|  |
| --- |
| CHU Ynov |
| Plan de Reprise d’Activité |
| [Sous-titre du document] |

|  |
| --- |
| Xavier Martin  [Date] |

Table des matières

[1. Objectifs du Plan de Reprise d’Activité (PRA) 2](#_Toc201525833)

[2. Périmètre du PRA 3](#_Toc201525834)

[3. Scénarios de déclenchement 5](#_Toc201525835)

[4. Organisation et responsabilités 7](#_Toc201525836)

[5. Phases du PRA 9](#_Toc201525837)

[6. Moyens techniques 12](#_Toc201525838)

[7. Ordre de priorité de reprise 14](#_Toc201525839)

[8. Communication de crise 15](#_Toc201525840)

[9. Maintenance et tests du PRA 18](#_Toc201525841)

# 1. Objectifs du Plan de Reprise d’Activité (PRA)

Le Plan de Reprise d’Activité (PRA) du CHU Ynov a pour finalité de garantir la résilience opérationnelle du système d’information hospitalier après un incident majeur, en s’assurant que les fonctions numériques vitales soient restaurées de façon coordonnée, sécurisée et dans des délais compatibles avec la criticité métier.

**1.1 : Garantir la continuité des soins et de la prise en charge des patients**

L’interruption du système d’information, notamment du DPI, peut compromettre la sécurité des patients, provoquer des erreurs de prescription, retarder des interventions, ou désorganiser les services d’urgence.

Le PRA vise à :

* Réduire au strict minimum les interruptions de soins informatisés.
* Permettre l’accès rapide aux données vitales (dossier patient, imagerie, biologie, traitements).
* Préserver la coordination entre services (transferts, hospitalisations, alertes médicales).

**1.2 Rétablir les services critiques selon les délais RTO/RPO définis**

Le PRA intègre des niveaux de service attendus (SLA) et des engagements de délai pour la reprise de chaque brique du SIH, en fonction de son impact clinique ou organisationnel.

Le RTO (Recovery Time Objective) définit le délai maximal d’interruption acceptable.

Le RPO (Recovery Point Objective) désigne l’ancienneté maximale acceptable des données restaurées.

Ces deux critères guident les priorisations de restauration, l’architecture de sauvegarde, et les stratégies de réplication.

**1.3 Restaurer les données à partir des sauvegardes vérifiées**

Afin d’éviter la perte de données cliniques ou administratives :

* Le PRA prévoit des procédures de restauration depuis des sauvegardes validées, intègres et sécurisées.
* Il impose un cycle de test régulier des supports de sauvegarde (tests de restauration, vérification d’intégrité).
* Il inclut des politiques de conservation différenciées (quotidienne, hebdomadaire, mensuelle) en local et en site distant (air gap, cloud HDS).

**1.4 Coordonner efficacement les équipes techniques et métiers durant la reprise**

Le PRA fournit un cadre de gouvernance structuré pendant toute la durée de la reprise, avec :

* Une cellule de crise SI activée dès la détection de l’incident.
* Une hiérarchie claire des responsabilités : DSI, RSSI, direction générale, métiers.
* Une documentation opérationnelle prête à l’emploi (procédures, fiches de rôles, checklists).
* Une communication transversale vers les services, les utilisateurs et les autorités.

Cette coordination est essentielle pour éviter les erreurs de restauration, les conflits entre priorités et les relances prématurées.

**1.5 Réintégrer les systèmes dans un environnement stable et conforme**

Après la restauration :

* Les services doivent être progressivement remis en production, dans un environnement sécurisé (patché, contrôlé, validé).
* L’état des bases de données et des journaux doit être validé par les métiers et le RSSI.
* Une surveillance renforcée post-reprise est mise en œuvre pendant 72 heures minimum.

L’ensemble de la séquence est documenté pour audit et intégré au retour d’expérience (RETEX).

# 2. Périmètre du PRA

Le périmètre du Plan de Reprise d’Activité (PRA) du CHU Ynov est défini afin de couvrir l’ensemble des composantes du système d’information dont la restauration rapide est indispensable à la continuité des soins, à la sécurité des patients, et à la stabilité organisationnelle de l’établissement.

