LOUIS70 CONSEIL

Sécurité • Stratégie • Discrétion

RAPPORT D'AUDIT ORGANISATIONNEL

Sécurité des Systèmes d'Information

Client :

EHPAD Les Tilleuls — Établissement fictif à des fins de démonstration

Commune de Beaumont-sur-Vingeanne (21), 48 résidents

Référence mission : L70C-2026-EHPAD-001

Date : avril 2026

Classification : CONFIDENTIEL — Diffusion restreinte

Sommaire

1. Contexte et objectifs de la mission

1.1 Contexte

L'EHPAD Les Tilleuls est un établissement médico-social accueillant 48 résidents permanents. Il emploie 32 personnes (soignants, administratifs, direction) et dispose d'un système d'information constitué de postes bureautiques, d'un logiciel métier de gestion des soins (Osiris Care), d'une connexion Internet partagée et d'équipements de téléphonie fixe.

La direction a sollicité LOUIS70 CONSEIL dans le cadre d'une démarche volontaire de mise en conformité, consécutive à plusieurs incidents mineurs (tentatives de phishing, perte de matériel) et à la montée en charge des obligations réglementaires applicables aux établissements de santé (RGPD, référentiel HDS, circulaire ANSSI).

1.2 Objectifs

- Évaluer le niveau de maturité SSI de l'établissement
- Identifier les vulnérabilités organisationnelles et techniques prioritaires
- Formuler des recommandations adaptées au contexte et aux moyens de la structure
- Proposer un plan d'action hiérarchisé et réaliste

2. Méthodologie

La mission s'est déroulée sur deux jours en présentiel, complétés par une phase d'analyse documentaire à distance. Elle a mobilisé les approches suivantes :

Entretiens

Entretiens semi-directifs conduits avec la directrice, la responsable administrative, l'infirmière coordinatrice et le prestataire informatique externe. Ces entretiens ont permis de recueillir la perception des risques, les pratiques réelles et les points de tension organisationnels.

Revue documentaire

Analyse des documents existants : contrat de maintenance informatique, charte utilisateur (absente), registre des traitements RGPD (partiel), inventaire matériel (incomplet), procédures métier.

Observation terrain

Visite des locaux techniques, observation des postes de travail, vérification de la signalétique et des accès physiques aux équipements sensibles.

Référentiels appliqués

- Guide d'hygiène informatique ANSSI (42 mesures)
- Référentiel de sécurité des données de santé (HDS)
- RGPD — Règlement (UE) 2016/679
- ISO/IEC 27001:2022 (lecture de maturité)

3. Périmètre audité

Domaine	Éléments couverts	Inclus
Gouvernance SSI	Politique, responsabilités, sensibilisation	**Oui**
Gestion des accès	Comptes utilisateurs, mots de passe, droits	**Oui**
Postes de travail	10 postes Windows, 2 tablettes	**Oui**
Réseau et télécom	Box opérateur, switches, Wi-Fi	**Oui**
Logiciel métier	Osiris Care — données de soins	**Oui**
Sauvegardes	Politique et tests de restauration	**Oui**
Sécurité physique	Accès locaux techniques, serveurs	**Oui**
Tests d'intrusion	Audit technique offensif	**Non (hors périmètre)**

4. Cartographie des actifs IT et obsolescence

4.1 Cartographie par criticité métier

Préalablement à tout audit de sécurité, l'identification des actifs IT selon leur criticité pour la continuité des soins est indispensable. Cette cartographie classe les systèmes en trois niveaux : vitaux (arrêt immédiatement préjudiciable aux résidents), fonctionnels (dégradation de l'activité sans risque direct) et périphériques (impact administratif uniquement).

