPÍTULO 7 — RECURSOS E PROVEDORES

Competência de Pessoal e Monitoramento em Campo (Cláusula 6.1)

A ISO/IEC 17020:2026 muda o foco da gestão de pessoal: de qualificações estáticas para uma **avaliação dinâmica e contínua de competência prática em campo**. A norma ajusta a redação para exigir que o organismo tenha *"acesso a um número suficiente"* de pessoal competente, normatizando o uso regular de inspetores contratados sob demanda, especialistas terceirizados e consultores associados — desde que submetidos ao sistema de gestão do organismo.

CAPÍTULO 7 — RECURSOS E PROVEDORES

Programa de Monitoramento de Inspetores em Campo

1

Observação Sistemática em Campo

Inspetores em exercício são observados por inspetores seniores autorizados durante a execução de suas atividades (Cláusula 6.1.5).

2

Fundamento Baseado em Risco

O programa deve considerar riscos e complexidades da inspeção, histórico de desempenho técnico anterior e novas tecnologias implementadas.

3

Resposta a Atualizações

Novas atualizações metodológicas, legislativas ou tecnológicas devem ser incorporadas ao programa de monitoramento de forma documentada e fundamentada.

CAPÍTULO 7 — RECURSOS E PROVEDORES

Verificações em Serviço de Equipamentos (Cláusula 6.4)

Nova Obrigatoriedade — In-Service Checks

A Cláusula 6.4.4 introduz a obrigatoriedade de **procedimentos documentados para verificações em serviço** de todos os equipamentos de medição de influência significativa nos resultados de inspeção.

O organismo deve definir **técnicas e frequências** para verificar se os instrumentos mantêm precisão metrológica aceitável **entre as calibrações formais**.

Por Que Isso É Crítico?

A calibração periódica formal é necessária, mas não suficiente. Instrumentos podem sofrer desvios entre calibrações — em condições de campo, transporte, impactos ou variações térmicas. As **verificações em serviço** minimizam de forma controlada o risco de medições com desvios não detectados durante operações em campo, protegendo a validade técnica dos relatórios emitidos.

A Expansão do Conceito de Provedores Externos (Cláusula 6.3)

Na edição de 2012, o controle externo limitava-se à subcontratação direta de inspeção. A nova norma realizou uma **expansão conceitual severa e mandatória**: a Cláusula 6.3 passa a cobrir qualquer produto ou serviço de terceiros que possa influenciar a validade técnica das atividades de inspeção.

Serviços de Calibração

Fornecedores de calibração metrológica e laboratórios de ensaios de apoio

Empresas de NDT

Terceirizados de ensaios não destrutivos e consultores técnicos especialistas

Software e TI

Desenvolvedores de software de inspeção personalizado e provedores de infraestrutura de rede e nuvem

Auditores Internos

Consultorias responsáveis pela execução de auditorias internas terceirizadas

O organismo deve manter registro compulsório e documentado de todos os provedores externos aprovados, com avaliações de admissão e revisões periódicas anuais de desempenho.