Ce périmètre repose sur une analyse d’impact métier (BIA) menée en collaboration avec les pôles cliniques, administratifs et techniques. Il identifie l’ensemble des briques fonctionnelles, logicielles et matérielles essentielles, dont la perte ou l’indisponibilité prolongée aurait des conséquences graves sur :

* La qualité et la sécurité des soins apportés aux patients
* Le fonctionnement opérationnel des services hospitaliers
* Le respect des obligations réglementaires (PGSSI-S, RGPD, certification HDS)
* L’image, la réputation et la responsabilité juridique de l’établissement.

Les composants retenus sont regroupés en trois grandes catégories : systèmes métiers, infrastructures techniques, et réseaux & communications.

**2.1 Systèmes métiers**

Les applications et bases de données suivantes sont considérées comme critiques :

* Dossier Patient Informatisé (DPI) : cœur du système médical, il contient toutes les données cliniques (consultations, prescriptions, imagerie, biologiques), et constitue un point de convergence pour les différents services.
* Laboratoire (LIMS, Middleware) : les délais de traitement d’analyses conditionnent la prise de décision médicale (urgence, infectiologie, onco-hématologie).
* Radiologie (RIS/PACS) : la visualisation des examens (IRM, scanner, radio) est indispensable au diagnostic et à la planification opératoire.
* Pharmacie hospitalière : les systèmes de dispensation, de stock et de traçabilité des médicaments sont essentiels pour la sécurité des soins.
* Applications spécialisées : régulation (SAMU), soins critiques (réa, bloc), cancérologie, DPI de maternité.
* Gestion des patients : admissions, identito-vigilance, planification, gestion des lits et mouvements.

**2.2 Infrastructures techniques**

Le fonctionnement des services ci-dessus dépend d’infrastructures robustes, elles aussi intégrées au périmètre du PRA :

* Annuaire d’entreprise (Active Directory / LDAP) : sans authentification centralisée, aucun service n’est accessible ;
* Serveurs virtualisés et hyperviseurs : la majorité des applications sont hébergées en environnement virtualisé (VMware ou Hyper-V).
* Baies de stockage (SAN, NAS) : elles hébergent l’ensemble des fichiers critiques (bases de données, dossiers, images).
* Solutions de sauvegarde/restauration : systèmes de sauvegarde avec réplication, déduplication, gestion des versions, stockage sécurisé hors site.
* Automates de déploiement / scripts d’auto-réinstallation : nécessaires pour relancer rapidement les services applicatifs.

**2.3 Communications et réseau**

Commutation réseau, firewalls, VLAN critiques

VPN, accès distants

Téléphonie IP (standard médical)

# 3. Scénarios de déclenchement

Le déclenchement du Plan de Reprise d’Activité (PRA) du CHU Ynov repose sur une décision formelle prise par la cellule de crise SSI, sur proposition conjointe du RSSI et de la DSI, lorsqu’un incident dépasse les capacités de reprise normales ou rend inopérant le fonctionnement standard du SI.

**3.1 Critères de déclenchement**

Le PRA est activé dès lors que l’un des événements suivants se produit :

Sinistre physique majeur : incendie, inondation, dégât des eaux, effondrement ou tout autre événement affectant les infrastructures hébergeant le SI.

Incident électrique ou climatique critique : panne prolongée de l’alimentation électrique (malgré les onduleurs et groupes électrogènes), panne de climatisation des salles serveurs entraînant un risque de surchauffe.

Cyberattaque grave : détection confirmée de ransomware, intrusion massive, compromission de comptes à privilège, exfiltration de données, ou altération volontaire des systèmes critiques.

Panne matérielle majeure : défaillance simultanée ou non récupérable d’un cluster de virtualisation, corruption de baies SAN/NAS, défaillance de sauvegarde empêchant une restauration.

Échec de la reprise standard : échec du redémarrage via les procédures courantes d’incident (PCA inefficace ou hors périmètre), ou indisponibilité des équipes clés.

