[Date]

Xavier Martin

CHU YNOV

Document d’exploitation global du SI – CHU Ynov

Table des matières

[1 : Introduction et périmètre 2](#_Toc202468758)

[2. Gouvernance et rôles 6](#_Toc202468759)

[3. Architecture opérationnelle 10](#_Toc202468760)

[4. Exploitation quotidienne 15](#_Toc202468761)

[5. Maintenance et mises à jour 20](#_Toc202468762)

[6. Supervision et alerting 25](#_Toc202468763)

[7. Gestion des sauvegardes et restaurations 30](#_Toc202468764)

[8. GESTION DU CHIFFREMENT ET DES CLÉS 35](#_Toc202468765)

[9. Gestion des incidents et réponse 40](#_Toc202468766)

[10. Contrôles, audits et conformité 44](#_Toc202468767)

[11. Formation et sensibilisation opérationnelle 48](#_Toc202468768)

[12. Amélioration continue et retours d’expérience 53](#_Toc202468769)

# 1 : Introduction et périmètre

Cette section définit la raison d’être et les objectifs généraux de la Politique de Sécurité des Systèmes d’Information (PSSI) du CHU Ynov.

Elle formalise les engagements de l’établissement en matière de cybersécurité, décrit les finalités attendues et précise le cadre stratégique dans lequel s’inscrit la protection du système d’information, des données de santé et des services critiques.

**1.1. Contexte général**

Le Centre Hospitalier Universitaire (CHU) Ynov est un établissement public de santé majeur, assurant des missions de soins, d’enseignement et de recherche. Son système d’information (SI) est un élément critique pour la continuité et la qualité des soins, l’efficacité administrative et la coopération inter-hospitalière.

Le SI du CHU héberge et traite notamment :

Les données de santé des patients (Dossiers Médicaux Informatisés, résultats biologiques, imagerie, prescriptions, historiques).

Les données administratives et financières (gestion des ressources humaines, facturation, achats, contrats).

Des données stratégiques et de pilotage (indicateurs qualité, épidémiologie, recherche clinique).

Le SI est donc un actif vital exposé à des menaces majeures :

* Cyberattaques ciblées (rançongiciels, vol de données).
* Pannes matérielles, incendie, sinistre physique.
* Erreurs humaines ou malveillances internes.
* Non-conformité réglementaire (HDS, RGPD).

Le présent document d’exploitation formalise l’organisation, les processus et les règles de fonctionnement du SI en environnement de production et de secours. Il vise à :

* Garantir la continuité des soins et des services hospitaliers.
* Assurer la confidentialité, intégrité, disponibilité des données.
* Répondre aux exigences réglementaires et aux référentiels (PGSSI-S, HDS, RGPD).
* Permettre une exploitation sécurisée, industrialisée et auditable.

**1.2. Objectifs du document**

Ce document d’exploitation définit :

* Les modalités de gestion opérationnelle du SI du CHU (production, PRA/PCA).
* Les rôles et responsabilités des acteurs internes et externes.
* Les processus quotidiens et périodiques (sauvegarde, supervision, maintenance, incidents).
* Les mécanismes de sécurité : chiffrement, accès, sauvegarde, audit.
* Les KPI et indicateurs pour un pilotage de la qualité de service et de la sécurité.
* Les plans d’amélioration continuent (conformité, formation, retour d’expérience).

Il constitue la référence opérationnelle pour :

* Les équipes internes (DSI, RSSI, exploitation, sécurité).
* Les référents métiers et chefs de service.
* Les prestataires et partenaires sous contrat.
* Les autorités de tutelle ou auditeurs (ARS, ANSSI, CNIL, certification HDS).

**1.3. Périmètre technique couvert**

Le périmètre d’exploitation décrit comprend :

a) Infrastructures physiques et virtuelles

Data Centers on-premise : salles informatiques principales (DC1) et site de secours (DC2/PRA).

Environnements virtualisés (VMware cluster, hyperviseurs Windows/Linux).

Stockage SAN/NAS, appliances de sauvegarde, réseaux de fibres.

b) Plateformes cloud

Cloud Azure France (HDS) : VM IaaS, PaaS SQL Server avec TDE, Key Vault pour la gestion des clés.

Services hybrides : sauvegarde dans Azure Backup, réplication Rubrik, authentification via Azure AD.

c) Réseau et sécurité périmétrique

Firewalls physiques (FortiGate), proxies.

Segmentation VLAN (médical, administratif, biomédical, invité, DMZ).

IPS inline et IDS en mode surveillance.

VPN site-to-site (IPsec, SSL VPN).

Wi‑Fi hospitalier (SSID internes et publics, NAC).

d) Systèmes d’information hospitaliers

Applications médicales critiques :

Dossier Patient Informatisé (DPI) conforme PGSSI-S.

RIS/PACS (Radiologie, Imagerie), LIMS (Laboratoire).

Applications de prescription et suivi pharmaceutique.

Applications administratives :

ERP hospitalier.

Gestion des ressources humaines (GRH).

Facturation et finances.

Applications de support :

Portails patients.

Référentiels qualité et planification.

e) Données et contenus

Données de santé à caractère personnel (sensibilité maximale).

Données administratives et financières.

Journaux et logs systèmes, applicatifs, réseau.

Sauvegardes locales et externalisées.

**1.4. Cadre réglementaire et normatif applicable**

L’exploitation du SI s’inscrit dans les obligations suivantes :

Code de la santé publique (articles L.1111-8 et suivants).

Règlement Général sur la Protection des Données (RGPD).

Référentiel HDS (Hébergeur de Données de Santé) en vigueur.

Politique Générale de Sécurité des Systèmes d’Information de Santé (PGSSI-S).

Recommandations ANSSI (RGS, guides techniques).

Contrats et DPA avec prestataires et éditeurs.

**1.5. Contraintes et enjeux spécifiques**

Disponibilité 24/7 : service hospitalier en continu.

Sécurisation des données sensibles : secret médical, confidentialité patiente.

Traçabilité et auditabilité : conformité HDS/RGPD.

Résilience face aux attaques : ransomware, exfiltration, sabotage.

Interopérabilité : échanges MSSanté, Apicrypt, DMP, portails régionaux.

Support des évolutions : ouverture de nouveaux services numériques, connectivité biomédicale (IoT médical).

**1.6. Public cible du document**

Équipes DSI (chefferie de projet, exploitation, support).

RSSI et équipe sécurité.

Administrateurs systèmes et réseaux.

Responsables applicatifs et métiers.

Prestataires externes (opérateurs de sauvegarde, intégrateurs, éditeurs).

Auditeurs externes (certification HDS, conformité CNIL).

**1.7. Organisation du document**

Parties 2-3 : Gouvernance, rôles et responsabilités.

Parties 4-6 : Exploitation quotidienne, maintenance, supervision.

Parties 7-9 : Sauvegardes/restaurations, gestion du chiffrement, gestion des incidents.

Parties 10-12 : Audits, formation, amélioration continue.

# 2. Gouvernance et rôles

Cette partie précise le périmètre d’application de la PSSI. Elle délimite les ressources, les acteurs, les flux et les systèmes concernés par les règles de sécurité, en tenant compte des spécificités de l’environnement hospitalier et des obligations légales. Elle vise à garantir une couverture complète et cohérente des enjeux de sécurité pour l’ensemble de l’établissement.

**2.1. Principes directeurs de gouvernance**

La gouvernance du SI du CHU La Timone repose sur :

Clarté des responsabilités : chaque acteur connaît son périmètre et ses tâches.

Séparation des pouvoirs (SoD) : aucune personne ne cumule tous les accès critiques.

Traçabilité des actions : tous les changements et accès sensibles sont journalisés et auditables.

Approche collaborative : la sécurité n’est pas une compétence isolée mais intégrée dans l’ensemble des processus.

Alignement stratégique : les choix techniques et organisationnels doivent respecter la PSSI, le schéma directeur SI et les budgets validés.

**2.2. Structure de gouvernance SSI**

Le CHU Ynov adopte une structure de gouvernance s’appuyant sur :

Un Comité stratégique SSI (bi-annuel)

Un Comité opérationnel SSI (mensuel)

Une Équipe sécurité opérationnelle (SOC / exploitation / RSSI / DSI)

Schéma organisationnel :

Comité stratégique SSI

↳ RSSI

↳ Comité opérationnel SSI

↳ Équipe Sécurité (Admin, SOC)

↳ Équipe Exploitation

↳ DSI

↳ Référents métiers

**2.3. Comité stratégique SSI**

Périmètre : arbitrages stratégiques et budgétaires SSI.

Participants : Direction générale, RSSI, DSI, DAF, représentant qualité.

Périodicité : 2 fois par an.

Missions principales :

Valider les priorités et investissements SSI (PRA/PCA, outils SIEM, IDS/IPS).

Suivre les indicateurs globaux (KPI, incidents majeurs, audit conformité).

Arbitrer les grands choix techniques (hébergement, cloud, externalisation).

Garantir l’adéquation PSSI avec la stratégie globale.

**2.4. Comité opérationnel SSI**

Périmètre : suivi technique et pilotage des actions SSI.

Participants : RSSI (président), DSI, Admin sécurité, exploitants, référents métiers, SOC.

Périodicité : mensuelle.

Missions principales :

Examiner les rapports d’incidents et alertes SIEM.

Valider la feuille de route patch management.

Suivre les résultats des tests de restauration PRA.

Vérifier la mise en œuvre des plans d’action RGPD/HDS.

Suivre les plans de formation et de sensibilisation.

