Plan de Continuité d'Activité (PCA) et Plan de Reprise d’activité (PRA)

Projet Hospital

Kenzi BOUGHADOU

Hugo GRILLET

Table des matières

Plan de Continuité d'Activité

1. Objectif du PCA

Le Plan de Continuité d'Activité (PCA) a pour but de garantir le maintien des activités critiques de l'établissement hospitalier en cas d'incident majeur affectant le système d'information (panne, attaque, sinistre).
L'objectif est d'assurer que les soins aux patients, la disponibilité des données médicales et les communications vitales puissent se poursuivre sans interruption significative, afin de protéger la santé des patients et la réputation de l'établissement.

2. Périmètre du PCA

Le PCA couvre :

- Les serveurs critiques (contrôleurs de domaine, base de données patient, applications métiers).
- Les réseaux (infrastructure VLAN, VPN, pare-feu OPNSense).
- Les équipements utilisateurs critiques (postes de travail pour les médecins et infirmiers).
- Les systèmes de communication interne (messagerie professionnelle, téléphonie IP).
- Les sauvegardes de données et la réplication cloud HDS.

3. Analyse d'impact (BIA)

Une interruption des services informatiques pourrait entraîner :

- Un arrêt de l'accès aux dossiers médicaux.
- Un retard critique dans la délivrance des soins.
- Une perte de données sensibles (personnelles et médicales).
- Des conséquences juridiques et réglementaires.

Activité critique	Temps Maximal d'Interruption (RTO)	Priorité
Dossier médical patient (DMP)	1 heure	Critique
Accès aux résultats de laboratoire	2 heures	Critique
Téléphonie interne	4 heures	Haute
Système de facturation administrative	24 heures	Moyenne

4. Scénarios de crise couverts

- Défaillance matérielle d'un serveur ou d'un stockage.
- Cyberattaque de type ransomware paralysant le réseau.

- Catastrophe naturelle affectant le site principal (incendie, inondation).
- Perte de connectivité Internet de longue durée.

5. Stratégies de continuité

- **Serveurs critiques répliqués** sur une infrastructure de secours locale (NAS) et cloud certifié.
- **Active Directory en haute disponibilité** avec deux contrôleurs AD (AD1 et AD2).
- **Segmentation réseau** (VLAN) limitant la propagation des incidents.
- **VPN sécurisé** pour accès distant de secours.
- **Procédures documentées** pour commutation vers les environnements de secours.

6. Communication de crise

- Activation d'une cellule de crise sous 30 minutes par le RSSI et la DSI.
- Communication aux personnels médicaux via SMS, emails alternatifs ou téléphone IP.
- Mise à disposition d'une ligne d'information téléphonique pour les patients et partenaires.

7. Tests de continuité

- Exercices de bascule (failover) semestriels pour tester la robustesse du dispositif.
- Révision annuelle du plan après simulation et retour d’expérience.

Plan de Reprise d’activité

1. Objectif du PRA

Le Plan de Reprise d'Activité (PRA) vise à restaurer rapidement le système d'information de l’établissement après un sinistre majeur.
Il prévoit les actions techniques, humaines et organisationnelles nécessaires pour remettre en service les infrastructures informatiques tout en minimisant l'impact sur les activités critiques hospitalières.

2. Périmètre du PRA

Le PRA s'applique à :

- La totalité du système d'information (serveurs, applications, réseau).
- Les bases de données critiques (patients, laboratoires, pharmacie).
- Les moyens de communication (mails, téléphone IP).
- Les postes de travail essentiels au sein des services critiques.

3. Phases de reprise

Phase 1 — Contenir la crise (0–2 heures)

- Isolement du système ou du réseau impacté par cloisonnement VLAN (via OPNSense).
- Suspension immédiate des accès externes (VPN) si compromission détectée.
- Notification rapide au Comité de Gestion de Crise.

Phase 2 — Évaluer les dommages (2–4 heures)

- Évaluation de l’ampleur de l’incident par l'équipe cybersécurité (Wazuh, Zabbix).
- Priorisation des services à restaurer selon l'impact patient / métier.
- Documentation des systèmes affectés et analyse des failles.

Phase 3 — Restaurer les services critiques (4–12 heures)

- Basculement sur les sauvegardes les plus récentes (NAS / Cloud HDS) selon les procédures validées.
- Redémarrage des serveurs Active Directory, BDD Patient, Systèmes de messagerie.
- Rétablissement prioritaire des accès aux dossiers médicaux et aux résultats de laboratoire.

Phase 4 — Reprise totale (12–72 heures)

- Réintégration progressive des postes utilisateurs après validation.
- Tests d'intégrité et vérifications de sécurité.
- Retour à la production normale avec un suivi renforcé (monitoring Zabbix/Wazuh).

4. Ressources mobilisées

- Sauvegardes automatisées journalières locales + sauvegarde cloud certifiée.
- Documentation PRA détaillée avec instructions claires (procédures de restauration, reconfiguration réseau).
- Liste des contacts d'urgence (DSI, RSSI, prestataires externes, hébergeur cloud HDS).
- Infrastructure de secours prête à être activée en cas de besoin.

5. Formation et tests

- Formations régulières du personnel IT sur les procédures de PRA.
- Réalisation annuelle d’exercices de PRA complets (restauration + retour en production simulés).
- Mises à jour trimestrielles du plan selon les évolutions techniques et incidents constatés.