**3.2 Acteurs autorisés à initier le PRA**

Le déclenchement peut être proposé par :

* Le Responsable Sécurité des Systèmes d’Information (RSSI)
* Le Directeur des Systèmes d’Information (DSI)
* Le Responsable de l’exploitation ou le chef de poste de supervision
* Le Directeur général ou son représentant, en lien avec la cellule de crise institutionnelle

Une fois déclenché, le PRA est considéré comme prioritaire absolu. Les ressources techniques, humaines et contractuelles nécessaires à sa mise en œuvre doivent être immédiatement mobilisées.

**3.3 Corrélation avec les autres dispositifs**

Le PRA peut être déclenché :

De manière conjointe avec le Plan de Continuité d’Activité (PCA) si l’événement impacte à la fois l’organisation humaine et le SI

En complément du Plan Blanc ou du Plan de Crise interne en cas de catastrophe ou d’afflux massif de victimes

Sur demande de l’ARS, de l’ANS ou des autorités judiciaires dans le cadre d’un incident réglementaire ou pénal.

Chaque déclenchement fait l’objet d’un enregistrement dans le journal de crise du PRA, accompagné des décisions prises, de leur justification et des personnes responsables de chaque action. (Incendie, inondation, coupure électrique prolongée)

Incident cyber (ransomware, compromission massive)

Panne matérielle critique (hyperviseur, baies de stockage)

Échec du redémarrage standard ou du PCA

# 4. Organisation et responsabilités

La réussite d’un Plan de Reprise d’Activité repose sur une gouvernance claire, définissant les rôles, responsabilités et circuits de décision. Le CHU Ynov formalise ainsi une organisation spécifique pour piloter efficacement les actions de reprise en cas d’incident majeur.

**4.1 Gouvernance générale**

Direction Générale :

* Décide de l’activation du PRA sur recommandation du RSSI/DSI.
* Assure la communication institutionnelle vers les autorités sanitaires (ARS, ANS).
* Alloue les ressources humaines et financières nécessaires.

Comité de crise SSI :

* Structure opérationnelle transversale dédiée à la gestion de crise SI.
* Composé du DSI, RSSI, direction médicale, direction qualité, direction des soins.
* Coordonne la priorisation des actions et arbitrages entre métiers et technique.

**4.2 Responsabilités techniques**

Directeur des Systèmes d’Information (DSI) :

* Coordonne techniquement toutes les opérations de restauration.
* Supervise les équipes infrastructures, exploitation, et applications.
* Gère les relations avec les hébergeurs, éditeurs et infogérants.

Responsable Sécurité des Systèmes d’Information (RSSI) :

* Apporte une expertise sur l’intégrité et la conformité des systèmes restaurés.
* Valide l’absence de résidus malveillants avant remise en production.
* Gère les outils de traçabilité, de journalisation et d’investigation post-incident.

Responsable de l’Exploitation :

* Pilote la relance des serveurs, VM, équipements réseau.
* Veille à l’application rigoureuse des procédures documentées.
* Supervise la bonne exécution des scripts de restauration et le respect de la chronologie des redémarrages.

**4.3 Rôles métiers**

Référents métiers (soins, urgences, laboratoire, pharmacie) :

* Vérifient le bon fonctionnement des outils restaurés sur le plan clinique ou logistique.
* Participent à la recette fonctionnelle et valident la reprise d’activité de leur périmètre.
* Transmettent les besoins métiers spécifiques à intégrer dans les priorités de reprise.

Responsables applicatifs :

* Supervisent la cohérence des données restaurées dans leur logiciel.
* Mettent à disposition les plans de reprise spécifiques à chaque application.

**4.4 Partenaires et prestataires**

Éditeurs et infogérants :

* Fournissent une assistance technique à la restauration logicielle ou système.
* Participent à la résolution d’erreurs critiques post-restauration.

Prestataires d’hébergement ou cloud :

* Rétablissent les services externalisés selon les SLA contractuels.
* Coopèrent au maintien de la sécurité et de l’intégrité des environnements restaurés.

