	PNQS **Formulário IGS 2025** **Prêmio da Inovação da Gestão em Saneamento Ambiental**	**ID Case** 074/25

INSTRUÇÕES PARA PREENCHIMENTO

MANTER TODOS OS ENUNCIADOS, INCLUSIVE ESTE, E NUMERAR AS PÁGINAS.

LIMITE DE PÁGINAS DO FORMULÁRIO PREENCHIDO: 13 páginas (não inclui Glossário e Bibliografia), formato tamanho A4. fonte Arial ou Times New Roman, tamanho 10. Tabelas Arial 8, Figuras Arial 6. Apenas o conteúdo relatado será avaliado utilizando o "Quadro de Notas IGS" da publicação "Critérios IGS 2025", não havendo fatores estéticos.

Salvar arquivo em formato PDF para ser carregado no SINP, com o nome "IGS 2025 XXX - YYYYYYYY", onde "XXX" é o ID do Case e "YYYYYYYYYY" é o nome do Case. O ID é o número dado pelo SINP ao preencher a Ficha de Inscrição e o nome do Case é o que foi informado nela. Não é permitida a alteração no nome do Case submetido à Elegibilidade. Caso isso ocorra, o CNQA não se responsabiliza pela não localização da Ficha de Inscrição aprovada, e, por consequência, possível perda da submissão do Case. Consultar os Critérios IGS 2025 para enquadramento no tema apropriado. No caso de dúvidas de preenchimento, entrar em contato **com** cnqa@abes-dn.org.br.

RESUMO DO CASE

Nome do Case (prática de gestão implantada) - o mesmo da Ficha de Elegibilidade, **máximo 60 caracteres**	**Case submetido em ciclo IGS anterior?** (_)Sim (X)Não	**Ano implant.** últ 3 anos) **2024**
Gestão Integrada TI e TO: Excelência em Segurança Digital		

Tema central da Prática de gestão

(_) **Pessoas** (_) **ESG** (_) **Comunicação** (x) **Segurança digital** (_) **Financeira**
(_) **Suprimentos** (_) **Inteligência Artificial** (_) **Gestão Avançada (outros)**

Resumo da prática de gestão e de seus resultados: (**Até 20 linhas**, baseado no resumo informado na respectiva Ficha de Inscrição)

Em 20212022, o Grupo Águas do Brasil (GAB) instituiu o **Comitê de Segurança Cibernética** e lançou um programa de **convergência TI–TO** para resiliência operacional, redução de perdas e sustentabilidade. A prática foi **institucionalizada** na política corporativa e orientada por **NIST CSF, ISO 27001 e ISA/IEC 62443**, operando em **metodologia híbrida**: demandas entram por canal único (SIP), passam por **triagem multidisciplinar** e **priorização por Benefício×Esforço×Risco**, seguem para **PI Planning trimestral**, execução em **SPRINTs**, **gates** (Diagnóstico → Go/No-Go → Homologação → Go-Live → Hypercare) e **gestão de mudanças via CAB**. A governança usa **RACI**, **dashboards executivos** (incidentes, MTTR, conformidade, % capacitado, avanço), **SOC 24×7** e **captura de benefícios**.

No eixo tecnológico, destacam-se **SIEM com IA**, **segmentação/Zero Trust**, **IDS/IPS industriais**, **VPN com MFA** e **datalake** integrando dados OT/IT. Isso habilita **detecção e resposta automatizadas**, analítica para **Gestão de Risco/Incidentes/Vulnerabilidades** e inteligência operacional para **Perdas (NRW)**: DMAs, macro×micro, detecção de anomalias e **gestão de pressões** para localizar vazamentos não visíveis, reduzir **kWh/m³**, minimizar **descarte de água tratada** e emissões — benefícios **ambientais** e **sociais** alinhados aos **ODS 6 e 13**. Em 2024, o SIEM com IA **processou >31 bilhões de eventos**, encaminhando **~5 mil** ao Blue Team (triagem altamente automatizada).

A prática é **replicável** entre unidades e **alinhada ao Sistema de Inovação** (scouting com startups/universidades, benchmarks setoriais e POCs), garantindo atualização contínua. Os **resultados medidos** — queda consistente de **incidentes críticos** e do **MTTR**, **conformidade regulatória**, **capacitação massiva** e **redução de perdas e energia** — estão consolidados na Seção C, com séries históricas e evidências. Com **orçamento de R$ 2 milhões/3 anos**, o programa entregou **governança previsível**, **resiliência cibernética** e **ganhos operacionais e ESG**, convertendo risco em **vantagem competitiva sustentável**.

No caso de Case já submetido em ciclo anterior, mesmo com outro nome, incluir acima aspecto que evoluiu na Prática ou Resultados desde então.

A QUALIDADE DO RESUMO ACIMA É PONTUADA NAS QUESTÕES "B.2" – RESUMO DA PRÁTICA E "C.1" – RESUMO DO RESULTADO

Na descrição dos Critérios A, B e C, consultar, como referência, os fatores de pontuação da questão a ser respondida.

INFORMAÇÕES DA ORGANIZAÇÃO

Denominação da organização candidata: Águas de Pará de Minas S/A	**Trata-se de:** **(x) Organização completa** **(_) Unidade Autônoma** **(_) Unidade de Apoio**	**... de Operador direto ou indireto de:** **(x) Abastecimento de água** **(x) Esgotamento sanitário** **(_) Manejo de águas pluviais** **(_) Manejo de resíduos sólidos** **(_) Manejo de efluentes industriais** **(_) de Fornecedor de operador** **(_) de Regulador**
Atividades principais da organização candidata: Abastecimento de água e esgotamento sanitário		
Quantidade de empregados próprios da org. candidata (porte): 145	**Endereço principal da organização candidata:** Rodovia MG431, S/N, Km 23, Sit Lagoinha - Pará de Minas - MG - CEP 35660-384	
Razão social responsável pela organização candidata: Águas de Pará de Minas S/A	**CNPJ da organização candidata:** 18.494.424/0001-15	
Nome do Autor, para se obter informações adicionais: Marcelo Olaso	**Email Autor:**	marcelo.olaso@grupoaguasdobrasil.com.br
	Fone Comercial Autor:	(21) 99606-8935
	Celular Autor:	(21) 99606-8935
Dirigente responsável que autoriza a candidatura Marcia Regina Freiberg		

DECLARAÇÃO	**AUTENTICAÇÃO**
A organização candidata concorda em responder a eventuais consultas do Especialista para esclarecimento de dúvidas, bem como, no caso de o Case ser finalista, concorda em responder a eventuais consultas de	O dirigente responsável pela organização candidata autoriza a submissão do Case à ABES e responsabiliza-se pela autenticidade das informações fornecidas, bem como autoriza sua análise pelos Especialistas designados pelo CNQA e a divulgação do Case.

interessados, para compartilhar seu conhecimento em prol do saneamento ambiental.	

