ÁREA TEMÁTICA: TECNOLOGIA, INTELIGÊNCIA ARTIFICIAL E TRANSFORMAÇÃO DIGITAL EM ADMINISTRAÇÃO

LINHA DE BASE DE CONTROLES DE SEGURANÇA DA INFORMAÇÃO PARA MITIGAÇÃO DOS RISCOS DE NEGÓCIO NO SETOR DE SANEAMENTO

Resumo: O setor de saneamento opera infraestruturas críticas cuja continuidade depende da integração entre Tecnologia da Informação (TI) e Tecnologia da Automação (TA), o que transforma a segurança da informação em requisito para a prestação de serviços essenciais à população. Os referenciais de controles disponíveis, contudo, foram concebidos para ambientes corporativos e não contemplam as especificidades das companhias brasileiras de água e esgoto. O objetivo deste estudo é propor uma linha de base de controles de segurança da informação para mitigação dos riscos de negócio em organizações de saneamento. Trata-se de pesquisa aplicada, exploratória e descritiva, de abordagem mista, conduzida como estudo de caso em uma empresa brasileira de saneamento de grande porte, em três fases. A primeira empregou dez entrevistas semiestruturadas com gestores e técnicos de TA, tratadas por análise de conteúdo e estruturadas pela técnica Bow-Tie. A segunda utilizou grupos focais com especialistas internos para mapear riscos operacionais de automação e associá-los aos controles do NIST SP 800-53 Rev. 5. A terceira categorizou esses controles por função de segurança e propôs controles complementares setoriais. Foram identificados dez riscos de negócio e um conjunto de riscos operacionais de TA, conectados por matrizes de rastreabilidade que evidenciam as famílias de controle de acesso, proteção física e auditoria como as mais transversais. A integração dos controles do NIST com dez controles complementares resulta em uma linha de base aplicável à empresa estudada e adaptável a companhias de perfil semelhante, demonstrando que medidas exclusivamente tecnológicas são insuficientes.

Palavras-chave: Segurança da informação. Controles NIST SP 800-53. Infraestrutura crítica. Automação industrial. Bow-Tie.

Abstract: The sanitation sector operates critical infrastructures whose continuity depends on the integration of Information Technology (IT) and Operational Technology (OT), which turns information security into a requirement for the delivery of essential services to the population. Available control frameworks, however, were designed for corporate environments and do not address the specificities of Brazilian water and wastewater utilities. The objective of this study is to propose a baseline of information security controls for mitigating business risks in sanitation organizations. This is an applied, exploratory, and descriptive research with a mixed-methods approach, conducted as a case study in a large Brazilian sanitation company, in three

phases. The first employed ten semi-structured interviews with OT managers and technicians, processed through content analysis and structured using the Bow-Tie technique. The second used focus groups with internal specialists to map operational automation risks and associate them with the controls of NIST SP 800-53 Rev. 5. The third categorized these controls by security function and proposed complementary sector-specific controls. Ten business risks and a set of OT operational risks were identified, connected by traceability matrices that highlight the access control, physical protection, and audit families as the most cross-cutting. Integrating NIST controls with ten complementary controls results in a baseline applicable to the studied company and adaptable to utilities of similar profile, demonstrating that exclusively technological measures are insufficient.

Keywords: *Information security. NIST SP 800-53 controls. Critical infrastructure. Industrial automation. Bow-Tie.*

1. Introdução

O saneamento básico é uma infraestrutura essencial para a saúde pública e a qualidade de vida. Companhias estaduais e distritais operam extensas redes de abastecimento e esgotamento, dependentes da integração entre Tecnologia da Informação (TI) e Tecnologia da Automação (TA), cujos sistemas de controle exigem elevados níveis de disponibilidade e segurança, impactando diretamente a continuidade dos serviços (Stouffer et al., 2015; AWWA, 2014).

Casos reais evidenciam esses riscos. Em 2021, um ataque à estação de Oldsmar (EUA) explorou vulnerabilidades de acesso remoto para alterar parâmetros químicos da água (G1, 2021). Em 2020, sistemas em Israel sofreram tentativas semelhantes (INCIBE-CERT, 2020). Em 2000, na Austrália, um ex-funcionário manipulou o sistema SCADA e causou transbordamentos de esgoto (Abrams & Weiss, 2008). Tais eventos reforçam a necessidade de controles específicos para o setor.

No Brasil, o marco regulatório amplia essas exigências, com a Lei Geral de Proteção de Dados (Brasil, 2018) e a Estratégia Nacional de Segurança Cibernética (Brasil, 2025). A literatura aponta desafios de governança, infraestrutura e cultura organizacional (Georg et al., 2022), além de diferenças na percepção de risco entre atores do setor (Shapira et al., 2021).

A gestão de riscos em saneamento possui especificidades não totalmente cobertas por *frameworks* genéricos, devido às características da TA (NIST, 2023). Assim, investiga-se quais controles devem compor uma linha de base para mitigação de riscos em ambientes integrados de TA, assumindo-se que essa linha requer controles técnicos, organizacionais e de gestão de pessoas.

O objetivo é propor essa linha de base, com base em estudo de caso em uma empresa brasileira. Especificamente, busca-se identificar riscos de negócio, mapear riscos operacionais de TA, associá-los ao NIST SP 800-53 Rev. 5, construir matriz de rastreabilidade e propor controles setoriais. A análise limita-se à TA, e os dados quantitativos são ilustrativos devido à confidencialidade.