**4.5 Documentation de responsabilité**

Chaque acteur impliqué dans le PRA dispose d’une fiche de rôle détaillée, annexée au plan. Cette fiche décrit :

* Ses missions en phase de déclenchement, restauration et validation.
* Les procédures à appliquer et outils à utiliser.
* Les responsabilités de reporting et de documentation post-action.

# 5. Phases du PRA

Le processus de reprise d’activité se décompose en cinq phases chronologiques, conçues pour répondre à des objectifs clairs et garantir la relance des services SI critiques de façon ordonnée, sécurisée et validée.

**5.1 Phase 1 – Déclenchement**

Objectif : Formaliser l’activation du PRA, alerter les équipes et initier la mobilisation des ressources.

Étapes :

Etape une : Surveillance continue des incidents (monitoring, SOC, remontées utilisateurs).

Etape deux : Identification d’un incident majeur répondant aux critères définis.

Etape trois : Convocation immédiate de la cellule de crise SSI.

Etape quatre : Analyse rapide de l’impact opérationnel (sur le SI et les soins).

Etape cinq : Prise de décision par la Direction Générale sur proposition du DSI/RSSI.

Etape six : Diffusion de l’ordre officiel de déclenchement du PRA.

Livrables attendu et outils utilisés :

* Journal de crise (papier ou électronique).
* Fiches de notification PRA.
* Liste des contacts d’urgence métiers et techniques.

**5.2 Phase 2 – Diagnostic**

Objectif : Évaluer l’étendue des dégâts et définir une stratégie de restauration réaliste et hiérarchisée.

Étapes :

Etape une : Identification précise des services applicatifs et infrastructures affectées.

Etape deux : Évaluation de la dernière sauvegarde fiable disponible (RPO réel).

Etape trois : Diagnostic des causes premières (root cause analysis).

Etape quatre : Identification des dépendances critiques entre composants.

Etape cinq : Estimation des délais de reprise réalistes par domaine.

Livrables attendu et outils utilisés :

* Cartographie impact/système.
* Plan de restauration priorisé.
* État de santé des infrastructures (tableau synthèse).

**5.3 Phase 3 – Restauration**

Objectif : Recréer un environnement stable et sécurisé à partir de sauvegardes validées, et remettre en fonctionnement les services dans un ordre défini.

Étapes :

Etape une : Réinitialisation ou reconstruction des environnements (VM, OS, AD, etc.).

Etape deux : Restauration applicative depuis les sauvegardes intègres.

Etape trois : Contrôle de l’intégrité (checksum, cohérence, logs applicatifs).

Etape quatre : Reconnexion des services à leurs bases de données.

Etape cinq : Isolation ou désinfection préalable si suspicion de code malveillant.

Etape six : Synchronisation progressive avec les autres environnements.

Livrables attendu et outils utilisés :

* Scripts d’automatisation de restauration.
* Checklists système par serveur.
* Journalisation complète des actions techniques.

**5.4 Phase 4 – Tests de validation**

Objectif : S’assurer de la fonctionnalité technique, de la cohérence métier, et de l’absence de résidus malveillants.

Étapes :

Etape une : Recette technique par les équipes exploitation/infra (ping, services, authentification).

Etape deux : Recette fonctionnelle par les référents métiers sur échantillons critiques.

Etape trois : Tests utilisateurs sur chaînes applicatives (DPI, prescription, imagerie).

Etape quatre : Vérification de l’intégrité des données restaurées (données biologiques, prescriptions, historiques).

Etape cinq : Certification provisoire des systèmes avant redémarrage général.

Livrables attendu et outils utilisés :

* Protocoles de tests standardisés.
* Fiches de validation par application.
* PV de recette technique et fonctionnelle.

**5.5 Phase 5 – Retour à la normale**

Objectif : Revenir progressivement à un fonctionnement nominal tout en assurant un suivi renforcé.

Étapes :

Etape une : Notification de remise en production à l’ensemble des services.

Etape deux : Reconnexion des services extérieurs ou inter-établissements.

Etape trois : Bascule des données temporaires vers les bases de production.

Etape quatre : Déactivation des environnements de secours.

Etape cinq : Surveillance intensive pendant 72h (logs, antivirus, comportement utilisateurs).