A. A OPORTUNIDADE (peso 15)
A.1 Qual foi a oportunidade (insight, problema, dificuldade, desafio) tratada pela prática de gestão implementada? **Informar** de que forma a oportunidade surgiu ou foi identificada. **Destacar** eventuais sistemáticas de estímulo à inovação (atividades ou programas de sugestão, de experimentação, de benchmarking ou similares) ou de análise/avaliação de desempenho, que levaram à identificação da oportunidade e desenvolvimento da ideia. **Complementar** com informações sobre o potencial de ganhos que foi estimado com a adoção de nova abordagem ou reversão de resultados adversos identificados em análises/avaliações de desempenho realizadas no período anterior ao desenvolvimento da ideia. **Descrever** a ligação da oportunidade com os objetivos estratégicos da organização, incluindo os relacionados ao desenvolvimento sustentável ou ODS's. **Informar** como essa oportunidade se manifesta ou pode se manifestar no setor, segundo fontes conhecidas.
Fatores de avaliação A.1.1 Origem da oportunidade A.1.2 Relevância da oportunidade para a organização A.1.3 Relevância da oportunidade para as organizações do setor e para sociedade ou meio ambiente

A.1.1 Origem da oportunidade

Até 2021, os ambientes de Tecnologia da Informação (TI) e Tecnologia Operacional (TO) funcionavam em silos, sem integração de políticas, ferramentas ou processos. Auditorias internas e avaliações regulatórias expuseram fragilidades críticas — inventário de ativos fragmentado, protocolos industriais pouco protegidos (p.ex., Modbus, DNP3) e controles de acesso inconsistentes. Em paralelo, alertas de analistas (como projeções do Gartner sobre a intensificação de ataques a infraestruturas críticas até 2025) e incidentes internacionais (Oldsmar/EUA, Colonial Pipeline/EUA, ransomware Clop no Reino Unido) evidenciaram a urgência de uma mudança de abordagem.

A oportunidade foi identificada por meio do processo corporativo de análise (auditorias, SIP/triagem, Comitê e Sistema de Inovação), combinando evidências internas e benchmarks externos documentados. A inovação proposta pela Concessionária Águas de Pará de Minas (CAPAM), empresa do Grupo Águas do Brasil (GAB), foi justamente antecipar uma tendência ainda incipiente à época: convergir TI e TO de forma deliberada, algo pouco comum no mercado — especialmente no setor de utilidades — para transformar gestão de risco em vantagem competitiva. Essa decisão inaugurou um novo desenho de governança e arquitetura, com foco em resiliência cibernética e uso inteligente de dados. Ao integrar dados de sensores e sistemas de TO com informações de TI, viabilizou-se analítica avançada para otimização de ativos, eficiência operacional e consumo de recursos, além de capacidades preditivas (manutenção, qualidade, perdas). Assim, o que era uma vulnerabilidade recorrente converteu-se em plataforma de inovação e diferenciação: uma prática pioneira de convergência TI-TO, alinhada à proteção de serviços essenciais e ao fortalecimento dos objetivos estratégicos da organização.

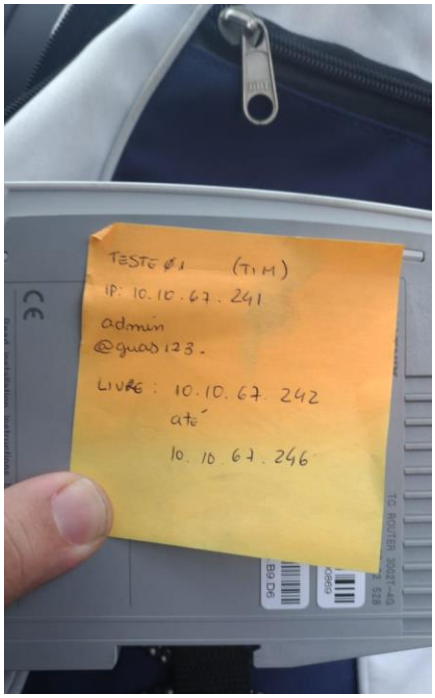


Figura 1.: Situação encontrada em campo

Figura 2: A senha de acesso a rede, colada em um post-it e uma unidade operacional na rua.

Referencias:

https://agenciabrasil.ebc.com.br/internacional/noticia/2021-02/hacker-tenta-envenenar-agua-de-cidade-da-florida
https://pt-br.tenable.com/blog/colonial-pipeline-ransomware-attack-how-to-reduce-risk-in-ot-environments
https://www.forescout.com/blog/analysis-of-clops-attack-on-south-staffordshire-water-uk/?utm_source=chatgpt.com

A.1.2 Relevância da oportunidade para a organização

A relevância do projeto é mitigar riscos e proteger os ativos críticos de CAPAM, de ameaças cibernéticas de forma a garantir o abastecimento água a hospitais, escolas e milhares de cidadãos. A prática reposicionou a segurança cibernética como alavanca de transformação digital: ao convergir TI e TO — antes operando em silos — foi criada uma base segura para automação, telemetria e orquestração de dados em um datalake corporativo, habilitando BI, análises preditivas e aplicações de IA/ML. Com maior visibilidade fim a fim, foi possível antecipar falhas, otimizar recursos, fortalecer a governança de riscos e garantir a continuidade do abastecimento de água a hospitais, escolas e milhares de cidadãos, convertendo vulnerabilidades em vantagem competitiva e inovação sustentável.

Essa mesma infraestrutura foi determinante para o Projeto de Perdas (no âmbito do Programa Água de Valor 2.0, do GAB). A integração TI-TO permitiu reconciliação macro-micro (macromedição x hidrômetros), criação de Distritos de Medição e Controle (DMAs), uso de algoritmos de detecção de anomalias para vazamentos não visíveis, gestão ativa de pressões, identificação de fraudes/irregularidades e priorização inteligente da substituição de redes e hidrômetros. A correlação de dados operacionais (bombeamento, válvulas, pressões), comerciais (perfil de consumo) e de campo (ordens de serviço) acelerou o ciclo "detectar-localizar-intervir", reduzindo o tempo de detecção e de reparo, o volume perdido e o retrabalho das equipes.

O impacto é relevante sob três dimensões:

Financeira — redução de perdas reais e aparentes aumenta o volume faturado sem CAPEX proporcional, reduz OPEX (energia de bombeamento, insumos químicos), posterga investimentos, melhora EBITDA e previsibilidade;

Ambiental — menor captação em mananciais, menor consumo energético e emissões, menos rompimentos e descartes de água tratada, alinhado a ODS 6 e 13;

Social — mais continuidade e qualidade no abastecimento, menos interrupções e obras emergenciais em vias públicas, tarifas mais sustentáveis no longo prazo e maior transparência ao cidadão. Indicadores como IPD (Índice de Perdas na Distribuição), índice de macromedição, índice de hidrometração, ILI (Infrastructure Leakage Index), volume recuperado (m^3/mês) e tempos médios de detecção e reparo passaram a compor painéis executivos e metas monitoradas, assegurando governança e melhoria contínua em linha com os objetivos estratégicos definidos em A.1.

A.1.3 Relevância da oportunidade para as organizações do setor e para a sociedade ou meio ambiente

Trata-se de uma oportunidade muito relevante para o setor de saneamento e, sobretudo, para o meio ambiente e a sociedade: ao fortalecer a resiliência cibernética e a confiabilidade da automação, a prática viabiliza gestão ativa de perdas, uso eficiente de energia e operação estável de sistemas de água e esgoto — pilares diretamente ligados à segurança hídrica e à saúde pública.

A relevância é evidenciada por fatos constatados em fontes conhecidas do setor: bases como SNIS e ANA apontam historicamente elevados índices de perdas na distribuição e forte participação da energia no custo operacional; organismos internacionais (ONU-Água/OMS, IWA) endossam que reduzir perdas e otimizar bombeamento diminui a captação em mananciais, o consumo de insumos químicos e as emissões associadas. Além disso, autoridades de segurança (CISA/EPA e congêneres) têm registrado incidentes que demonstram a necessidade de proteger a infraestrutura crítica de água.

Na prática, a integração segura TI-TO e a analítica avançada (telemetria, DMAs, detecção de anomalias, gestão de pressões) reduzem vazamentos e fraudes, encurtam o tempo de detecção e reparo e baixam o consumo energético por m^3 tratado e distribuído. O resultado combina:

- Ambiental: menor retirada de água de rios e aquíferos, menos descartes de água tratada e menor pegada de carbono (ODS 6 e 13).
- Social: continuidade e qualidade do abastecimento para hospitais, escolas e comunidades, com menos interrupções e obras emergenciais.
- Setorial: elevação da maturidade digital e operacional, com práticas replicáveis e aderentes a diretrizes e métricas amplamente reconhecidas.

