Reglyze

Exercício de tabletop NIS 2 / RJC — Briefing — Acesso prolongado pós-saída — falha de offboarding

PT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-07-11T15:06:51.242Z

Classification: Confidential

Acesso prolongado pós-saída — falha de offboarding

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	**Genérico (transversal)**
Severidade	Significativo (incidente reportável)
Duração sugerida	75 minutos
Identificador	`pt-insider-threat-offboarding-gap`
Emitido em	11/07/2026

Contexto

Uma PME portuguesa do setor de tecnologia (qualifica como entidade importante nos termos do RJC — médias empresas que prestam serviços críticos), com ~240 colaboradores e faturação anual de ~22 M€, classifica-se no Anexo II do RJC (provedores de serviços geridos / MSP). O exercício surfa o cenário arquetípico de ameaça interna pós-saída: um colaborador técnico saiu há cinco semanas, a sua conta nunca foi revogada, e há evidência de acessos noturnos a partir de um IP estrangeiro.

A empresa não tem ainda PAM (Privileged Access Management) formal. O processo de offboarding existe em papel mas não foi seguido. O contexto força a equipa a navegar três jurisdições em simultâneo: NIS2 (notificação CNCS dentro de 24h), Lei do Cibercrime (queixa-crime à PJ), e LGPD-PT/RGPD (potencial violação de dados pessoais se os ficheiros acedidos incluírem dados de colaboradores ou clientes).

O exercício é particularmente relevante para PME portuguesas em fase de maturação cyber — ilustra que «entidade importante» não escapa às obrigações de notificação NIS2 só por ser mais pequena (apenas escapa às inspeções proativas — sujeita-se a supervisão ex post nos termos do art. 33 NIS2 + art. 56.º RJC).

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. 11:24. A nova engenheira de TI nota acessos noturnos à VPN com a conta de um colaborador que saiu da empresa há cinco semanas. A conta nunca foi desativada. Os logs mostram 17 sessões nas últimas três semanas, todas a partir de um IP num país vizinho. Algumas sessões tocaram em ficheiros do servidor de partilha — desenhos, propostas comerciais, listas de fornecedores.	1
T+15min	T+15min. A engenheira desativa a conta imediatamente. Convoca o responsável de TI e o director-geral. Documenta os timestamps de todas as sessões. Não há ainda informação sobre o que foi exfiltrado — só que houve acesso.	2

Momento	Injeção	#
T+1h	T+1h. O director-geral pergunta se isto é um incidente significativo. A empresa tem 240 colaboradores, factura ~22 M€/ano, qualifica como entidade importante nos termos do RJC. O Diretor de Recursos Humanos confirma que o processo de saída do antigo colaborador foi normal — não foi conflituoso, mas a checklist de offboarding falhou na linha «revogação de contas técnicas».	3
T+4h	T+4h. A análise forense detalha o que foi acedido — 423 ficheiros, incluindo a proposta comercial para o maior cliente em curso. Não há ainda confirmação de exfiltração mas o padrão de acessos é compatível com cópia para fora. A direção debate notificar a polícia (PJ — unidade de cibercrime) e o CNCS. A equipa jurídica pondera o art. 4.º Lei do Cibercrime.	4
T+24h	T+24h. Decisão tomada: notificação ao CNCS via plataforma eletrónica (incidente importante, impacto substancial em informação comercial confidencial + perda de confidencialidade de informação de cliente). Queixa-crime apresentada à PJ. Auditoria forense da estação do antigo colaborador para identificar canal de saída dos ficheiros. Cliente principal informado em reunião presencial.	5
T+72h	T+72h. Atualização de 72h ao CNCS submetida. PJ confirma abertura de inquérito. Plano de remediação: checklist de offboarding revista (inclui agora revogação de TODAS as contas técnicas em <2h da saída, validação por dois pares); gestão de privilégios revista (PAM ferramenta a avaliar); auditoria trimestral de contas dormentes adicionada ao calendário. Cliente principal reforça contrato com cláusula de notificação imediata.	6

Perguntas para discussão

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

1. Existe um inventário documentado de todas as contas com privilégios técnicos? Quando foi a última auditoria de contas dormentes?
2. A checklist de offboarding tem revogação de TODAS as contas (não apenas a conta principal de email)? Inclui validação por dois pares?
3. Quem decide a queixa-crime? A direção sozinha? Há advogado de empresa envolvido na decisão?
4. Que ficheiros estavam acessíveis através da partilha? Há classificação de informação documentada? Há controlo de acesso por necessidade-de-saber?
5. O cliente principal foi informado em reunião presencial — quem foi à reunião? Que documentação escrita ficou registada?
6. A organização tem MFA em todas as contas técnicas? Em todas as contas administrativas? Em VPN? O ex-colaborador conseguiu entrar — quê falhou?
7. Como se documenta a decisão do órgão de gestão (art. 25.º RJC) de qualificar o incidente como significativo, dado que entidade importante = supervisão ex post?

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. Desativar imediatamente a conta do antigo colaborador + forçar reset de MFA em todas as contas com privilégios técnicos.
2. Convocar Direção + RH + Jurídico em reunião conjunta. Documentar formalmente a decisão de qualificação como incidente importante (RJC art. 25.º — responsabilidade do órgão de gestão).
3. Notificar o CNCS via plataforma eletrónica (art. 42.º n.º 1 RJC) — a entidade importante notifica nos mesmos prazos do que a entidade essencial. Critério: art. 40.º n.º 3 RJC (impacto substancial em informação confidencial).
4. Apresentar queixa-crime à PJ ao abrigo da Lei do Cibercrime (acesso ilegítimo + interceção ilegítima); preservar cadeia de custódia para suporte processual.
5. Reunir prova forense: imagem da estação do antigo colaborador, logs do servidor de partilha, logs da VPN, logs do gateway de email, registos do EDR.
6. Informar o cliente afetado em reunião presencial — não por email — antes de qualquer divulgação pública; rever cláusulas de confidencialidade do contrato.
7. Submeter atualização de 72h ao CNCS (art. 42.º n.º 3) e calendarizar relatório final 30 dias úteis após fim do impacto significativo (art. 44.º n.º 1).
8. Revisão completa da política de offboarding: cláusula de revogação <2h, validação por dois pares, auditoria trimestral de contas dormentes, política de PAM/MFA para contas técnicas.

Referências regulatórias

Funções QNRCS (proxy NIST CSF 2.0)	PR · DE · RS · GR
Artigos da Diretiva (UE) 2022/2555	• Article 21(2)(g) • Article 21(2)(i) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b) • Article 33
Artigos do RJC (DL n.º 125/2025 — anexo)	• art. 25.º RJC (deveres do órgão de gestão — entidade importante igualmente) • art. 27.º n.º 1 al. f) RJC (higiene + formação) • art. 27.º n.º 1 al. h) RJC (controlo de acessos + gestão de ativos) • art. 27.º n.º 1 al. i) RJC (MFA + comunicações seguras) • art. 42.º n.º 1 RJC (24h notificação inicial — também para entidade importante) • art. 42.º n.º 3 RJC (72h) • art. 56.º RJC (supervisão ex post de entidade importante)

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