Reglyze

Exercício de tabletop NIS 2 / RJC: briefing · DDoS contra o portal municipal de uma entidade pública relevante

Cenário de exercício de tabletop

Organização: Reglyze

Versão: v1

Data: 2026-11-25

Classificação: confidencial

DDoS contra o portal municipal de uma entidade pública relevante

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

Setor	**Genérico (transversal)**
Severidade	Suave (treino básico)
Duração sugerida	60 minutos
Identificador	`pt-municipal-ddos-public-relevant`
Emitido em	25/11/2026

Contexto

Uma câmara municipal portuguesa (~600 colaboradores, ~80 mil habitantes) opera os portais de atendimento ao munícipe online, plataforma de marcação de atendimento, serviços de finanças locais e a gestão indireta dos serviços municipalizados de água. Não tendo sido qualificada como entidade essencial nem importante, a câmara é uma entidade pública relevante (art. 7.º n.º 1 RJC), do Grupo A, como entidade da administração autónoma com mais de 250 trabalhadores no seu quadro de pessoal (art. 7.º n.º 2 al. e)): uma categoria portuguesa que alarga o RJC para além das classes da NIS 2.

O exercício é um DDoS volumétrico + camada 7 que perturba os portais de atendimento mas não toca a infraestrutura OT da água. É deliberadamente um cenário mais ligeiro do que os anteriores: o objetivo é treinar a articulação com o CERT.PT, o plano B de atendimento presencial, a comunicação aos munícipes via canais oficiais, e o reflexo de notificação ao CNCS mesmo quando o impacto é principalmente de disponibilidade administrativa.

Ilustra também o regime próprio destas entidades: notificam os incidentes significativos como as essenciais e as importantes (arts. 40.º a 44.º RJC), cumprirão as medidas que o CNCS fixar por regulamento para o seu grupo (art. 33.º, com efeitos a partir de 22 de junho de 2028, DL n.º 125/2025, art. 10.º n.º 2) e ficam sujeitas às medidas de execução do art. 56.º e à supervisão ex post do art. 55.º (art. 33.º n.º 3).

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. 08:55. Os portais de atendimento ao munícipe da câmara municipal começam a responder com erros 503. O CDN reporta tráfego anómalo: pico de 14 Gbps com padrões SYN flood + L7 GET	1

Momento	Injeção	#
	burst no portal de marcação online. Os funcionários do balcão informam que as listas de chamada da plataforma de marcação estão a falhar.	
T+15min	T+15min. O CDN ativou mitigação automática mas o tráfego continua. O portal principal está intermitente. A linha de apoio ao munícipe enche-se. O Vereador da Modernização Administrativa pede ponto de situação.	2
T+1h	T+1h. O CERT.PT confirma estar a observar um cluster de DDoS contra portais municipais em vários distritos. Atribuição preliminar a um grupo hacktivista por mensagem em fórum. Os sistemas OT dos serviços municipalizados de água estão intactos. O ataque é exclusivamente contra o atendimento administrativo.	3
T+4h	T+4h. Mitigação CDN aumentada (regras WAF L7 + scrubbing center upstream). Tráfego malicioso reduzido em ~80%. Portais voltam a responder. Plano B de atendimento presencial reforçado: senhas em papel; pedidos urgentes (urbanismo, ação social, faturação da água) tratados primeiro. Imprensa local pede declarações.	4
T+24h	T+24h. Notificação inicial submetida ao CNCS na plataforma eletrónica: a câmara notifica enquanto entidade pública relevante do Grupo A (arts. 7.º n.º 2 al. e) e 40.º n.º 1 RJC). O Vereador comunica em conferência de imprensa. Investigação preliminar com o CERT.PT em curso. Plano de continuidade de atendimento sustentado durante o pico.	5
T+72h	T+72h. Mitigação estabilizada; os portais operam normalmente desde a véspera e a câmara notificou o fim do impacto significativo ao CNCS nas 24 horas seguintes (art. 43.º n.º 1 RJC). Não foi necessária a atualização das 72 horas, que o art. 42.º n.º 3 RJC só pede quando necessário. Lições aprendidas: a capacidade contratada do CDN estava subdimensionada; o runbook de comunicação aos munícipes necessita revisão; o plano B em papel funcionou mas tem limites de escala. Relatório final em preparação, 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. A câmara é uma entidade pública relevante (art. 7.º RJC) ou foi qualificada como essencial (art. 6.º n.º 1 al. d) RJC)? De que grupo? Quando recebeu a notificação da sua qualificação (art. 8.º n.º 5 RJC)?
2. Qual é a capacidade de scrubbing contratada com o CDN? Foi suficiente para o pico de 14 Gbps? Qual é o SLA de escalamento para scrubbing center upstream?
3. Quem é o porta-voz nas redes sociais oficiais da câmara durante um incidente cyber? Existe runbook documentado para esta articulação?
4. O plano B de atendimento presencial em papel: qual é a sua capacidade real? Em quanto tempo se esgota se o portal estiver fora durante 24h?
5. A câmara distribui água através dos serviços municipalizados: não será também uma entidade do Anexo I (setor 6, água potável), com outra qualificação e outros deveres? Que notificação seria devida se o ataque tocasse esses sistemas?

