Reglyze

Exercício de tabletop NIS 2 / RJC — Briefing — Compromisso de fornecedor OT — cadeia de abastecimento da água

PT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-05-24T02:09:24.044Z

Classification: Confidential

Compromisso de fornecedor OT — cadeia de abastecimento da água

Exercício de tabletop NIS 2 — Artigo 21(2)(f) · RJC (DL n.º 125/2025) art. 27.º al. f) e art. 39.º

Setor	**Águas**
Severidade	Significativo (incidente reportável)
Duração sugerida	75 minutos
Identificador	`pt-water-utility-supply-chain-mfa-gap`
Emitido em	24/05/2026

Contexto

Uma empresa municipal de águas (estilo Taviraverde E.M., ~35 colaboradores, três estações elevatórias e dois reservatórios) qualifica como entidade essencial nos termos do RJC (Anexo I — água potável). A SCADA e os PLCs das estações são mantidos por um integrador OT externo (estilo NETisON), com acesso remoto contínuo via VPN para gestão de firmware e configuração de PLCs.

O contexto do exercício é uma cadeia de eventos clássica: o integrador é comprometido por ransomware nas suas próprias redes, e o acesso remoto do integrador aos clientes torna-se um vetor de propagação. O exercício explora o reflexo «o nosso fornecedor foi atacado — somos vítima por extensão» e força a equipa a fundamentar a decisão de notificação significativa ao abrigo do RJC, mesmo na ausência de impacto efetivo na qualidade da água.

É também o cenário em que o registo MyCiber e o widget de pré-preenchimento de notificações (Task 4.2 pt-market-parity) prestam valor operacional concreto — a equipa deve usar os dados pré-preenchidos como ponto de partida para a notificação inicial.

Sequência de injeções (T+0 → T+72h)

Os tempos seguem o relógio do RJC art. 42.º (24h alerta inicial / 72h notificação). O facilitador lê cada injeção em voz alta no momento marcado ou comprime o exercício num bloco de 60-90 minutos.

Momento	Injeção	#
T+0	T+0. 14:08. O integrador OT que mantém a SCADA da empresa municipal de águas envia um boletim urgente: detetou-se ransomware na sua infraestrutura interna na noite anterior. O acesso remoto que o integrador usa para gerir os PLCs da estação elevatória pode ter sido comprometido. O integrador suspendeu todas as sessões mas o registo de acesso indica três logins recentes vindos de IPs não habituais nas últimas 36 horas.	1
T+15min	T+15min. A operadora SCADA verifica que as últimas alterações de setpoint nas bombas P-01 e P-03 foram feitas há 19 horas a partir do canal do integrador. As alterações parecem técnicas e	2

Momento	Injeção	#
	normais à primeira vista. Não existe registo independente que confirme que a operação foi autorizada pelo eng.º de turno daquela noite.	
T+1h	T+1h. O delegado de cibersegurança do município contacta a empresa. O Presidente da Câmara quer saber se há risco para a qualidade da água. Análises laboratoriais estão a ser intensificadas. O CNCS confirma estar a investigar um cluster de incidentes ligados ao mesmo integrador noutros municípios.	3
T+4h	T+4h. A revisão forense do log do PLC mostra que um dos comandos enviados tentou alterar o dosagem de hipoclorito de 1.1 mg/L para 0.3 mg/L — falhou porque excedia o limite hardcoded no PLC. Não houve alteração efetiva à qualidade da água. Mas a tentativa existiu. A direção debate se isto é «incidente significativo» nos termos do RJC.	4
T+24h	T+24h. Notificação inicial ao CNCS submetida há ~6 horas (decisão tomada após reunião do órgão de gestão: a tentativa de alteração de dosagem com potencial impacto na saúde pública qualifica). O contrato com o integrador está sob revisão jurídica. A Câmara emitiu comunicado sereno sublinhando que a água continua segura. Surgem questões do jornal local sobre auditoria a outros fornecedores OT.	5
T+72h	T+72h. Atualização de 72h ao CNCS (art. 42.º n.º 3 RJC) submetida com avaliação completa: vetor de origem identificado (acesso remoto do integrador sem MFA), nenhum cliente afetado, medidas aplicadas (revogação de credenciais, MFA obrigatório em todos os canais de fornecedores OT, auditoria iniciada à cadeia de abastecimento). Plano de remediação para apresentar na CNCS dentro do prazo de 30 dias úteis após fim do impacto (art. 44.º RJC).	6

Perguntas para discussão

Para o facilitador ler verbatim. Surfar lacunas — não fornecer respostas.

