Reglyze

Exercício de tabletop NIS 2 / RJC: briefing · Compromisso de fornecedor OT na cadeia de abastecimento da água

Cenário de exercício de tabletop

Organização: Reglyze

Versão: v1

Data: 2026-11-25

Classificação: confidencial

Compromisso de fornecedor OT na cadeia de abastecimento da água

Exercício de tabletop NIS 2 — Artigo 21(2)(f) · RJC (DL n.º 125/2025) art. 27.º n.º 1 al. e)

Setor	**Águas**
Severidade	Significativo (incidente reportável)
Duração sugerida	75 minutos
Identificador	`pt-water-utility-supply-chain-mfa-gap`
Emitido em	25/11/2026

Contexto

Uma empresa municipal de águas (~35 colaboradores, três estações elevatórias e dois reservatórios; Anexo I do RJC, setor 6, água potável). Pela sua dimensão ficaria fora do RJC, mas uma perturbação do abastecimento pode afetar consideravelmente a saúde pública: está abrangida independentemente da dimensão (art. 3.º n.º 2 al. c) RJC) e o CNCS qualificou-a como entidade essencial (art. 6.º n.º 1 al. f) RJC). A SCADA e os PLCs das estações são mantidos por um integrador OT externo, 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 vítimas 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 a informação já comunicada na plataforma eletrónica do CNCS (art. 8.º n.º 1 RJC) e um modelo de notificação preparado com antecedência poupam tempo: a equipa parte deles para a notificação inicial.

Sequência de injeções (T+0 → T+72h)

Os tempos seguem o relógio do art. 42.º do RJC: notificação inicial até 24 horas após a verificação do incidente significativo e, quando necessário, a sua atualização até 72 horas. 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

Momento	Injeção	#
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 normais à primeira vista. Não existe registo independente que confirme que a operação foi autorizada pelo eng.º de turno daquela noite.	2
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 a dosagem de hipoclorito de 1,1 mg/L para 0,3 mg/L; falhou porque excedia o limite fixo programado 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 da notificação inicial enviada ao CNCS (art. 42.º n.º 3 RJC), com a avaliação inicial: 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). Relatório final a submeter ao CNCS no prazo de 30 dias úteis a contar da notificação do fim de impacto (art. 44.º n.º 1 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 fixo programado no PLC, que travou a alteração de dosagem, é um controlo de segurança intencional ou um feliz acaso? Está documentado como controlo de segurança formal?
4. Quem, na organização, decide que um incidente é significativo, e em quanto tempo? O procedimento interno di-lo, e o órgão de gestão aprovou-o, como aprova as medidas de cibersegurança (art. 25.º n.º 1 al. a) RJC)?
5. A tentativa de alteração de dosagem (que falhou) é um incidente significativo? Que parâmetros do art. 40.º n.º 3 RJC pesam aqui, e o que muda o facto de a definição (art. 2.º al. l) RJC) abranger o que «seja suscetível de causar» graves perturbações?
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. Decidir, pelo procedimento interno de resposta a incidentes, se o incidente é significativo (art. 2.º al. l) RJC: basta que «seja suscetível de causar» graves perturbações); registar quem decidiu, a hora e a fundamentação, e informar o órgão de gestão, que aprova e supervisiona as medidas de cibersegurança (art. 25.º n.º 1 als. a) e b) RJC).
4. Notificar o CNCS na plataforma eletrónica (art. 40.º n.º 6 RJC) até 24 horas depois de concluir que o incidente significativo existe ou «possa vir a existir» (art. 42.º n.º 1 RJC), mesmo sem impacto efetivo na qualidade da água.
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. Enviar ao CNCS, quando necessário, a atualização da notificação inicial até 72 horas após a verificação (art. 42.º n.º 3 RJC); notificar o fim do impacto significativo nas 24 horas seguintes (art. 43.º n.º 1 RJC) e calendarizar o relatório final no prazo de 30 dias úteis a contar da notificação do fim de impacto significativo (art. 44.º n.º 1 RJC).
8. Lançar uma 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

Objetivos QNRCS	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 (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 n.os 1 e 6 RJC (dever de notificar; plataforma eletrónica) • art. 42.º n.º 1 RJC (24h) • art. 42.º n.º 3 RJC (atualização até 72h, quando necessário) • art. 2.º al. l) RJC (incidente significativo) • 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