CAPÍTULO 8 — MATRIZ COMPARATIVA

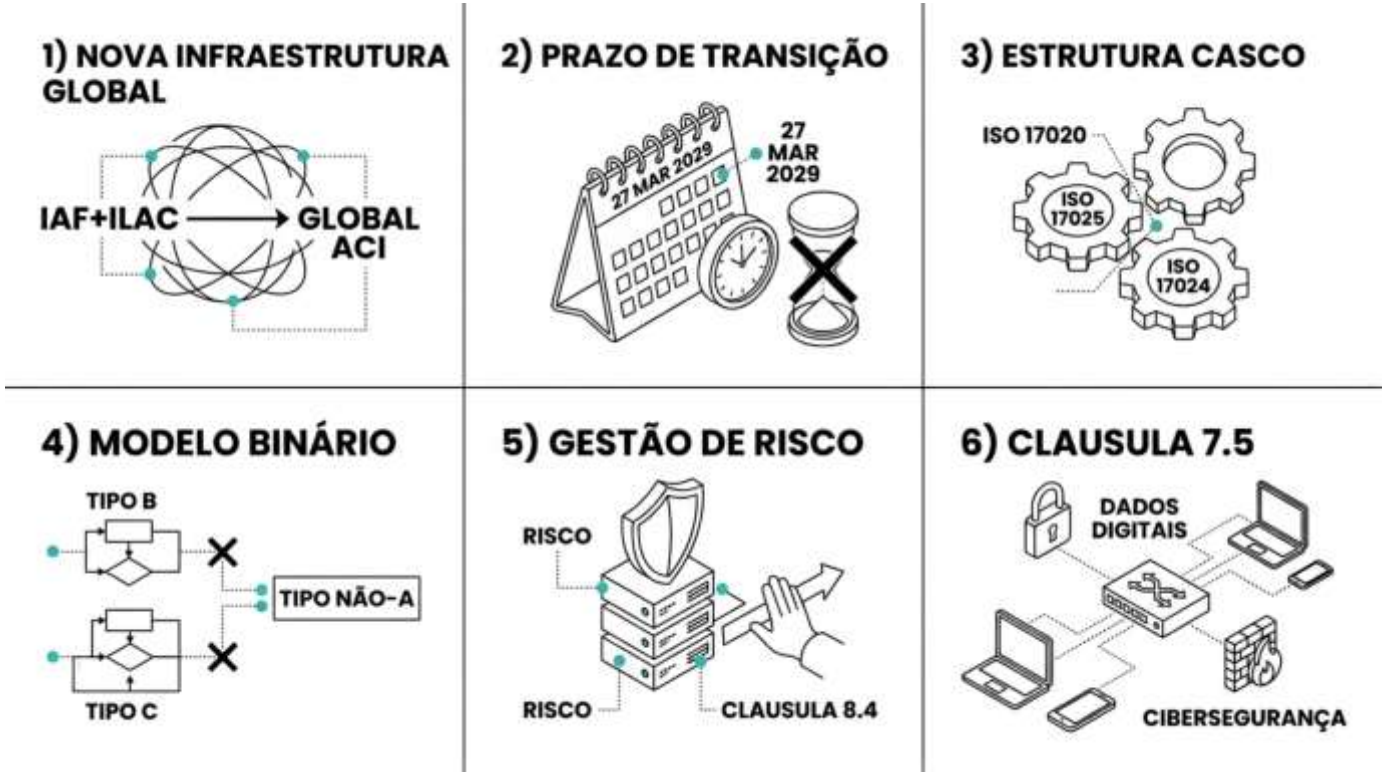
Matriz de Comparação Cláusula a Cláusula: 2012 vs. 2026

ISO 17020:2012	ISO 17020:2026	Natureza da Mudança
Título da Norma	Título da Norma	Removida a expressão "vários tipos de", refletindo aplicabilidade universal
4.1 Imparcialidade	4.1 Imparcialidade	Reforço no monitoramento contínuo de ameaças e mapeamento de relações técnicas
5.1 Independência	5.1 + Anexo A	Transição do modelo tripartite (A/B/C) para modelo binário (Tipo A / não-A)
6.1 Pessoal	6.1 Personnel	Foco em "acesso a pessoal competente" e monitoramento contínuo em campo
6.3 Subcontratação	6.3 Externally Provided Services	Expansão drástica de controle para abranger TI, nuvem, calibração e auditores internos
— (sem equivalente)	7.5 Control of Data	**Nova cláusula** — controle de dados digitais, integridade e validação de software
8.5 Ações Corretivas e Prev.	8.4 Riscos e Oportunidades	Ação preventiva abolida; integrada à mentalidade baseada em risco (Cláusula 8.4)