**2.5. Rôles et responsabilités détaillés**

|  |  |
| --- | --- |
| Acteur | Missions spécifiques |
| RSSI | • Définir et mettre à jour la PSSI  • Valider les politiques de sauvegarde, PRA, PCA  • Superviser incidents SSI  • Assurer veille réglementaire et technologique  • Piloter les audits internes et externes |
| DSI | • Superviser l’exploitation SI  • Piloter les projets techniques  • Maintenir la documentation d’architecture  • Valider les choix techniques (infra, réseau, cloud) |
| Équipe exploitation | • Exécuter les routines quotidiennes (sauvegardes, supervision, patching)  • Maintenir les serveurs et applications  • Assurer la disponibilité et la performance du SI |
| Admin sécurité | • Gérer le KMS (Azure Key Vault, HSM)  • Implémenter les règles IAM et RBAC  • Surveiller et maintenir IDS/IPS  • Superviser la rotation des clés, certificats |
| SOC / SIEM | • Analyser et corréler les alertes  • Classer les incidents (criticité, impact)  • Gérer les escalades vers RSSI  • Produire des rapports mensuels |
| Référents métiers | • Définir les exigences RTO/RPO  • Valider les restaurations (préprod, production)  • Collaborer sur les analyses d’impact métier |
| Prestataires externes | • Maintenir les systèmes sous contrat (HSM, appliances, cloud)  • Fournir SLA et reporting  • Participer aux audits et plans d’amélioration |

**2.6. Séparation des pouvoirs (SoD)**

Pour éviter tout risque de fraude ou de compromission :

Les rôles « Admin sécurité » et « Exploitation » sont strictement séparés.

Les accès aux systèmes critiques (HSM, Key Vault, Rubrik) nécessitent une double validation.

Les opérations de destruction de clés nécessitent l’approbation du RSSI et du DPO.

Les droits d’administration réseau sont séparés des droits d’administration système.

**2.7. Documentation et reporting**

GED Sécurisée : stockage des politiques, procédures, runbooks.

Rapports mensuels : incidents, sauvegardes, supervision.

Rapports trimestriels : indicateurs SSI (rotation des clés, succès sauvegardes, taux incidents).

Comptes rendus comités : formalisés et validés, conservés 5 ans.

Suivi des tickets ITSM : traçabilité des interventions, des incidents et des demandes métiers.

**2.8. Alignement réglementaire**

Toutes ces structures et responsabilités sont conçues pour répondre :

Au RGPD (accountability, registre des traitements, PIA).

À la certification HDS (politique de sécurité, contrôle des accès, journalisation, PRA/PCA).

À la PGSSI-S (principes directeurs et guide d’implémentation pour SI hospitaliers).

Aux recommandations ANSSI (RGS, guides PRA, chiffrement, segmentation réseau).

# 3. Architecture opérationnelle

Cette section décrit les textes, référentiels et obligations réglementaires qui encadrent la sécurité des systèmes d’information hospitaliers. Elle rappelle les exigences imposées par le Code de la santé publique, le RGPD, la certification HDS, la PGSSI-S et les recommandations de l’ANSSI, afin de démontrer l’alignement de la politique sur les standards applicables.

3.1. Vision générale

L’architecture du SI du CHU Ynov est conçue pour garantir :

La disponibilité des services 24/7.

La sécurité des données de santé (confidentialité, intégrité, traçabilité).

La résilience face aux sinistres, cyberattaques ou défaillances techniques.

La conformité aux normes HDS, PGSSI-S et RGPD.

Elle combine :

Des infrastructures on-premise (datacenters locaux) pour la production principale et le PRA.

Des services cloud HDS (Azure France) pour la sauvegarde, la haute disponibilité et certains applicatifs.

Une segmentation réseau avancée et des solutions de sécurité périmétrique et interne.

Des mécanismes de chiffrement et de gestion de clés robustes.

**3.2. Data Centers**

**3.2.1. DC1 – Datacenter principal (Production)**

Localisé sur site hospitalier sécurisé (contrôle badge, vidéosurveillance, redondance électrique).

Infrastructure VMware : cluster de 6 hôtes ESXi, vSAN avec RAID 10, tolérance n+1.

Stockage SAN Dell EMC : double contrôleur actif-actif, déduplication et snapshots locaux.

Réseau cœur 40 Gbps : commutateurs Cisco Nexus.

Firewalls FortiGate actifs-passifs.

HSM Thales pour la gestion des clés locales.

Fonctions hébergées :

✅ Applications critiques (DPI, LIMS, RIS/PACS).

✅ Bases de données SQL (TDE activé).

✅ Active Directory et LDAP.

✅ Appliances Rubrik et Veeam pour sauvegardes locales.

**3.2.2. DC2 – Datacenter secondaire (PRA)**

Situé à > 10 km du site principal (exigence HDS).

Connectivité fibre dédiée (VPN IPsec redondé).

Réplication Veeam et Rubrik en mode "failover orchestré".

HSM secondaire pour clés maître (back-up chiffré, rotation manuelle).

Objectifs :

Support PRA (RTO ≤ 8 h pour l’ensemble des services critiques).

Tests de restauration semestriels grandeur nature.

Hébergement minimal viable pour DPI et systèmes cliniques.

**3.2.3. Cloud HDS (Azure France)**

Hébergement HDS certifié.

VM IaaS : workloads secondaires, web front-end, batch jobs.

SQL PaaS : bases applicatives avec TDE.

Azure Key Vault (HSM-Backed) : gestion des secrets, clés de chiffrement, certificats.

Azure Backup : rétention longue durée des sauvegardes chiffrées (12 mois).

Private Link & ExpressRoute : connectivité sécurisée et basse latence.

Utilisation :

Complément à la production locale.

Réplication externalisée et résilience ransomware (air gap logique).

Stockage des backups et snapshots immuables.

**3.3. Réseau et Sécurité Périmétrique**

**3.3.1. Segmentation réseau**

VLAN dédiés :

* VLAN Médical : DPI, imagerie, biomédical.
* VLAN Administratif : RH, finances, bureautique.
* VLAN IoT biomédical : dispositifs connectés.
* DMZ : portails web, MSSanté, interop régionales.
* Wi-Fi invité et hospitalier : SSID séparés avec NAC.

Firewalls : FortiGate HA, filtrage basé sur zones et règles explicites.

IPS inline : inspection des flux, blocage signatures connues (Snort/Suricata).

IDS en mode SPAN : surveillance passive des anomalies réseau.

**3.3.2. Accès distants**

VPN IPsec site-to-site : entre DC1, DC2, et Azure.

SSL VPN : accès utilisateurs distants avec MFA.

Bastion SSH : administration sécurisée des VM Linux.

RDP Gateway : accès contrôlé aux serveurs Windows.

**3.4. Sauvegardes et Stockage**

**3.4.1. Orchestrateurs**

Rubrik : snapshots, immutabilité, Live Mount, gestion multi-sites.

Veeam : réplication VM, SureBackup, restauration granulaire.

Atempo Tina : sauvegardes de bases et fichiers lourds (NAS).

**3.4.2. Politique 3-2-1**

3 copies : prod, site PRA, cloud Azure Backup.

2 supports : disque local (SAN/NAS), cloud HDS.

1 copie offline : bandes hors réseau avec rotation mensuelle.

**3.4.3. Chiffrement**

AES-256 au repos (volumes BitLocker, LUKS).

TLS 1.3 en transit (VPN, HTTPS, SFTP).

Clés stockées dans HSM et Azure Key Vault avec rotation annuelle.

**3.5. Gestion des Clés et Chiffrement**

Primary KMS : Azure Key Vault (HSM-Backed).

Secondary KMS : HSM Thales local.

Cycle de vie des clés :

Création : approbation double opérateur.

Rotation : automatisée (AKV policies), annuelle pour data keys.

Sauvegarde : export chiffré HSM offline.

Destruction : purge API AKV, validation RSSI et DPO.

Utilisations :

BitLocker (Windows Servers).

LUKS (Linux).

TDE (SQL Server).

Certificats TLS publics et internes.

Chiffrement des sauvegardes (Rubrik/Veeam/Atempo).

**3.6. Services applicatifs**

**3.6.1. Applications Cliniques**

DPI (PGSSI-S conforme) : accès RBAC, logs audités.

RIS/PACS : DICOM sur TLS, gestion imagerie.

LIMS : résultats labo, intégrations HL7.

Prescription électronique : bases chiffrées, MFA prescripteur.

**3.6.2. Applications Administratives**

ERP hospitalier : RH, paie, comptabilité.

Gestion financière et logistique : approvisionnements, contrats.

GED : documents RH, juridiques.

**3.6.3. Applications Support**

Portail patient : messagerie MSSanté.

Interfaces région/DMP : Apicrypt, ProSanté Connect.

BI : rapports anonymisés, contrôle RBAC.

**3.7. Journaux et Logs**

Collecte : Syslog, journaux Windows Event, logs applicatifs.

Centralisation : ELK Stack (ElasticSearch, Logstash, Kibana).

Archivage : stockage horodaté et signé, rétention 18 mois.

Surveillance SIEM : corrélation, détection d’anomalies, alerting SOC.

Conformité RGPD : accès journalisé, purge après délai légal.

**3.8. Interopérabilité et Échanges**

Flux MSSanté : TLS 1.2+, certificat CNAM.

Apicrypt : chiffrement PGP pour résultats labo.

DMP : connexion sécurisée aux services régionaux.

Intégration HL7/FHIR : bus d’interop centralisé (Mirth Connect).

API internes : exposées via reverse proxy sécurisé (WAF).

