25/06/2025

Xavier Martin

CHU Ynov

Plan de sauvegarde

CHU Ynov

Table des matières

[1. Objectifs du plan de sauvegarde 2](#_Toc202214260)

[2. Périmètre fonctionnel et technique 3](#_Toc202214261)

[3. Typologie des données sauvegardées 4](#_Toc202214262)

[4. Stratégie de sauvegarde 5](#_Toc202214263)

[5. Outils et infrastructures 7](#_Toc202214264)

[6. Contrôles d’intégrité et tests 8](#_Toc202214265)

[7. Responsabilités 11](#_Toc202214266)

[8. Conformité et documentation 13](#_Toc202214267)

[9. Suivi, revue et amélioration continue 16](#_Toc202214268)

# 1. Objectifs du plan de sauvegarde

Le Plan de Sauvegarde du CHU Ynov a pour vocation d’assurer la disponibilité, l’intégrité, la confidentialité et la résilience des données critiques produites et exploitées dans l’environnement hospitalier. Il a été conçu pour répondre aux besoins de continuité d’activité (PCA), de reprise après sinistre (PRA), et de conformité réglementaire (PGSSI-S, RGPD, HDS). Il permet également d’anticiper les incidents numériques (cyberattaques, défaillances matérielles, erreurs humaines) et de garantir la récupération fiable et rapide des systèmes essentiels au bon fonctionnement de l’établissement.

Ses objectifs spécifiques sont les suivants :

Garantir la disponibilité opérationnelle des données et systèmes cliniques : dossiers médicaux, prescriptions, résultats biologiques, imagerie, logs et flux critiques doivent être accessibles dans des délais acceptables pour assurer la continuité des soins.

Prévenir la perte définitive de données sensibles : toute information liée à l’identité, au parcours de soins, à la facturation ou à l’organisation hospitalière doit pouvoir être restaurée intégralement dans un état conforme.

Soutenir les dispositifs de continuité (PCA) et de reprise (PRA) : les sauvegardes doivent permettre une restauration planifiée, priorisée, et automatisée pour limiter l’impact d’un sinistre ou d’une compromission du système d’information.

Respecter les exigences réglementaires : le plan s’aligne sur les obligations du Code de la santé publique (article L.1111-8), du RGPD (droit à la portabilité, notification de violation), et des référentiels HDS pour l’hébergement et l’archivage de données de santé.

Fournir des moyens de contrôle, de vérification et d’amélioration continue : chaque sauvegarde est journalisée, testée, et documentée pour permettre un audit régulier et l’amélioration du dispositif en fonction des retours d’expérience.

# 2. Périmètre fonctionnel et technique

Le périmètre du Plan de Sauvegarde couvre l’ensemble des ressources numériques dont la perte ou l’altération pourrait compromettre la continuité, la qualité ou la légalité des activités de soins, de gestion, ou de support de l’établissement. Il prend en compte les aspects suivants :

**2.1 Systèmes d'information cliniques**

Dossier Patient Informatisé (DPI) : incluant les modules de suivi de soins, prescriptions, compte-rendus opératoires, résultats d’examens.

Systèmes de gestion de laboratoire (LIMS), pharmacie (GTP), radiologie (RIS / PACS) : fortement interdépendants et critiques pour la prise en charge médicale.

Systèmes de rendez-vous, de pré-admission, d’hébergement, de transport patient.

**2.2 Bases de données applicatives**

SGBD Oracle, SQL Server, PostgreSQL, MySQL : hébergeant les données métiers et techniques.

Clustering, réplication, et snapshots gérés selon les politiques de haute disponibilité.

Stockage logique et physique documenté dans la cartographie d’architecture SI.

**2.3 Données bureautiques critiques**

Documents contractuels, rapports médicaux, courriers officiels.

Documents RH sensibles (dossiers agents, arrêtés, feuilles de service).

Documents financiers et de commande, logs juridiques et assurances.

**2.4 Journaux et traçabilité**

Fichiers de logs applicatifs, OS, base de données, proxy, firewall, AD.

Traces de connexion, logs de changement, alertes de supervision.