1. Quantos fornecedores externos têm acesso remoto à infraestrutura OT? Esse registo está atualizado? Existe MFA obrigatório em todos os canais?
2. Qual é o SLA contratual de notificação de incidente do integrador? Está documentado? Foi cumprido neste exercício?
3. O limite hardcoded no PLC que travou a alteração de dosagem é um controlo de segurança intencional ou um acaso afortunado? Está documentado como controlo de segurança formal?
4. Quem na organização tem autoridade para decidir que um incidente é «significativo» nos termos do RJC? É decisão do órgão de gestão (art. 25.º) ou pode ser delegada?
5. A tentativa de alteração de dosagem (que falhou) qualifica como incidente significativo? Que critérios do art. 40.º RJC se aplicam? (Pista: «possa vir a existir».)
6. Como se comunica com a Câmara/município sem entrar em pânico público? Quem é o porta-voz único?
7. O contrato com o integrador OT prevê auditorias de cibersegurança? Inclui cláusulas de notificação imediata? Inclui responsabilidade por compromisso de credenciais?

Ações esperadas (chave de correção pós-exercício)

Linha de base do que uma organização madura faz neste cenário. Comparar com o desempenho da equipa durante o debriefing.

1. Revogar imediatamente as credenciais e tokens VPN do integrador OT; forçar reset de MFA em todas as contas administrativas; bloquear os IPs suspeitos identificados nos logs.
2. Reverter todas as alterações de setpoint nos PLCs P-01 e P-03 aos valores de referência conhecidos; reforçar amostragem laboratorial em todos os pontos a jusante das estações afetadas.
3. Convocar reunião do órgão de gestão para decisão formal sobre qualificação do incidente como significativo (art. 25.º RJC — não delegável); registar a decisão e a fundamentação.
4. Notificar o CNCS via plataforma eletrónica dentro do prazo de 24h após a decisão (art. 42.º n.º 1 RJC), mesmo na ausência de impacto efetivo — a «possibilidade de existir» é suficiente (art. 42.º n.º 1).
5. Coordenar com o município/Câmara como entidade responsável da operação; alinhar comunicação pública com o CNCS antes de divulgação.
6. Avaliar o contrato com o integrador OT à luz do art. 28.º RJC (cadeia de abastecimento) — práticas de cibersegurança do fornecedor, MFA obrigatório, monitorização de acessos, cláusula de incidente.
7. Submeter atualização de 72h ao CNCS (art. 42.º n.º 3) e calendarizar o relatório final dentro de 30 dias úteis após fim do impacto significativo (art. 44.º n.º 1 RJC).
8. Lançar auditoria a toda a cadeia de abastecimento OT — quantos fornecedores têm acesso remoto? Qual é o controlo de acessos? Existe MFA? Qual é o SLA de notificação de incidentes do fornecedor?

Referências regulatórias

Funções QNRCS (proxy NIST CSF 2.0)	ID · PR · DE · RS
Artigos da Diretiva (UE) 2022/2555	• Article 21(2)(d) • Article 21(2)(i) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b)

Artigos do RJC (DL n.º 125/2025 — anexo)	• art. 27.º n.º 1 al. c) RJC (cadeia de abastecimento) • art. 28.º RJC (capítulo dedicado à cadeia de abastecimento) • art. 27.º n.º 1 al. h) RJC (controlo de acesso e gestão de ativos) • art. 27.º n.º 1 al. i) RJC (MFA) • art. 40.º RJC (regra geral de notificação) • art. 42.º n.º 1 RJC (24h) • art. 42.º n.º 3 RJC (72h) • art. 44.º n.º 1 RJC (30 dias úteis)

Este documento é um briefing de cenário Reglyze para exercício offline. Não constitui aconselhamento jurídico. Para casos complexos consulte o seu jurista ou o CNCS através de myciber.gov.pt.

Reglyze · https://reglyze.com