**3.9. Diagrammes et Cartographies**

Diagramme d’architecture réseau (VLAN, firewalls, IPS/IDS).

Diagramme flux applicatifs (exemple : DPI → SQL → sauvegarde).

Cartographie des sauvegardes (Rubrik/Veeam/Atempo).

Cartographie des clés et cycle de vie (AKV/HSM).

# 4. Exploitation quotidienne

Cette partie présente l’organisation mise en place pour piloter la sécurité des systèmes d’information au sein du CHU La Timone. Elle définit les rôles, responsabilités et instances de décision (RSSI, DSI, comité SSI), et décrit les mécanismes de pilotage, de coordination et de reporting qui garantissent la cohérence et l’efficacité des actions de sécurité.

**4.1. Principes directeurs**

L’exploitation quotidienne du SI du CHU La Timone doit assurer :

La disponibilité continue des applications critiques pour la prise en charge des patients.

La sécurité des données sensibles (données de santé, administratives, RH).

La conformité avec les obligations réglementaires (HDS, RGPD, PGSSI-S).

La traçabilité complète des actions administratives et techniques.

La préparation permanente aux scénarios de sinistre ou cyberattaque.

Elle s’appuie sur :

Des routines quotidiennes formalisées et tracées.

Des rôles et responsabilités clairs (séparation des pouvoirs).

Des outils centralisés de supervision et de ticketing.

Une documentation opérationnelle partagée et versionnée.

**4.2. Activités quotidiennes principales**

Tableau récapitulatif des tâches quotidiennes :

|  |  |  |  |
| --- | --- | --- | --- |
| Activité | Responsable | Fréquence | Outil/Support |
| Vérification jobs de sauvegarde | Exploitation | Quotidien | Rubrik, Veeam, Tina |
| Contrôle intégrité des sauvegardes | Exploitation | Quotidien | SHA-256, journaux Rubrik |
| Vérification santé AKV/HSM | Admin Sécurité | Quotidien | Azure Portal, HSM Tool |
| Surveillance certificats expirants | Exploitation | Quotidien | Cert Manager |
| Monitoring IDS/IPS | SOC/Sécurité | Continu | SIEM, FortiAnalyzer |
| Revue alertes critiques | SOC, Admin Sécurité | Continu | SIEM, ticket ITSM |
| Vérification état systèmes critiques | Exploitation | Quotidien | Zabbix, Centreon |
| Analyse logs sécurité | SOC | Quotidien | SIEM, ELK Stack |
| Gestion tickets ITSM | Exploitation, SOC | Continu | GLPI ou ServiceNow |
| Point quotidien exploitation | Exploitation + Sécurité | Matinée | Réunion courte (15-30 min) |

**4.3. Routines formelles et consignes**

**4.3.1. Vérification sauvegardes**

Contrôle journal des jobs terminés.

Vérification taux de succès global ≥ 99 %.

Contrôle des logs d’intégrité (hash SHA-256) générés par Rubrik/Veeam.

Identification et planification de la relance des jobs échoués.

Archivage quotidien des rapports dans la GED sécurisée.

Exemple de log journalisé :

[Date] [JobID] [Status] [Hash] [Relance prévu]

2025-07-03 DPI-Full SUCCESS abc123... NA

2025-07-03 RH-Incr FAIL - Relance 03/07 22h

**4.3.2. Contrôle AKV et HSM**

Vérification disponibilité (API status / Latence API < 50 ms).

Journalisation des accès et rotations effectuées.

Contrôle des anomalies dans les logs HSM : erreurs cryptographiques, alarmes physiques.

Report des incidents au RSSI via ticket ITSM.

**4.3.3. Surveillance certificats TLS**

Monitoring expirations < 60 j, < 30 j (alerte prioritaire).

Liste hebdomadaire des certificats à renouveler.

Vérification conformité algorithmes (SHA-2, RSA ≥ 2048 bits).

Déclenchement procédure de renouvellement (validation CSR, mise à jour AKV).

**4.3.4. IDS/IPS et SIEM**

Analyse continue des alertes IPS inline (blocages en temps réel).

Revue journalière des logs IDS en mode sniffer.

Corrélation SIEM avec logs système, firewall, AD, AKV.

Qualifications incidentes avec classification (critique, élevé, modéré, faible).

Notification et escalade vers RSSI si critique.

**4.3.5. Supervision systèmes et réseaux**

Vérification uptime serveurs (Zabbix).

Charge CPU < 80 %, utilisation disque < 75 %, latence réseau < 50 ms.

Surveillance spécifique des VM critiques (DPI, SQL, PACS).

Monitoring réseau : VLAN segmentation, règles firewall actives.

4.3.6. Gestion des tickets ITSM

Enregistrement systématique de toute anomalie ou demande.

Priorisation basée sur criticité métier et impact.

Assignation équipe ou personne responsable.

Suivi jusqu’à clôture, documentation post-mortem si incident majeur.

Exemple de flux ITSM :

Ticket ouvert → Qualification → Affectation → Action → Résolution → Clôture → Retex si nécessaire

**4.4. Réunions et coordination**

Stand-up quotidien (8h30) :

Présence : exploitation, sécurité, DSI.

Durée : 15-30 min.

Ordre du jour type :

Revue des incidents ouverts.

Validation des relances sauvegardes.

Planning des maintenances du jour.

Point alertes sécurité.

Point quotidien sécurité (10h) :

Présence : RSSI, Admin sécurité, SOC.

Revue incidents sécurité détectés.

Suivi alertes IDS/IPS, SIEM.

Validation des escalades et des mesures de mitigation.

**4.5. Documentation et traçabilité**

Tous les contrôles quotidiens consignés dans runbooks partagés (GED).

Journalisation automatique des jobs (Rubrik/Veeam/Atempo).

Logs systèmes consolidés dans ELK, archivés 18 mois.

Tickets ITSM documentés et versionnés.

Reporting quotidien automatisé vers RSSI et DSI.

**4.6. Séparation des pouvoirs (SoD)**

Exploitation n’a pas accès à la rotation des clés AKV/HSM.

Admin Sécurité n’a pas les droits pour modifier configurations applicatives.

SOC analyse les logs mais ne peut exécuter de changements directs.

Toute opération critique requiert approbation double (RSSI + DSI).

**4.7. Bonnes pratiques imposées**

Authentification MFA pour consoles d’administration.

Accès VPN sécurisé, filtré par adresse IP et profil RBAC.

Bastion SSH pour accès aux VM Linux.

Journalisation complète et non falsifiable.

Scripts d’automatisation signés et stockés en versioning Git interne.

4.8. Indicateurs et KPI suivis quotidiennement

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Source |
| Taux succès sauvegardes | ≥ 99 % | Rubrik/Veeam |
| Taux alertes IDS/IPS fausses positives | < 5 % | SIEM |
| Temps moyen résolution tickets critiques | < 4 h | ITSM |
| Taux de disponibilité services critiques | ≥ 99,95 % | Zabbix/Centreon |
| Latence AKV/HSM | < 50 ms | Azure Monitor / HSM Tool |

# 5. Maintenance et mises à jour

Cette section expose la démarche systématique d’analyse des risques adoptée pour identifier, évaluer et traiter les menaces pesant sur le système d’information hospitalier. Elle détaille la méthodologie (ex. EBIOS RM), les périmètres analysés et les résultats attendus pour construire un dispositif de sécurité proportionné, adapté et évolutif.

**5.1. Principes directeurs**

Garantir la sécurité et la stabilité du SI grâce à un cycle de vie maîtrisé des composants.

Réduire la surface d’attaque en appliquant les correctifs de sécurité de manière contrôlée.

Assurer la compatibilité des mises à jour avec l’ensemble des composants métier.

Respecter les exigences réglementaires (HDS, RGPD, PGSSI‑S) en matière de patch management.

Maintenir la traçabilité complète des changements pour auditabilité.

**5.2. Politique de maintenance**

Le CHU Ynov applique une politique de maintenance structurée reposant sur :

Des fenêtres de maintenance planifiées et validées.

Une classification des mises à jour par criticité.

Des processus formalisés pour validation, tests, déploiement et documentation.

Une séparation stricte entre environnements (préproduction, production).

L’automatisation des déploiements pour limiter les erreurs humaines.

**5.3. Typologie des mises à jour**

|  |  |  |
| --- | --- | --- |
| Type de mise à jour | Description | Exemples |
| Critique sécurité | Correctif d'une vulnérabilité exploitée ou CVSS ≥ 7 | Patch Microsoft KB, mise à jour FortiOS IPS, CVE critique |
| Fonctionnelle majeure | Nouvelle version applicative ou changement majeur | Montée de version DPI, évolution RIS/PACS |
| Mineure | Correctifs de bugs non critiques | Hotfix applicatif, patch mineur OS |
| Signature/Definition update | Bases antivirus, IPS/IDS, malware signatures | Signatures Snort, Sophos AV |
| Firmware | Mise à jour du micrologiciel équipements | Switch Cisco, SAN Dell EMC, appliances Fortinet |

5.4. Organisation et responsabilités

|  |  |
| --- | --- |
| Rôle | Responsabilités spécifiques |
| RSSI | Valide le calendrier de patching, surveille les vulnérabilités, pilote les exceptions. |
| DSI | Coordonne le calendrier général, valide les fenêtres métiers, supervise le MCO. |
| Équipe Exploitation | Exécute le patching, documente dans ITSM, teste la disponibilité des services. |
| Admin Sécurité | Implémente règles IPS/IDS, met à jour certificats et clés, surveille impact sécurité. |
| Référents métiers | Valident les impacts métiers, participent aux tests de non régression. |
| Prestataires | Appliquent les mises à jour spécifiques sous contrat, fournissent la documentation. |

**5.5. Planification des fenêtres de maintenance**

Fenêtres planifiées et publiées dans le calendrier DSI :

Critique sécurité : sous 72 h après publication CVE/KB (hors rollback planifié).

