**Anexo A — Checklist de Hardening**

Ubuntu LTS e Kubernetes (resumo CIS)

Data: 06/11/2025

## A.1 Ubuntu LTS — Sistema Operativo

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Descrição | Comando/Verificação | Estado |
| Actualizações | Activar actualizações automáticas e patching de segurança. | apt-get update && apt-get dist-upgrade unattended-upgrades | ☐ / ☑ |
| Controlo de acesso | Bloquear root via SSH; usar sudo; 2FA admins. | sshd\_config: PermitRootLogin no adduser sudo; pam\_u2f/pam\_google\_authenticator | ☐ / ☑ |
| Firewall | Política restritiva por defeito; permitir apenas portas necessárias. | ufw default deny incoming ufw allow 443/tcp | ☐ / ☑ |
| Auditd | Activar auditoria do kernel e regras CIS. | apt install auditd auditctl -l | ☐ / ☑ |
| Logs | Centralização e retenção; rotação configurada. | /etc/rsyslog.d/ e /etc/logrotate.d/ | ☐ / ☑ |
| Criptografia | LUKS para volumes; TLS 1.3 por defeito. | lsblk -f (ver crypt) sslyze / testssl.sh | ☐ / ☑ |
| Serviços | Desactivar serviços não utilizados; ports limpos. | ss -tulpen; systemctl disable --now <svc> | ☐ / ☑ |
| NTP | Sincronização segura de tempo (chrony). | apt install chrony chronyc sources -v | ☐ / ☑ |
| Integração SIEM | Agente Wazuh/OSSEC e FIM activos. | wazuh-agent status | ☐ / ☑ |

## A.2 Kubernetes — Control Plane e Nodes

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Descrição | Comando/Verificação | Estado |
| RBAC estrito | Papéis por namespace; princípio do menor privilégio. | kubectl auth can-i --as=<user> --list | ☐ / ☑ |
| Admission control | OPA/Gatekeeper para políticas; bloquear imagens sem assinatura. | kubectl get constraints cosign verify | ☐ / ☑ |
| Segredos | KMS/HSM (OpenBao) e encriptação em repouso. | kube-apiserver --encryption-provider-config | ☐ / ☑ |
| NetworkPolicy | Tráfego L3/L4/7 minimizado por namespace. | kubectl get networkpolicy -A | ☐ / ☑ |
| Pod Security | PSA/PodSecurity admission com baseline/restricted. | kubectl get ns -L pod-security.kubernetes.io/enforce | ☐ / ☑ |
| mTLS interno | Service-to-service mTLS (SPIFFE/SPIRE) quando aplicável. | spiffe-env, certificados rotativos | ☐ / ☑ |
| Auditoria | Audit-logs activos e exportados para SIEM. | kube-apiserver --audit-log-path=... | ☐ / ☑ |
| Nós hardenizados | Kernel lockdown; sysctls seguras; sem login directo. | sysctl -a; /etc/ssh/sshd\_config | ☐ / ☑ |
| Imagem & Supply chain | Assinatura (cosign), SBOM, scans SAST/DAST. | cosign attest; trivy image | ☐ / ☑ |

## A.3 Backups e DR (WORM)

• pgBackRest com retenção WORM (3-2-1). Ensaios de restauro trimestrais documentados.

• Snapshots Ceph programados e espelhamento inter-DC (RBD mirroring).