Niveau	Système / Service	Usage critique	État observé
VITAL	**Logiciel métier Osiris Care**	Dossier résident, prescriptions, traçabilité soins	Obsolète — v2019, non maintenu
VITAL	**Messagerie sécurisée (MSSanté)**	Échanges avec médecins, hôpitaux, pharmacie	Absente — usage messagerie grand public
VITAL	**Réseau local (LAN)**	Interconnexion postes, NAS, imprimantes soins	Switch non managé, firmware inconnu
FONCTIONNEL	**Messagerie interne**	Communication inter-services	Gmail partagé non chiffré
FONCTIONNEL	**Bureautique (Word, Excel)**	Plannings, courriers, tableaux de bord	Office 2016 — hors support étendu
FONCTIONNEL	**Numérisation documents**	Résultats examens, ordonnances entrants	Scanner isolé, pas d'archivage structuré
ÉMERGENT	**IA lecture résultats examens**	Aide interprétation bilans biologiques	Non déployé — à évaluer
ÉMERGENT	**Télémédecine / téléconsultation**	Suivi médical à distance	Usage ad hoc, non sécurisé
PÉRIPHÉRIQUE	**Site internet établissement**	Information familles	Statique, non critique

4.2 Diagnostic d'obsolescence

L'inventaire réalisé révèle un parc informatique vieillissant, caractéristique d'établissements dont les cycles de renouvellement sont contraints par les budgets médico-sociaux. L'obsolescence n'est pas seulement un problème de performance — elle constitue un vecteur de vulnérabilité majeur, les équipements hors support ne recevant plus de correctifs de sécurité.

Équipement / Logiciel	Version / Âge	Support	Risque	Urgence
Windows 10 (8 postes)	21H2 — 3 ans	Fin oct. 2025	CRITIQUE	Immédiate
Windows 7 (2 postes)	EOL 2020	Terminé	CRITIQUE	Immédiate
Osiris Care	v2019 — 7 ans	Arrêté éditeur	ÉLEVÉ	< 6 mois
Office 2016	10 ans	Support étendu terminé	ÉLEVÉ	< 6 mois
Switch réseau	Firmware 2018	Inconnu	ÉLEVÉ	< 6 mois
NAS Synology	DSM 6.x	Fin support 2024	MODÉRÉ	< 12 mois
Tablettes Android	Android 9	Hors support Google	MODÉRÉ	< 12 mois

Deux postes sous Windows 7 (EOL depuis janvier 2020) sont encore en production active. Ils hébergent des accès au logiciel métier. Ce constat, à lui seul, justifie une intervention d'urgence indépendamment des autres résultats de l'audit.

4.3 Plan de migration et continuité de service

La migration d'un parc obsolète en environnement médico-social impose une contrainte absolue : la continuité des soins ne peut être interrompue. Tout arrêt de l'accès au dossier résident ou au module de prescription est un événement à risque patient. Le plan de migration doit donc être séquencé, testé et réversible.

Principes directeurs

- Priorité aux systèmes vitaux (dossier résident, prescriptions) — migration en premier avec double fonctionnement en parallèle
- Aucune bascule sans test de restauration validé sur l'environnement cible
- Fenêtres de migration hors plages de soins (nuit, week-end)
- Plan de retour arrière (rollback) documenté pour chaque étape
- Formation du personnel avant bascule, pas après

Séquencement proposé

Phase	Horizon	Actions	Condition de bascule
P0 — Urgence	Immédiat	Isolation des 2 postes Windows 7 du réseau soins. Déploiement postes de remplacement temporaires sous Windows 11.	*Validation prestataire + direction*
P1 — Réseau	M+1 à M+2	Remplacement switch. Segmentation VLAN soins / admin / Wi-Fi résidents. Mise à jour firmware.	*Tests de connectivité validés sur tous segments*
P2 — Logiciel métier	M+2 à M+4	Migration Osiris Care vers version actuelle ou remplacement (NetSoins, Titan). Migration données. Formation personnel.	*Double fonctionnement 4 semaines + test restauration*
P3 — Bureautique	M+3 à M+6	Migration Office 2016 vers Microsoft 365 ou LibreOffice. Déploiement messagerie MSSanté.	*Formation + validation par utilisateurs référents*
P4 — Émergents	M+6 à M+12	Évaluation solutions IA lecture examens. Encadrement télémédecine. Mise en conformité HDS si hébergement données de santé.	*Analyse coût/bénéfice + avis DPD*

Note sur les services émergents : l'introduction d'outils d'IA (lecture automatisée de résultats biologiques, aide à la prescription) dans un établissement médico-social est soumise aux exigences du règlement européen sur l'IA (AI Act), qui classe ces systèmes en risque élevé. Leur déploiement impose une évaluation de conformité préalable et une supervision médicale maintenue.