Matriz Comparativa — Continuação

ISO 17020:2012	ISO 17020:2026	Natureza da Mudança
4.2 Confidencialidade	4.2 Confidentiality	Exigência de compromissos juridicamente vinculativos e cibersegurança correlata
5.2 Estrutura Administrativa	5.2 Legal Entity & Liabilities	Fusão e expansão de requisitos de análise de risco de responsabilidade civil
5.3 Organização	5.3 Organization & Management	Definição formal de technical management competente e funções técnicas
6.2 Instalações e Equipamentos	6.2 Facilities & Equipment	Inclusão de in-service checks e controle detalhado de novas tecnologias de TI
7.1 Exame de Contratos	7.1 Review of Requests & Contracts	Inclusão de verificação prévia obrigatória de riscos de imparcialidade no contrato
7.2 Métodos de Inspeção	7.2 Inspection Methods & Procedures	Definição de métodos não-padrão e validação obrigatória no uso de novas tecnologias
7.3 Amostragem e Amostras	7.3 Handling of Items	Uso unificado do termo "item", com proteção detalhada contra deterioração

Visão Panorâmica das Mudanças Estruturais



A ISO/IEC 17020:2026 representa a maior atualização da norma de inspeção em mais de uma década, com impacto simultâneo em governança global, estrutura da norma, vocabulário técnico, gestão de independência, pensamento baseado em risco e requisitos de tecnologia da informação.

Plano de Ação Recomendado para Organismos de Inspeção

1 Realizar Gap Analysis Imediato

Mapear lacunas entre o sistema de gestão atual e os requisitos da ISO/IEC 17020:2026, priorizando as Cláusulas 7.5, 8.4, 8.5 e o Anexo A (modelo binário).

2 Atualizar Documentação e Vocabulário

Retirar dos manuais e procedimentos os termos descontinuados (Tipo B, Tipo C, ação preventiva, subcontratação) e substituir pelas novas nomenclaturas.

3 Implementar Controles de Dados (Cláusula 7.5)

Validar formalmente todos os softwares, estabelecer procedimentos de controle de mudanças e implementar logs de auditoria para todos os sistemas de TI relevantes.

4 Preparar para Auditoria de Transição

Submeter o proforma de Gap Analysis ao organismo de acreditação com antecedência e treinar a equipe técnica nas novas exigências antes da auditoria de transição.

Datas Críticas Consolidadas para 2026–2029

Mar/2026

Publicação ISO/IEC 17020:2026 — início do período de transição global

Abr/2026

Lançamento da GAC MRA Mark para uso oficial imediato

Jun–Set/2026

IAS (EUA) inicia e torna mandatória a nova norma para todos os solicitantes

Set/2026

UKAS (UK) inicia avaliações e aceita apenas novas acreditações sob a versão 2026

Jan/2027

SAC (Singapura) inicia avaliações exclusivamente sob ISO/IEC 17020:2026 para novos solicitantes

Jan/2028

UKAS e SAC: todas as auditorias obrigatoriamente sob a nova versão, sem exceções

Jan/2029

Descontinuação definitiva das marcas IAF MLA e ILAC MRA em relatórios e certificados

Mar/2029

Prazo final absoluto: acreditações sob ISO/IEC 17020:2012 perdem validade jurídica e reconhecimento GAC MRA

Principais Takeaways desta Atualização Técnica

Uma Única Entidade Global

IAF + ILAC = Global ACI. O GAC MRA substitui todos os acordos anteriores. Atualize referências regulatórias e contratuais agora.

Modelo Binário de Independência

Tipos B e C extintos. Apenas Tipo A e Tipo não-A. Revise sua classificação e implemente as salvaguardas correspondentes.

Pensamento Baseado em Risco

"Ação preventiva" abolida. O Risk Loop integrado (Cláusula 8.4) é o novo padrão. Documente riscos e oportunidades proativamente.

Cláusula 7.5 — Inovação Crítica

Validação de software, controle de mudanças, logs de auditoria e cibersegurança são agora requisitos normativos explícitos.

Conformidade como Vantagem Competitiva

A ISO/IEC 17020:2026 não é apenas uma atualização normativa — é uma **reconfiguração estratégica** da infraestrutura global de confiança em inspeção. Organismos que antecipam a transição, investem em sistemas robustos de gestão de risco, e demonstram domínio das novas exigências de dados e independência serão percebidos pelo mercado global como parceiros de conformidade de excelência. O prazo de **27 de março de 2029** é improrrogável — mas a oportunidade de diferenciação começa agora.

GLOBAL ACI · ISO/IEC 17020:2026 · AGOSTO 2026