Reglyze

Exercício de tabletop NIS 2 / RJC — Briefing — Ransomware no Sistema de Gestão Hospitalar (HIS)

PT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-05-24T02:12:25.114Z

Classification: Confidential

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 al. f) e art. 39.º

Setor	**Saúde**
Severidade	Significativo (incidente reportável)
Duração sugerida	90 minutos
Identificador	`pt-hospital-ransomware-his`
Emitido em	24/05/2026

Contexto

Um hospital distrital português, qualificado como entidade essencial nos termos do RJC (Anexo I — saúde), 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 dispõe de ponto de contacto designado junto do CNCS.

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 deve trabalhar contra um cronómetro: o prazo de 24h conta-se a partir do momento em que existe «conclusão de 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 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	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
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

Momento	Injeção	#
T+1h	T+1h. O CSIRT.PT (CNCS) liga ao ponto de contacto 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 ANPC (Autoridade Nacional de 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. Foi enviada uma notificação inicial ao CNCS via plataforma eletrónica há 14 horas (dentro do prazo de 24h). 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 de 72h ao CNCS submetida (art. 42.º n.º 3 RJC). Avaliação inicial confirma 'incidente significativo' (impacto substancial em serviço crítico de saúde + risco substancial para utentes). 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 é a pessoa nomeada para submeter a notificação inicial ao CNCS via plataforma eletrónica? 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 único com o CNCS está acessível 24/7? Tem credenciais válidas na plataforma eletrónica do CNCS 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 terminasse em menos de 2 horas, ainda seria necessária notificação inicial 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, suspender RDP saindo, desactivar contas comprometidas. Mapeamento de 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 via plataforma eletrónica (art. 8.º n.º 7 RJC) dentro do prazo de 24h após verificação (art. 42.º n.º 1 RJC) — guardar comprovativo do ticket.
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 utentes via SMS/portal + linha de apoio dedicada; manter porta-voz único; alinhar comunicado de imprensa com a ANPC + CNCS antes de público.
7. Submeter atualização de 72h ao CNCS (art. 42.º n.º 3 RJC) com avaliação de gravidade, indicadores de exposição, medidas de mitigação aplicadas.
8. Após fim do impacto significativo: submeter notificação de fim (art. 43.º RJC) e iniciar o prazo de 30 dias úteis para o relatório final (art. 44.º n.º 1 RJC).

Referências regulatórias

Funções QNRCS (proxy NIST CSF 2.0)	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. 40.º RJC (regra geral de notificação) • art. 42.º n.º 1 RJC (24h) • art. 42.º n.º 3 RJC (72h) • art. 43.º RJC (fim de impacto) • 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