Reglyze

Exercício de tabletop NIS 2 / RJC — Briefing — DDoS contra portal municipal — entidade pública relevante

PT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-05-24T02:15:08.507Z

Classification: Confidential

DDoS contra portal municipal — entidade pública relevante

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	**Plataforma SCADA / ICT**
Severidade	Suave (treino básico)
Duração sugerida	60 minutos
Identificador	`pt-municipal-ddos-public-relevant`
Emitido em	24/05/2026

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. A câmara qualifica como entidade pública relevante nos termos do art. 7.º do RJC (Grupo A — administração pública local) — uma categoria PT-específica que estende o âmbito subjetivo do RJC para além das categorias NIS2 essencial/importante padrão.

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 «mild» do que os anteriores — o objetivo é treinar a articulação com o CSIRT.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 a particularidade portuguesa do art. 56.º n.º 4 RJC: as entidades públicas relevantes são supervisionadas em moldes próximos à entidade importante (supervisão ex post), mas têm obrigações de notificação substancialmente iguais às essenciais — uma sobre-extensão deliberada do legislador português sobre a NIS2.

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. 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 burst no portal de marcação online. Os funcionários do balcão informam que as listas de chamada da plataforma de marcação estão a falhar.	1
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	2

Momento	Injeção	#
	pede ponto de situação.	
T+1h	T+1h. O CSIRT.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. A câmara também opera serviços de abastecimento de água por contrato municipal — esses sistemas (OT) 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 maliciosos reduzido em ~80%. Portais voltam a responder. Plano B de atendimento presencial reforçado: senhas em papel; processos prioritários (certidões de óbito, registo de eleitor) priorizados. Imprensa local pede declarações.	4
T+24h	T+24h. Notificação inicial submetida ao CNCS via plataforma eletrónica — câmara enquanto entidade pública relevante (Grupo A nos termos do art. 7.º RJC). O Vereador comunica em conferência de imprensa. Investigação preliminar com CSIRT.PT em curso. Plano de continuidade de atendimento sustentado durante o pico.	5
T+72h	T+72h. Atualização de 72h ao CNCS submetida. Mitigação estabilizada; portais a operar normalmente. Ataque arrefeceu. Lições aprendidas: capacity contratada do CDN era subestimada; runbook de comunicação aos munícipes necessita revisão; plano B em papel funcionou mas tem limites de escala. Relatório final em preparação dentro de 30 dias úteis (art. 44.º n.º 1 RJC).	6

Perguntas para discussão

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

1. A câmara qualifica como entidade pública relevante nos termos do art. 7.º RJC? Qual é o Grupo (A ou B)? Quem foi formalmente notificado dessa qualificação?
2. Qual é a capacity 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 opera serviços municipalizados de água por contrato — esses sistemas têm ponto de contacto distinto com o CNCS? Há duplicação de notificação?
6. Que IOCs se partilham com o CSIRT.PT? Em que canal? Em que formato (MISP, STIX, email)?
7. Como se documenta a decisão do órgão de gestão para qualificar como incidente significativo, dado que entidade pública relevante segue a regra geral do art. 40.º RJC?

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 via plataforma eletrónica (art. 42.º n.º 1 RJC) — entidade pública relevante notifica nos mesmos prazos (art. 56.º n.º 4 RJC).
4. Manter o atendimento presencial reforçado durante o pico; priorizar serviços críticos (certidões, registo, urbanismo de emergência); registar processos manualmente para sincronização posterior.
5. Comunicar com a CCDR e o ANSR/MAI conforme aplicável; alinhar declarações públicas com o CNCS antes de conferência de imprensa.
6. Coordenar com o CSIRT.PT no esforço de atribuição + assinatura técnica do ataque (IOCs partilháveis com outras câmaras afetadas).
7. Submeter atualização de 72h ao CNCS (art. 42.º n.º 3) com avaliação de gravidade + indicadores; relatório final dentro de 30 dias úteis após fim do impacto (art. 44.º n.º 1 RJC).
8. Pós-incidente: rever capacity 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

Funções QNRCS (proxy NIST CSF 2.0)	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 (entidade pública relevante — Grupos A e B, extensão nacional) • art. 27.º n.º 1 al. b) RJC (continuidade e gestão de crises) • art. 27.º n.º 1 al. i) RJC (autenticação e comunicações seguras) • 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 para relatório final) • art. 56.º n.º 4 RJC (supervisão ex post de entidade pública relevante)

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