Logs consolidés dans le SIEM et archivés dans un format horodaté et signé.

**2.5 Infrastructures et machines virtuelles**

VM de production (Linux / Windows), plateformes d’administration (AD, LDAP, DNS, DHCP, NTP).

Outils d’ordonnancement, de supervision, de sauvegarde, de déploiement.

Environnements de préproduction critiques (tests réglementaires, recette métier).

Le périmètre est revu semestriellement, mis à jour à chaque nouvelle intégration applicative ou refonte d’infrastructure, et validé par la cellule d’architecture DSI.

# 3. Typologie des données sauvegardées

Les données sauvegardées sont catégorisées selon leur usage, leur sensibilité, leur fréquence de mise à jour et leur impact potentiel en cas de perte. Chaque type de donnée est associé à un référentiel de conservation, à un plan de sauvegarde spécifique et à des précautions techniques particulières.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Catégorie | Donnés concernées | Niveau de criticité | Fréquence de mise à jour | Impacts en cas de perte | Responsable |
| Données de santé | Dossiers patients, prescriptions, comptes rendus, résultats biologiques | Critique | Temps réel à 4h | Interruption de soins, perte d’historique médical, risque vital | DSI / DPM |
| Données administratives | RH, paie, contrats, finances, logistique, juridiques | Importante | Quotidienne | Non-conformité légale, blocage des paiements, RH | DRH / DAF |
| Paramétrage & config | Scripts, fichiers de configuration, fichiers système, OS | Critique | À chaque modification | Perte de cohérence applicative, indisponibilité longue | DSI |
| Logs & traçabilité | Journaux de sécurité, accès, connexions, modifications système | Critique | Continue (SIEM temps réel) | Non-respect RGPD, impossibilité d’audit, risque d’impunité | RSSI |

Chaque catégorie fait l’objet de politiques de sauvegarde différenciées, intégrant le niveau de protection requis, les délais de restauration (RTO), la durée maximale de perte acceptable (RPO) et les obligations de conservation réglementaire.

# 4. Stratégie de sauvegarde

La stratégie de sauvegarde repose sur un équilibre entre fréquence, redondance, performance, sécurité, et accessibilité. Elle est conçue pour respecter les objectifs suivants :

* RTO (Recovery Time Objective) : rétablir les systèmes critiques dans un délai inférieur à 4h pour les applications cliniques, 8h pour les applications administratives.
* RPO (Recovery Point Objective) : limiter la perte de données à un maximum de 4 heures pour les flux critiques, et 24 heures pour les systèmes de support.

**4.1 Fréquence et type de sauvegarde**

Sauvegardes complètes (Full) : hebdomadaires, tous les dimanches soir, pour tous les serveurs critiques, avec vérification post-tâche par l’équipe exploitation.

Sauvegardes incrémentales : toutes les 4h pour le DPI, laboratoire et pharmacie.

Sauvegardes différentielles : quotidiennes pour les systèmes administratifs et RH.

Snapshots journaliers : pour les machines virtuelles de l’hyperviseur principal.

**4.2 Plan de rotation et conservation**

Rotation sur bande virtuelle ou disque avec cycle de 30 jours pour les incrémentales.

Conservation longue durée (12 mois) sur site secondaire pour les Full hebdomadaires.

Externalisation sécurisée (SecNumCloud ou HDS) de la dernière Full chaque semaine.

Archivage réglementaire distinct pour les données médico-légales.

**4.3 Localisation et redondance**

Sites de stockage primaire : baie SAN double contrôleur, architecture RAID 10.

Sites secondaires : Datacenter PRA (HDS, bâtiment physique distinct, VPN chiffré).

Cloud souverain : sauvegardes chiffrées en redondance à l'extérieur du réseau local.

**4.4 Mécanismes de chiffrement et d’accès sécurisé**

Chiffrement AES-256 des flux et des disques.

Signature numérique et jeton d’authentification (token HMAC/SHA256).

ACL et bastion pour accès administrateur, journalisation complète des actions.

**4.5 Journalisation et traçabilité**

Rapport journalier d’intégrité et d’achèvement des tâches de sauvegarde.