Assim, a oportunidade transcende a mitigação de riscos: consolida um modelo sustentável e replicável que agrega valor ambiental, social e econômico, sustentado por referências públicas e respeitadas do setor.

B. A IDEIA (peso 50)
B.1. De que forma a prática de gestão foi planejada ou concebida para superar obstáculos identificados? **Informar** quais as lideranças e profissionais, internos e/ou externos, foram envolvidos no projeto ou planejamento da prática de gestão. **Resumir** a função de cada um deles nesse projeto. **Informar** qual a sistemática de trabalho em projeto, citando a metodologia de projeto adotada. **Apresentar** um ou mais objetivos da prática, com os quais os resultados de C.1 têm relação.. **Resumir** as principais etapas planejadas e os recursos (financeiros, humanos e materiais) orçados e realizados no projeto, até a implementação final e entrada em regime. **Informar** os principais obstáculos identificados, antes ou durante a implantação, e a forma para superar as dificuldades**.** **Citar** fontes de inspiração, internas e/ou externas, para apoiar o desenvolvimento da ideia (literatura, entidades de classe, academia, consultorias, fornecedores, congressos, feiras, empresas do setor ou de fora dele, outras unidades da mesma controladora ou outras) e eventuais oportunidades identificadas ou lições aprendidas nessas fontes, incluindo sobre resultados possíveis ou alcançados por elas, **informando** quando as localizações das fontes forem decorrentes de práticas de busca de conhecimento disseminadas na organização. Se não houver lição aprendida nas fontes, **declarar** o fato. **Descrever** qualquer atividade prévia de capacitação de pessoas, se houver, e sua abrangência. Informar como a evolução do projeto foi controlada.
Fatores de avaliação B.1.1 Planejamento e gerenciamento de projeto B.1.2 Sistemática de trabalho em projeto B.1.3 Uso de informações de outras fontes de referência

B.1.1 Planejamento e gerenciamento de projeto

Em 2022, o **Comitê de Segurança Cibernética** foi criado pelo Grupo Águas do Brasil, reunindo diretoria, lideranças de TI e TO e executivos da alta gestão. O grupo foi responsável por planejar a integração entre ambientes corporativos e operacionais, com objetivos estratégicos de:

- reduzir incidentes críticos em **30%**;
- reduzir o tempo médio de resposta (MTTR) em **50%**;
- atingir **100% de conformidade** em auditorias regulatórias;
- capacitar **80% da equipe** em cibersegurança aplicada a ambientes industriais.

O programa foi dividido em vários projetos:

1. **Diagnóstico:** auditorias internas e externas, inventário inicial de ativos e avaliação de vulnerabilidades.
2. **Infraestrutura tecnológica:** SIEM corporativo integrado a um SOC 24x7, segmentação de redes, IDS/IPS para protocolos industriais e VPN com MFA.
3. **Processos:** criação de **10 playbooks de incidentes**, hardening e gestão de vulnerabilidades.
4. **Pessoas:** treinamentos presenciais e remotos, campanhas de conscientização e simulações práticas.

Esse programa foi regido por um **processo único de gestão de demandas**: entrada centralizada via **SIP** e formulário padrão; **triagem técnica** multidisciplinar; **backlog priorizado**; **PI Planning/Refinamento**; e definição, já no início, de benefícios, riscos, esforço e complexidade de cada demanda.

A priorização passou a usar **matriz/"calculadora" de Benefício × Esforço** e **Comitê de Negócio trimestral**, garantindo aderência às prioridades e alocação de responsáveis.

A **cadência trimestral** (planejamento sincronizado no fim de cada trimestre, com **acompanhamento semanal, mensal e trimestral**) organizou as entregas em pacotes e reduziu mudanças não planejadas.

Na execução, os times atuam por **esteiras e cards vinculados** à demanda principal (consultiva), com **entregas em SPRINTs**, **teste/homologação alinhados ao Negócio**, **estratégia de go-live** e **captura de benefícios**. Esse arranjo reforçou governança, previsibilidade e integração TI-TO, além de facilitar **identificação de interdependências** e **aprovação funcional**.

Portfólio do Programa — conceito, objetivo e obstáculos por projeto

1) Diagnóstico
Conceito. Levantamento estruturado (auditorias internas/externas), **inventário de ativos** e avaliação de vulnerabilidades como *gate* para as demais frentes.
Objetivo. Obter visão unificada do risco OT/IT e basear a priorização do backlog com evidências de benefício/risco/esforço.
Obstáculos. Dados dispersos e inventário inexistente/estático; janelas restritas nas operações; cultura reativa. **Como foi endereçado:** entrada única via SIP, triagem técnica, padronização de conceitos/status e acompanhamento desde a etapa inicial.

2) Infraestrutura tecnológica

Conceito. Camada de segurança e observabilidade (SIEM+SOC 24×7, segmentação, IDS/IPS industriais, VPN com MFA) implantada em ondas, conforme pacotes trimestrais.
Objetivo. Reduzir incidentes críticos e MTTR ao habilitar detecção, resposta e contenção padronizadas, priorizadas por **matriz Benefício × Esforço**.
Obstáculos. Protocolos legados sem proteção nativa; integração com ativos OT; restrição orçamentária. **Como foi endereçado:** Comitê de Negócio para decisão de trade-offs, planejamento sincronizado para remover interdependências e go-live controlado com testes/homologação.

3) Processos
Conceito. Playbooks de incidente, hardening e **gestão de vulnerabilidades** com fluxos, papéis e indicadores definidos no backlog.
Objetivo. Padronizar resposta (quem faz o quê, quando e como), criando repetibilidade e medição contínua; priorizar correções por valor de negócio e risco.
Obstáculos. Heterogeneidade entre unidades e múltiplas dependências. **Como foi endereçado:** planejamento trimestral sincronizado, acompanhamento semanal/mensal, e **alocação clara de responsáveis** por demanda.

4) Pessoas
Conceito. Capacitação técnica e comportamental (treinamentos, campanhas e simulações) amarrada ao ciclo trimestral de entregas.
Objetivo. Atingir **80% de colaboradores capacitados** em cibersegurança aplicada ao ambiente industrial e consolidar cultura de integração TI-TO.
Obstáculos. Disponibilidade de agenda e engajamento em operações 24×7. **Como foi endereçado:** priorização trimestral com Comitê de Negócio, fracionamento em SPRINTs e **captura/visibilidade de benefícios** para sustentar adesão.
Orçamento e governança. O programa operou com **R$ 2 milhões/3 anos**, orquestrado em pacotes **Q1–Q4** com **revisão no fim de cada trimestre**, alterações apenas como exceção e avaliação explícita de desperdício, sempre com reporte estruturado nas esteiras.
Resultado: o processo de **gestão de demandas e projetos** tornou-se repetível, auditável e orientado a valor, reduzindo riscos e acelerando a execução por meio de uma governança que integra **priorização objetiva**, **planejamento sincronizado** e **entrega com captura de benefícios**.

Programa: Convergência TI-TO												
Diagnostico (inventario, auditoria, vulnerabilidades)												
Pessoas (capacitação, campanhas e simulações)												
Processos (playbooks, hardening, gestão de vulnerabilidades)												
Infraestrutura (Siem+Soc, Segmentação, IDS/IPS)												
	21 Q1	**21 Q2**	**21 Q3**	**21 Q4**	**22 Q1**	**22 Q2**	**22 Q3**	**22 Q4**	**23 Q1**	**23 Q2**	**23 Q3**	**23 Q4**

B.1.2 Sistemática de trabalho em projeto

Foi adotada uma sistemática de gestão já implantada na política de gestão de projetos e demandas da empresa, onde as demandas entram por **canal único** (formulário/sistema.