Este artigo está organizado da seguinte forma: a seção 2 apresenta a fundamentação teórica sobre risco, controles e frameworks de segurança, além dos trabalhos correlatos; a seção 3 detalha a metodologia em três fases; a seção 4 apresenta e discute os resultados; e a seção 5 retoma os objetivos, expõe as contribuições, as limitações e a agenda de pesquisas futuras.

2. Referencial Teórico

2.1 Risco, categorias e gestão de riscos

O risco é o efeito da incerteza sobre os objetivos, entendido como desvio em relação ao esperado (ABNT, 2018). Embora possa representar oportunidade ou ameaça, na segurança da informação refere-se geralmente ao potencial de ameaças explorarem vulnerabilidades e causarem danos à organização (IEC, 2018). Uma definição única de risco é inviável, pois seu significado depende do contexto (Aven et al., 2018).

Os riscos podem ser operacionais, legais, regulatórios, reputacionais, estratégicos ou de negócio; estes últimos frequentemente abrangem riscos estratégicos e reputacionais (Crouhy, Galai & Mark, 2014). Relacionam-se a incertezas sobre demanda, qualidade e custos, sendo relevantes quando afetam atividades críticas (Chapelle, 2019).

A gestão de riscos compreende atividades coordenadas para orientar e controlar a organização diante dos riscos (ABNT, 2018). Como elemento da governança e da estratégia (COSO, 2017), requer visão integrada dos riscos e de seus efeitos cumulativos nos objetivos (NIST, 2018). A avaliação envolve identificação, análise e avaliação, subsidiando decisões de tratamento e alocação de recursos (NIST, 2012).

A técnica Bow-Tie (ABNT, 2012; ISO, 2019), originária da indústria de óleo e gás, conecta uma árvore de falhas (causas) a uma árvore de eventos (consequências) por meio de um evento de topo. Ela mapeia ameaças, barreiras preventivas e mitigatórias e fatores escaladores. Sua aplicação em infraestrutura crítica é estratégica para visualizar cadeias completas de materialização de riscos e localizar barreiras insuficientes (CCPS, 2008).

2.2. Segurança da informação, controles e frameworks

A segurança da informação é a proteção de dados e sistemas contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação ou destruição, com o propósito de preservar confidencialidade, integridade e disponibilidade (Paulsen & Byers, 2019). A segurança cibernética, por sua vez, é entendida como a capacidade de proteger o uso do ambiente digital contra ações maliciosas, constituindo subconjunto do campo mais amplo da segurança da informação (Stanger, 2023; ISC2, 2023).

Os controles são instrumentos que viabilizam a segurança por meio de procedimentos, estruturas organizacionais e práticas administrativas, técnicas ou legais (Galegale, Fontes & Galegale, 2017). Sua seleção baseia-se na análise de riscos, embora uma linha de base mínima deva considerar aspectos do negócio, como funcionalidade e efetividade (Barnard & Solms, 2000). A implementação enfrenta limitações orçamentárias e impactos na produtividade (Yevseyeva et al., 2015).

Entre os principais frameworks estão as normas NBR ISO/IEC 27001, 27002 e 27005, o NIST Cybersecurity Framework, os CIS Controls, o COBIT, o MITRE ATT&CK e o NIST SP 800-53. Este estudo adota o NIST SP 800-53 Rev. 5 (NIST, 2020) pela granularidade, maturidade no setor público brasileiro, caráter aberto e compatibilidade com ambientes de TA via NIST SP 800-82 Rev. 3 (NIST, 2023). Contudo, reconhece-se que o catálogo foi concebido para TI corporativa, que a disponibilidade tende a ser prioritária em ambientes industriais e que normas como a ISA/IEC 62443 (ISA & IEC, 2018) podem ser mais adequadas a contextos específicos.

2.3. Trabalhos relacionados

A literatura sobre segurança da informação no setor público brasileiro concentra-se em órgãos dos três Poderes e em modelos genéricos de governança (Georg et al., 2022; Galegale, Fontes & Galegale, 2017; TCU, 2018; Machado, 2018), sem tratar da operação de companhias de saneamento e ambientes de TA própria desse setor. Os trabalhos sobre infraestrutura crítica oferecem princípios aplicáveis a sistemas de controle industrial e orientações de customização de controles para tecnologia operacional (Stouffer et al., 2015; NIST, 2023; AWWA, 2014), porém em perspectiva genérica e ancorada no contexto internacional. Os estudos sobre seleção de controles fornecem métodos formais e quantitativos, sem aplicação setorial (Barnard & Solms, 2000; Yevseyeva et al., 2015).

Dessa leitura emergem três lacunas convergentes: a ausência de estudos aplicados de segurança cibernética no saneamento brasileiro; a cobertura limitada de ambientes de automação pelos frameworks de TI tradicionais, cuja adaptação ao contexto nacional permanece pouco documentada; e a inexistência de correspondência direta entre o catálogo do NIST e exigências brasileiras como a ABNT NBR 5419, a Portaria GM/MS 888/2021, a Resolução 16/2019 do órgão regulador de saneamento e a LGPD.