6. Que IOCs se partilham com o CERT.PT? Em que canal? Em que formato (MISP, STIX, email)?
7. Quem, na câmara, decide que o incidente é significativo, com que parâmetros (art. 40.º n.º 3 RJC), e onde fica registada essa decisão?

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. Ativar a mitigação CDN/WAF nos níveis máximos contratados; escalar para scrubbing center upstream se disponível.
2. Comunicar aos munícipes via SMS + redes sociais oficiais + meios locais: portais intermitentes, plano B de atendimento presencial ativo, números prioritários.
3. Notificar o CNCS na plataforma eletrónica (art. 40.º n.º 6 RJC) até 24 horas depois de concluir que o incidente é significativo (art. 42.º n.º 1 RJC): a entidade pública relevante notifica como as essenciais e as importantes (art. 40.º n.º 1).
4. Manter o atendimento presencial reforçado durante o pico; priorizar os pedidos urgentes (certidões, urbanismo, ação social); registar processos manualmente para sincronização posterior.
5. Participar o ataque ao Ministério Público ou à PJ (Lei do Cibercrime, Lei n.º 109/2009); alinhar as declarações públicas com o CNCS antes da conferência de imprensa.
6. Coordenar com o CERT.PT a análise técnica do ataque e a partilha de indicadores de compromisso com as outras câmaras afetadas.
7. Enviar ao CNCS, quando necessário, a atualização até 72 horas após a verificação (art. 42.º n.º 3 RJC); notificar o fim do impacto significativo nas 24 horas seguintes ao seu termo (art. 43.º n.º 1 RJC); relatório final no prazo de 30 dias úteis a contar da notificação do fim de impacto (art. 44.º n.º 1 RJC).
8. Pós-incidente: rever a capacidade contratada do CDN; rever runbook de comunicação aos munícipes; validar plano B em papel num exercício de stress; documentar decisão do órgão de gestão.

Referências regulatórias

Objetivos QNRCS	PR · DE · RC
Artigos da Diretiva (UE) 2022/2555	• Article 21(2)(c) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b)
Artigos do RJC (DL n.º 125/2025 — anexo)	• art. 7.º RJC (entidades públicas relevantes, Grupos A e B) • art. 33.º RJC (medidas fixadas pelo CNCS para as entidades públicas relevantes)

	• 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. 43.º n.º 1 RJC (fim do impacto significativo, 24h) • art. 44.º n.º 1 RJC (30 dias úteis para relatório final) • art. 55.º RJC (supervisão ex post) • art. 56.º RJC (medidas de execução, por força do art. 33.º n.º 3)

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