Metodologia. Sistemática híbrida (ágil + tradicional) já prevista na política corporativa: entrada única (SIP/formulário) → triagem técnica multidisciplinar → priorização por Benefício × Esforço × Risco → aprovação em Comitê. PI Planning trimestral organiza capacidade e escopo; a execução ocorre em SPRINTs quinzenais, com PDCA e retrospectivas a cada ciclo. Padrões de referência integrados: NIST CSF, ISO 27001 e ISA/IEC 62443.

Forma de trabalho da equipe. Entregas realizadas por **esteiras** com **cards vinculados** à demanda principal, **testes/homologação** com o Negócio, **go-live pactuado** e **hypercare**. Há **captura de benefícios** e registro de **lições aprendidas** em repositório único.

Cronogramas e controles. Cronograma-mestre em **pacotes trimestrais** com **gates**: *Diagnóstico → Go/No-Go → Homologação → Go-Live → Hypercare*. **Baseline** de escopo/prazo/custo controlada, **RAID log** (riscos, premissas, issues, decisões), **gestão de dependências TI–TO** e **métricas de saúde** do projeto.

Responsabilidades (RACI).

- **Sponsor/Diretoria:** metas, orçamento e remoção de impedimentos.
- **Comitê de Segurança/Programa:** priorização, decisões e acompanhamento.

- **PM/PMO:** integração de cronogramas, orçamento, qualidade e riscos.
- **PO/Negócio:** escopo, aceite e benefícios.
- **Líder de TI:** SIEM/SOC, redes, IAM/VPN e integrações.
- **Líder de TO:** protocolos industriais, janelas operacionais e continuidade.
- **RH:** trilhas de capacitação e campanhas.
- **Fornecedores (SOC 24×7/consultorias):** SLAs, entregas técnicas e transferência de conhecimento.

Sistema de comunicação. Dailies por frente; **reunião semanal** de integração TI–TO; **cerimônia quinzenal** de alinhamento; **steering mensal** executivo; **Comitê trimestral** de decisão. **Dashboards** (incidentes, **MTTR**, conformidade, **% capacitado**, avanço do pacote), **status report** padrão, **atas** em repositório e **War Room** com **playbooks** para incidentes críticos.

Gestão de mudanças. CAB (normal/urgente/emergencial) com análise de impacto, janela, plano de reversão e comunicação; exceções ao pacote em execução só com aprovação formal. **BCM/DRP** testado periodicamente.

Processos de ciber integrados ao projeto.

- **Gestão de risco:** identificação, avaliação (probabilidade/impacto), tratamento e priorização no backlog conforme apetite de risco.
- **Gestão de vulnerabilidades:** varreduras cíclicas, criticidade e janelas de correção alinhadas à operação.
- **Gestão de incidentes:** detecção/containment (**SIEM com IA** + **SOC 24×7**), comunicação, *post-mortem* e atualização de playbooks.
- **Indicadores (KPIs/KRIs):** incidentes críticos, **MTTR**, conformidade de auditorias/patches, cobertura de logs, **% capacitação**, avanço de pacotes — revisados **semanal/mensal/trimestralmente**.

Aplicação por frente do Programa
1) Diagnóstico — Conceito/Objetivo. Auditorias, inventário e avaliação de vulnerabilidades para estabelecer **linha de base** e **backlog priorizado**.
Obstáculos. Dados dispersos, inventário estático e janelas curtas. **Tratativa.** Coleta automatizada, entrevistas guiadas, janelas coordenadas e *gate* de conclusão.
2) Infraestrutura — Conceito/Objetivo. SIEM+SOC 24×7, segmentação, **IDS/IPS industriais** e **VPN com MFA** para reduzir incidentes e **MTTR**.
Obstáculos. Legados/protocolos sem proteção nativa, integrações OT e orçamento. **Tratativa.** Ondas por criticidade, testes/homologação, **CAB** e acompanhamento por **SLAs/OKRs**.
3) Processos — Conceito/Objetivo. Playbooks de incidente, **hardening** e **gestão de vulnerabilidades** com papéis, gatilhos e **KPIs** definidos.
Obstáculos. Heterogeneidade entre unidades e dependências cruzadas. **Tratativa.** Padronização **RACI**, versionamento, auditorias internas e metas por ciclo.
4) Pessoas — Conceito/Objetivo. Trilhas de **capacitação** (presencial/e-learning), campanhas e simulações para atingir **80%** treinados e consolidar a cultura TI–TO.
Obstáculos. Agendas 24×7 e engajamento. **Tratativa.** Turmas recorrentes, comunicação segmentada por público, certificação e medição de eficácia (pré/pós-teste).
Resultado da sistemática. Governança previsível, **visibilidade executiva** e **entregas incrementais**, com aderência aos padrões (**NIST/ISO/ISA**), cumprimento de prazos e **captura comprovada de benefícios**, permitindo **replicação entre unidades**.
Com isso, o projeto mantém **governança previsível**, **visibilidade executiva** e **entregas incrementais**, assegurando aderência aos padrões (NIST/ISO/ISA), cumprimento de prazos e captura de benefícios.

B.1.3 Uso de informações de outras fontes de referência

Foram analisados casos internacionais emblemáticos — **Oldsmar**, **Colonial Pipeline** e o ataque **Clop** no Reino Unido — que evidenciaram impactos reais de falhas de cibersegurança em serviços essenciais e serviram como base comparativa para decisões.

Em paralelo, o que já é uma pratica na organização, o **Sistema de Inovação** (Comitê, Núcleo e Rede) foi acionado para buscar **fontes externas vindas da inovação**: o **Núcleo de Inovação** realizou *tech scouting* com **startups, universidades e laboratórios**, conduziu **benchmarks** com utilities e setores adjacentes (energia, óleo & gás) e pilotou **POCs**; a **Rede de Inovação** capturou dores/ideias de campo para qualificar os desafios; e o **Comitê de Inovação** validou diretrizes e priorização. Além disso, **relatórios de analistas** (p. ex., tendências do Gartner para infraestruturas críticas), **congressos e feiras de cibersegurança/automação** e **fóruns setoriais** forneceram repertório de soluções e **boas práticas** de outras concessionárias.

Lição aprendida: ao integrar inteligência técnica (casos, normas, análises) com a **inteligência de ecossistema** trazida pela área de inovação (scouting, POCs, benchmarks), risco foi transformado em **oportunidade de inovação**, aprendizado foi acelerado e **vantagem competitiva sustentável foi reforçada**.

B.2. Como funciona a prática de gestão?
Descrever a sistemática implantada, **mencionando** os usuários e os principais padrões gerenciais associados à prática (plano, procedimento, rotina, programa ou similar).
Elencar as características de originalidade e, se existirem.
Citar uma ou mais características promotoras de consequências positivas no meio ambiente, na sociedade ou na governança[1] (ESG) ou para os ODS's, **resumindo** as vantagens advindas dessas características e **explicando** quais delas representam novidade ou diferenciais de práticas conhecidas e quais representam ruptura radical na forma de gerir.
Descrever qualquer característica relevante de a) otimização ou simplificação, b) proatividade (que previnam problemas na gestão), c) agilidade (adaptação ágil a novas demandas), d) incorporação de tecnologia digital[2], destacando, se houver, o emprego de IA, e) abrangência, f) integração ao sistema de padrões existente da organização (manuais, procedimentos, sistemas informatizados ou outros), g) ferramentas de controle e eventuais indicadores de monitoramento da eficiência, eficácia ou efetividade.
Fornecer informações sobre o ineditismo da prática de gestão implantada, se houver, na organização candidata, na sua controladora ou no próprio setor - no país ou no mundo.
Incluir uma ou mais metas almejadas para indicadores de monitoramento.
Informar eventuais capacitações ou instruções requeridas para realização da prática pelos usuários.
Informar como os padrões são aprendidos pelas pessoas nas áreas pertinentes.
O Resumo do Case no início deste documento deve sumarizar com clareza a abordagem inovadora ou exemplar relatada.