Etape six : Organisation d’un debrief global avec l’ensemble des acteurs (RETEX).

Etape sept : Mise à jour des procédures PRA sur la base des leçons apprises.

Livrables attendu et outils utilisés :

* Rapport post-incident.
* Recommandations d’amélioration.
* Mise à jour des documents de crise et des procédures.
* Sauvegardes locales et externalisées (quotidiennes, hebdomadaires)
* Serveurs de secours préconfigurés
* Procédures de restauration automatisées
* Plans de configuration documentés

Réseau de secours / liaisons alternatives

# 6. Moyens techniques

Le bon déroulement du PRA repose sur la disponibilité de moyens techniques robustes, testés, maintenus à jour, et adaptés aux besoins de restauration rapide du SI. Ces moyens sont répartis dans les catégories suivantes :

**6.1 Infrastructures de sauvegarde**

Sauvegardes locales : Stockées dans des serveurs dédiés en ligne directe avec les clusters de production, dotées de systèmes de chiffrement AES-256.

Sauvegardes externalisées : Hébergées hors site dans un datacenter certifié HDS (Health Data Hosting), via fibre sécurisée ou transfert VPN.

Fréquence des sauvegardes :

Données critiques (DPI, prescription, pharmacie) : toutes les 4 heures (incremental/diff).

Serveurs applicatifs secondaires : sauvegarde quotidienne avec rétention de 7 à 30 jours.

Technologies utilisées : Veeam, Atempo Tina, Rubrik, solutions NAS-S3, snapshot ZFS.

Mesures de sécurité :

Stockage immutable (WORM)

Tests de restauration mensuels

Suivi de l’intégrité via hachage (SHA-256)

**6.2 Environnements de secours**

Clusters de secours : Hyperviseurs (VMware/Hyper-V) configurés en mode standby avec images systèmes prêtes à être déployées.

Serveurs physiques de repli : Stations ou serveurs physiques « bare metal » pour relancer les services réseau essentiels (DNS, AD, VPN).

Stockage redondant : SAN/NAS secondaire répliqué toutes les 24h.

Applications critiques préinstallées : Imagerie disque complète prête à être restaurée en quelques minutes.

**6.3 Procédures automatisées**

Scripts de restauration automatisés (Ansible, PowerShell) pour :

Recréer les VMs

Réintégrer les systèmes dans l’AD

Réinstaller les configurations applicatives

Orchestration via outils type Rundeck / GitOps / Jenkins

Documentation pas-à-pas pour toutes les actions critiques avec versions synchronisées via Git

**6.4 Équipements et communication**

Infrastructure réseau PRA : VLANs isolés pour les tests, switchs redondants, liaisons fibre vers datacenter.

Firewall de secours : appliances Fortinet/Palo Alto configurées pour bascule automatique.

Téléphonie analogique de crise : lignes indépendantes du réseau IP pour la cellule de crise.

Stations de travail portables préconfigurées : pour DSI, RSSI, référents applicatifs.

**6.5 Supervision, traçabilité et auditabilité**

SIEM / SOC régional : corrélation d’événements PRA, alertes automatiques, anomalies détectées en temps réel.

Centreon / Zabbix : supervision des serveurs restaurés et des connexions inter-systèmes.

Logs centralisés : tous les événements de restauration sont journalisés et signés numériquement.

Audit post-reprise : les actions réalisées sont contrôlées a posteriori pour vérifier leur conformité à la politique SSI.

# 7. Ordre de priorité de reprise

L'ordre de priorité de reprise des systèmes d'information repose sur une évaluation croisée de plusieurs critères décisionnels :

Impact clinique : effet direct sur la santé ou la sécurité des patients.

Dépendances techniques : interconnexion avec d'autres systèmes (ex : le DPI nécessite l'AD, la base SQL, le réseau).

Continuité de service : capacité à maintenir les soins même en mode dégradé.

Risque juridique ou réglementaire : exposition RGPD, HDS, certification HAS.