Archivage automatique des journaux d’activité dans le SIEM pour 18 mois.

Notification automatisée en cas d’échec de tâche ou de tentative d’accès non autorisé.

# 5. Outils et infrastructures

Le dispositif de sauvegarde repose sur une architecture technique robuste, redondante, segmentée et supervisée, combinant solutions logicielles éprouvées, stockage sécurisé, et contrôle réseau dédié. Il s’inscrit dans une logique de résilience multisite et d’administration centralisée.

**5.1 Solutions logicielles de sauvegarde**

Veeam Backup & Replication : pour la protection des machines virtuelles, snapshots, réplication intersites, restauration granulaire.

Atempo Tina : gestion des sauvegardes de bases de données, fichiers critiques, support bande ou disques.

Rubrik : solution intégrée compatible HDS et SecNumCloud, avec fonctionnalités de déduplication, immutabilité et gestion des versions.

Scripts personnalisés : PowerShell, Bash ou Ansible pour automatiser les tâches spécifiques (sauvegarde de configurations, exports SQL, rotation de journaux).

**5.2 Infrastructures de stockage**

SAN Dell EMC PowerStore : baie primaire en RAID 10, tolérance de panne n+1, snapshots locaux.

NAS NetApp : pour les fichiers utilisateurs critiques et sauvegardes intermédiaires.

Stockage objet S3 compatible (MinIO, AWS, OVHcloud Public Cloud) : pour les exports longue durée et les sauvegardes dans le cloud souverain.

Air gap : solutions de stockage déconnecté (périodique) pour immuniser certaines sauvegardes contre les ransomwares.

**5.3 Réseau et segmentation**

VLAN dédié aux sauvegardes : isolé logiquement, filtré par firewall, avec limitations de bande passante via QoS.

Flux chiffrés (VPN site-to-site) vers les datacenters distants ou sites PRA.

Supervision réseau : contrôle de l’encombrement, des paquets perdus, du temps de traitement par tâche de sauvegarde.

**5.4 Supervision, alertes et corrélation**

Zabbix / Centreon : suivi en temps réel de l’état des agents de sauvegarde, disques de stockage, bande passante.

SIEM régional (SOC GHT ou externe) : corrélation d’événements liés à la sécurité, alertes en cas d’échec de tâche ou comportement suspect.

Tableau de bord dédié : taux de réussite, erreurs critiques, dernières restaurations validées, affiché dans la console de pilotage DSI/RSSI.

**5.5 Localisation des équipements**

Datacenter principal HDS dans les locaux du CHU (niveau de redondance 2N).

Datacenter secondaire PRA distant de plus de 10 km, sur fibre dédiée, certifié ISO 27001.

Sauvegardes répliquées automatiquement ou manuellement chaque nuit avec horodatage et contrôle d’intégrité.

L’ensemble de ces composants est revu chaque année lors du plan directeur SI et à chaque évolution d’architecture ou d’équipement critique.

# 6. Contrôles d’intégrité et tests

Le dispositif de contrôles d’intégrité et de tests de restauration est une composante centrale du Plan de Sauvegarde du CHU Ynov. Son objectif est de garantir que les sauvegardes ne sont pas seulement réalisées, mais exploitables, fiables, et conformes aux engagements de continuité et de reprise (PCA/PRA). Cette section décrit les objectifs, les moyens, la planification et la gouvernance des tests et des contrôles appliqués.

**6.1 Objectifs des contrôles d’intégrité et des tests**

Cette sous-partie explicite les finalités stratégiques des contrôles et des tests de restauration, en les reliant directement aux enjeux métiers et réglementaires.

Garantir la fiabilité des sauvegardes et prévenir toute corruption ou altération des données sensibles.

Vérifier la capacité effective à restaurer les systèmes critiques selon les délais définis dans les objectifs RTO/RPO.

S’assurer de la conformité réglementaire (PGSSI-S, RGPD, HDS) et permettre la traçabilité des opérations pour les audits.

Favoriser une culture de la résilience au sein de la DSI et des équipes métiers.

