MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

Direction générale
de l'offre de soins

Les mesures prioritaires de sécurité des systèmes d'information

Référentiel à destination des établissements de santé

OCTOBRE 2022

Le référentiel de mesures prioritaires de sécurité des systèmes d'information (MPR) à destination de l'ensemble des établissements de santé (ES) a été élaboré collégialement avec l'atelier SSI (sécurité des systèmes d'information), dans le cadre de la composition du référentiel MATURIN'H, et avec le club RSSI (responsables SSI) des établissements de santé.

Ces mesures sont considérées comme prioritaires par le SHFDS, la DGOS, la DNS et les RSSI des ES, en raison du poids des menaces actuelles – cybercriminalité, actes de malveillance multiformes -.

Ces mesures constituent un retour d'expérience suite à l'observation systématisée des cyberattaques et incidents de sécurité, en particulier de type rançongiciel, survenus entre 2019 et 2022.

Les mesures présentées ci-après constituent un socle de sécurité minimal repris dans la plupart des référentiels applicables (Directive NIS destinée aux opérateurs de services essentiels OSE, Instruction 309, PSSI-MCAS, ISO/CEI 27001:2013,…)[1] qui permettent d'améliorer significativement la sécurité des systèmes d'information.

Elles contribuent également au pilotage : le suivi régulier de leur degré d'application concourt à une meilleure gouvernance à l'échelle hospitalière, régionale et nationale, permettant à tous d'améliorer la maturité SSI du système de santé.

Le recueil des mesures est réalisé de manière déclarative au travers du questionnaire défini dans le volet OPSSIES de la plateforme OSIS V2[2].

La première partie du présent document introduit les mesures prioritaires applicables aux établissements de santé, la seconde les modalités de leur contrôle.

[1] Voir glossaire des référentiels

[2] OPSSIES : l'observatoire permanent de la maturité SSI des établissements sera l'outil de déclaration de conformité des ES aux différentes mesures.

Sommaire

1 GOUVERNANCE DES ETABLISSEMENTS DE SANTE

1.1 Management et cartographie des risques

Prise en compte des risques cyber dans la cartographie des risques de l'établissement. Cartographie des risques à mettre à jour en fonction de l'évolution des métiers de la structure et du niveau de maturité en sécurité numérique.

Identifiant	Libellé de la mesure
1	L'établissement dispose d'une cartographie des risques liés aux services numériques actualisée annuellement basée sur une méthodologie qui permette de comparer les résultats d'une itération à l'autre.
2	La cartographie des risques liés aux services numériques est consolidée dans une cartographie globale des risques[3] portant sur l'établissement.
3	Une analyse de risque, validée par les responsables métiers des services concernés, est réalisée lors de l'introduction d'un nouveau service numérique (application, matériel IT, équipement biomédical et technique, GTB/GTC) .
4	Le plan d'action associé à l'analyse de risque est suivi et priorisé.
5	Le principe de la réalisation d'une analyse de risques numériques est accepté par la Direction (acceptation des risques résiduels).

1.2 RSSI / conseiller sécurité numérique

Le directeur de l'établissement, en tant qu'AQSSI[4], doit s'appuyer sur un responsable de la sécurité des systèmes d'information (RSSI), formé à cet effet, qui rend compte semestriellement à la gouvernance de l'établissement de :

- l'évolution des risques cyber
- des avancées dans la conformité des actions vis-à-vis de la stratégie de l'établissement.

Cette fonction peut être mutualisée (par exemple au niveau du GHT) voire externalisée.

Identifiant	Libellé de la mesure
6	Une personne en charge de la fonction sécurité du système d'Information (SSI) ou RSSI est nommée au sein de l'établissement.
7	La personne prenant en charge la sécurité des systèmes d'information ou RSSI a au moins un rendez-vous semestriel formel avec le Directeur Général de l'établissement.
8	Le rendez-vous a minima semestriel formel avec le Directeur Général de l'établissement donne lieu à un compte rendu (document de preuve).