5. Constats et analyse des risques

5.1 Gouvernance et organisation

Aucune politique de sécurité formalisée n'existe au sein de l'établissement. La sécurité informatique est assurée de facto par le prestataire externe, sans mandat ni feuille de route SSI. Aucun référent interne n'est désigné. La direction identifie le risque informatique comme existant mais ne dispose pas d'outils pour l'évaluer ou le prioriser.

Constat notable : la charte informatique destinée aux utilisateurs n'a jamais été rédigée ni signée. Les personnels soignants utilisent des équipements numériques sans cadre formel d'usage.

5.2 Gestion des accès et authentification

L'audit révèle des pratiques d'authentification insuffisantes. Les mots de passe observés sont courts, non complexes, partagés entre collègues dans plusieurs cas, et jamais renouvelés. Le compte administrateur local du logiciel métier utilise un mot de passe constructeur non modifié depuis l'installation.

Aucun mécanisme d'authentification multifacteur (MFA) n'est déployé, y compris pour les accès à distance du prestataire informatique.

5.3 Sauvegardes et continuité

Une sauvegarde automatique nocturne est en place sur un NAS local. Cependant, aucune sauvegarde externalisée n'existe. Le NAS est situé dans la même salle que les équipements principaux, sans protection incendie spécifique. Aucun test de restauration n'a été réalisé depuis la mise en place du dispositif (18 mois).

En cas de sinistre (incendie, inondation, ransomware), la perte totale des données est un scénario réaliste dans l'état actuel.

5.4 Facteur humain, sensibilisation et gestion de la confiance

Le facteur humain constitue statistiquement le premier vecteur de compromission des systèmes d'information, devant les vulnérabilités techniques. Dans un environnement médico-social, ce risque est amplifié par plusieurs caractéristiques structurelles : turnover élevé du personnel soignant, présence régulière d'intervenants extérieurs (prestataires, bénévoles, familles, stagiaires), culture professionnelle fondée sur la confiance et l'entraide, et charge de travail incompatible avec une vigilance informatique soutenue. Aucune action de sensibilisation aux risques numériques n'a été conduite auprès du personnel. Les tentatives de phishing reçues ces derniers mois n'ont pas donné lieu à une procédure de signalement formalisée.

Ingénierie sociale et abus de confiance

L'ingénierie sociale exploite précisément les ressorts humains qui font la qualité d'un établissement de soins : bienveillance, disponibilité, sens du service. Un appel téléphonique d'un prétendu technicien demandant un accès à distance, un mail imitant la direction de l'ARS ou du médecin coordonnateur, une clé USB abandonnée dans le parking -- ces vecteurs d'attaque ne nécessitent aucune compétence technique de la part de l'attaquant.

Constat : aucune procédure de vérification d'identité n'est en place pour les demandes d'accès téléphoniques ou à distance. Le personnel interrogé a spontanément indiqué qu'il fournirait volontiers son mot de passe à quelqu'un se présentant comme le support informatique.

Gestion différenciée des droits d'accès — principe du besoin d'en connaître

L'établissement n'applique pas de différenciation des droits d'accès selon les fonctions. Tous les personnels disposent d'un accès identique au logiciel métier, y compris aux données de résidents dont ils n'ont pas la charge. Cette absence de cloisonnement expose l'établissement sur deux plans : risque de fuite de données (RGPD) et risque d'accès malveillant ou involontaire à des dossiers sensibles.

Dans l'esprit du principe militaire du besoin d'en connaître, chaque utilisateur ne devrait accéder qu'aux données strictement nécessaires à l'exercice de ses fonctions. Ce principe, formalisé dans les référentiels SSI sous le terme de moindre privilège, est applicable et nécessaire dans tout système hébergeant des données de santé.

Gestion des entrées et sorties du personnel

Aucune procédure formalisée n'existe pour la création et la suppression des comptes utilisateurs lors des arrivées et départs de personnel. L'audit a identifié trois comptes actifs correspondant à des agents ayant quitté l'établissement depuis plus de six mois. Ces comptes constituent des portes d'entrée potentielles, notamment si les anciens titulaires conservent connaissance des mots de passe.