Veale e Brown (2020) argumentam que a proteção efetiva requer visão que transcenda soluções exclusivamente tecnológicas, perspectiva que sustenta a hipótese deste trabalho, enquanto Ross, Winstead e McEvilley (2022) reforçam a necessidade de incorporar requisitos de segurança desde o projeto, o que justifica a presença de controles preventivos na linha de base proposta.

3. Metodologia

Trata-se de uma pesquisa aplicada, exploratória e descritiva, com abordagem mista (quali-quanti). Utilizou-se estudo de caso em uma empresa brasileira de saneamento de grande porte (Yin, 2015), combinando pesquisa bibliográfica, documental e análise de percepções de profissionais. Essa integração metodológica é adequada para explicar fenômenos complexos e sistematizar riscos em contextos reais de infraestrutura crítica (Creswell, 2014; Gil, 2019; Lakatos & Marconi, 2010).

Os procedimentos técnicos incluíram pesquisa bibliográfica e documental, que forneceu a base conceitual e as categorias de análise (Lakatos & Marconi, 2010), e estudo de caso em uma empresa brasileira de saneamento de grande porte, método adequado à compreensão de fenômenos contemporâneos inseridos em contexto real e complexo (Yin, 2015). A opção pela anonimização da organização é decisão metodológica deliberada, motivada pela natureza de

infraestrutura crítica do setor e pelos riscos associados à divulgação não controlada de informações sobre vulnerabilidades em sistemas de controle industrial. A separação entre o relatório técnico confidencial entregue à empresa e a versão pública assegura que a contribuição metodológica seja reproduzível sem expor detalhes operacionais sensíveis. O estudo foi estruturado em três fases sequenciais e integradas, conforme a Figura 1.



Figura 1 – Fases da metodologia.

Fonte: Autores (2026)

3.1 Fase 1: identificação e avaliação de riscos de negócio

A Fase 1 identificou e avaliou os riscos de negócio mais relevantes relacionados à segurança da informação. Foram realizadas dez entrevistas semiestruturadas, conduzidas entre agosto de 2025 e fevereiro de 2026, com participantes selecionados por amostragem não probabilística por conveniência segundo três critérios: atuação em cargos de gestão, análise ou operação em TI corporativa ou TA; mínimo de dois anos de experiência no cargo; e envolvimento direto com processos críticos do escopo. As entrevistas foram gravadas com autorização, transcritas integralmente e tiveram duração média de 45 a 60 minutos. O encerramento seguiu o critério de saturação teórica (Flick, 2009), observado quando as categorias temáticas passaram a se repetir sem emergência de novas causas ou consequências relevantes.

A análise seguiu a técnica de análise de conteúdo (Bardin, 2011), organizada em pré-análise, exploração do material e tratamento dos resultados, com codificação manual pela pesquisadora e revisão pelo orientador. As categorias emergiram do material e foram consolidadas em quatro grupos: causas de eventos de risco, consequências potenciais, controles existentes e contexto operacional. Em seguida, os riscos foram estruturados em diagramas Bow-Tie, o que permitiu visualizar a cadeia de efeitos desencadeada por falhas ou ataques. Convém destacar que a técnica Bow-Tie pertence ao campo da análise de risco e não se confunde com a análise de conteúdo, que pertence ao campo da pesquisa qualitativa.

3.2 Fase 2: levantamento de medidas de segurança e riscos operacionais

A Fase 2 aprofundou a identificação dos riscos técnicos e operacionais dos sistemas de automação e controle industrial, com foco exclusivo em TA. Foram conduzidos grupos focais com quatro especialistas internos, dois gestores e dois técnicos, técnica adequada à validação e ao aprofundamento colaborativo de achados qualitativos (Flick, 2009). Os participantes revisaram os riscos da Fase 1, discutiram as medidas de segurança existentes e identificaram riscos operacionais específicos, categorizados em áreas temáticas como controle de acesso e segregação, manutenção e gestão de ativos, capacitação e gestão de pessoas, disponibilidade e continuidade operacional, integridade de dados, segurança física, conformidade regulatória e gestão de prestadores de serviço.

Para cada risco operacional foram catalogados as suas causas, as suas consequências potenciais e o nível de risco inerente. A probabilidade e o impacto foram avaliados em escala de cinco pontos, a saber, Muito Baixo (1), Baixo (2), Médio (5), Alto (8) e Muito Alto (10). O produto entre probabilidade e impacto foi classificado em quatro categorias: Baixo (0 a 9,9), Moderado (10 a 39,9), Elevado (40 a 79,9) e Crítico (80 a 100). Comparou-se os riscos levantados aos controles do NIST SP 800-53 Rev. 5, adotado pela empresa. O critério de inclusão de um controle foi sua aplicabilidade direta ao risco em pelo menos um cenário operacional plausível, e o critério de exclusão foi a ausência de relação entre o objeto do controle e o vetor de ataque ou a consequência do risco. Por fim, construiu-se a matriz de rastreabilidade que conecta riscos operacionais e riscos de negócio, sendo cada correspondência contabilizada como uma conexão direta.

Ressalta-se que os dados da Tabela 2 são ilustrativos e simulados para fins didáticos. Essa opção metodológica preserva a confidencialidade da infraestrutura crítica estudada e evita a exposição de vulnerabilidades operacionais reais.