Fatores de avaliação
B.2.1 Enfoque sistemático, enxuto e com padrões gerenciais claros (Resumo do Case o sumariza)
B.2.2 Enfoque original, inusitado ou inédito, com emprego de tecnologia digital e IA (Resumo do Case o sumariza)
B 2.3 Enfoque promotor do desenvolvimento sustentável ou do alcance dos ODS's
B.2.4 Enfoque proativo, prevenindo problemas na gestão
B.2.5 Enfoque ágil, para resposta rápida
B.2.6 Aplicação é suficientemente abrangente e controlada
B.2.7 Integração ao sistema de padrões da organização

B.2.1 Enfoque sistemático, enxuto e com padrões gerenciais claros (Resumo do Case o sumariza)

A prática foi organizada com um **fluxo padronizado e replicável**: **entrada única** da demanda (SIP/formulário), **registro e triagem técnica** por time multidisciplinar e **padronização de status/conceitos** para **reporte estruturado**. Em seguida, ocorre a **priorização** por **matriz de prioridade (benefício × esforço)** e **Comitê de Negócio**, que valida o alinhamento com as prioridades corporativas e encaminha às áreas de execução.

O **planejamento é sincronizado trimestralmente** (PI Planning), agrupando entregas em **pacotes por trimestre** para reduzir desperdícios e organizar interdependências; **alterações no pacote em execução** só ocorrem **como exceção**, com **avaliação do impacto e aprovação da liderança**. A **comunicação** segue **ritos de acompanhamento semanal, mensal e trimestral**, com **fóruns** para garantir a entrega e **dashboards/relatórios** de avanço. Na **execução**, os trabalhos são organizados em **esteiras e cards vinculados** à demanda principal, mantendo rastreabilidade ponta a ponta. As **entregas** são sustentadas por **testes/homologação** com o Negócio, **estratégia de go-live** pactuada com os líderes e **captura de benefícios** comunicada aos envolvidos. O processo explicita **interdependências** entre demandas e consolida um **pacote trimestral** com responsáveis definidos e **aprovação funcional**.

No âmbito de **cibersegurança**, a governança está ancorada em **NIST CSF**, **ISO 27001** e **ISA/IEC 62443** (referenciais já adotados), traduzidos em **processos operacionais**:

- **Gestão de Risco**: identificação, avaliação e tratamento com critérios de probabilidade/impacto e priorização integrada ao backlog.
- **Gestão de Incidentes**: detecção/containment, comunicação e *post-mortem* com lições aprendidas incorporadas aos playbooks.
- **Gestão de Vulnerabilidades**: varreduras periódicas, classificação por criticidade e janelas de correção alinhadas às operações.
- **Indicadores e Reporte**: métricas de valor e de desempenho (ex.: riscos mitigados, incidentes, MTTR, conformidade, itens do pacote) acompanhadas nos **fóruns semanais/mensais/trimestrais** e consolidadas para decisão do **Comitê**.

Esse arranjo — **ritos de planejamento**, **comunicação constante**, **gestão de mudanças com governança** e **comitês decisórios** — garante **repetitividade, controle e evolução contínua**, assegurando consistência entre unidades, previsibilidade de entregas e **captura de benefícios** para o negócio.

[1] As características promotoras da governança estão associadas direcionamento e controles externos, à transparência, à ética, à avaliação da atuação ESG e afins.
[2] Ver glossário "tecnologia digital" no MEGSA®ESG

B.2.2 Enfoque original, inusitado ou inédito, com emprego de tecnologia digital e IA (Resumo do Case o sumariza)

A prática incorpora originalidade e ruptura radical na forma de gerir a cibersegurança, ao adotar um modelo de convergência TI–TO apoiado em inteligência artificial. O diferencial está no uso de um SIEM de nova geração, com algoritmos de IA e machine learning capazes de analisar, em tempo real, grandes volumes de dados oriundos tanto de sistemas de TI quanto de sensores de OT. Essa capacidade de correlação inteligente permite detectar padrões anômalos e antecipar ameaças avançadas, como ransomware ou tentativas de acesso não autorizado, que dificilmente seriam identificados por ferramentas tradicionais baseadas apenas em regras estáticas.

A inovação não se restringe à segurança: os dados operacionais capturados também foram integrados a um datalake corporativo inteligente, possibilitando análises preditivas sobre eficiência, manutenção de ativos e consumo de recursos. Assim, a IA transformou riscos antes latentes em oportunidades de inovação e geração de valor estratégico.

O Resumo do Case destaca esse uso disruptivo da IA como um marco na evolução da prática, evidenciando que não se trata de uma simples melhoria, mas de uma mudança de paradigma na gestão integrada de TI e TO. Os resultados apresentados na seção "C" comprovam a mudança de patamar de desempenho, com maior resiliência, redução de incidentes críticos e benefícios tangíveis para toda a organização.

Em 2024, nosso **SIEM com IA** processou **mais de 31 bilhões** de eventos de segurança e **resolveu-os automaticamente**; apenas **cerca de 5 mil** (**≈0,00002%**) exigiram análise do **Blue Team** — desempenho equivalente a **99,99998%** de triagem automática.

B 2.3 Enfoque promotor do desenvolvimento sustentável ou do alcance dos ODS's

A prática evidencia **múltiplas características inovadoras e gerenciais**, diretamente relacionadas aos pilares **ESG (Environmental, Social and Governance)**, reforçando sua contribuição para o desenvolvimento sustentável.

