Reglyze

Exercício de tabletop NIS 2 / RJC — Briefing — Fuga de credenciais — notificação dupla CNCS + CNPD

PT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-05-24T02:14:34.451Z

Classification: Confidential

Fuga de credenciais — notificação dupla CNCS + CNPD

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	Significativo (incidente reportável)
Duração sugerida	75 minutos
Identificador	`pt-credential-leak-dual-notification`
Emitido em	24/05/2026

Contexto

Uma empresa portuguesa de telecomunicações (entidade essencial nos termos do RJC, Anexo I — comunicações eletrónicas, regulada também pela ANACOM) opera um portal de cliente com ~600 mil contas ativas. Um investigador de segurança em divulgação responsável reporta a exposição de um índice Elasticsearch num ambiente de desenvolvimento que ficou acessível desde o exterior. ~38 mil utilizadores estão potencialmente expostos.

O contexto do exercício é a sobreposição NIS2 + RGPD: o incidente toca matéria de cibersegurança (RJC art. 27.º al. f) — higiene + formação, e art. 27.º al. h) — controlo de acessos e gestão de ativos) mas também matéria de proteção de dados pessoais (RGPD art. 32.º + 33.º). A equipa deve navegar dois prazos distintos: 24h para o CNCS (art. 42.º n.º 1 RJC) e 72h para a CNPD (art. 33.º RGPD).

O exercício surfa também a particularidade portuguesa do art. 35 NIS2 (coordenação CNCS/CNPD para evitar non-bis-in-idem em matéria de coimas) — a equipa deve documentar a fundamentação para não vir a ser sancionada duas vezes pela mesma falha.

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. 09:17. Um investigador de segurança escreve à empresa em divulgação responsável: o portal de cliente da empresa de telecomunicações expõe email + hash de palavra-passe via um índice Elasticsearch num ambiente de desenvolvimento esquecido. Estima 38000 contas afetadas.	1
T+15min	T+15min. A equipa confirma a existência do índice e que está acessível desde o exterior há pelo menos seis semanas. Faz takedown imediato. O hash usado é SHA-256 com salt — mas houve scraping detetado nos logs do bucket nos últimos quatro dias.	2

Momento	Injeção	#
T+1h	T+1h. O Encarregado da Proteção de Dados pede ponto de situação. A direção convoca reunião extraordinária. Não é claro ainda se isto qualifica como «incidente significativo» nos termos do RJC — é principalmente um problema RGPD com sobreposição NIS2.	3
T+4h	T+4h. A análise forense confirma 38421 utilizadores expostos, com scraping de pelo menos 12000 registos identificados nos logs. A direção decide notificar tanto o CNCS (NIS2) quanto a CNPD (RGPD). Comunicação aos utentes a ser preparada com força reset de palavra-passe próxima sessão.	4
T+24h	T+24h. Notificação inicial ao CNCS submetida via plataforma eletrónica (art. 42.º n.º 1 RJC). Notificação à CNPD a ser concluída antes das 72h (art. 33.º RGPD). Comunicação aos titulares dos dados em curso (art. 34.º RGPD). Imprensa especializada já tem a história.	5
T+72h	T+72h. Atualização de 72h ao CNCS (art. 42.º n.º 3 RJC) submetida. Notificação à CNPD entregue dentro do prazo de 72h RGPD. Comunicação aos utentes finalizada via email + banner no portal. Forçada redefinição de palavra-passe na próxima sessão. Iniciada auditoria a todos os ambientes de desenvolvimento — 14 ambientes identificados, 3 com exposição residual a corrigir.	6

Perguntas para discussão

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

1. Qual é a articulação prática entre o Encarregado da Proteção de Dados e o ponto de contacto CNCS? Reúnem-se com que frequência? Quem decide o conteúdo das notificações?
2. Os 38421 registos afetados são titulares de dados portugueses na sua maioria? Há jurisdições adicionais que devem ser notificadas (Autoridades de Proteção de Dados de outros EM)?
3. O hash SHA-256 com salt mitiga o risco para os titulares? Justifica não comunicar nos termos do art. 34.º RGPD?
4. Como se evita o non-bis-in-idem entre coima CNCS (art. 61.º RJC) e coima CNPD (art. 83.º RGPD) pela mesma falha de controlo? (Pista: art. 35 NIS2.)
5. Quem é o porta-voz único? A imprensa especializada já tem a história — qual é a janela entre notificação às autoridades e divulgação pública?
6. Quantos ambientes de desenvolvimento existem na organização? Há inventário? Qual é o ciclo de vida documentado de um ambiente dev?
7. A força redefinição de palavra-passe na próxima sessão é tecnicamente exequível em <72h? Há canal alternativo (SMS, email) para os utilizadores que não voltam a entrar?

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. Takedown imediato do índice Elasticsearch + IP block na infraestrutura periférica; recolha de logs do bucket e do balanceador para análise forense.

2. Convocar o Encarregado da Proteção de Dados e a direção para reunião conjunta — decisão formal de notificação dupla (NIS2 + RGPD) registada em ata.
3. Notificar o CNCS via plataforma eletrónica (art. 42.º n.º 1 RJC) dentro de 24h da decisão de qualificação como incidente significativo. Critério principal: art. 40.º n.º 3 RJC, impacto substancial em dados pessoais.
4. Notificar a CNPD nos termos do art. 33.º RGPD dentro de 72h, mesmo se a notificação NIS2 já tiver sido feita — são procedimentos distintos. O CNCS e a CNPD coordenam-se ao abrigo do art. 35 NIS2 + art. 8.º RJC.
5. Comunicar aos titulares dos dados nos termos do art. 34.º RGPD quando o risco for elevado — banner no portal + email + forced password reset na próxima sessão.
6. Coordenar comunicação de imprensa com o porta-voz único; alinhar conteúdo com o CNCS + CNPD antes de divulgação.
7. Submeter atualização de 72h ao CNCS (art. 42.º n.º 3) com avaliação inicial de gravidade + indicadores de exposição (12000 registos com scraping confirmado).
8. Pós-incidente: inventário completo de ambientes de desenvolvimento; controlo de acesso + segregação de redes; auditoria periódica adicionada ao plano anual.

Referências regulatórias

Funções QNRCS (proxy NIST CSF 2.0)	DE · RS · ID
Artigos da Diretiva (UE) 2022/2555	• Article 21(2)(g) • Article 21(2)(i) • Article 23(4)(a) • Article 23(4)(b) • Article 35
Artigos do RJC (DL n.º 125/2025 — anexo)	• art. 27.º n.º 1 al. f) RJC (higiene e formação) • art. 27.º n.º 1 al. h) RJC (controlo de acesso e gestão de ativos) • art. 40.º n.º 3 RJC (critérios de incidente significativo) • art. 42.º n.º 1 RJC (24h CNCS) • art. 42.º n.º 3 RJC (72h CNCS) • art. 35.º NIS2 transposto via coordenação CNCS/CNPD

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