**6.2 Contrôle d’intégrité automatisé**

Cette sous-partie détaille les mécanismes techniques automatisés permettant de vérifier l’intégrité des sauvegardes dès leur création et tout au long de leur cycle de vie.

Application d’algorithmes de hachage CRC32 et SHA-256 à chaque bloc de données sauvegardé pour détecter toute altération.

Signature numérique des empreintes pour garantir l’authenticité et l’intégrité.

Vérification post-sauvegarde automatique avec journalisation des résultats.

Alertes en cas d’échec ou d’incohérence détectée, transmises au SOC ou au SIEM régional.

Validation périodique des sauvegardes archivées pour détecter la corruption dite « silencieuse » sur le long terme.

**6.3 Tests de restauration réguliers**

Cette sous-partie décrit les différentes catégories de tests planifiés, leurs objectifs spécifiques, leur fréquence et leurs modalités de validation technique et métier.

Tests mensuels ciblés : restauration partielle (VM, bases critiques) sur environnement isolé pour valider la cohérence et la compatibilité applicative.

Tests trimestriels fonctionnels : scénarios couvrant plusieurs systèmes métiers interconnectés, validés par les utilisateurs métiers (DPI, LIMS, pharmacie).

Tests annuels grandeur nature : simulation complète de sinistre avec restauration et bascule vers le site PRA, chronométrage des RTO/RPO, validation de la reprise interservices.

Tests exceptionnels : obligatoires après toute mise à jour majeure du SI ou après un incident de sécurité (tentative d’intrusion, ransomware).

**6.4 Outils et environnements de test**

Cette sous-partie précise les moyens techniques, logiciels et infrastructures utilisés pour réaliser les tests de restauration dans des conditions maîtrisées et représentatives.

Solutions logicielles : Veeam, Atempo Tina, Rubrik avec consoles dédiées permettant les restaurations granulaires et les scénarios complexes.

Environnements d’exécution : PRA physique ou virtualisé, plateforme de préproduction pour tests unitaires sans impact sur la production.

Automatisation et scripts : PowerShell, Bash, Ansible pour standardiser les étapes et réduire les erreurs manuelles.

Journalisation complète : logs détaillés de chaque test, résultats et métriques enregistrés dans la GED sécurisée.

**6.5 Planification et suivi**

Cette sous-partie explique l’organisation du cycle de tests et contrôles, la gouvernance associée, et les modalités de reporting et de traçabilité.

Élaboration d’un plan annuel des tests validé en comité de pilotage SSI, incluant la couverture des différents systèmes et processus.

Documentation des scénarios avec définition des objectifs, des indicateurs clés (RTO/RPO) et des prérequis techniques.

Suivi via un tableau de bord cybersécurité mis à jour après chaque campagne de test, partagé entre la DSI, le RSSI et la Direction générale.

Archivage des rapports de tests (résultats, écarts, plans d’action) pendant 3 ans dans la GED sécurisée et auditée.

**6.6 Analyse des résultats et amélioration continue**

Cette sous-partie décrit comment les résultats des tests sont analysés, comment les écarts sont traités, et comment l’ensemble alimente un cycle d’amélioration continue.

Analyse systématique des écarts entre objectifs contractuels (SLA) et résultats réels : temps de restauration, intégrité des données.

Identification des causes racines des éventuels échecs ou lenteurs.

Élaboration et mise en œuvre de plans d’action correctifs techniques et organisationnels, validés par le RSSI et la DSI.

Intégration des résultats et enseignements dans la mise à jour annuelle du Plan de Sauvegarde, du PRA et des procédures associées.

Harmonisation avec les autres dispositifs de gestion de crise (PCA, Plan Blanc) pour garantir une cohérence globale de la stratégie de résilience.

# 7. Responsabilités

Le succès du Plan de Sauvegarde repose sur une répartition claire, documentée et validée des rôles et responsabilités. Cette section définit les missions de chaque acteur impliqué dans la planification, l’exécution, le suivi et l’amélioration des sauvegardes. Une gouvernance partagée et des circuits de validation explicites permettent de réduire les risques d’erreur humaine, d’assurer la conformité réglementaire et de garantir une réaction coordonnée en cas d’incident.