3.3 Fase 3: proposta de controles de segurança

A Fase 3 transformou os riscos priorizados em ações estruturadas, considerando o contexto organizacional, as restrições operacionais e o ambiente de infraestrutura crítica. Os controles do NIST foram categorizados por função de segurança e, a partir da identificação de lacunas frente a normas brasileiras, regulamentações setoriais e guias técnicos especializados, foram propostos controles complementares organizacionais, técnicos e processuais, alinhados a boas práticas reconhecidas (NIST, 2020; NIST, 2023) e ao nível de maturidade da organização.

3.4 Validação e ameaças à validade

Na Fase 1, a validação ocorreu pela análise de consistência interna dos dados das entrevistas e pela aplicação da técnica Bow-Tie. Na Fase 2, a validação foi realizada em grupo focal, segundo quatro critérios: coerência interna entre riscos operacionais e riscos de negócio; plausibilidade técnica e operacional dos cenários; exaustividade quanto às fases operacionais relevantes; e pertinência ao contexto regulatório. Os ajustes incorporados incluíram a reformulação de descrições para refletir a terminologia interna, a inclusão de riscos não cobertos pela proposta inicial e a remoção de associações risco-controle pouco aplicáveis ao ambiente.

Adotando a estrutura de Yin (2015), a validade de construto é sustentada pelo uso de múltiplas fontes de evidência, ainda que remanesça a ausência de dupla codificação independente. A validade interna apoia-se na triangulação entre as fases e na matriz de rastreabilidade, que explicita o caminho de inferência entre os dados e a linha de base. A validade externa é limitada pelo estudo de caso único, embora a metodologia seja transferível a companhias com características operacionais e regulatórias semelhantes. A confiabilidade é amparada pela descrição do protocolo de caso e pela documentação dos artefatos intermediários.

3.5 Justificativa da abordagem híbrida

A escolha por essa metodologia híbrida, combinando análise documental, APP, Bow Tie e NIST SP 800-53 Rev. 5, justifica-se por sua aderência ao problema de pesquisa e sua aplicabilidade em contextos reais de infraestrutura crítica. Ao utilizar métodos consolidados e *frameworks* reconhecidos globalmente (como NIST SP 800-53 e ISO 31000), o estudo garante rigor analítico e utilidade prática, contribuindo para a tomada de decisão estratégica na gestão de riscos cibernéticos na esfera pública (Mendes; Silva, 2017; International Organization for Standardization, 2018; International Organization for Standardization, 2022).

4. Análise e Discussão dos Resultados

Os resultados integrais da avaliação constam de relatório técnico confidencial entregue exclusivamente à empresa de saneamento. Esta seção tem por finalidade demonstrar a metodologia empregada nas três fases, de modo que outras organizações do setor possam reproduzi-la. Para tanto, são apresentados quatro riscos técnicos ilustrativos, identificados como RE-01 a RE-04 e suficientes para evidenciar como riscos de negócio e riscos técnicos podem ser construídos e relacionados. Os valores de probabilidade, impacto e nível de risco inerente exibidos são dados de simulação, elaborados para fins didáticos e sem correspondência com os resultados reais.

4.1 Fase 1: riscos de negócio

A consolidação das entrevistas resultou na definição de dez riscos de negócio considerados críticos para a companhia, apresentados na Tabela 1. Para cada um deles foram mapeadas as causas por meio de diagramas Bow-Tie, com destaque recorrente para falhas em estações elevatórias e de tratamento, ausência de redundância hidráulica e elétrica, manutenção preventiva insuficiente, falhas de integração entre TI e TA que atrasam respostas a incidentes, dependência de fornecedores terceirizados, compartilhamento inadequado de credenciais, sistemas legados sem atualização de segurança, ausência de trilhas de auditoria automatizadas e carência de capacitação em segurança da informação.

Tabela 1 – Riscos de negócio identificados na Fase 1.

Nr.	Risco	Descrição
RN1	Interrupção do abastecimento ou do tratamento de água e esgoto	Falhas que impeçam a continuidade dos serviços essenciais prestados à população.

Nr.	Risco	Descrição
RN2	Danos ambientais, poluição e contaminação de mananciais	Comprometimento da qualidade da água e do meio ambiente por falhas em processos de tratamento e descarte.
RN3	Perda de vidas humanas ou danos graves à saúde	Acidentes e exposições a agentes nocivos que coloquem em risco a integridade física de trabalhadores e comunidades.
RN4	Vazamento, manipulação ou perda de informações e dados pessoais	Exposição indevida de dados operacionais ou pessoais decorrente de falhas de segurança da informação.
RN5	Alteração ou falsificação de registros operacionais, financeiros ou comerciais	Manipulação intencional ou erro em registros que afete a confiabilidade das informações corporativas.
RN6	Inadimplência e perdas de receita	Redução de arrecadação por falta de pagamento, fraudes ou perdas comerciais.
RN7	Exposição a multas, sanções e penalidades legais	Infrações legais, ambientais ou contratuais que resultem em penalidades à companhia.
RN8	Diminuição da eficiência operacional e elevação de custos	Uso ineficiente de recursos humanos, materiais e financeiros que impacta a produtividade e o orçamento.
RN9	Abalo na imagem e na confiança pública	Perda de credibilidade institucional em razão de falhas operacionais, ambientais ou de comunicação.
RN10	Perda de capacidade de planejamento e de tomada de decisão	Enfraquecimento da gestão e da governança, comprometendo metas e resultados organizacionais.