Mensuelle régulière : dernier dimanche du mois, 02h00–06h00.

Majeure annuelle : fenêtre exceptionnelle validée en comité stratégique.

Notification préalable :

Minimum 7 jours avant intervention planifiée.

Minimum 24 h pour patch critique validé en cellule de crise SSI.

Canaux : email interne, Teams, tableau d’affichage intranet.

Validation :

RSSI, DSI et référents métiers valident chaque mise en production majeure.

Comité opérationnel SSI informe la direction générale en cas d’impact majeur.

**5.6. Processus formel de gestion des mises à jour**

Étape 1 – Veille et identification

Analyse CERT Santé, ANSSI, Microsoft, éditeurs applicatifs.

Identification vulnérabilités exploitables : scoring CVSS, exploit public.

Filtrage automatique des CVE avec règles SIEM.

Veille RSSI + Admin Sécurité + SOC.

Exemple :

CVE-2025-0001 – Score 9.8 – Critique – FortiOS IPS – Update sous 48 h.

Étape 2 – Qualification et planification

Qualification impact applicatif (équipe exploitation + référent métier).

Évaluation dépendances techniques (bases, middleware).

Planification dans la fenêtre mensuelle ou ad hoc si critique.

Mise à jour du planning de maintenance dans ITSM.

Étape 3 – Préproduction et tests

Application sur environnement de préproduction.

Tests de non régression :

Disponibilité service.

Intégrités données.

Performances acceptables.

Validation par référents métiers.

Étape 4 – Mise en production

Execution automatisée (Ansible, SCCM, WSUS).

Journaux détaillés des actions (runbooks).

Supervision en temps réel de la charge et des erreurs.

Communication aux équipes impactées.

Étape 5 – Validation post déploiement

Vérification disponibilité services via Zabbix/Centreon.

Contrôle des logs applicatifs et systèmes.

Tests fonctionnels métier (validation référent métier).

Clôture ticket ITSM avec rapport détaillé.

Étape 6 – Documentation et archivage

Logs déploiement stockés dans GED sécurisée.

Changelogs mis à jour dans la documentation technique.

Récapitulatif intégré au rapport mensuel SSI.

**5.7. Outils utilisés**

WSUS / SCCM : déploiement patch Microsoft.

Ansible : patch Linux, scripts idempotents.

FortiManager / FortiAnalyzer : gestion policies, signatures IPS.

Veeam / Rubrik / Atempo : snapshots avant/after.

ITSM : suivi des tickets de changement.

SIEM : détection vulnérabilités critiques, alertes corrélées.

GED : stockage versionné des procédures et logs.

**5.8. Journalisation et traçabilité**

Chaque étape journalisée dans l’outil ITSM.

Logs d’installation / rollback exportés en GED.

Revue mensuelle des patchs appliqués en comité opérationnel SSI.

Logs SIEM : corrélation des anomalies post patch (authentifications, erreurs système).

**5.9. Gestion des exceptions**

Dérogation temporaire documentée si patch impossible (incompatibilité métier).

Analyse de risque formalisée et validée RSSI.

Mesures compensatoires (IPS, ACL, segmentation, surveillance SIEM).

Suivi des exceptions en réunion mensuelle SSI.

5.10. Indicateurs et reporting

|  |  |  |
| --- | --- | --- |
| KPI | Objectif | Source ITSM/SIEM |
| Taux de patching critique | 100 % sous 72 h | Ticket ITSM |
| Taux patchs mensuels appliqués | ≥ 95 % | Rapport automatisé |
| Temps moyen de déploiement | < 4 h (critique) | Logs Ansible/SCCM |
| Nombre d’exceptions ouvertes | < 5 simultanées | Registre exceptions SSI |
| Incidents post patch critiques | 0 | SIEM |

# 6. Supervision et alerting

Cette partie décrit les activités quotidiennes nécessaires au maintien en conditions opérationnelles et de sécurité du SI. Elle précise les routines, contrôles, outils et rôles impliqués pour garantir la disponibilité des services, la fiabilité des sauvegardes, la surveillance continue et la traçabilité des actions d’exploitation.

**6.1. Principes directeurs**

Garantir la disponibilité en continu des services critiques.

Détecter précocement les défaillances techniques ou tentatives d’intrusion.

Faciliter la priorisation des interventions en fonction de la criticité.

Assurer la traçabilité et l’auditabilité des alertes et des réponses apportées.

Soutenir la conformité réglementaire (HDS, RGPD, PGSSI‑S).

**6.2. Objectifs opérationnels**

Surveiller en temps réel l’état de santé de l’ensemble des infrastructures : serveurs, réseaux, applications, sauvegardes.

Garantir la corrélation des événements de sécurité pour identifier les attaques complexes.

Générer des alertes contextuelles et priorisées, évitant les faux positifs massifs.

Fournir une vue consolidée (tableaux de bord) à la DSI et au RSSI.

Faciliter la gestion des incidents en automatisant la création des tickets ITSM.

**6.3. Architecture technique de supervision**

Schéma général (décrit en annexe) :

Agents → Collecteurs → Plateforme de supervision → SIEM → Alerting ITSM

Composants principaux :

Zabbix / Centreon :

Supervision disponibilité, ressources système, services applicatifs.

Monitoring de seuils critiques (CPU, RAM, stockage, disponibilité applicative).

Elastic SIEM (ELK Stack) :

Centralisation logs systèmes, applicatifs, réseau.

Corrélation des événements.

Détection de comportements anormaux.

FortiAnalyzer :

Journalisation et reporting des firewalls et IPS.

Analyse signatures et alertes.

Rubrik/Veeam Dashboards :

Monitoring succès/échecs des sauvegardes.

Contrôle intégrité des données via hash.

Azure Monitor / Sentinel :

Santé Azure Key Vault (AKV).

Monitoring latence API, taux d’erreurs.

Journalisation accès aux secrets.

**6.4. Périmètre supervisé**

|  |  |
| --- | --- |
| Domaine | Éléments surveillés |
| Infrastructure physique | Baies SAN/NAS, serveurs physiques, alimentation redondante. |
| VM et hyperviseurs | VMware cluster (uptime, CPU, RAM, stockage VM). |
| |  | | --- | |  |  |  | | --- | | Réseau | | Switchs, Firewalls, VPN tunnels, latence inter-sites. |
| Applications | DPI, RIS/PACS, LIMS, ERP, portails web. |
| Sauvegardes | Jobs Rubrik/Veeam/Atempo. |
| Cloud Azure HDS | VM IaaS, SQL PaaS, AKV. |
| Sécurité périmétrique | IPS inline, IDS en sniffer, WAF (reverse proxy). |
| Certificats | Dates d’expiration, conformité SHA-2/RSA2048+. |

**6.5. Supervision technique détaillée**

**6.5.1. Infrastructure système**

CPU < 80 % (alerte à 90 %).

RAM disponible > 15 %.

Utilisation disque < 75 %.

Uptime services applicatifs vérifié (HTTPS 200 OK).

Monitoring processus critiques (SQL Server, Tomcat, IIS).

**6.5.2. Réseau**

Latence inter-VLAN < 50 ms.

Taux erreurs interface < 0,1 %.

VPN tunnels actifs.

QoS priorisation VLAN médical.

Flow monitoring (NetFlow) pour détection exfiltration.

**6.5.3. Sauvegardes**

Taux de succès jobs > 99 %.

Vérification hash SHA-256 des sauvegardes.

Taux de réplication vers Azure Backup.

Alertes Rubrik sur job échoué ou intégrité compromise.

**6.5.4. Cloud Azure**

Azure Monitor Health pour AKV : latence < 50 ms, disponibilité > 99,9 %.

Surveillance facturation et quotas.

Supervision des accès aux secrets dans AKV.

**6.6. Supervision sécurité**

**6.6.1. SIEM**

Collecte logs Windows Event, syslog Linux.

Ingestion logs appliances réseau, firewalls, proxies.

Journaux AKV et HSM.

Journaux IPS/IDS.

Consolidation dans ELK Stack.

Corrélation :

Tentatives de connexion suspectes.

Mouvement latéral interne.

Accès non autorisés KMS.

Exploits signatures connues (Snort).

**6.6.2. IPS/IDS**

Inline : blocage automatique signatures critiques.

Sniffer : alertes pour pattern comportementaux.

Signatures mises à jour quotidiennes.

Logs détaillés archivés > 18 mois.

**6.6.3. Certificats et chiffrement**

Monitoring expirations < 60 j / < 30 j (niveau Alerte).

Vérification conformité (RSA ≥ 2048, SHA-256+).

Supervision renouvellement via Cert Manager.

**6.7. Alerting**

Types d’alertes

|  |  |  |
| --- | --- | --- |
| Niveau | Délai réponse | Exemple d’incident |
| Critique | 1 h réaction | Intrusion confirmée, échec restauration, AKV down. |
| Élevé | 4 h réaction | Latence AKV > 50 ms, IPS blocage récurrent. |
| Modéré | 24 h | Sauvegarde partielle échouée, certificat expirant < 30 j. |

Canal d’alerte

SIEM → ticket ITSM (GLPI/ServiceNow).

Notification mail DSI/RSSI.

SMS/Teams pour Critique.

Dashboard Grafana dédié.

