**Anexo D — Playbooks de Resposta a Incidentes**

Detecção, Contenção, Erradicação, Recuperação e Pós‑Incidente

Data: 06/11/2025

## D.1 Compromisso de Credenciais (phishing / sessão)

Detecção:  
• Alertas do IdP (Keycloak): falhas de MFA, logins anómalos, IPs improváveis.  
• SIEM: correlação de eventos e uso fora de horário.

Contenção:  
• Reset forçado de tokens e sessões para contas afectadas.  
• Aumentar requisitos de MFA temporariamente para o domínio afectado.

Erradicação:  
• Reimagem de estações comprometidas; rotação de segredos.  
• Caça de indicadores (IOC) em endpoints e logs.

Recuperação:  
• Restaurar acessos mínimos; monitorizar por 14 dias.  
• Treino rápido anti‑phishing para equipa impactada.

Pós‑Incidente:  
• Lições aprendidas em 72 h; melhoria de regras do IdP e de deteção no SIEM.

## D.2 Ransomware / Cripto‑malware

Detecção:  
• Detecção via EDR/Wazuh (criptação massiva, processos suspeitos).

Contenção:  
• Isolar segmentos/rede; bloquear C2; desligar partilhas.

Erradicação:  
• Remover binários maliciosos; aplicar patches; reimagem dos hosts.

Recuperação:  
• Restaurar de backups imutáveis (pgBackRest/Ceph) após validação.  
• Verificação de integridade de dados.

Pós‑Incidente:  
• Auditoria completa; reforço de segmentação; exercícios de restauração trimestrais.

## D.3 Exfiltração de Dados

Detecção:  
• Alarmes de volume anómalo (NetFlow/Zeek); acessos a buckets S3 fora do padrão.

Contenção:  
• Cortar chaves/API suspeitas; bloquear egress temporário por tag/namespace.

Erradicação:  
• Revogar chaves; rotação de segredos; varrimento de logs para âmbitos afectados.

Recuperação:  
• Notificar titulares e autoridades conforme RGPD; restaurar configurações seguras.

Pós‑Incidente:  
• Revisão de políticas de minimização e \*data loss prevention\*; etiquetagem e encriptação por classificação.

## D.4 DDoS a Serviços Públicos

Detecção:  
• Picos de tráfego e queda de SLI de disponibilidade.

Contenção:  
• Activar protecções no gateway/WAF; \*rate‑limit\* agressivo; \*caching\* quando possível.

Erradicação:  
• Ajustar \*autoscaling\*; activar \*shields\* de upstreams.

Recuperação:  
• Comunicar estado no portal de estado público; manter canais alternativos.

Pós‑Incidente:  
• \*Post‑mortem\* com métricas de saturação e melhorias no \*capacity planning\*.

## D.5 RACI (papéis)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tarefa | Responsável (R) | Aprovador (A) | Consultado (C) | Informado (I) |
| Classificação do incidente | SOC Nível 2 | Gestor de Segurança | Equipa de Domínio | Comunicação |
| Contenção técnica | Plataforma/NetOps | Gestor de Segurança | Domínio afectado | Negócio/Executivo |
| Notificação RGPD | DPO | Direcção | Jurídico | Autoridade/Utentes |
| \*Post‑mortem\* | Equipa de Domínio | Direcção Técnica | Segurança/Plataforma | Executivo |