**7.1 Direction des Systèmes d’Information (DSI)**

La DSI est le pilote opérationnel du dispositif de sauvegarde. Elle est responsable de sa mise en œuvre technique, de sa maintenance et de son amélioration continue.

Élaboration et mise à jour de la stratégie de sauvegarde, en lien avec le RSSI.

Planification des fréquences, des fenêtres de sauvegarde et des rotations de supports.

Maintien en condition opérationnelle (MCO) des logiciels et matériels de sauvegarde.

Supervision quotidienne des tâches (succès, échecs, alertes) et résolution des incidents techniques.

Coordination avec les prestataires et les éditeurs pour le support technique et les évolutions.

**7.2 Responsable de la Sécurité des Systèmes d’Information (RSSI)**

Le RSSI assure la gouvernance sécurité du plan, son alignement avec la PSSI et la conformité aux exigences réglementaires.

Validation de la politique de sauvegarde dans le cadre du SMSI (ISO 27001 si applicable).

Contrôle des accès et des habilitations sur les consoles et environnements de sauvegarde.

Revue régulière des journaux et des rapports de tests d’intégrité et de restauration.

Analyse des incidents de sécurité liés aux sauvegardes (tentatives d’accès non autorisé, corruption).

Animation du comité de pilotage SSI pour les mises à jour annuelles du plan.

**7.3 Référents applicatifs et métiers**

Les référents applicatifs (DSI ou métiers) garantissent l’adéquation des sauvegardes aux besoins fonctionnels et la capacité de reprise.

Validation des périmètres de données et des fréquences de sauvegarde pour leur domaine.

Participation aux tests de restauration pour vérifier la cohérence applicative.

Contribution à la rédaction des scénarios de tests et à l’analyse des résultats.

Identification des impacts métier en cas de perte ou de décalage temporel (RPO).

**7.4 Equipe Exploitation et Support**

Chargée de l’exécution quotidienne des tâches et du suivi des résultats.

Lancement et supervision des jobs de sauvegarde programmés.

Vérification des journaux quotidiens et reporting des erreurs.

Application des correctifs de configuration ou relance des tâches en échec.

Préparation des supports physiques (bandes, disques) si rotation offline.

**7.5 Prestataires et éditeurs**

Acteurs externes intégrés dans la stratégie de sauvegarde selon les contrats de service (SLA) établis.

Maintenance et support des solutions logicielles (Veeam, Atempo, Rubrik).

Support matériel des baies de stockage et des bandes virtuelles.

Gestion des mises à jour, patchs de sécurité, et évolutions contractuelles.

Engagements de disponibilité et d’intervention en cas d’incident critique (astreintes, délais contractuels).

**7.6 Comité de pilotage SSI / PCA / PRA**

Organe de gouvernance interdisciplinaire pour la validation des grandes orientations du plan.

Approbation de la stratégie annuelle de sauvegarde.

Validation des résultats des tests et des retours d’expérience (RETEX).

Arbitrage des priorités budgétaires et techniques.

Coordination entre les différents volets de continuité (PCA, PRA, Plan Blanc).

**7.7 Documentation et traçabilité des responsabilités**

Tous les rôles et responsabilités sont formalisés et mis à disposition dans la GED sécurisée.

Organigramme des acteurs et fiches de rôle détaillées.

Journal des actions critiques : modifications de configuration, restaurations exceptionnelles, incidents sécurité.

Contrats et engagements des prestataires conservés et audités régulièrement.

Accès restreint et contrôlé selon la matrice des habilitations définie par la DSI et le RSSI.

# 8. Conformité et documentation

Le Plan de Sauvegarde du CHU Ynov est conçu pour être pleinement conforme aux exigences réglementaires et normatives applicables à un établissement de santé. Cette section précise les textes de référence, les obligations associées et les exigences documentaires, afin d’assurer la transparence, la traçabilité et l’auditabilité du dispositif de sauvegarde.