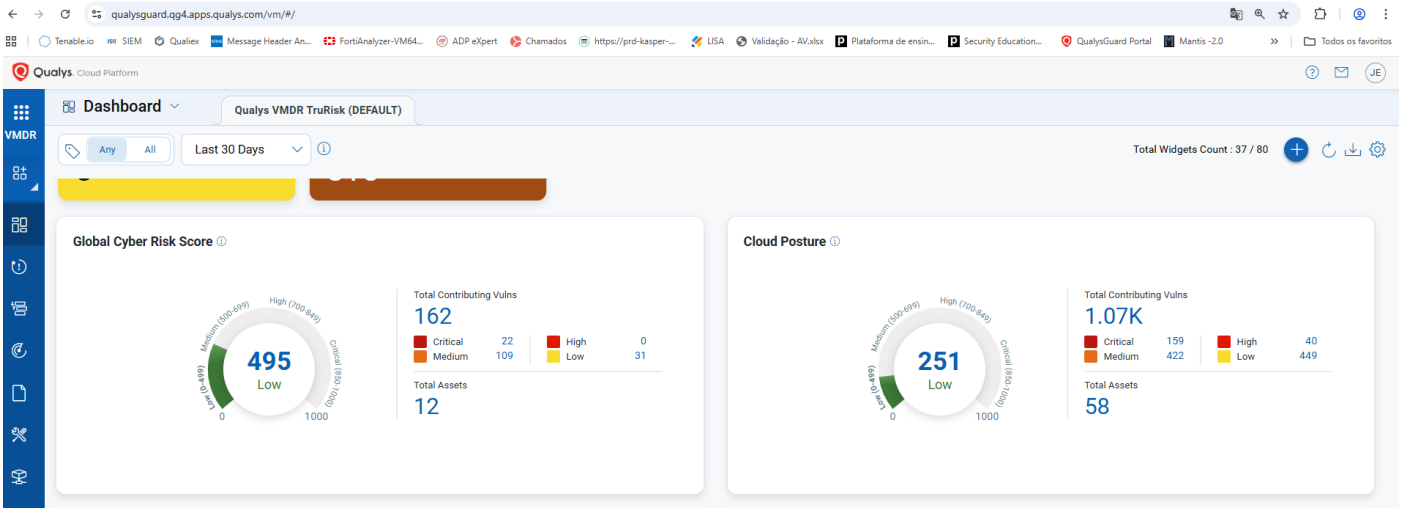
- **• Environmental (Ambiental):** A convergência TI–TO consolidou dados de sensores OT (pressão, vazão, nível, qualidade) e medições macro/micro em um datalake corporativo, habilitando analítica de perdas (NRW) — reais (vazamentos) e aparentes (medição/fraude). Com DMAs, balanço de massa e algoritmos de detecção de anomalias, passou-se a localizar vazamentos não visíveis, otimizar pressões e priorizar substituição de redes/hidrômetros. O efeito ambiental direto: menor captação em mananciais, queda do kWh/m³ bombeado, menor uso de produtos químicos e redução do descarte de água tratada, além de menos rompimentos e emissões associadas (escopo 2). Resultado: redução de desperdícios e pegada ambiental menor, alinhado às melhores práticas globais e aos ODS 6 e 13.
- **Social:** O uso de **inteligência artificial aplicada ao SIEM** fortaleceu a capacidade de prever e responder a incidentes cibernéticos, assegurando a continuidade de serviços essenciais prestados à sociedade. Essa característica garante maior **confiabilidade e segurança para clientes, comunidades e colaboradores**, além de reforçar a imagem institucional como provedora de serviços críticos que respeitam a qualidade de vida das pessoas.
- **Governance (Governança):** A prática adota **processos gerenciais padronizados e replicáveis**, monitorados por indicadores estratégicos e submetidos a revisões periódicas. Esse modelo garante **transparência, rastreabilidade e conformidade regulatória**, fortalecendo a governança corporativa e ampliando a confiança de stakeholders internos e externos.

Assim, ao reunir inovação tecnológica (IA no SIEM), eficiência operacional (dados de sensores OT) e gestão estruturada (modelos de controle e governança), a prática transcende os ganhos técnicos e passa a ser um **exemplo de aplicação concreta de princípios ESG**, com benefícios diretos para a **sustentabilidade ambiental, social e econômica** e para a **perenidade da organização**.

B.2.4 Enfoque proativo, prevenindo problemas na gestão

A prática foi concebida com **características suficientes para prevenir os principais problemas** que poderiam comprometer sua efetividade e sustentabilidade ao longo do tempo. O desenho sistemático contemplou mecanismos de **monitoramento contínuo**, com uso de indicadores de desempenho e alertas inteligentes no SIEM, apoiados por inteligência artificial, garantindo a **detecção antecipada de anomalias** em ambientes de TI e TO. Além disso, a integração com dados de sensores OT permite identificar falhas operacionais e riscos de indisponibilidade antes que gerem impactos relevantes.

Foram incorporados **controles gerenciais e operacionais padronizados**, incluindo planos de contingência, redundância tecnológica, processos de auditoria interna e ciclos de melhoria contínua (PDCA), assegurando que a prática se mantenha **replicável, confiável e resiliente**. Dessa forma, não apenas se evitam falhas recorrentes, mas também se fortalece a **capacidade de adaptação e inovação**, garantindo benefícios sustentados e alinhados aos objetivos estratégicos da organização.



Gestão de vulnerabilidades

(esse sistema, monitora os ativos da empresa e alerta contra bugs, brechas, etc.. ajudando a prevenir paradas no ambiente)

Segurança Defensiva

(Esse BI, é um relatório executivo de todos os ataques que sofremos e respondemos mensalmente. Separados por categoria e no final temos 0 ataques efetivos)

B.2.5 Enfoque ágil, para resposta rápida

A estrutura de **SOC 24x7** e a adoção de metodologias ágeis na gestão de incidentes possibilitam adaptação rápida a novas ameaças.

O **tempo médio de resposta (MTTR)** caiu em 50%, garantindo que eventos que antes levariam horas ou dias para serem mitigados agora possam ser tratados em minutos.

O modelo de **ciclos trimestrais de revisão** também assegura flexibilidade para incorporar rapidamente novas tecnologias e práticas de segurança.

B.2.6 Aplicação é suficientemente abrangente e controlada

A prática foi estruturada de forma a abranger suficientemente todas as áreas, processos, produtos e partes interessadas pertinentes, garantindo que nenhum aspecto crítico fosse deixado de fora. Sua implantação envolveu tanto os ambientes de TI e TO, quanto áreas de governança, operação e atendimento ao cliente, assegurando alinhamento organizacional completo.

Para garantir a consistência, foram definidos mecanismos de controle robustos, baseados em padrões corporativos documentados e revisados periodicamente. A prática dispõe de indicadores de eficiência e eficácia, com metas claras, monitoradas em dashboards executivos e relatórios periódicos, assegurando acompanhamento contínuo e tomada de decisão ágil. Esses indicadores incluem, por exemplo, a redução no número de incidentes críticos detectados pelo SIEM com IA, o tempo médio de resposta a falhas operacionais e o índice de disponibilidade dos serviços essenciais.

Dessa forma, além de garantir sua abrangência transversal, a prática demonstra controle efetivo sobre os padrões de aplicação, sustentando ganhos mensuráveis e alinhados aos objetivos estratégicos da organização.

A prática cobre toda a operação do Grupo Águas do Brasil:

- **2.600 estações de trabalho**, **1.700 smartphones corporativos**, **37 sistemas críticos**, **25 sedes administrativas**, **32 lojas de atendimento** e **143 unidades operacionais**.
  A abrangência garante que tanto os ambientes corporativos (TI) quanto os operacionais (TO) estejam sob o mesmo modelo de governança.
  O **controle é realizado por meio de indicadores quantitativos e metas estabelecidas**, monitorados pelo Comitê de Segurança Cibernética e reportados trimestralmente ao Conselho de Administração.

B.2.7 Integração ao sistema de padrões da organização

A prática foi **institucionalizada na Governança de Cibersegurança da companhia**, integrada ao **sistema de gestão corporativa** e ao **planejamento estratégico**, com patrocínio do **Comitê de Segurança Cibernética** e reporte periódico à alta administração. O modelo define **políticas e padrões** (NIST/ISO/ISA), **papéis e responsabilidades (RACI)**, **apetite de risco** e **três linhas de defesa** (operações/SOC, gestão de riscos/controles internos e auditoria). Os processos de **gestão de riscos, vulnerabilidades, mudanças (CAB) e incidentes** são monitorados por **KPIs/KRIs** (p. ex., incidentes críticos, MTTR, conformidade de patches, SLA de correção), com **dashboards executivos** e **auditorias internas/externas** vinculadas a **planos de continuidade (BCM/DRP)** e requisitos regulatórios (LGPD, etc.). Assim, a segurança deixa de ser "um projeto de TI" e passa a ser **prática de gestão corporativa**, com **accountability clara**, **financiamento previsível** e **melhoria contínua**.