**6.8. Workflow d’alerting**

Détection → Qualification SOC → Notification ITSM → Assignation → Remédiation → Clôture → Retex

**6.9. Reporting et indicateurs**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence |
| Taux de succès sauvegardes | ≥ 99 % | Quotidien |
| Nombre d’incidents critiques | 0 | Hebdo/Mensuel |
| Temps moyen réaction incidents | < 4 h | Hebdo |
| Latence AKV/HSM | < 50 ms | Quotidien |
| % certificats conformes | 100 % | Hebdo |

Rapports :

Quotidien : synthèse incidents / alertes critiques.

Hebdomadaire : tendance incidents / top alertes.

Mensuel : KPI consolidés pour RSSI et comité SSI.

**6.10. Journalisation et conservation**

Logs Zabbix / Centreon : 12 mois.

Logs SIEM / Elastic : 18 mois.

Logs appliances FortiAnalyzer : 24 mois.

Export régulier en GED pour audit HDS.

Accès journalisé et sécurisé (RBAC + MFA).

# 7. Gestion des sauvegardes et restaurations

Cette section présente la stratégie complète de sauvegarde et de restauration du SI du CHU. Elle détaille les périmètres couverts, les outils utilisés, la fréquence des sauvegardes, les méthodes de validation et les procédures de restauration. L’objectif est de garantir la disponibilité, l’intégrité et la confidentialité des données de santé même en cas d’incident majeur.

**7.1. Principes directeurs**

Garantir la disponibilité et la continuité des soins même après un incident majeur.

Protéger l’intégrité et la confidentialité des données de santé.

Permettre une restauration rapide et fiable pour minimiser l’impact métier.

S’aligner sur les obligations réglementaires (HDS, RGPD, PGSSI-S).

Appliquer la stratégie 3-2-1 : redondance et diversification des supports.

**7.2. Objectifs opérationnels**

Prévenir la perte définitive de données critiques (DPI, labo, pharmacie).

Respecter des RPO/RTO définis avec les métiers.

Garantir des sauvegardes immuables face aux ransomwares.

Supporter le PCA/PRA en cas de sinistre.

Offrir une traçabilité et auditabilité totales des opérations.

**7.3. Périmètre couvert**

|  |  |
| --- | --- |
| Domaine | Contenu sauvegardé |
| Applications cliniques | DPI, RIS/PACS, LIMS, prescription électronique. |
| Applications admin | ERP, RH, finances, logistique. |
| Bases de données | SQL Server, Oracle, PostgreSQL, MySQL. |
| Machines virtuelles | Snapshots VMware. |
| Documents bureautiques | GED RH, contrats, courriers, rapports. |
| Logs & traces | Journaux applicatifs, systèmes, réseau, AKV, HSM. |
| Configurations | Scripts Ansible, PowerShell, fichiers de configuration systèmes. |

**7.4. Orchestration et outils**

Rubrik :

Snapshots immuables.

Sauvegardes multi-sites.

Live Mount pour restauration rapide.

Veeam :

Réplication entre DC1 et DC2.

SureBackup pour tests automatisés.

Restauration granulaire.

Atempo Tina :

Sauvegarde de gros volumes NAS.

Gestion des bandes.

Azure Backup :

Sauvegardes externalisées sur cloud HDS.

Air gap logique contre ransomware.

**7.5. Stratégie de sauvegarde**

**7.5.1. Fréquences**

|  |  |  |
| --- | --- | --- |
| Type de donnée | Type de sauvegarde | Fréquence |
| Critique (DPI, labo) | Incrémentale / Snap | Toutes les 4h |
| Complète VM | Full | Hebdomadaire |
| Administratif | Différentielle | Quotidienne |
| Snapshots hyperviseur | Instantanés | Journalier |

**7.5.2. Plan 3-2-1**

3 copies : prod, PRA, cloud.

2 supports différents : disques, bandes cloud.

1 copie offline : bandes stockées hors réseau.

**7.5.3. Chiffrement**

Données au repos : AES-256.

Données en transit : TLS 1.2/1.3.

Clés gérées dans Azure Key Vault et HSM on-prem.

Rotation annuelle des clés de sauvegarde.

**7.6 Processus de sauvegarde**

**7.6.1. Planification**

Fenêtres horaires définies pour limiter l'impact.

Synchronisation avec les opérations métiers.

Orchestration automatisée (Rubrik/Veeam/Atempo).

**7.6.2. Exécution**

Agents installés sur VMs, bases de données.

Jobs planifiés selon politique RTO/RPO.

Hash SHA-256 vérifié après chaque backup.

Journalisation complète des jobs (logs immuables).

**7.7. Contrôle et validation des sauvegardes**

Vérification quotidienne des jobs :

Statut terminé avec succès.

Hash intégrité validé.

Résultat archivé dans GED.

Tests automatisés :

Veeam SureBackup : boot VM restaurée en bac à sable.

Rubrik Live Mount : restauration instantanée VM ou fichier.

Revue mensuelle en comité SSI :

Taux succès ≥ 99 %.

Analyse des échecs.

Plan d’amélioration.

**7.8. Processus de restauration**

**7.8.1. Étapes formelles**

Ticket ITSM : demande par référent métier.

Qualification : impact, objet précis, point de restauration.

Sélection du backup : point précis validé.

Restauration en préproduction : validation métier.

Passage en production : bascule planifiée.

Tests post-restauration : intégrité, fonctionnalité.

Clôture ticket : documentation et archivage.

**7.8.2. Types de restauration**

Granulaire : fichiers individuels, tables SQL.

VM complète : failover rapide.

Base de données : export/import contrôlé.

Site PRA : bascule orchestrée.

**7.8.3. Scénarios testés**

Perte complète DC1 (PRA activé).

Corruption base DPI.

Restauration fichiers RH sensibles.

Ransomware → restauration immuable.

**7.9. SLA et RTO/RPO définis**

|  |  |  |
| --- | --- | --- |
| Service Critique | RTO | RPO |
| DPI, LIMS, RIS/PACS | ≤ 4 h | ≤ 1 h |
| Administratif/RH | ≤ 8 h | ≤ 4 h |
| Logs / Journaux | ≤ 12 h | ≤ 6 h |

**7.10. Sécurisation et conformité**

Sauvegardes chiffrées AES-256.

Flux chiffrés TLS 1.3.

Accès restreint (RBAC) avec MFA.

Journalisation des actions.

Audit annuel pour HDS et RGPD.

Alignement sur PGSSI-S et guides ANSSI.

**7.11. Journalisation et traçabilité**

Logs Rubrik/Veeam : statut, durée, volume, erreurs.

Archivage dans GED pour 24 mois.

Accès sécurisé, journalisé.

Logs liés restaurations tracés et signés.

Intégration logs SIEM pour corrélation.

**7.12. Indicateurs et reporting**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence |
| Taux succès jobs sauvegarde | ≥ 99 % | Quotidien |
| Temps moyen restauration | ≤ 4 h (critique) | Mensuel |
| Nombre incidents restauration | 0 | Hebdo |
| Volumétrie totale sauvegardée | Suivi croissant | Mensuel |
| % sauvegardes immuables | 100 % sur critiques | Mensuel |

Reporting automatisé : PDF/HTML transmis RSSI/DSI.

Analyse des tendances et anomalies.

# 8. GESTION DU CHIFFREMENT ET DES CLÉS

Cette partie formalise la stratégie de chiffrement des données sensibles, qu’elles soient en transit, au repos ou sur les terminaux. Elle décrit les algorithmes, les méthodes de gestion des clés (HSM, AKV), les procédures de rotation et de révocation, ainsi que les mesures de protection associées pour prévenir toute compromission.

**8.1. Principes directeurs**

Protéger la confidentialité des données sensibles à caractère personnel et médical.

Garantir l’intégrité et l’authenticité des flux d’information.

Limiter l’impact d’un vol de données en les rendant inexploitables sans les clés.

Répondre aux exigences du RGPD, de la certification HDS et de la PGSSI‑S.

Appliquer une gouvernance rigoureuse des clés de chiffrement, incluant leur cycle de vie, leur stockage, et leur usage.

**8.2. Objectifs opérationnels**

Chiffrer les données au repos, en transit et sur les terminaux mobiles.

Sécuriser le stockage et l’accès aux clés de chiffrement.

Assurer une traçabilité totale des accès, modifications et destructions de clés.

Appliquer une rotation régulière des clés de données et certificats.

Permettre une restauration rapide et contrôlée des données chiffrées.

**8.3. Identification des données sensibles à chiffrer**

|  |  |  |  |
| --- | --- | --- | --- |
| Catégorie | Exemples | Sensibilité | Obligation légale |
| Données de santé | Dossier patient, prescriptions, résultats biologiques, imagerie | Très élevée | RGPD, HDS |
| Données RH | Paie, contrats, arrêts, données sociales | Élevée | RGPD |
| Données financières | Facturation, comptabilité, contrats fournisseurs | Moyenne | RGPD, GBCP |
| Logs d’administration | Journaux d’accès, traces de modification, logs d’authentification | Haute | PGSSI-S, CNIL |
| Données cloud et sauvegardes | Snapshots, exports, fichiers .bak, dump base de données | Très élevée | RGPD, HDS |

**8.4. Choix des méthodes et standards de chiffrement**

|  |  |  |  |
| --- | --- | --- | --- |
| Usage | Algorithme recommandé | Mode de chiffrement | Norme utilisée |
| Fichiers et disques | AES-256 | XTS ou CBC | NIST SP 800-38E |
| Bases de données | TDE (Transparent Data Encryption) | AES-256 | FIPS 140-2, ISO/IEC 18033-3 |
| Flux HTTPS | TLS 1.3 ou 1.2 avec PFS | RSA-2048+, ECC (ED25519) | RFC 8446 (TLS 1.3) |
| Sauvegardes | AES-256 + HMAC (intégrité) | Full disk encryption | Rubrik/Veeam/Atempo standards |
| Hachage des mots de passe | Argon2id, bcrypt (≥12) | Salage aléatoire | OWASP, RFC 9106 |
| Tokens API, identifiants | JWT chiffrés avec JWE + AES-256 | JWT + JWS + JWE | RFC 7519, RFC 7516 |

**8.5 Chiffrement des données au repos**

BitLocker (Windows Servers) : activé avec TPM et stockage des clés dans Azure Key Vault.

