Reglyze

Exercício de tabletop NIS 2 / RJC: briefing · Ransomware no Sistema de Gestão Hospitalar (HIS)

Cenário de exercício de tabletop

Organização: Reglyze

Versão: v1

Data: 2026-11-25

Classificação: confidencial

Ransomware no Sistema de Gestão Hospitalar (HIS)

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

Setor	**Saúde**
Severidade	Significativo (incidente reportável)
Duração sugerida	90 minutos
Identificador	`pt-hospital-ransomware-his`
Emitido em	25/11/2026

Contexto

Um hospital distrital português, entidade essencial nos termos do art. 6.º n.º 1 al. a) do RJC (Anexo I, setor 5, saúde, acima dos limiares das médias empresas), opera um Sistema de Gestão Hospitalar (HIS) on-premises, PACS de imagiologia, portal do utente, sistema de gestão laboratorial e ~200 workstations clínicas. Trabalham no hospital ~1200 colaboradores, com ~80 médicos especialistas. O hospital integra a Rede Nacional de CSIRTs e comunicou ao CNCS o seu ponto de contacto permanente (art. 32.º RJC).

O contexto deste exercício é uma campanha de ransomware coordenada que atinge simultaneamente o HIS, a farmácia hospitalar e parte do bloco operatório. O exercício explora a articulação entre continuidade clínica (atendimento em modo papel), notificação de incidente significativo ao CNCS dentro do prazo de 24h (art. 42.º n.º 1 RJC), notificação à CNPD por violação de dados pessoais sensíveis (art. 33.º RGPD), e comunicação pública.

A equipa trabalha contra um cronómetro: as 24 horas contam-se a partir do momento em que o hospital conclui «que existe, ou possa vir a existir, um incidente significativo» (art. 42.º n.º 1 RJC), não a partir do ataque em si.

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	06:42. O administrador de sistemas do hospital chega ao centro de dados e encontra um ecrã com nota de resgate. Os pedidos de marcação no portal do utente devolvem erro 500. As cinco workstations do bloco operatório mostram a mesma nota. O sistema de gestão hospitalar (HIS) está inacessível; os PACS continuam a responder mas com latência elevada.	1

Momento	Injeção	#
T+15min	T+15min. A diretora clínica de serviço pergunta se as cirurgias programadas para as 08:00 devem ser canceladas. Não há acesso ao histórico do utente nem à lista de medicação alérgica. O suporte 24/7 do fornecedor do HIS confirma um pico de tickets idênticos em três outros hospitais portugueses.	2
T+1h	T+1h. O CERT.PT (CNCS) liga ao ponto de contacto permanente do hospital após uma deteção transversal nos sensores nacionais. A direção de informática confirma encriptação em 47 servidores. O backup mais recente verificado tem 31 horas. Não existe procedimento documentado de operação em modo degradado para o HIS.	3
T+4h	T+4h. Os técnicos de TI iniciaram a restauração a partir do backup offsite. As cirurgias eletivas foram canceladas; a urgência opera com registo em papel. O conselho de administração reúne-se; a porta-voz prepara comunicado. A ANEPC (Autoridade Nacional de Emergência e Proteção Civil) pede ponto de situação. CNN Portugal e Público têm jornalistas ao telefone.	4
T+24h	T+24h. Recuperaram-se 38 dos 47 servidores. O HIS está operacional em modo só-leitura; a gestão de medicação ainda não. A notificação inicial foi submetida ao CNCS na plataforma eletrónica há 14 horas, dentro do prazo de 24 horas. A CNPD ainda não foi notificada: o âmbito de exposição de dados pessoais (potencialmente registos clínicos) está sob avaliação.	5
T+72h	T+72h. Atualização da notificação inicial enviada ao CNCS (art. 42.º n.º 3 RJC), com a avaliação inicial da gravidade e do impacto: graves perturbações operacionais dos serviços clínicos e risco de danos consideráveis para os utentes (art. 2.º al. l) RJC). Restauração técnica concluída a 89%; a equipa forense identificou o vetor inicial (anexo de phishing aberto por colaborador da farmácia). Notificação RGPD art. 33.º entregue à CNPD na hora 71. Comunicação proativa aos utentes em curso.	6