5.5 Journalisation, traçabilité et détection

La journalisation des actions sur les systèmes d'information est le dispositif qui permet, après incident, de reconstituer ce qui s'est passé -- et qui permet, en temps réel, de détecter des comportements anormaux. Son absence ne prévient pas les incidents mais les rend invisibles jusqu'à ce qu'il soit trop tard.

État des lieux

Aucune journalisation centralisée n'est en place. Le logiciel métier Osiris Care dispose d'un journal interne non consulté. Les équipements réseau (switch, box opérateur) ne sont pas configurés pour conserver les logs de connexion. Les accès distants du prestataire ne sont pas tracés. En cas d'incident -- fuite de données, accès non autorisé, action malveillante interne -- il est aujourd'hui impossible de reconstituer la séquence des événements.

Cas concret : si un dossier résident était consulté ou modifié de manière inappropriée, l'établissement serait dans l'incapacité de le prouver, de l'identifier ou de le contester. Cette situation est incompatible avec les obligations de l'article 32 du RGPD et engage la responsabilité de la direction.

Ce que la journalisation doit couvrir

- Authentifications réussies et échouées sur tous les systèmes (postes, logiciel métier, accès distants)
- Accès aux dossiers résidents : qui a consulté quoi et quand
- Actions administratives : création, modification, suppression de comptes
- Connexions entrantes du prestataire : horodatage, durée, actions effectuées
- Alertes sur comportements anormaux : connexions hors horaires, volumes de données inhabituels, tentatives d'accès refusées répétées

La mise en place d'une journalisation minimale ne nécessite pas d'investissement lourd. Elle repose sur une configuration adaptée des outils existants et d'un processus de revue mensuelle par le référent SSI désigné.

5.6 Sécurité physique

Le local technique hébergeant le serveur et le NAS est accessible sans contrôle d'accès spécifique. La clé est partagée avec le local de ménage. Aucune traçabilité des accès n'existe. Le Wi-Fi de l'établissement diffuse un réseau unique pour le personnel, les équipements médicaux connectés et les résidents.

6. Synthèse des vulnérabilités

Domaine	Constat principal	Niveau	Priorité
Gouvernance	Absence de politique SSI et de référent interne	**CRITIQUE**	**P1**
Authentification	Mots de passe faibles, partagés, non renouvelés	**CRITIQUE**	**P1**
Sauvegardes	Pas de sauvegarde externalisée, aucun test de restauration	**ÉLEVÉ**	**P1**
Facteur humain	Ingénierie sociale non couverte, comptes orphelins actifs, droits non différenciés	**ÉLEVÉ**	**P1**
Journalisation	Aucune traçabilité des accès et actions — incident non détectable	**ÉLEVÉ**	**P2**
Accès distants	Accès prestataire sans MFA ni traçabilité	**ÉLEVÉ**	**P2**
Sensibilisation	Aucune formation, pas de procédure de signalement	**ÉLEVÉ**	**P2**
Sécurité physique	Local technique non sécurisé, réseau Wi-Fi non segmenté	**MODÉRÉ**	**P2**
Conformité RGPD	Registre des traitements incomplet, DPD non désigné	**MODÉRÉ**	**P3**

7. Plan de recommandations

Priorité 1 — Actions immédiates (0 à 3 mois)

R1 — Désigner un référent SSI interne

Désigner un membre de l'encadrement comme référent SSI, chargé du suivi des incidents, de la relation avec le prestataire et de la mise en oeuvre du plan d'action. Rédiger une fiche de mission formelle.

R2 — Réinitialiser et sécuriser tous les mots de passe

Procéder à la réinitialisation immédiate de l'ensemble des mots de passe, en imposant des critères de complexité (12 caractères minimum, majuscules, chiffres, caractères spéciaux). Mettre en place un gestionnaire de mots de passe. Modifier sans délai le mot de passe constructeur du logiciel métier.

R3 — Mettre en place une sauvegarde externalisée

Déployer une solution de sauvegarde externalisée chiffrée (cloud souverain ou site distant). Programmer des tests de restauration trimestriels et en documenter les résultats.

R4 — Auditer et purger les comptes utilisateurs

Effectuer immédiatement un inventaire exhaustif des comptes actifs sur l'ensemble des systèmes (postes, logiciel métier, accès réseau). Désactiver sans délai tous les comptes orphelins (personnel parti). Mettre en place une procédure d'offboarding formalisée : à chaque départ, suppression des accès le jour même, restitution du matériel, modification des mots de passe partagés le cas échéant.

