# Reglyze

## Exercício de tabletop NIS 2 / RJC: briefing · Fuga de credenciais: notificação dupla ANACOM + CNPD

Cenário de exercício de tabletop

**Organização:** Reglyze

**Versão:** v1

**Data:** 2026-11-25

**Classificação:** confidencial

# Fuga de credenciais: notificação dupla ANACOM + CNPD

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

| | |
|---|---|
| Setor | **Plataforma SCADA / ICT** |
| Severidade | Significativo (incidente reportável) |
| Duração sugerida | 75 minutos |
| Identificador | `pt-credential-leak-dual-notification` |
| Emitido em | 25/11/2026 |

## Contexto

Uma empresa portuguesa de telecomunicações (entidade essencial nos termos do art. 6.º n.º 1 do RJC; Anexo I, infraestruturas digitais) opera um portal de cliente com ~600 mil contas ativas. A sua autoridade de cibersegurança competente não é o CNCS mas a ANACOM, autoridade setorial para as comunicações eletrónicas (art. 2.º al. b) e art. 15.º n.º 2 al. a) RJC). 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 n.º 1 als. d), f) e h): segurança no desenvolvimento, ciber-higiene e formação, controlo do acesso e gestão de ativos) mas também matéria de proteção de dados pessoais (RGPD arts. 32.º e 33.º). A equipa trabalha com dois prazos distintos: 24 horas para a ANACOM (art. 42.º n.º 1 RJC) e 72 horas para a CNPD (art. 33.º RGPD).

O exercício trabalha também o art. 79.º RJC, que transpõe o art. 35.º da NIS 2: a autoridade de cibersegurança informa a CNPD quando uma infração pode implicar uma violação de dados pessoais; se a CNPD aplicar uma coima, a autoridade de cibersegurança fica impedida de aplicar outra pela mesma infração (non-bis-in-idem, n.º 2), podendo ainda impor as medidas de execução das als. a) a h) do n.º 1 do art. 56.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. 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 |

| Momento | Injeção | # |
|---|---|---|
| **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 registos de acesso do cluster nos últimos quatro dias. | 2 |
| **T+1h** | T+1h. O Encarregado da Proteção de Dados pede ponto de situação. A direção convoca reunião extraordinária. Ainda não é claro se isto é um «incidente significativo» nos termos do RJC: é sobretudo um problema de RGPD, com sobreposição à NIS 2. | 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 a ANACOM, autoridade de cibersegurança competente para as comunicações eletrónicas (RJC), e a CNPD (RGPD). A comunicação aos utentes está a ser preparada, com redefinição forçada da palavra-passe na próxima sessão. | 4 |
| **T+24h** | T+24h. Notificação inicial à ANACOM submetida na plataforma eletrónica (arts. 40.º n.º 6 e 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 da notificação inicial enviada à ANACOM (art. 42.º n.º 3 RJC). Notificação à CNPD entregue dentro do prazo de 72h RGPD. Comunicação aos utentes concluída por email e banner no portal. Redefinição forçada da 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 permanente (art. 32.º RJC)? 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. Se a mesma falha de controlo der lugar a uma coima da CNPD (art. 83.º RGPD), pode a ANACOM aplicar outra ao abrigo do art. 61.º RJC? (Pista: non-bis-in-idem, art. 79.º n.º 2 RJC.)
5. Quem é o porta-voz único? A imprensa especializada já tem a história: qual é a janela entre a notificação às autoridades e a 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 redefinição forçada da palavra-passe na próxima sessão é tecnicamente exequível em menos de 72 horas? Há canal alternativo (SMS, email) para os utilizadores que não voltam a entrar?
8. Que regulamentos da ANACOM sobre segurança e integridade das redes e serviços continuam em vigor ao lado do RJC (DL n.º 125/2025, art. 8.º n.º 3), e o que exigem neste incidente?

## 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. Retirar de imediato o índice Elasticsearch do acesso público e bloquear os endereços IP de origem na infraestrutura periférica; recolher os registos de acesso do cluster e do balanceador para análise forense.
2. Convocar o Encarregado da Proteção de Dados e a direção para uma reunião conjunta; registar em ata a decisão de notificar ao abrigo do RJC e do RGPD.
3. Notificar a ANACOM, autoridade de cibersegurança competente para as comunicações eletrónicas (art. 2.º al. b) e art. 15.º n.º 2 al. a) RJC), na plataforma eletrónica (art. 40.º n.º 6), até 24 horas depois de concluir que o incidente é significativo (art. 42.º n.º 1). Fundamento: danos consideráveis possíveis para os titulares das contas (art. 2.º al. l) RJC), ponderados os parâmetros do art. 40.º n.º 3.
4. Notificar a CNPD nos termos do art. 33.º RGPD, no prazo de 72 horas, mesmo que a notificação ao abrigo do RJC já tenha sido feita: são deveres distintos (art. 40.º n.º 5 RJC). A articulação entre a autoridade de cibersegurança e a CNPD está no art. 79.º RJC.
5. Comunicar aos titulares dos dados nos termos do art. 34.º RGPD quando o risco for elevado: banner no portal, email e redefinição forçada da palavra-passe na próxima sessão.
6. Coordenar a comunicação de imprensa com o porta-voz único; alinhar o conteúdo com a ANACOM e a CNPD antes da divulgação.
7. Enviar à ANACOM, quando necessário, a atualização da notificação inicial até 72 horas após a verificação (art. 42.º n.º 3 RJC), com a avaliação inicial da gravidade e do impacto e os indicadores disponíveis (12000 registos com scraping confirmado). Notificar o fim do impacto significativo nas 24 horas seguintes (art. 43.º n.º 1 RJC) e entregar 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. Pós-incidente: inventário completo de ambientes de desenvolvimento; controlo de acesso + segregação de redes; auditoria periódica adicionada ao plano anual.

## Referências regulatórias

| | |
|---|---|
| **Objetivos QNRCS** | DE · RS · ID |
| **Artigos da Diretiva (UE) 2022/2555** | • Article 21(2)(g)<br>• Article 21(2)(i)<br>• Article 23(4)(a)<br>• Article 23(4)(b)<br>• Article 35 |
| **Artigos do RJC (DL n.º 125/2025 — anexo)** | • art. 2.º al. b) e art. 15.º n.º 2 al. a) RJC (ANACOM, autoridade setorial para as comunicações eletrónicas) |

| | |
|---|---|
| | • art. 27.º n.º 1 al. f) RJC (higiene e formação)<br>• art. 27.º n.º 1 al. h) RJC (controlo de acesso e gestão de ativos)<br>• art. 40.º n.º 3 RJC (parâmetros do impacto significativo)<br>• art. 42.º n.º 1 RJC (notificação inicial, 24h)<br>• art. 42.º n.º 3 RJC (atualização até 72h, quando necessário)<br>• art. 79.º RJC (violação de dados pessoais: articulação com a CNPD; transpõe o art. 35.º NIS 2) |

---

*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