Fonte: Autores (2026)

4.2 Fase 2: riscos operacionais de Tecnologia da Automação

Os grupos focais aprofundaram os riscos técnicos e operacionais dos sistemas de automação. A Tabela 2 apresenta os quatro riscos utilizados como exemplo, que cobrem os quatro níveis da escala adotada. O RE-01 decorre da ausência de inventário de documentação técnica e de cópias de segurança, o que prolonga a recuperação após falhas e aumenta a dependência de fornecedores. O RE-02 origina-se da inexistência de revisão formal de parâmetros e de controle de mudança, podendo silenciar alertas críticos e retardar a identificação de desvios de qualidade. O RE-03 resulta do uso de contas genéricas, da ausência de autenticação multifator e da falta de segregação de funções, viabilizando alterações indevidas em lógica de controle. O RE-04 decorre de canais de acesso remoto não documentados, interfaces expostas sem segmentação e protocolos sem criptografia, cenário de maior severidade por permitir manipulação dos processos químicos e biológicos de tratamento.

Tabela 2 – Riscos operacionais de TA utilizados como exemplo e nível de risco inerente simulado.

Id	Risco operacional	P	I	Nível inerente
RE-01	Extravio de documentação técnica de equipamentos de campo	2	2	Baixo (4)

Id	Risco operacional	P	I	Nível inerente
RE-02	Configuração incorreta de limiares de alarme em sistemas de supervisão local	5	5	Moderado (25)
RE-03	Ausência de controles de autenticação em estações de engenharia de sistemas SCADA	8	5	Elevado (40)
RE-04	Acesso remoto não autorizado a sistemas de controle de processos de tratamento	10	10	Crítico (100)

Fonte: Autores (2026)

A classificação decorre da matriz de probabilidade versus impacto adotada pela organização, reproduzida na Figura 2, que permite identificar rapidamente os riscos que demandam atenção prioritária e orientar a alocação de recursos para controles técnicos, físicos e organizacionais de maior impacto sobre a continuidade dos serviços essenciais.

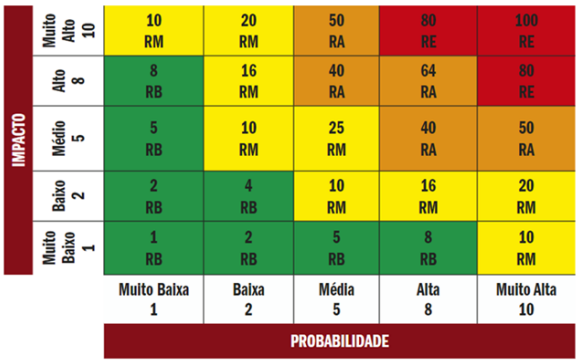


Figura 2 – Matriz de risco resultante da análise de riscos.

Fonte: Tribunal de Contas da União (TCU, 2018).

4.3 Matriz de rastreabilidade entre riscos e controles

A conexão entre as camadas de risco evidencia como falhas em ativos, processos e pessoas no nível operacional se materializam em impactos estratégicos, afetando a continuidade dos serviços, a segurança das operações, a conformidade regulatória e a confiança da sociedade. O mapeamento seguiu três etapas: varredura semântica do catálogo do NIST a partir das descrições dos riscos operacionais; refinamento por afinidade conceitual, com revisão do orientador; e validação interna em grupo focal, que confirmou ou rejeitou cada associação. A matriz consolidada, apresentada na Tabela 3, estabelece vinte conexões diretas entre os dez riscos de negócio e os quatro riscos operacionais ilustrativos, associadas a vinte e sete controles distintos do NIST SP 800-53 Rev. 5.

Tabela 3 – Matriz de rastreabilidade entre riscos de negócio, riscos operacionais de TA e controles NIST.

Risco de negócio	Riscos operacionais de TA	Controles NIST SP 800-53 Rev. 5
RN1 - Interrupção do abastecimento ou do tratamento	RE-02, RE-04	AU-2, AU-3, AU-6, SI-4, CM-2, CM-6, AC-17, AC-20, SC-7, SC-8, SC-10, IR-4, CP-2, CP-9