R5 — Différencier les droits d'accès par fonction

Appliquer le principe de moindre privilège : chaque utilisateur n'accède qu'aux données nécessaires à ses fonctions. Dans le logiciel métier, créer des profils distincts (soignant, administratif, direction, prestataire). Réviser les droits trimestriellement. Cette mesure réduit l'exposition en cas de compromission d'un compte et protège l'établissement en cas de litige RGPD.

Priorité 2 — Actions à court terme (3 à 6 mois)

R6 — Mettre en place une journalisation centralisée minimale

Configurer la journalisation des authentifications et accès sur le logiciel métier, les postes administrateur et les équipements réseau. Mettre en place un tableau de bord mensuel de revue des logs par le référent SSI. Conserver les journaux 12 mois minimum. Paramétrer des alertes sur les événements critiques : connexions hors horaires, tentatives d'authentification échouées répétées, accès distants non planifiés.

R7 — Former le personnel à la détection de l'ingénierie sociale

Conduire un exercice de simulation de phishing ciblé, suivi d'un débriefing collectif non culpabilisant. Définir et afficher une procédure de signalement claire : que faire quand on reçoit un mail suspect, quand un inconnu demande un accès, quand un comportement informatique est inhabituel. Nommer un point de contact interne (le référent SSI) pour tout signalement.

R8 — Rédiger et diffuser la charte informatique

Rédiger une charte d'utilisation des outils numériques, adaptée au contexte médico-social. La faire signer par l'ensemble du personnel. L'intégrer au livret d'accueil des nouveaux arrivants.

R9 — Sécuriser le local technique et contrôler les accès physiques

Équiper le local technique d'une serrure dédiée, distincte du local de ménage. Tenir un registre des accès (qui entre, quand, pourquoi). Installer un extincteur adapté aux équipements électroniques. Envisager une alarme intrusion sur ce local. Ces mesures de base protègent l'intégrité physique des équipements critiques.

R10 — Segmenter le réseau Wi-Fi

Créer des réseaux Wi-Fi distincts pour le personnel, les équipements médicaux connectés et les résidents/visiteurs. Cette segmentation limite la propagation d'un incident d'un segment à l'autre.

R11 — Sécuriser les accès distants du prestataire

Imposer l'authentification multifacteur pour tous les accès distants à distance. Mettre en place un journal de traçabilité des interventions. Formaliser les plages horaires d'accès autorisées.

Priorité 3 — Actions à moyen terme (6 à 12 mois)

R12 — Compléter la mise en conformité RGPD

Finaliser le registre des activités de traitement. Désigner un Délégué à la Protection des Données (DPD), éventuellement mutualisé avec d'autres EHPAD du territoire. Mettre à jour les mentions d'information.

R13 — Conduire une action de sensibilisation annuelle

Organiser annuellement une séance de sensibilisation aux risques numériques pour l'ensemble du personnel : phishing, gestion des mots de passe, comportements en cas d'incident. Format court (1h), adapté au personnel soignant.

8. Conclusion

L'EHPAD Les Tilleuls présente un niveau de maturité SSI faible, caractéristique d'établissements médico-sociaux de taille modeste qui n'ont pas encore engagé de démarche structurée. Les risques identifiés sont réels et documentés — en particulier le risque ransomware, qui a touché plusieurs établissements similaires ces dernières années avec des conséquences opérationnelles sévères.

Les recommandations formulées sont volontairement pragmatiques et calibrées à la réalité d'une structure de 32 agents. Elles ne supposent pas d'investissements lourds mais une organisation, une méthode et une volonté de la direction. La mise en oeuvre des actions de priorité 1 est réalisable en moins de trois mois avec l'appui du prestataire existant.

LOUIS70 CONSEIL reste disponible pour accompagner la mise en oeuvre de ce plan d'action, former le référent SSI désigné ou conduire un audit de suivi à l'issue de la première phase.

Intervenir avec méthode. Décider avec lucidité. Agir avec discrétion.

Louis BONJEAN — LOUIS70 CONSEIL
contact@louis70conseil.fr | +33 6 89 17 57 62 | louis70conseil.fr
27 route de Souhières — 70270 Mélisey