L’objectif est de rétablir en priorité les fonctions vitales à l’activité médicale, puis de remonter progressivement vers les fonctions de support et d’administration.

|  |  |  |  |
| --- | --- | --- | --- |
| Priorité | Système | Délai max de reprise | Justification |
| 1 | DPI, Prescription, Urgences | < 2 h | Systèmes indispensables à la prise en charge immédiate des patients. |
| 2 | Laboratoire, imagerie, pharmacie | < 4h | Services support critiques pour le diagnostic et la médication. |
| 3 | Téléphonie, accès réseau, fichiers | < 6h | Moyens de communication et d’accès essentiels pour les services de soins. |
| 4 | Applications administratives | < 12h | Fonction support pouvant être traitée en mode dégradé temporairement. |

Ce tableau est mis à jour chaque année en coordination avec les métiers et la direction. Il sert de guide pour la phase de restauration (cf. section 5.3) et alimente le scénario de test du PRA.

# 8. Communication de crise

La communication en situation de crise liée à la sécurité des systèmes d’information doit être structurée, fiable, traçable et en cohérence avec les enjeux réglementaires, médicaux, institutionnels et de cybersécurité. Le RSSI, en lien étroit avec la Direction Générale, la DSI et la communication institutionnelle, contribue à piloter cette composante essentielle du PRA.

**8.1 Objectifs**

Les objectifs sont les suivants :

Garantir une circulation fluide, contrôlée et sécurisée de l'information entre les acteurs de la crise.

Prévenir la diffusion de rumeurs, d’informations inexactes ou prématurées pouvant aggraver la situation.

Répondre aux obligations légales de notification (CNIL, ARS, ANS, DPO).

Maintenir la confiance des usagers, du personnel et des partenaires dans la résilience numérique du CHU.

**8.2 Plan de communication internes**

Le plan de communication interne au CHU est détaillé dans le tableau suivant :

|  |  |  |
| --- | --- | --- |
| Canal | Usage Principal | Responsable |
| Email sécurisé | Diffusion de consignes opérationnelles | DSI / RSSI |
| Téléphonie de secours | Coordination de la cellule de crise | Responsable Exploitation |
| Affichage papier | Communication dans les services | Référents métiers |
| Intranet PRA | Centralisation documentaire et fil d’actualité | Service communication / DSI |
| Outils de messagerie instantanée | Coordination rapide entre les experts | Cellule de crise SSI |

Tous les messages internes doivent suivre un canevas validé, horodaté, signé et archivé.

**8.3 Plan de communication externe**

Plan de communication vers les autorités sanitaires :

Alerte à l’ARS sous 1h si atteinte à la disponibilité des soins ou incident majeur.

Notification CNIL et ANS si suspicion de fuite de données (avec l’appui du DPO).

Rapport technique post-incident transmis sous 72h.

Plan de communication vers les prestataires :

Partage d’informations techniques sur la nature de l’incident et les besoins de rétablissement.

Demande d’activation des clauses spécifiques PRA/PCA prévues dans les contrats.

Vers les établissements du GHT / réseau régional :

Notification immédiate en cas d’interruption de flux ou de rupture d’interopérabilité.

Proposition de solutions de repli (ex. : hospitalisation dans un autre site du GHT).

Plan de communication vers les usagers (patients, familles, visiteurs) :

Affichage dans les halls d’accueil et services concernés.

Publication web ou réseaux sociaux institutionnels (si validée par la Direction).

**8.4 Responsabilités organisationnelles**

Voici les rôles des différents responsable et directeurs du CHU en cas de crise :

Directeur Général :

Valide les messages stratégiques externes.

Coordonne la communication institutionnelle avec les autorités et médias.

Directeur des Systèmes d’Information (DSI) : coordonne la remontée des informations techniques avec le RSSI, valide les éléments à diffuser, et s’assure de la cohérence des messages transmis aux directions métier et aux prestataires.

Responsable de la Sécurité des Systèmes d’Information (RSSI) avec le DSI :

Garantit la véracité des informations techniques transmises.

Évalue les risques de communication mal calibrée sur la surface d’attaque.

Responsable communication :

Rédige les messages, briefe les porte-parole, assure la veille image.