Risco de negócio	Riscos operacionais de TA	Controles NIST SP 800-53 Rev. 5
RN2 - Danos ambientais e contaminação de mananciais	RE-02, RE-04	AU-2, AU-3, AU-6, SI-4, CM-2, CM-6, SA-10, AC-17, AC-20, SC-7, SC-8, IR-4, IR-6, SI-3
RN3 - Perda de vidas humanas ou danos graves à saúde	RE-04	AC-17, AC-20, SC-7, SC-8, SC-10, IR-4, IR-6, SI-3
RN4 - Vazamento ou perda de informações e dados pessoais	RE-03, RE-04	AC-2, AC-3, AC-5, AC-6, IA-2, IA-5, SC-28, AC-17, AC-20, SC-7, SC-8, AU-2, AU-3, AU-6
RN5 - Alteração ou falsificação de registros	RE-02, RE-03	AU-2, AU-3, AU-6, AU-9, AU-10, SI-4, SI-7, CM-6, AC-5, AC-6, IA-2, IA-5
RN6 - Inadimplência e perdas de receita	RE-01, RE-02	MP-3, MP-4, CM-8, MA-2, AU-2, AU-3, AU-6, SI-4, CM-2
RN7 - Exposição a multas, sanções e penalidades legais	RE-02, RE-04	AU-2, AU-3, AU-6, CM-2, CM-6, SA-10, AC-17, AC-20, SC-7, IR-4, IR-6
RN8 - Diminuição da eficiência operacional e custos	RE-01, RE-02, RE-03	MP-3, MP-4, MP-5, CM-8, MA-2, AU-2, AU-6, SI-4, CM-2, CM-6, AC-2, AC-3, AC-5, AC-6, IA-2
RN9 - Abalo na imagem e na confiança pública	RE-02, RE-04	AU-2, AU-3, AU-6, SI-4, AC-17, AC-20, SC-7, SC-8, SC-10, IR-4, IR-6
RN10 - Perda de capacidade de planejamento e decisão	RE-01, RE-03	MP-3, MP-4, CM-8, MA-2, AC-2, AC-3, AC-6, IA-2, IA-5, SC-28

Fonte: Autores (2026)

Nos exemplos apresentados, as famílias AC (Access Control), CM (Configuration Management), SC (System and Communications Protection) e SI (System and Information Integrity) são as mais transversais. Na análise dos resultados reais, as famílias mais relevantes são AC (Controle de Acesso), PE (Proteção Física e Ambiental) e AU (Auditoria e Responsabilização). A estrutura viabiliza rastreabilidade ascendente, ao permitir compreender como falhas técnicas específicas materializam riscos estratégicos, e rastreabilidade descendente, ao indicar quais controles devem ser priorizados para proteger objetivos institucionais críticos, além de apoiar a priorização de investimentos e a tradução de riscos técnicos em linguagem de impacto de negócio para a alta administração.

A aplicação do NIST SP 800-53 em ambientes de TA exige customização (NIST, 2023). Quatro condicionantes destacam-se: a primazia da disponibilidade e da segurança operacional; as janelas de manutenção limitadas em operações contínuas, que tornam essenciais controles compensatórios como segmentação e monitoramento quando a correção não é viável; o ciclo de vida estendido dos ativos, que exige gestão de

obsolescência; e a integração com processos físicos, que amplia o escopo da análise para além do domínio cibernético.

4.4 Fase 3: controles complementares para o setor de saneamento

A categorização dos controles do NIST por função de segurança revelou predominância de medidas preventivas, associadas às famílias AC, IA, PE, CM, AT e PS, seguidas por controles de detecção (AU, SI), de resposta (IR, SC) e de recuperação (CP), distribuição alinhada ao princípio de defesa em profundidade recomendado para infraestruturas críticas. Como o NIST SP 800-53 é um *framework* genérico, foram identificados dez controles complementares derivados de normas brasileiras, regulamentações setoriais e guias técnicos especializados, apresentados na Tabela 4.

Tabela 4 – Controles complementares propostos para o setor de saneamento.

Id	Controle	Descrição e lacuna coberta
CC-01	Proteção contra descargas atmosféricas	Implementar programa de SPDA conforme a ABNT NBR 5419:2015, incluindo projeto, instalação, inspeção e manutenção. O NIST trata proteção ambiental de forma genérica (PE-9), sem prescrever padrão para descargas atmosféricas.
CC-02	Monitoramento de qualidade da água	Monitorar em tempo real pH, cloro residual e turbidez, conforme a Portaria GM/MS 888/2021. O catálogo do NIST não contempla obrigações setoriais de qualidade do produto.
CC-03	Reporte de interrupções ao órgão regulador	Notificar interrupções programadas e não programadas conforme a Resolução 16/2019. A família IR cobre a resposta a incidentes, mas não o dever de reporte regulatório setorial.
CC-04	Inventário de dados pessoais e RIPD para automação	Inventariar dados pessoais e elaborar Relatório de Impacto para sistemas SCADA que armazenam identificação de operadores e registros de acesso, conforme a LGPD, não coberta pela família PT.
CC-05	Segmentação de redes OT/IT	Segmentar redes corporativas e de automação conforme o modelo Purdue e o NIST SP 800-82 Rev. 3. O controle SC-7 aborda perímetro de forma genérica, sem prescrever a arquitetura industrial.
CC-06	Desligamento seguro de estações de tratamento	Documentar procedimentos de safe shutdown que preservem a integridade dos processos químicos e biológicos. A família CP considera a recuperação sob perspectiva de TI, sem tratar do processo físico.
CC-07	Gestão de obsolescência de ativos legados	Estabelecer estratégia formal para ativos com ciclo de vida de 15 a 30 anos, com plano de atualização ou controles compensatórios. O SA-22 trata de componentes sem suporte, sem orientar o ciclo de vida industrial.
CC-08	Avaliação de segurança de fornecedores de automação	Avaliar riscos na cadeia de suprimentos de integradores e prestadores com acesso direto a sistemas críticos, conforme a ISO/IEC 27036. A família SR e o SA-9 têm detalhamento insuficiente para o contexto de TA.