LUKS (Linux) : chiffré à la création, clé dérivée via PBKDF2.

TDE SQL Server / Oracle : chiffrement base entière avec clés gérées dans AKV.

NAS et SAN : disque auto-chiffrant (SED) et verrouillage à distance.

Rubrik / Veeam / Atempo : sauvegardes chiffrées à l’écriture avec hachage d’intégrité.

**8.6 Chiffrement des données en transit**

Flux internes (LAN/VLAN) :

SFTP pour transferts fichiers sensibles.

LDAPS pour authentification.

TLS 1.3 entre services DPI, RIS/PACS, LIMS.

Flux inter-sites (DC1 ↔ DC2 ↔ Cloud) :

VPN IPsec site-to-site avec chiffrement AES-256-GCM.

ExpressRoute Azure chiffré + Private Link.

Flux applicatifs web (patients, pro de santé) :

HTTPS avec certificats TLS RSA-2048 ou ECC.

Certificats publics Let’s Encrypt ou Sectigo + OCSP.

**8.7 Chiffrement sur les terminaux et supports mobiles**

Ordinateurs portables : BitLocker obligatoire, supervisé par Azure AD.

Clés USB : uniquement modèles chiffrés (IronKey, Kingston Datalocker).

Smartphones / tablettes pro : MDM + chiffrement natif (iOS/Android entreprise).

Interdiction des supports non chiffrés : politique de sécurité physique intégrée à la PSSI.

**8.8. Gestion des clés de chiffrement**

**8.8.1. Infrastructure de gestion**

|  |  |
| --- | --- |
| Composant | Description |
| Azure Key Vault (AKV) | Coffre-fort cloud HDS certifié, API REST sécurisée |
| HSM Thales Luna | Clé maîtresse locale, niveau FIPS 140-2 Level 3 |
| Intégration LDAP/AD | Authentification des accès au KMS |
| SIEM | Audit des actions liées aux clés |

**8.8.2. Cycle de vie des clés**

|  |  |  |
| --- | --- | --- |
| Étape | Fréquence | Validation nécessaire |
| Création | À la demande | Double approbation RSSI + DSI |
| Rotation | Tous les 12 mois | Automatisée via policy AKV |
| Révocation | Dès suspicion ou sortie | RSSI + DPO |
| Destruction | Fin de traitement RGPD | Validation + preuve horodatée |

**8.8.3. Sécurité du stockage**

Clés stockées dans AKV Premium (HSM-Backed).

Aucune exportabilité des clés de chiffrement (usage only).

Backup chiffré des clés HSM stocké offline.

ACL restreintes par rôle : lecture seule, création, gestion.

**8.9. DME chiffrés (Dispositifs médicaux électroniques)**

Les DME (IRM, moniteurs, scanners) connectés au réseau utilisent :

TLS embarqué pour le flux DICOM.

Chiffrement des données locales (SDD chiffré si stockage interne).

Authentification centralisée sur l’AD ou via certificats.

Gestion via VLAN biomédical isolé + firewall + proxy TLS d’inspection (si possible).

Logs d’accès journalisés et injectés dans le SIEM.

**8.10. Solutions de chiffrement utilisées**

|  |  |  |
| --- | --- | --- |
| Validation + preuve horodatée | Usage principal | Fournisseur/Statut |
| BitLocker | Chiffrement disques Windows | Microsoft (natif) |
| LUKS | Chiffrement Linux | Natif GNU/Linux |
| TDE | Chiffrement base SQL | Microsoft / Oracle |
| Azure Key Vault | Gestion des clés cloud | Microsoft (HDS) |
| Thales HSM Luna | Clés locales, certif. HDS / FIPS | Clés locales, certif. HDS / FIPS |
| Rubrik / Veeam | Sauvegardes chiffrées | Logiciel + stockage |
| GPG / PGP | Mails sensibles (RH, juridique) | Interne / MSSanté |
| JWE / JWT | API sécurisées | Dev interne |

**8.11. Sécurité des applications utilisant le chiffrement**

Audit des modules de chiffrement des logiciels métiers.

Contrôle de la génération des clés applicatives (ex. modules web).

Chiffrement natif des bases sensibles (médico-administratives).

Stockage des secrets (DB, token API) dans AKV ou vault local.

**8.12. Bonnes pratiques imposées**

Clé différente par usage (sauvegarde, transit, base, app).

Rotation régulière obligatoire.

Pas de stockage local des clés applicatives.

Aucun mot de passe en clair dans les scripts ou bases.

Évaluation annuelle de la politique de chiffrement par le RSSI.

**8.13. Indicateurs et tableaux de bord**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence |
| Taux de données critiques chiffrées | 100 % | Mensuel |
| Taux de conformité des certificats | 100 % conformes | Hebdo |
| Nombre de clés expirées | 0 | Continu |
| % accès KMS non autorisés | 0 | Instantané |
| Temps de rotation clés critiques | ≤ 24 h (automatisé) | Mensuel |

**8.14. Journalisation et auditabilité**

Journalisation centralisée des accès et modifications de clés.

Logs injectés dans SIEM, corrélés avec l’authentification.

Conservation 18 mois (obligation HDS).

Export horodaté, signé, stocké dans GED sécurisée.

# 9. Gestion des incidents et réponse

Cette section détaille l’organisation, les procédures et les outils mis en œuvre pour détecter, analyser et traiter les incidents de sécurité. Elle décrit les workflows de gestion des alertes, les mécanismes d’escalade, la constitution de la cellule de crise SSI et les obligations réglementaires de notification des violations de données.

**9.1. Principes directeurs**

Assurer une détection rapide, une réponse structurée et une remédiation efficace aux incidents de sécurité.

Minimiser l’impact sur les activités cliniques, administratives et la confidentialité des données.

Respecter les obligations légales de notification (CNIL, ANSSI, ARS).

Tirer parti de chaque incident pour améliorer en continu les capacités de défense et de réponse.

S’appuyer sur une cellule de crise SSI clairement identifiée et entraînée.

**9.2. Objectifs opérationnels**

Détecter les incidents le plus tôt possible (détection proactive).

Qualifier et prioriser les incidents selon leur impact réel.

Réagir avec des procédures prédéfinies et documentées.

Notifier les autorités en respectant les délais réglementaires.

Organiser un retour d’expérience pour capitaliser sur l’événement.

**9.3. Définition d’un incident de sécurité**

Un incident de sécurité est tout événement ayant un impact avéré ou potentiel sur :

La disponibilité (ex. panne, déni de service).

L’intégrité (ex. altération de données, corruption de base).

La confidentialité (ex. fuite de données, accès non autorisé).

La traçabilité (ex. altération de journaux).

La conformité réglementaire (ex. non-respect RGPD, HDS, PGSSI-S).

9.4. Typologie des incidents

|  |  |  |
| --- | --- | --- |
| Type d’incident | Exemple typique | Gravité possible |
| Cyberattaque externe | Ransomware, phishing ciblé, tentative d’intrusion réseau | Critique |
| Erreur humaine | Mauvaise configuration, suppression involontaire | Élevée à critique |
| Défaillance matérielle | Crash SAN, panne VM, perte alimentation datacenter | Élevée |
| Compromission interne | Utilisation frauduleuse de droits légitimes | Critique |
| Défaut de configuration | Mise en ligne d’un service sans filtrage | Modéré à élevé |

9.5. Organisation de la gestion des incidents

a. Équipe de réponse à incident (ERT / CSIRT local)

|  |  |
| --- | --- |
| Rôle | Fonction |
| RSSI | Responsable du traitement global |
| DSI | Superviseur technique et opérationnel |
| SOC/SIEM | Détection, qualification, investigation |
| Admin sécurité | Contention, contre-mesures |
| Référents métiers | Évaluation de l’impact fonctionnel |
| DPO | Notification RGPD, analyse juridique |
| Com DIR / DG | Communication externe et interne |

**9.6. Processus de traitement d’incident**

Étapes structurées :

Détection → via SIEM, IDS/IPS, monitoring, alerte humaine.

Qualification → analyse impact, criticité, nature.

Escalade → activation cellule de crise si niveau ≥ Élevé.

Réaction immédiate → isolement, blocage, containment.

Remédiation → restauration, patch, durcissement.

Notification légale → CNIL (≤ 72h), ANSSI/ARS si nécessaire.

Retour d’expérience (REX) → documentation, analyse, amélioration.

**9.7. Classification des incidents**

|  |  |  |
| --- | --- | --- |
| Niveau | Critères | Exemple |
| Critique | Interruption soins, exfiltration avérée, ransomware | Chiffrement DPI |
| Élevé | Altération de données, fuite mineure | Export fichier RH non sécurisé |
| Modéré | Indisponibilité temporaire ou erreur humaine isolée | Arrêt VM RIS 15 minutes |
| Mineur | Aucune atteinte SI ni données | Échec de login, scan réseau |

**9.8. Mécanismes de détection**

SIEM (ELK) : corrélation logs AD, AKV, serveurs, DPI.

