Reglyze

Exercício de tabletop NIS 2 / RJC: briefing · Acesso prolongado após a saída: falha de offboarding

Cenário de exercício de tabletop

Organização: Reglyze

Versão: v1

Data: 2026-11-25

Classificação: confidencial

Acesso prolongado após a saída: falha de offboarding

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	Significativo (incidente reportável)
Duração sugerida	75 minutos
Identificador	`pt-insider-threat-offboarding-gap`
Emitido em	25/11/2026

Contexto

Uma PME portuguesa de tecnologia, prestadora de serviços geridos (MSP; Anexo I do RJC, setor 9, gestão de serviços TIC entre empresas), com ~240 colaboradores e faturação anual de ~22 M€: média empresa, é entidade importante (art. 6.º n.º 2 RJC). O exercício trabalha 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 obriga a equipa a trabalhar três regimes em simultâneo: o RJC (notificação ao CNCS até 24 horas), a Lei do Cibercrime (queixa à PJ por acesso ilegítimo) e o RGPD com a Lei n.º 58/2019 (possível violação de dados pessoais, se os ficheiros acedidos incluírem dados de colaboradores ou clientes).

O exercício é particularmente relevante para PME portuguesas: a entidade importante tem os mesmos deveres de notificação que a essencial (arts. 40.º a 44.º RJC). O que muda é a supervisão: a autoridade aplica-lhe as medidas de supervisão ex post «sempre que obtenha provas, indícios ou informações» de incumprimento (art. 55.º n.º 1 RJC), sem os controlos aleatórios e as auditorias regulares previstos para as entidades essenciais (art. 54.º n.º 1).

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. 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 abriram ficheiros do servidor de partilha: desenhos, propostas comerciais, listas de fornecedores.	1

Momento	Injeção	#
T+15min	T+15min. A engenheira desativa a conta imediatamente. Convoca o responsável de TI e o diretor-geral. Documenta os timestamps de todas as sessões. Ainda não se sabe o que foi exfiltrado, apenas que houve acesso.	2
T+1h	T+1h. O diretor-geral pergunta se isto é um incidente significativo. A empresa tem 240 colaboradores e fatura ~22 M€/ano: média empresa de um setor do Anexo I, é entidade importante (art. 6.º n.º 2 RJC). O Diretor de Recursos Humanos confirma que o processo de saída do antigo colaborador foi normal, sem conflito, 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. Ainda não há confirmação de exfiltração, mas o padrão de acessos é compatível com cópia para fora. A direção debate a queixa à PJ (unidade de cibercrime) e a notificação ao CNCS. A equipa jurídica pondera o art. 6.º da Lei do Cibercrime (acesso ilegítimo).	4
T+24h	T+24h. Decisão tomada: notificação inicial ao CNCS na plataforma eletrónica (incidente significativo: possíveis perdas financeiras para a empresa e danos consideráveis para o cliente, art. 2.º al. l) RJC). 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 da notificação inicial enviada ao CNCS (art. 42.º n.º 3 RJC). O Ministério Público abre inquérito, com investigação da PJ. 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: o que falhou?
7. Se a autoridade, perante indícios de incumprimento, pedir provas da aplicação das políticas de controlo do acesso (art. 55.º n.º 2 al. g) RJC), que registos apresenta a empresa?

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 a direção, os recursos humanos e o jurídico. Registar quem decidiu que o incidente é significativo, a hora e o fundamento (art. 2.º al. l) RJC): a autoridade pode pedir essas provas (art. 55.º n.º 2 al. g) RJC).
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 importante notifica nos mesmos prazos que a essencial (art. 40.º n.º 1).
4. Apresentar queixa à PJ ou ao Ministério Público por acesso ilegítimo (art. 6.º da Lei do Cibercrime, Lei n.º 109/2009); preservar a 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. Enviar ao CNCS, quando necessário, a atualização da notificação inicial até 72 horas após a verificação (art. 42.º n.º 3 RJC); notificar o fim do impacto significativo nas 24 horas seguintes (art. 43.º n.º 1 RJC) e calendarizar 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. 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

Objetivos QNRCS	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. 6.º n.º 2 RJC (entidade importante) • art. 25.º RJC (deveres do órgão de gestão, também na entidade importante) • 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 (notificação inicial em 24h, também para a entidade importante)

	• art. 42.º n.º 3 RJC (atualização até 72h, quando necessário) • art. 55.º RJC (supervisão ex post de entidades importantes e públicas relevantes)

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