B.3. Como funciona a sistemática de avaliação da efetividade[3] e de melhoria da prática de gestão depois de implementada? **Informar** a frequência e participantes da avaliação e como ela é conduzida. **Mencionar** indicador(es) e outras informações utilizadas para avaliar o desempenho da prática de gestão, depois da implantação. **Exemplificar** eventuais melhorias incorporadas em função das avaliações iniciais. **Citar** atividades relacionadas à replicação ou disseminação da prática em outras áreas da organização e os ganhos conhecidos ou em outras empresas..
Fatores de avaliação B.3.1 Mecanismo de aprendizado da prática de gestão (avaliação da efetividade e melhoria) B.3.2 Consistência dos indicadores para avaliar a efetividade da prática de gestão B.3.3 Potencial de replicação

B.3.1 Mecanismo de aprendizado da prática de gestão (avaliação da efetividade e melhoria)

Após a implementação, foi estabelecida uma **sistemática estruturada de avaliação recorrente**. O **Comitê de Segurança Cibernética** realiza reuniões **trimestrais**, com participação de diretores, gestores de TI e TO, especialistas do SOC 24x7 e área de compliance. Além disso, são conduzidas **auditorias externas anuais** e **simulações práticas de ataque (red team/blue team)**, garantindo validação independente da efetividade.

Esse modelo permitiu um **ciclo contínuo de aprendizado**: cada rodada de avaliação gera recomendações, que são transformadas em planos de ação, revisados no ciclo seguinte. Exemplos concretos incluem o **reforço do MFA** após testes iniciais e a **criação de conectores específicos** para integração de sistemas legados ao SIEM. Assim, a prática evolui continuamente, reforçando maturidade e confiabilidade.

B.3.2 Consistência dos indicadores para avaliar a efetividade da prática de gestão

Os **indicadores** foram desenvolvidos em conjunto pelo Comitê, com base em **benchmarks internacionais** (NIST, ISO 27001, IEC 62443) e experiências de utilities que sofreram ataques cibernéticos. Esse processo garantiu **alinhamento estratégico**, **mensurabilidade prática** e **comparabilidade externa**.

Os principais indicadores são:

[3] Ver nos Critérios MEGSA®ESG o fator "Efetivo", usado para avaliar processos gerenciais, para melhor compreensão

- Número de **incidentes críticos** (meta: redução de 30%);
- **MTTR médio** (meta: redução de 50%);
- **% de conformidade em auditorias externas e regulatórias** (meta: 100%);
- **Security Scorecard** corporativo (meta: elevar a nota até nível A);
- **% de equipe treinada** em cibersegurança aplicada a ambientes industriais (meta: 80%).

Cada indicador possui **meta definida**, é acompanhado **trimestralmente** e reportado ao Conselho de Administração, assegurando rastreabilidade e consistência na avaliação da efetividade da prática.

B.3.3 Potencial de replicação

A prática já foi **replicada em outras unidades do Grupo Águas do Brasil**, garantindo padronização em diferentes estados e operações. A experiência também foi **compartilhada em fóruns setoriais de saneamento e eventos de cibersegurança**, inclusive sendo premiada em um evento da 4Network, permitindo que outras empresas adotem os aprendizados.

Além disso, o modelo tem potencial para ser aplicado em **utilities de energia, transporte e infraestrutura crítica**, uma vez que combina **gestão de riscos cibernéticos com inovação digital (BI, datalake, machine learning)**. Esse potencial de disseminação amplia os ganhos, fortalece a segurança de setores estratégicos e consolida a prática como referência de mercado.

C. OS RESULTADOS (peso 35)
C.1 Apresentar um ou mais resultados relevantes, medidos antes e depois da implementação da prática. A demonstração dos resultados de desempenho deve ser compatível com as descrições do ganho potencial ou da situação adversa mencionados em A.1 e dos objetivos da prática citados em B.1. Ex.: se os maiores impactos eram o custo elevado por reparo e a baixa produtividade por reparo e o objetivo reduzir custos, deveriam ser demonstradas reduções de custo por reparo e de tempo por reparo. Se o resultado apresentado não decorreu preponderantemente da prática, justificar sua correlação com ela. Os resultados podem ser expressos quantitativamente por meio de indicador(es) de desempenho[4] com resultados "antes" e "depois" ou por comparação com grupos de controle relevantes em que a melhoria do desempenho de uma prática pode ser avaliada por comparação com outra organização que não implementou a prática e manteve o mesmo processo anterior que era comum a ambas. A mudança significativa de patamar se configura quando o nível de desempenho após a implementação da prática mudar para patamar significativo acima do nível de desempenho do período anterior à prática. **O Resumo do Case no início deste documento deve sumarizar com clareza o principal resultado da Prática de Gestão desta questão.** Apresentar referenciais comparativos pertinentes (ver Glossário Critérios de Avaliação MEGSA®ESG), do setor ou do mercado, que permitam avaliar a competitividade do resultado alcançado pela prática. Se o resultado apresentado não decorrer preponderantemente da prática, justificar sua correlação com ela.
Fatores de avaliação C.1.1 Evolução de resultados comprova ganho (Resumo do Case o sumariza) C.1.2 Nível de desempenho alcançado demonstra competitividade

C.1.1 Evolução de resultados comprova ganho (Resumo do Case o sumariza)

A prática implantada demonstrou evolução clara e mensurável em relação à situação inicial, superando as metas estabelecidas no planejamento:

- **Redução de incidentes críticos:**
  - Antes (2021): média de **12 incidentes críticos/ano**.
  - Depois (2024): **4 incidentes críticos/ano** → queda de **67%**.
- **Tempo médio de resposta (MTTR):**
  - Antes (2021): **18 horas** em média para tratamento de incidentes.
  - Depois (2024): **6 horas** → redução de **67%**, superando a meta de 50%.
- **Conformidade em auditorias regulatórias:**
  - Antes (2021): **65% de conformidade**.
  - Depois (2024): **100% de conformidade** com requisitos regulatórios e auditorias externas.
- **Capacitação de equipe:**
  - Antes (2021): **15% da equipe** treinada em cibersegurança industrial.
  - Depois (2024): **82% da equipe** treinada, ultrapassando a meta de 80%.

[4] Ver glossário "Indicadores" no MEGSA®ESG.

- **Indice de Perdas (indicador mais importante para sociedade e meio ambiente)**

  2021 – 20,61%
  2022 – 17,05%
  2023 – 16,86%
  2024 – 14,38%

Esses avanços comprovam a **mudança de patamar de desempenho**: de um cenário de vulnerabilidades críticas para um ambiente de **alta maturidade digital, controle e governança integrada**.

Desde a implantação da prática não houve nenhum incidente de cibersegurança.

C.1.2 Nível de desempenho alcançado demonstra competitividade

Os resultados obtidos colocaram a organização em posição de destaque frente ao setor:

- **Security Scorecard (benchmark internacional):**
  - Média do setor de utilities na América Latina (2024): nota **C**.
  - Grupo Águas do Brasil (2021): nota **C**.
  - Grupo Águas do Brasil (2024): nota **A**, posicionando-se entre as **3 melhores concessionárias do setor no país**.
- **Comparativo setorial:** enquanto diversas utilities ainda operam com inventários manuais e baixa integração TI/TO, a prática implantada elevou a organização ao patamar , com **SOC 24x7**, **SIEM integrado**, **datalake corporativo** e aplicação de **machine learning** para prevenção de falhas.

Esse nível de desempenho demonstra não apenas competitividade no setor de saneamento, mas também **caráter de inovação com potencial de liderança em utilities de infraestrutura crítica**.

No ano de 2024 foi realizado um assessment junto a Fortinet, um dos maiores players de segurança do mundo, que nos colocou como uma empresa que estava no TOP 5 de maturidade de segurança em TI e TO na américa.