Id	Controle	Descrição e lacuna coberta
CC-09	Contingência para perda de comunicação com estações remotas	Desenvolver procedimentos de operação manual que mantenham o serviço mínimo sem dependência do SCADA. O CP-8 trata de telecomunicações sob perspectiva de continuidade de TI.
CC-10	Retenção de conhecimento técnico e sucessão	Documentar procedimentos, implementar treinamento cruzado e planos de sucessão para profissionais-chave de TA. As famílias AT e PS não abordam a retenção de conhecimento crítico em automação.

Fonte: Autores (2026)

A integração dos controles do NIST com os dez controles complementares constitui uma linha de base abrangente para a segurança da informação em ambientes de TA no setor público de saneamento, aplicável à empresa estudada e adaptável a outras companhias brasileiras de características operacionais e regulatórias semelhantes, sujeita a validação em cada contexto.

4.5 Discussão

A predominância das famílias de Controle de Acesso, Proteção Física e Ambiental e Auditoria e Responsabilização tem três implicações práticas. A primeira é que a proteção do acesso lógico a estações de engenharia e a sistemas de supervisão é condição central para a continuidade do serviço, em coerência com os riscos de negócio relacionados à interrupção do abastecimento e à manipulação de parâmetros operacionais. A segunda é que a proteção física do ambiente permanece relevante mesmo em discussões centradas em segurança cibernética, em consonância com as exigências mobilizadas pelo controle CC-01. A terceira é que a rastreabilidade por auditoria é pré-requisito para a resposta a incidentes industriais, que combinam consequências operacionais e ambientais e geram dever de reporte ao órgão regulador, conforme tratado pelo CC-03.

Os achados confirmam e estendem a literatura. A centralidade de controles organizacionais e de pessoas, ao lado dos controles técnicos, é consistente com a perspectiva de Veale e Brown (2020) sobre as dimensões técnica, organizacional e de governança da segurança cibernética. A necessidade de adaptação de *frameworks* de TI a ambientes industriais corrobora as orientações de Stouffer et al. (2015) e do NIST (2023) quanto à customização de controles para tecnologia operacional. A constatação de que normas brasileiras exigem controles complementares específicos converge com a literatura nacional sobre adaptação de frameworks ao contexto institucional (Galegale, Fontes & Galegale, 2017; TCU, 2018).

Quanto à hipótese, o critério de verificação considerava-a sustentada caso ao menos uma das famílias mais transversais fosse de natureza organizacional ou de gestão de pessoas. Entre as famílias mais transversais encontram-se PE e AU, ambas de natureza organizacional, ao lado de AC, predominantemente técnica. A presença concomitante de famílias técnicas e organizacionais sustenta a hipótese e indica que controles exclusivamente tecnológicos não são suficientes para a mitigação dos riscos no setor.

5. Conclusão

O objetivo de propor uma linha de base de controles de segurança da informação para mitigar riscos de negócio no setor de saneamento foi atingido. A pesquisa identificou dez riscos de negócio (Fase 1), mapeou riscos operacionais de TA e seus níveis inerentes (Fase 2), associou-os aos controles do NIST SP 800-53 Rev. 5 e elaborou matrizes de rastreabilidade entre as camadas. Na Fase 3, classificou os controles por função de segurança e propôs dez controles complementares setoriais. Portanto, a questão de pesquisa foi respondida mediante uma linha de base estruturada, vinculada aos riscos e fundamentada na integração de controles técnicos, organizacionais e de gestão de pessoas.

As contribuições abrangem três dimensões. Teoricamente, o estudo articula riscos de negócio, riscos operacionais de automação e controles reconhecidos, contribuindo para suprir lacuna no saneamento brasileiro. Na dimensão prática, disponibiliza instrumento para priorização de investimentos, explicita requisitos normativos e subsidia a demonstração de conformidade, além de comunicar riscos técnicos à alta administração. Socialmente, pode favorecer a resiliência de serviços essenciais à saúde pública.

O estudo possui limitações: amostra de dez entrevistados selecionados por conveniência, delimitação da Fase 2 à TA de uma estação de tratamento de esgoto, dependência de percepções internas e ausência de validação externa dos controles complementares. Ademais, foi adotado exclusivamente o NIST SP 800-53 Rev. 5, e o recorte temporal retrata um momento particular da organização. Destaca-se também, como limitação relevante, a impossibilidade de divulgação dos resultados reais da Fase 2, substituídos por dados ilustrativos e simulados em razão de restrições de confidencialidade impostas pela empresa, o que impede a replicação exata dos achados, ainda que preserve a validade da metodologia proposta.

Como agenda futura, recomenda-se aplicar a linha de base em outras companhias, utilizando a técnica Delphi; validar os controles com especialistas; compará-los à ISA/IEC 62443; aplicar métricas de maturidade; e avaliar quantitativamente a redução de riscos em estudos longitudinais. Sugere-se, ainda, empregar análise multicritério para ponderar ativos e estender a análise à TI corporativa, promovendo visão integrada. A revisão periódica da linha de base é necessária diante da evolução das ameaças.

Referências

ABNT. **NBR ISO/IEC 31010: Gestão de riscos: técnicas para o processo de avaliação de riscos**. Rio de Janeiro, 2012.