IPS/IDS : blocage ou alerte sur signature ou comportement suspect.

Zabbix / Centreon : indisponibilité d’un service.

FortiAnalyzer : logs de pare-feu, VPN, trafic DNS.

Azure Sentinel : anomalies sur les accès cloud ou clés AKV.

Alerte humaine : via ITSM ou point de contact Sécurité.

**9.9. Journalisation et traçabilité**

Enregistrement systématique dans ITSM.

Conservation des logs SIEM > 18 mois.

Archivage du ticket, des actions, de la chronologie.

Signature numérique des rapports REX.

Logs d’accès aux clés ou fichiers restaurés horodatés.

**9.10. Notification aux autorités**

**CNIL (RGPD)**

Obligation de notifier dans un délai de 72h.

Contenu minimal : type de données, étendue, mesures prises, contact DPO.

**ARS / ANSSI**

En cas d’impact sur la disponibilité des soins ou compromission grave.

Notification via CERT Santé ou formulaire RSSI/DSI.

**9.11 Scénario-type : attaque par ransomware**

|  |  |
| --- | --- |
| Étape | Action |
| Détection | Blocage IPS + alerte SIEM |
| Qualification | Chiffrement détecté sur partages réseau |
| Activation cellule crise | Mise en quarantaine VLAN, communication DSI/RSSI/DG |
| Remédiation | Isolation serveurs, restauration depuis Rubrik (immutables) |
| Notification | CNIL dans les 72h, ARS par le Directeur |
| REX | Documenté, présenté au comité SSI, axes d’amélioration identifiés |

**9.12 Reporting et indicateurs**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence |
| Nombre d’incidents critiques | 0 | Mensuel |
| Temps moyen de détection (MTTD) | < 1 h | Mensuel |
| Temps moyen de réaction (MTTR) | < 4 h | Mensuel |
| % incidents clôturés avec REX | 100 % | Trimestriel |
| Taux de conformité notification RGPD | 100 % ≤ 72 h | En continu |

# 10. Contrôles, audits et conformité

Cette partie expose la stratégie de formation et de sensibilisation déployée pour l’ensemble des agents du CHU. Elle précise les publics cibles, les thématiques abordées, les méthodes pédagogiques et les outils mobilisés pour diffuser une culture SSI solide et homogène au sein de l’établissement.

**10.1. Principes directeurs**

Reconnaître l’humain comme maillon fort ou faible de la cybersécurité.

Favoriser la culture SSI à tous les niveaux : médical, administratif, technique.

Contribuer activement à réduire les risques liés aux erreurs humaines ou à la malveillance.

Répondre aux obligations réglementaires (PGSSI-S, HDS, RGPD).

S’inscrire dans une démarche d’amélioration continue intégrée au SMSI.

**10.2. Objectifs opérationnels**

Diffuser une compréhension claire et adaptée des enjeux de sécurité.

Former les utilisateurs aux gestes essentiels pour protéger les données patientes.

Réduire la surface d’attaque sociale (phishing, ingénierie sociale).

Mettre en place un socle homogène de bonnes pratiques.

Renforcer la capacité de détection et de signalement des incidents.

Répondre aux exigences d’audit HDS et CNIL sur la sensibilisation.

**10.3. Publics cibles et segmentation**

|  |  |  |
| --- | --- | --- |
| Public cible | Besoins spécifiques | Niveau de formation attendu |
| Personnel médical | Confidentialité patient, usage DPI sécurisé | Essentiel, pratique |
| Personnel soignant | Accès limité, hygiène numérique | Essentiel, pratique |
| Personnel administratif | Données RH/finances, email, bureautique | Essentiel, renforcé |
| DSI / Exploitation | Exploitation quotidienne, accès admin | Avancé (technique et organisation) |
| RSSI / Sécurité | Gouvernance, stratégie, techniques avancées | Expert |
| Prestataires | Conformité contrat, accès distants | Essentiel, contractualisé |

**10.4. Thématiques prioritaires de sensibilisation**

Protection des données de santé (secret médical).

Confidentialité des accès utilisateurs et RBAC.

Phishing et ingénierie sociale.

Hygiène des mots de passe et MFA.

Usage des terminaux mobiles et supports amovibles.

Chiffrement et stockage sécurisé.

Règles d’utilisation VPN et accès distants.

Signalement des incidents ou des suspicions.

Respect des politiques internes (PSSI, charte informatique).

Conformité RGPD et droits des patients.

**10.5. Programme de formation structuré**

**a. Formation initiale**

Obligatoire à l’embauche.

Présentation des règles PSSI et charte.

Séance en présentiel ou e-learning certifié.

Questionnaire d’évaluation.

Enregistrement dans le registre RH.

**b. Formation continue**

Séances annuelles obligatoires.

Adaptée par public cible (médical, administratif, technique).

Mise à jour selon menaces émergentes (ex. ransomware, phishing ciblé).

Scénarios pratiques (quiz, mise en situation).

Certificat nominatif conservé en GED.

**c. Sessions spécialisées**

Pour DSI / Exploitation :

Gestion clés / AKV / HSM.

SIEM, analyse logs.

Protocoles de restauration PRA.

**Pour RSSI / Sécurité :**

Analyse de risque EBIOS RM.

Pilotage crise SSI.

Notification CNIL.

**Pour référents métiers :**

Evaluation impact, plan de continuité.

**10.6. Méthodes pédagogiques**

Présentiel : cours, ateliers pratiques.

E-learning : modules interactifs.

Fiches mémos et affiches dans les services.

Campagnes internes (email, intranet).

Exercices de phishing simulé.

Quiz d’évaluation et attestations.

**10.7. Supports et outils**

Plateforme LMS (Learning Management System) avec suivi.

GED sécurisée pour archivage des attestations.

Newsletter cybersécurité mensuelle.

FAQ sécurité sur l’intranet.

Vidéos pédagogiques courtes.

Affiches « 10 bons réflexes » dans les services.

**10.8. Organisation et responsabilités**

|  |  |
| --- | --- |
| Acteur | Rôle |
| RSSI | Définir programme global, valider contenus. |
| DSI | Organiser logistique (salles, LMS). |
| DRH | Intégrer la formation dans le parcours RH. |
| Formateurs internes/externe | Animer les sessions spécialisées. |
| Référents métiers | Relayer les bonnes pratiques dans chaque service. |
| Prestataires | Suivre les formations imposées par contrat. |

**10.9. Suivi et évaluation**

Registre des formations suivies (par agent).

Statistiques de participation (KPI).

Résultats des quiz (validation des acquis).

Rapports mensuels RSSI/DRH.

Contrôle des exceptions (justificatif d’absence, reprogrammation).

**10.10. Indicateurs de performance (KPI)**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence suivi |
| Taux de couverture formation initiale | 100 % du personnel | Mensuel |
| Taux de couverture formation continue | ≥ 95 % | Trimestriel |
| Taux de réussite quiz | ≥ 90 % | Trimestriel |
| Taux de signalement phishing | En hausse | Annuel |
| Nombres incidents dus à erreur humaine | Tendance à la baisse | Annuel |

**10.11. Journalisation et conformité**

Conservation attestations ≥ 5 ans (conformité HDS).

Archivage des supports et programmes en GED.

Accès restreint (RBAC, MFA).

Traçabilité des modifications du programme de formation.

# 11. Formation et sensibilisation opérationnelle

Cette section explique la démarche d’audit et de conformité intégrée au SMSI du CHU. Elle détaille les référentiels suivis, les types d’audits menés, les rôles impliqués et le cycle d’amélioration continue, afin d’assurer la maîtrise des risques et la conformité réglementaire dans la durée.

**11.1. Principes directeurs**

Garantir la conformité réglementaire (HDS, RGPD, PGSSI-S).

Démontrer la maîtrise des risques grâce à des preuves formelles.

Identifier et corriger proactivement les vulnérabilités organisationnelles ou techniques.

Promouvoir une amélioration continue de la maturité SSI.

Maintenir un niveau de confiance élevé vis-à-vis des patients, des autorités et des partenaires.

**11.2. Objectifs opérationnels**

Évaluer régulièrement l’efficacité des mesures SSI mises en œuvre.

Vérifier la conformité aux obligations légales et contractuelles.

Identifier les écarts et dérives potentielles.

Définir des plans d’action correctifs et préventifs.

Alimenter la stratégie globale SSI (Schéma Directeur SI, SMSI).

**11.3. Référentiels de conformité applicables**

|  |  |
| --- | --- |
| Référentiel | Exigences principales |
| PGSSI-S | Gouvernance SSI, protection données santé. |
| HDS (certification) | Politique de sécurité, journalisation, PRA/PCA. |
| RGPD | Protection des données personnelles, droits des patients. |
| RGS/ANSSI | Chiffrement, signature électronique. |
| ISO 27001/27002 | Bonnes pratiques SMSI. |
| Instruction DGOS | Obligations spécifiques établissements de santé. |

**11.4. Typologie des audits réalisés**

**Audits internes**

Pilotés par le RSSI.

Basés sur la PSSI et le SMSI interne.

Fréquence : annuelle, ou à chaque changement majeur.

**Audits externes réglementaires**

HDS : audit annuel de surveillance ou de renouvellement.

RGPD : contrôles CNIL éventuels.

Certifications ANSSI/PGSSI-S.

**Audits techniques**

Tests d’intrusion.

Revue de configuration (firewalls, VPN, KMS).

Analyse des vulnérabilités (scans programmés).

