

Caso de estudo: AQUÁRIA – Águas do Vale Verde, S.A.

Caso ilustrativo, construído para fins pedagógicos. A empresa, as pessoas e os dados são fictícios.

A empresa

A AQUÁRIA é a concessionária dos serviços de abastecimento de água e saneamento de sete municípios do Vale Verde, servindo cerca de 410 mil habitantes. Tem 580 colaboradores e um volume de negócios de 96 milhões de euros. A concessão termina em 2028 e a negociação da renovação com os municípios e com o regulador do setor começa em 2027. Os critérios que vão pesar na decisão são conhecidos: continuidade do abastecimento, qualidade de serviço medida pelos indicadores do regulador, nível de perdas de água (atualmente 27%) e resposta às reclamações dos clientes.

A estratégia 2025–2028

A CEO, Marta Figueiredo, levou à administração uma estratégia com quatro prioridades:

- **Renovar a concessão:** garantir a renovação da concessão, demonstrando um serviço fiável e bem gerido;
- **Programa Rede Inteligente:** instalar 140 mil contadores inteligentes e telemetria em 220 estações elevatórias e reservatórios, com os dados centralizados numa plataforma na cloud fornecida por uma start-up. A meta é reduzir as perdas de água de 27% para 18%;
- **Crescer por aquisição:** integrar em 2026 os serviços municipalizados de um município vizinho, acrescentando cerca de 60 mil habitantes;
- **Eficiência:** reduzir 8% do custo operacional até 2028.

O que diz o último relatório ao Comité de Risco

- **Certificação.** A AQUÁRIA tem certificação ISO/IEC 27001 desde 2023. O âmbito cobre os sistemas de faturação, o ERP e a sede.
- **Investimento.** O orçamento de cibersegurança cresceu 45% em dois anos. Foram adquiridos EDR para todos os portáteis, um SIEM e um serviço de SOC externo 24x7 que monitoriza a rede de IT.
- **Pentest.** O teste de intrusão anual, feito às aplicações web de cliente, não encontrou vulnerabilidades críticas.
- **Phishing.** A taxa de clique nas simulações trimestrais de phishing é de 4%.
- **Rede SCADA.** A rede de supervisão e controlo (SCADA) é gerida por um fornecedor de automação, que faz manutenção remota através de uma ferramenta comercial de acesso remoto com uma conta partilhada pela sua equipa. Parte dos postos de operação ainda corre Windows 7, porque o software de supervisão não está certificado para versões mais recentes.
- **Rede Inteligente.** Os dados dos contadores inteligentes já instalados (cerca de 30 mil) são enviados para a plataforma cloud da start-up. O contrato foi negociado pela Direção de Operações e não inclui cláusulas de segurança nem direito de auditoria.

- **Incidente de março.** Em março, um ataque de ransomware ao prestador de serviços de pagamentos deixou o portal de clientes e a emissão de faturas indisponíveis durante três dias. Houve 2.300 reclamações e o regulador pediu explicações por escrito. Internamente, o evento foi classificado como "incidente de terceiro, sem impacto na infraestrutura AQUÁRIA" e não consta das estatísticas de incidentes de segurança.
- **Regulação.** A AQUÁRIA foi identificada como entidade essencial no novo regime jurídico de cibersegurança que transpõe a Diretiva NIS2, com obrigações de gestão de risco, notificação de incidentes e responsabilização do órgão de gestão.
- **Governo.** O CISO reporta ao Diretor de Sistemas de Informação. O Comité de Segurança reúne trimestralmente com o CIO, o CISO e o Diretor Jurídico; o Diretor de Operações, responsável pela rede de água e pela telemetria, não participa. O plano de continuidade de negócio foi revisto pela última vez em 2019 e centra-se em falhas de energia e cheias.
- **Aquisição.** A due diligence aos serviços municipalizados a adquirir indica que não existe função de segurança e que os sistemas de gestão comercial estão numa versão sem suporte.

Na última reunião, a administração concluiu: "A segurança está controlada. Temos certificação, temos SOC e não tivemos nenhum incidente grave."

O vosso trabalho

- A AQUÁRIA tem ou não um desafio de cibersegurança? Se sim, qual?
- Preparem um pitch de 2 minutos para a CEO com o vosso diagnóstico e o que propõem fazer.
- Podem usar IA generativa. Guardem o prompt que usaram.