DPO :

Intervient en cas de données à caractère personnel exposées.

Coordonne les notifications CNIL en lien avec la cellule juridique.

**8.5 Fréquence des points de situation**

Dans le contexte de crise un point est réalisé tous les 60 à 90 min en phase de restauration active.

Des points structurés sont remontés au COMEX 2 à 3 fois par jour pour les tenir informer de la situation.

Un Reporting final formel à chaud est réaliser après retour à la normale (RETEX à chaud).

Un second Reporting final est réaliser plusieurs semaines après, dans le but de savoir ce qui à fonctionne et ce qui n’as pas fonctionner.

Dans le but d’améliorer les processus en qui était en place dans le CHU

**8.6 Outils de communication de crise**

Modèles de messages pré-rédigés (incidents critiques, rétablissement, consignes utilisateurs).

Journal des communications : pour tracer l’ensemble des messages diffusés, leur contenu, leurs destinataires et les canaux utilisés.

Plan média (si impact majeur) : en coordination avec l’ARS ou le ministère.

# 9. Maintenance et tests du PRA

Le maintien opérationnel du Plan de Reprise d’Activité (PRA) repose sur un processus continu d’évaluation, de validation et d’amélioration. Une stratégie de tests réguliers et de mise à jour documentaire est indispensable pour garantir l'efficacité du plan en situation réelle.

**9.1 Objectifs de la maintenance**

Le premier objectif de la maintenance est de s'assurer que le PRA reste aligné avec les évolutions du système d'information, de l'organisation hospitalière et du contexte réglementaire.

Le second objectif de la maintenance est de détecter les écarts entre la documentation et la réalité technique ou métier.

Le troisième objectif est de vérifier l'efficacité, la coordination et les temps de reprise réels.

Le quatrième objectif est intégré les retours d’expérience issus des incidents ou exercices précédents.

**9.2 Typologie des tests**

Voici tous les types de tests qui sont réaliser une ou plusieurs fois dans l’année pour tester le PRA et s’il est toujours pertinent dans sa version actuelle.

Tests techniques complets (annuels) :

* Simulation réelle de sinistre avec restauration effective de plusieurs services.
* Chronométrage des délais (RTO/RPO) et validation par les référents métiers.

Tests documentaires ou papier (semestriels) :

* Révision des procédures à blanc.
* Vérification de la disponibilité des fiches rôles, des scripts et des coordonnées d’urgence.

Tests ciblés ou unitaires :

* Restauration ponctuelle de sauvegardes critiques.
* Bascule de l’annuaire, relance d’une VM critique, test de reconstruction.

Exercices de gestion de crise :

* Activation simulée de la cellule PRA.
* Coordination inter-services et décisions à l’échelle DSI/DG/COMEX.

**9.3 Suivi et traçabilité**

Tous les tests sont documentés dans un registre des tests PRA, avec les éléments suivants :

* Objectifs du test
* Participants
* Résultats mesurés (temps, succès/échec)
* Anomalies constatées et actions correctives
* Signature du responsable du test

Les résultats sont partagés au sein du comité SSI et les écarts font l'objet d'un plan d'action priorisé.

**9.4 Mise à jour du PRA**

Le PRA est révisé au minimum une fois par an, ou à chaque modification significative du SI :

* Changement d’architecture (nouvelle infra, hébergement, applications critiques)
* Refonte métier (nouveau DPI, organisation des soins)
* Intégration de nouveaux risques identifiés (ex. : cybermenace émergente)

Le PRA est également mis à jour après chaque incident majeur ou déclenchement réel, à partir du retour d'expérience (RETEX).

Un extrait synthétique du PRA est mis à disposition des parties prenantes métiers pour s’assurer de l’appropriation du plan.

**9.5 Intégration dans la gouvernance SSI**

Le PRA fait partie intégrante du système de management de la sécurité de l’information (SMSI).

Il est audité au sein du programme annuel de revue de la PSSI.

Son niveau de maturité est suivi dans le tableau de bord cybersécurité du CHU.

Le maintien du PRA est une responsabilité partagée entre la DSI, le RSSI, les métiers et la direction générale.