**Audits métiers**

Vérification respect charte informatique.

Analyse des droits RBAC dans le DPI.

Évaluation des PRA/PCA par les métiers.

**11.5. Gouvernance des audits**

|  |  |
| --- | --- |
| Acteur | Rôle |
| RSSI | Planification, cadrage, pilotage global. |
| DSI | Support technique, fourniture des accès et informations. |
| Equipe exploitation | Exécution des mesures correctives techniques. |
| Admin sécurité | Fourniture des configurations sécurité. |
| Référents métiers | Validation des périmètres et des plans d’action. |
| DPO | Suivi des volets RGPD et des droits des patients. |
| Direction général | Validation des plans stratégiques et budgétaires liés SSI. |

**11.6. Planification et cycle d’audit**

Élaboration d’un plan d’audit annuel validé en comité SSI.

Prise en compte :

Risques métier.

Incidents passés.

Changements SI (nouveaux logiciels, infrastructure).

Suivi dans le SMSI et dans l’outil ITSM (planification, ticketing).

Reporting trimestriel au comité SSI.

Plan annuel d’audit :

|  |  |  |
| --- | --- | --- |
| Période | Audit | Responsable |
| T1 | Audit interne PSSI | RSSI |
| T2 | Test d’intrusion externe | Prestataire |
| T2 | Vérification PRA/PCA | DSI, RSSI |
| T3 | Audit droits DPI | Référents métiers |
| T4 | Audit HDS (certification) | Auditeur externe |

**11.7. Méthodologie d’audit interne**

Cadrage et périmètre (contexte, objectifs, référentiels).

Analyse documentaire (PSSI, PRA/PCA, runbooks, logs).

Entretiens (RSSI, DSI, métiers).

Tests techniques (scans vulnérabilités, revue des logs SIEM).

Rédaction du rapport d’audit avec constats, non-conformités, recommandations.

Validation en comité opérationnel SSI.

Suivi des plans d’action avec responsables identifiés et échéances.

**11.8. Journalisation et traçabilité des audits**

Conservation des rapports ≥ 5 ans (conformité HDS).

Archivage sécurisé dans la GED avec droits RBAC.

Traçabilité des accès aux rapports (logs).

Intégration des recommandations dans le plan directeur SI.

Suivi des plans d’action dans ITSM (workflow dédié).

**11.9 Reporting et communication**

**Rapports d’audit détaillés :**

Objectifs et périmètre.

Constats, écarts.

Analyse des causes racines.

Plan d’action et priorisation.

**Diffusion contrôlée :**

RSSI / DSI.

Direction générale.

Référents métiers concernés.

Comité SSI pour validation globale.

**Présentation synthétique trimestrielle :**

KPI SSI consolidés.

Suivi des plans d’action.

État des risques résiduels.

**11.10 Indicateurs de performance (KPI)**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence suivi |
| Taux de couverture audits planifiés | 100 % | Annuel |
| Taux de conformité PSSI | ≥ 95 % | Annuel |
| Nombre d’écarts critiques ouverts | 0 | Trimestriel |
| Temps moyen de clôture des écarts majeurs | < 60 j | Trimestriel |
| Taux d’avancement plan d’action SSI | ≥ 90 % | Trimestriel |

**11.11. Amélioration continue**

**Boucle d’amélioration intégrée au SMSI :**

Analyse des incidents et REX.

Intégration des recommandations d’audit.

Mise à jour de la PSSI, procédures PRA/PCA, formations.

Suivi des indicateurs et des tendances.

Capitalisation dans les comités SSI pour pilotage stratégique.

**Implication des métiers :**

Sensibilisation spécifique sur les écarts détectés.

Validation des actions correctives.

Révision des processus métier impactés.

# 12. Amélioration continue et retours d’expérience

Cette partie présente le corpus documentaire de sécurité de l’établissement : PSSI, chartes utilisateurs et administrateurs, procédures opérationnelles, runbooks, matrices d’accès et configurations. Elle précise les règles de gestion documentaire, de validation et de conservation pour garantir une base fiable, à jour et auditée.

**12.1. Principes directeurs**

Assurer la cohérence et la standardisation des pratiques SSI.

Garantir la traçabilité des règles, processus et configurations.

Faciliter l’appropriation des consignes par tous les acteurs.

Répondre aux exigences de conformité réglementaire (HDS, RGPD, PGSSI-S).

Soutenir la transparence et la réversibilité des opérations SI.

**12.2. Objectifs opérationnels**

Formaliser les règles de sécurité applicables à tous les utilisateurs et prestataires.

Fournir des référentiels clairs pour l’administration technique.

Documenter les processus critiques (sauvegardes, restauration, gestion des incidents).

Permettre la formation et la sensibilisation des équipes.

Offrir une base pour les audits internes et externes.

**12.3. Politique de Sécurité des Systèmes d’Information (PSSI)**

Document cadre validé par la Direction.

Décline la stratégie SSI en objectifs, principes et règles.

Inclut :

Gouvernance SSI.

Analyse des risques.

Plan de sauvegarde et PRA/PCA.

Politique de gestion des accès.

Politique de gestion des incidents.

Politique de chiffrement.

Révision annuelle ou après tout événement majeur.

**12.4. Chartes utilisateurs et administrateurs**

**Charte Informatique Utilisateur**

Obligatoire à l’embauche.

Décrit les droits et devoirs.

Signée et archivée RH.

Inclut règles d’usage Internet, messagerie, supports amovibles.

**Charte Administrateur**

Obligations renforcées.

Accès restreint, journalisation des actions.

Principe de séparation des pouvoirs (SoD).

MFA obligatoire pour toutes consoles.

**12.5. Procédures opérationnelles formalisées**

|  |  |
| --- | --- |
| Domaine | Procédures associées |
| Sauvegarde | Plan de sauvegarde détaillé, runbooks Veeam/Rubrik/Atempo. |
| Restauration | Procédure ITSM, validation métier, test de conformité. |
| Gestion des incidents | Workflow ITSM, escalade cellule crise, notification CNIL. |
| PRA/PCA | Scénarios testés, déclenchement, bascule DC2, retour à la normale. |
| Gestion des accès | Demande, validation, provisioning, revue périodique. |
| Rotation des clés | Planification annuelle, validation double opérateur. |
| Mise en production | Validation pré-prod, plan de rollback, journalisation. |
| Patch management | Qualification, test, déploiement automatisé. |

Stockées dans GED sécurisée avec versioning.

**12.6. Documentation technique**

**Cartographies réseau et applicative :**

VLAN, firewalls, IPS/IDS.

Flux applicatifs internes et externes (MSSanté, DMP, Apicrypt).

Diagrammes PRA/PCA.

**Inventaire technique :**

Serveurs physiques et virtuels.

Bases de données et versions.

Équipements réseau et firmware.

**Configurations sauvegardées :**

Playbooks Ansible / PowerShell.

Fichiers de configuration (firewalls, VPN, AKV policies).

Export chiffré des configurations HSM.

**12.7. Documentation des accès et des droits**

**Matrice des habilitations :**

RBAC métier (DPI, RIS/PACS, LIMS).

Administrateurs systèmes et réseaux.

Accès prestataires (justification contractuelle).

**Journalisation des demandes :**

Ticket ITSM avec validation hiérarchique.

Archivage dans GED.

**Revue semestrielle des droits :**

Extraction des accès.

Revue conjointe RSSI/DSI/Référents métiers.

Ajustement immédiat des écarts détectés.

12.8. Gestion documentaire et versioning

**GED Sécurisée (SharePoint / Nextcloud HDS) :**

Contrôle des accès par rôle.

MFA obligatoire.

Logs d’accès et modifications.

Sauvegarde automatique quotidienne.

**Versioning systématique :**

Numérotation major.minor (ex. PSSI v1.2).

Historique des évolutions.

Archivage des versions obsolètes pour audit.

**Cycle de validation :**

Rédaction → Relecture → Validation RSSI/DSI → Publication.

Signature numérique possible des documents critiques.

**12.9. Formation et sensibilisation documentaire**

Intégration des chartes dans le parcours RH.

Accès libre aux documents dans l’intranet sécurisé.

Intégration dans la plateforme LMS pour e-learning.

Quiz et attestations nominatives conservées en GED.

Campagnes annuelles sur la mise à jour des politiques (PSSI, charte).

**12.10. Conformité réglementaire**

Alignement sur :

PGSSI-S : plan et politique de sécurité structurés.

HDS : documentation des procédures, PRA/PCA validés.

RGPD : registres d’accès, journalisation, notification des violations.

ANSSI : recommandations cryptographiques, cycle de vie des clés.

**Auditabilité :**

Preuves formelles stockées ≥ 5 ans.

Accessibilité aux auditeurs HDS ou CNIL.

Intégration dans le SMSI institutionnel.

**12.11 Indicateurs et KPI**

|  |  |  |
| --- | --- | --- |
| Indicateur | Objectif | Fréquence suivi |
| Taux de couverture chartes signées | 100 % | Mensuel |
| % procédures formalisées à jour | ≥ 95 % | Trimestriel |
| Nombre de révisions documentaires annuelles | ≥ 1 par document | Annuel |
| Taux de disponibilité GED | ≥ 99,9 % | Mensuel |
| Nombre d’accès non autorisés détectés | 0 | Continu |

**12.12. Journalisation et conservation**

Logs d’accès aux documents critiques conservés ≥ 24 mois.

Archivage automatique GED sécurisé avec backup chiffré.

Contrôle RBAC détaillé (lecture, écriture, suppression).

Notifications d’accès sensible au RSSI.