Perguntas para discussão

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

1. Quem submete a notificação inicial ao CNCS na plataforma eletrónica, e quem é o suplente?
2. O backup offsite verificado tem 31 horas. Qual é a janela de perda de dados clínicos aceitável? Existe procedimento documentado para reconstruir esse intervalo a partir de registos auxiliares?
3. Em que momento se decide notificar a CNPD? Quem coordena com o Encarregado da Proteção de Dados? Qual é a base jurídica da notificação se a exposição efetiva ainda não estiver confirmada?
4. O ponto de contacto permanente (art. 32.º RJC) está contactável 24 horas por dia, sete dias por semana, nos períodos de ativação comunicados pela autoridade? Tem credenciais válidas na plataforma eletrónica no momento do incidente?
5. Quem aprova a comunicação à imprensa? O conselho de administração foi informado dentro do prazo necessário para validação?
6. Se o incidente fosse resolvido nas duas horas após a sua deteção, que notificação seria ainda devida ao CNCS? (Pista: art. 41.º n.º 2 RJC.)
7. Que provas se reúnem nas primeiras 24h para suportar o relatório final (art. 44.º n.º 1 RJC)? Onde se centraliza essa cadeia de custódia?

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. Contenção imediata: isolar a VLAN do HIS, bloquear o RDP de saída, desativar as contas comprometidas. Mapear a propagação via EDR/SIEM.
2. Ativar o plano de continuidade clínica em modo papel; designar duty manager de informática + duty clinical lead em ronda contínua até resolução.
3. Notificar o CNCS na plataforma eletrónica (art. 40.º n.º 6 RJC), sem demora injustificada e até 24 horas depois de concluir que existe, ou possa vir a existir, um incidente significativo (art. 42.º n.º 1 RJC); guardar o comprovativo da submissão.
4. Avaliar exposição de dados pessoais (registos clínicos = categoria sensível RGPD art. 9.º); notificar a CNPD nas 72h se confirmada (art. 33.º RGPD). Coordenar com o Encarregado da Proteção de Dados.
5. Restaurar serviço a partir do backup offsite verificado; documentar idade do backup, abrangência da restauração, controlos de integridade.
6. Comunicar com os utentes por SMS e pelo portal, com linha de apoio dedicada; manter um porta-voz único; alinhar o comunicado de imprensa com a ANEPC e o CNCS antes de o divulgar.
7. Enviar ao CNCS, até 72 horas após a verificação, a atualização da notificação inicial, com a avaliação inicial da gravidade e do impacto e, se disponíveis, os indicadores de exposição a riscos (art. 42.º n.º 3 RJC, quando necessário: aqui é, porque o impacto ainda está a ser avaliado).
8. Após o fim do impacto significativo: submeter a notificação do fim de impacto nas 24 horas seguintes (art. 43.º n.º 1 RJC); o relatório final segue no prazo de 30 dias úteis a contar da notificação do fim de impacto significativo (art. 44.º n.º 1 RJC).

Referências regulatórias

Objetivos QNRCS	RS · RC
Artigos da Diretiva (UE) 2022/2555	• Article 21(2)(b) • Article 21(2)(c) • Article 21(2)(h) • Article 23(4)(a) • Article 23(4)(b) • Article 23(4)(d)
Artigos do RJC (DL n.º 125/2025 — anexo)	• art. 27.º n.º 1 al. a) RJC (tratamento de incidentes) • art. 27.º n.º 1 al. b) RJC (continuidade e gestão de crises) • art. 27.º n.º 1 al. g) RJC (criptografia) • art. 32.º RJC (ponto de contacto permanente)

	• art. 40.º n.os 1 e 6 RJC (dever de notificar; plataforma eletrónica) • art. 42.º n.º 1 RJC (24h) • art. 42.º n.º 3 RJC (atualização até 72h, quando necessário) • art. 43.º n.º 1 RJC (fim do impacto significativo, 24h) • art. 44.º n.º 1 RJC (30 dias úteis para relatório final)

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