ABNT. **NBR 5419: Proteção contra descargas atmosféricas: partes 1 a 4**. Rio de Janeiro, 2015.

ABNT. **NBR ISO 31000: Gestão de riscos: diretrizes**. Rio de Janeiro, 2018.

ABRAMS, M.; WEISS, J. **Malicious control system cyber security attack case study: Maroochy Water Services, Australia**. McLean: MITRE, 2008.

AVEN, T. et al. **Society for Risk Analysis glossary**. Society for Risk Analysis, 2018.

AWWA. **Process control system security guidance for the water sector**. Denver: American Water Works Association, 2014.

BARDIN, L. **Análise de conteúdo**. Lisboa: Edições 70, 2011.

BARNARD, L.; SOLMS, R. von. A formalized approach to the effective selection and evaluation of information security controls. **Computers & Security**, v. 19, n. 2, p. 185–194, 2000.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília, 2018.

BRASIL. **Decreto n. 12.573, de 4 de agosto de 2025**. Atualiza a Estratégia Nacional de Segurança Cibernética. Brasília, 2025.

BRASIL. Ministério da Saúde. **Portaria GM/MS n. 888, de 4 de maio de 2021**. Brasília, 2021.

CCPS. **Guidelines for hazard evaluation procedures**. 3. ed. Hoboken: Wiley, 2008.

CHAPELLE, A. **Operational risk management: best practices in the financial services industry**. Chichester: John Wiley & Sons, 2019.

COSO. **Enterprise risk management: integrating with strategy and performance**. Nova York, 2017.

CRESWELL, J. W. **Research design: qualitative, quantitative, and mixed methods approaches**. 4. ed. Thousand Oaks: SAGE, 2014.

CROUHY, M.; GALAI, D.; MARK, R. **The essentials of risk management**. 2. ed. Nova York: McGraw-Hill, 2014.

FLICK, U. **Introdução à pesquisa qualitativa**. 3. ed. Porto Alegre: Artmed, 2009.

G1. Hacker tentou contaminar água com aditivo químico em cidade da Flórida. **G1**, 2021.

GALEGALE, N. V.; FONTES, E. L. G.; GALEGALE, B. P. Uma contribuição para a segurança da informação: um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciência da Informação**, v. 22, n. 3, p. 75–97, 2017.

GEORG, M. A. C. et al. Os desafios da segurança cibernética no setor público federal do Brasil. **Revista Ibérica de Sistemas e Tecnologias de Informação**, n. E54, p. 602–616, 2022.

GIL, A. C. **Métodos e técnicas de pesquisa social**. 7. ed. São Paulo: Atlas, 2019.

IEC. **ISO/IEC 27000: Information technology – security techniques – information security management systems – overview and vocabulary**. Genebra, 2018.

INCIBE-CERT. **Israel frustra ataque a sus sistemas de agua**. Madri: Instituto Nacional de Ciberseguridad de España, 2020.

ISA; IEC. **ISA/IEC 62443: Industrial automation and control systems security**. Research Triangle Park, 2018.

ISC2. **Classroom-based CISSP official ISC2 textbook**. Alexandria, 2023.

ISO. **ISO 31010: Risk management – risk assessment techniques**. Genebra, 2019.

ISO/IEC. **ISO/IEC 27036-1: Cybersecurity – supplier relationships – part 1: overview and concepts**. Genebra, 2021.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MACHADO, M. B. **Taxonomia de eventos de risco operacional do Poder Judiciário**. Brasília: ENAP, 2018.

NIST. **Guide for conducting risk assessments: SP 800-30 Rev. 1**. Gaithersburg, 2012.

NIST. **Risk management framework for information systems and organizations: SP 800-37 Rev. 2**. Gaithersburg, 2018.

NIST. **Security and privacy controls for information systems and organizations: SP 800-53 Rev. 5**. Gaithersburg, 2020.

NIST. **Guide to operational technology (OT) security: SP 800-82 Rev. 3**. Gaithersburg, 2023.

NIST. **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg, 2024.

PAULSEN, C.; BYERS, R. **Glossary of key information security terms: NIST IR 7298 Rev. 3**. Gaithersburg, 2019.

ROSS, R.; WINSTEAD, M.; MCEVILLEY, M. **Engineering trustworthy secure systems: NIST SP 800-160 Vol. 1 Rev. 1**. Gaithersburg, 2022.

SHAPIRA, N. et al. Cybersecurity in water sector: stakeholders perspective. **Journal of Water Resources Planning and Management**, v. 147, n. 8, 2021.

STANGER, J. **What is the difference between IT security and cybersecurity?** Downers Grove: CompTIA, 2023.

STOUFFER, K. et al. **Guide to industrial control systems (ICS) security: NIST SP 800-82 Rev. 2**. Gaithersburg, 2015.

TCU. **Modelos de referência de gestão corporativa de riscos**. Brasília: Tribunal de Contas da União, 2018.

VEALE, M.; BROWN, I. Cybersecurity. **Internet Policy Review**, v. 9, n. 4, p. 1–22, 2020.

YEVSEYEVA, I. et al. Selecting optimal subset of security controls. **Procedia Computer Science**, v. 64, p. 1035–1042, 2015.

YIN, R. K. **Estudo de caso: planejamento e métodos**. 5. ed. Porto Alegre: Bookman, 2015.