#	VENDOR	SCORE	PERCENTILE	30-DAY	INDUSTRY	TAGS
1	Riomaissaneamento	A	90	11%	unknown	
2	Grupoaguasdobrasil	A	90	11%	manufacturing	
3	Igua	C	74	5%	financial services	
4	Aegea	C	74	1%	energy	
5	Brkambiental	C	72	3%	energy	
6	SABESP	F	51	-2%	energy	

Security Score Card

C.2. Quais são outros benefícios intangíveis decorrentes da implementação da prática, baseados em fatos, depoimentos ou reconhecimentos? **Resumir** os benefícios para cada parte interessada alcançada, **enfatizando** o impacto transformador positivo decorrente da prática. **Incluir** a contribuição para o alcance dos objetivos estratégicos da organização que foram citados em A.1.
Fatores de avaliação C.2.1 Benefícios intangíveis para as partes interessadas

C.2.1 Benefícios intangíveis decorrentes da prática

A implementação da integração entre TI e TO gerou uma série de **benefícios intangíveis**, que extrapolam os resultados quantitativos e se refletem em confiança, reputação e alinhamento estratégico.

Para colaboradores e lideranças

- **Cultura de segurança fortalecida:** workshops, treinamentos e simulações práticas aumentaram o engajamento e o senso de responsabilidade de todos os níveis hierárquicos. Hoje, colaboradores relatam maior clareza sobre seu papel na proteção da infraestrutura crítica.
- **Confiança organizacional:** a existência de playbooks, SOC 24x7 e processos padronizados reduziu a insegurança em situações de crise, trazendo tranquilidade operacional e confiança na capacidade de resposta da empresa.

Para a alta gestão e governança

- **Tomada de decisão baseada em dados:** a construção do **datalake corporativo** e os painéis de **BI** permitiram que decisões estratégicas fossem tomadas com base em evidências concretas, elevando a qualidade da governança.
- **Integração ao planejamento estratégico:** a prática reforçou objetivos já mencionados em A.1, como a continuidade dos serviços, a inovação tecnológica e a maturidade digital da organização.

Para clientes e sociedade

- **Segurança e confiabilidade do serviço:** hospitais, escolas e comunidades passaram a contar com maior confiabilidade no abastecimento de água, fortalecendo a percepção de responsabilidade social da empresa.
- **Reconhecimento externo:** a organização passou a ser vista como **referência** em boas práticas de segurança cibernética, sendo convidada a compartilhar sua experiência em fóruns e eventos técnicos.

Para reguladores e órgãos de controle

- **Transparência e conformidade:** auditorias tornaram-se mais ágeis e assertivas, com inventários dinâmicos e relatórios automatizados.

Os depoimentos internos e reconhecimentos externos demonstram que a prática teve um **impacto transformador positivo**, consolidando a cultura de segurança, fortalecendo a governança, aumentando a confiança social e elevando a reputação institucional da organização.

Esses benefícios intangíveis reforçam a contribuição da prática para o alcance dos **objetivos estratégicos da organização**, citados em A.1, e consolidam sua posição como **líder em inovação e proteção de infraestrutura crítica** no setor de saneamento.

C.3. Quais foram as principais lições aprendidas, favoráveis e desfavoráveis[5], com a implementação da prática e com o alcance de seus resultados? **Citar** as lições e resumir a importância delas, para outras organizações considerarem.
Fatores de avaliação C.3.1 Lições aprendidas

C.3.1 Lições aprendidas com a implementação da prática

A implantação da prática de integração entre TI e TO gerou um conjunto de **lições aprendidas**, tanto favoráveis quanto desfavoráveis, que foram decisivas para o alcance dos resultados e servem de referência para outras organizações.

Lições favoráveis

1. **Integração é mais eficaz quando há patrocínio da alta gestão:** o envolvimento do Conselho de Administração e da diretoria foi essencial para garantir recursos, engajamento e priorização estratégica.
2. **Automação de inventário e monitoramento reduz esforço e aumenta confiabilidade:** a criação de inventário dinâmico e o SIEM integrado permitiram maior assertividade em auditorias e respostas a incidentes.
3. **Treinamento recorrente transforma cultura:** a prática demonstrou que capacitação contínua gera engajamento e fortalece a percepção de que segurança é responsabilidade de todos.
4. **Transformar risco em oportunidade gera inovação:** a integração segura de TI e TO possibilitou a criação do datalake corporativo e abriu caminho para BI e machine learning, superando o escopo original de apenas proteger sistemas.

Lições desfavoráveis

1. **Resistência cultural inicial foi subestimada:** a percepção de que TI e TO tinham prioridades distintas atrasou algumas etapas. A lição foi intensificar workshops de sensibilização desde o início.
2. **Integração de sistemas legados demandou mais tempo e recursos do que o previsto:** alguns equipamentos antigos não possuíam conectores nativos, exigindo customizações. A lição foi incluir essa complexidade no planejamento e no orçamento.
3. **Dependência de fornecedores externos exige governança reforçada:** provedores de SOC e consultorias precisam ser avaliados continuamente para garantir aderência a padrões e metas.

Importância das lições

[5]Algo que não deu certo ou que poderia ter dado melhor resultado se fosse feito de forma diferente, requerendo cuidados ou atenção especial

Essas lições reforçam que:

- **Patrocínio da liderança, automação e cultura** são fatores críticos de sucesso para qualquer organização que deseje proteger sua infraestrutura crítica.
- **Planejamento realista e gestão da mudança** são indispensáveis para superar resistências culturais e técnicas.
- **Governança de fornecedores** deve ser tratada como parte do risco corporativo.
- **Inovação pode emergir da adversidade**, mostrando que práticas de segurança, quando bem estruturadas, também geram valor estratégico.

As lições aprendidas demonstram a maturidade da prática e ampliam seu valor para outras organizações do setor de saneamento e de utilities em geral. Elas oferecem **insumos replicáveis**, orientando tanto o que deve ser priorizado quanto os desafios que precisam ser antecipados, consolidando a prática como referência setorial.

---------- Limite de 13 Páginas aqui ----------

Glossário (opcional)
Citar, se necessário, glossário para siglas e termos não usuais. Não há pontuação para este tópico e não deve ser incluído contagem para limite de páginas.

CSF: Cybersecurity Framework – estrutura do NIST para gestão de riscos cibernéticos.

IA: Inteligência Artificial – sistemas que simulam inteligência humana.

IDS/IPS: Intrusion Detection/Prevention System – sistemas de detecção e prevenção de intrusões em redes.

IEC: International Electrotechnical Commission – organismo internacional de normalização elétrica/eletrônica.

ISA: International Society of Automation – associação global voltada à automação industrial.

ISO: International Organization for Standardization – organização internacional de padronização.

MFA: Multi-Factor Authentication – autenticação por múltiplos fatores.

MTTR: Mean Time to Repair/Recovery – tempo médio para reparar ou recuperar um sistema.

NRW: Non-Revenue Water – água produzida e não faturada (perdas físicas e comerciais).

NIST: National Institute of Standards and Technology – instituto dos EUA que define padrões, inclusive em segurança cibernética.

RACI: Responsible, Accountable, Consulted, Informed – matriz de responsabilidades em projetos.

SIP: Session Initiation Protocol – protocolo para iniciar e gerenciar comunicações VoIP.

TI: Tecnologia da Informação – gestão de dados, sistemas e infraestrutura digital.

TO: Tecnologia Operacional – sistemas e equipamentos de operação industrial.

VPN: Virtual Private Network – rede privada virtual que garante comunicação segura.

Referências Bibliográficas
Citar a bibliografia utilizada no âmbito do Case, exceto os Critérios MEGSA®ESG. Não há pontuação para este tópico e não deve ser incluído na contagem para limite de páginas.

Xxxxxxxxx: xxxxxxxxxx (incluir linhas se necessário)

Revisores 2025 Ver página 2 Critérios IGS