**8.1 Objectifs de conformité**

Cette sous-partie définit les finalités stratégiques en matière de conformité pour le plan de sauvegarde.

Garantir la protection des données de santé à caractère personnel conformément au RGPD.

Répondre aux obligations spécifiques de l’hébergement des données de santé (HDS) selon l’agrément ou la certification.

Respecter les règles de la PGSSI-S (Politique Générale de Sécurité des SI de Santé).

Permettre des audits internes et externes, notamment dans le cadre du SMSI ou des démarches de certification ISO 27001 ou HDS.

**8.2 Cadre réglementaire applicable**

Cette sous-partie explicite les textes et référentiels auxquels le plan de sauvegarde doit se conformer.

Règlement Général sur la Protection des Données (RGPD) : droits des personnes concernées (accès, portabilité), notification des violations, minimisation des données, conservation limitée.

Code de la santé publique (L.1111-8) : obligation d’hébergement agréé ou certifié HDS pour les données de santé.

Référentiel HDS : exigences sur la sécurité physique, logique, organisationnelle et sur la gestion des sauvegardes et restaurations.

PGSSI-S : cadre stratégique et règles de gouvernance pour la sécurité des SI de santé.

Instruction DGOS/PF2 sur l’archivage et la conservation des données médicales.

Politiques internes de l’AP-HM et du GHT : chartes d’utilisation, plan directeur SI.

**8.3 Exigences spécifiques sur les sauvegardes**

Cette sous-partie détaille les obligations concrètes de conformité qui s’appliquent aux sauvegardes.

Chiffrement systématique des sauvegardes en transit et au repos (AES-256 minimum).

Journalisation et traçabilité des opérations de sauvegarde et de restauration, horodatées et signées numériquement.

Contrôle des accès et habilitations : application du principe du moindre privilège, gestion des comptes à privilèges via bastion.

Plan de réversibilité permettant la restitution complète des données en cas de changement de prestataire ou d’arrêt de service.

Archivage réglementaire : respect des durées légales de conservation des dossiers médicaux (20 ans après le dernier passage du patient).

Notification des violations : capacité à détecter et déclarer rapidement toute compromission ou perte de données (CNIL, ARS).

**8.4 Documentation opérationnelle et référentielle**

Cette sous-partie décrit les exigences de formalisation et de maintien de la documentation liée aux sauvegardes.

Politique de sauvegarde : document formel validé en comité SSI, versionnée et archivée.

Procédures techniques détaillées : modes opératoires pour les sauvegardes Full, incrémentales, différentielles, rotations sur bande ou cloud.

Manuels d’administration des consoles de sauvegarde (Veeam, Atempo, Rubrik).

Scénarios de tests de restauration documentés avec résultats et plan d’action associé.

Registres des incidents liés aux sauvegardes et restaurations.

Contrats et SLA des prestataires décrivant les engagements de support et de disponibilité.

Journal des accès aux environnements de sauvegarde, consultable en cas d’audit ou d’incident.

**8.5 Gestion de la documentation**

Cette sous-partie précise les modalités de gestion, de diffusion et d’archivage de la documentation.

GED sécurisée (Gestion Électronique des Documents) avec contrôle des accès et historique des versions.

Classification des documents selon leur sensibilité et leur usage (public interne, confidentiel, restreint SSI).

Archivage long terme des rapports critiques (tests de restauration, journaux d’intégrité, incidents).

Mises à jour planifiées : revue annuelle en comité SSI, et mises à jour ponctuelles après toute évolution majeure (nouveau logiciel, migration SI, changement réglementaire).

**8.6 Auditabilité et transparence**

Cette sous-partie explicite comment le plan assure la capacité à être audité, en interne comme en externe.

Préparation des rapports et registres exploitables lors d’un audit HDS ou RGPD.

Conservation des logs détaillés des sauvegardes et restaurations pendant la durée légale ou contractuelle.

Capacité à démontrer la conformité des pratiques aux règles internes (PSSI) et aux référentiels réglementaires.

Participation active aux audits internes SSI et aux revues de la Direction générale ou du GHT.

# 9. Suivi, revue et amélioration continue

La mise en œuvre d’un plan de sauvegarde ne peut être figée : elle doit être régulièrement revue, adaptée et améliorée pour faire face à l’évolution des menaces, des technologies et des contraintes réglementaires. Cette section détaille les dispositifs mis en place au CHU Ynov pour garantir que la stratégie de sauvegarde reste efficace, pertinente et conforme dans la durée.

**9.1 Objectifs du suivi et de la revue**

Cette sous-partie précise les finalités stratégiques de la démarche de suivi et de revue du plan.

S’assurer que la stratégie de sauvegarde couvre l’ensemble des actifs critiques et les nouveaux périmètres SI.

Garantir la conformité continue avec les obligations réglementaires (RGPD, PGSSI-S, HDS).

Identifier proactivement les points faibles ou écarts de performance (RTO/RPO).

Mobiliser les acteurs autour d’un cycle d’amélioration continue documenter et traçable.

**9.2 Organisation du suivi**

Cette sous-partie décrit la gouvernance et les instances en charge du suivi du plan de sauvegarde.

Pilotage par la DSI en coordination avec le RSSI.

Réunions trimestrielles opérationnelles pour la revue des incidents, des alertes et des rapports de sauvegarde.

Comité de pilotage SSI annuel incluant la Direction générale, la DAF, les référents métiers et le RSSI.

Intégration au plan directeur SI et au SMSI (pour les établissements certifiés ISO 27001).

**9.3 Indicateurs et tableaux de bord**

Cette sous-partie décrit les métriques suivies pour évaluer l’efficacité du dispositif.

Taux de succès des sauvegardes planifiées (objectif >99,5 % sur 12 mois glissants).

Délai moyen de restauration par type de système et criticité.

Nombre d’incidents ou échecs critiques nécessitant intervention manuelle ou correction.

Taux de conformité aux RTO/RPO définis dans le PRA.

Nombre et résultats des tests de restauration effectués.

Rapports consolidés disponibles dans la GED sécurisée, consultables pour les audits.

**9.4 Modalités de revue annuelle**

Cette sous-partie détaille le processus de révision formelle du plan.

Organisation d’une revue annuelle structurée pilotée par la DSI et le RSSI.

Collecte des données de l’année écoulée : rapports de sauvegarde, incidents, résultats des tests.

Évaluation de la couverture fonctionnelle et technique : nouveaux SI, nouvelles applications, évolutions réglementaires.

Comparaison entre les objectifs et les résultats effectifs (écarts RTO/RPO).

Élaboration et validation d’un plan d’action annuel en comité SSI.

**9.5 Amélioration continue**

Cette sous-partie formalise la démarche d’amélioration du dispositif de sauvegarde.

Intégration systématique des RETEX (retours d’expérience) des incidents, des tests et des audits.

Priorisation des actions correctives : renforcement des fréquences, ajout de nouvelles sauvegardes, amélioration des procédures.

Suivi des plans d’action par le RSSI et la DSI : mise à jour des outils, formation des équipes, évolution des contrats prestataires.

Sensibilisation continue des acteurs concernés : formations ciblées pour l’équipe exploitation, la DSI, les référents métiers.

Harmonisation avec les autres plans institutionnels (PCA, PRA, Plan Blanc, PSSI).

**9.6 Documentation des évolutions**

Cette sous-partie explique la gestion documentaire des modifications du plan.

Versionnage rigoureux de la politique de sauvegarde et des procédures associées.

Archivage des anciennes versions pour traçabilité et auditabilité.

Mise à jour des fiches de rôle et des organigrammes de responsabilités.

Publication des nouvelles versions dans la GED sécurisée avec contrôle des accès.

**9.7 Interface avec les audits**

Cette sous-partie précise comment le suivi alimente la préparation des audits internes et externes.

Préparation des preuves documentaires : rapports de test, journaux de sauvegarde, indicateurs de performance.

Participation active aux audits HDS ou RGPD.

Réponse aux recommandations des auditeurs : plan d’action formalisé et suivi.

Suivi des engagements contractuels avec les prestataires : SLA, conformité HDS/SecNumCloud.