[3] La cartographie globale des risques : Intégrer les risques numériques aux risques métiers en reconnaissant le risque numérique comme impactant la gestion des ES

[4] L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI)

1.3 Budget sécurité numérique

Les mesures ci-dessous sont de nature à sensibiliser les établissements sur le volet budgétaire et constituent une première étape de la construction de celui-ci.

Identifiant	Libellé de la mesure
9	L'établissement calcule la part, en %, du budget global annuel de l'établissement consacrée au SI selon la méthodologie de l'enquête "charges et ressources" de la DGOS
10	L'établissement calcule annuellement le ratio budget SI rapporté au poste de travail.

2 DIAGNOSTIC SSI

2.1 Inventaire complet des matériels / cartographie applicative

Il est demandé aux établissements d'élaborer et de tenir à jour un inventaire complet des matériels et de réaliser une cartographie applicative. Ces documents ainsi validés constitueront le référentiel pour définir l'ordre de remise à disposition des applications aux métiers, notamment en cas de crise et aideront aussi le RSSI dans son analyse de risques et les équipes opérationnelles dans la sécurisation du SI. Ils doivent également permettre de lister l'ensemble des connexions réseaux avec les partenaires et plus largement l'ensemble des accès externes.

Identifiant	Libellé de la mesure
11	Un inventaire des matériels et logiciels (matériel: postes de travail, serveurs, machines virtuelles, équipements réseau, biomédical, etc) est réalisé et publié annuellement
12	Une cartographie applicative est réalisée et tenue à jour (flux d'échange entre applications et ensemble des flux) sur la base de celles demandées par l'ANSSI (cartographie du systèmes d'information).

2.2 Audits réguliers

Le contrôle du SI par le biais d'audits réguliers permet d'identifier les vulnérabilités et de proposer des mesures correctives. Il est demandé aux établissements de procéder aux audits suivant.

2.2.1 Exposition de vulnérabilités sur internet

Disposer d'un diagnostic factuel d'identification des vulnérabilités exposées sur Internet (pour l'ensemble des domaines portés par l'ES).
Le « service de cybersurveillance» porté par le CERT santé de l'Agence du numérique en santé (ANS) permet de réaliser cet audit à distance.
Ces informations se retrouvent dans L'onglet OPSSIES d'OSIS v2 via l'intégration des résultats dans OSIS, soit par intégration automatique des résultats des audits de cybersurveillance, soit par recueil des établissements eux-mêmes.

Identifiant	Libellé de la mesure
13	L'audit d'exposition de vulnérabilité sur internet du CERT Santé est réalisé au moins annuellement. Il comprend les résultats suivants : • date audit de cybersurveillance (récent) • nombre de domaines (récent) • appréciation (récent) • total vulnérabilités (récent) • nombre de vulnérabilités critiques

2.2.2 Sécurité de l'Active Directory

Disposer d'un diagnostic factuel d'identification des vulnérabilités sur l'« Active Directory » (AD), élément clé de l'infrastructure des ES.
Le service ADS[5] de l'ANSSI permet de réaliser cet audit à distance (via l'outil de collecte ORADAD fourni par l'ANSSI) sur l'ensemble des établissements.
Ces informations se retrouvent dans l'OPSSIES via l'intégration des résultats dans OSIS, soit par intégration automatique des résultats des audits de cybersurveillance, soit par recueil des établissements eux-mêmes.

Identifiant	Libellé de la mesure
14	L'audit d'identification des vulnérabilités sur l'« Active Directory » (AD) de L'ANSSI est réalisé au moins annuellement. Il comprend les résultats suivants : • date audit Active Directory (récent) • niveau de sécurité (récent) • progression totale (récent) • nombre d'utilisateurs (récent)
15	Un plan d'actions urgentes issu des conclusions des audits des mesures 13 et 14 est validé et mis en œuvre par la direction de l'établissement .
16	Des alertes sont en place pour surveiller la sécurité de l'annuaire AD.

2.2.3 Audit organisationnel

Un audit organisationnel permet de mesurer pour l'ES la maturité de la gouvernance, de contrôler la prise en compte de la sécurité au niveau organisationnel sur la gouvernance, les procédures de sécurité notamment vis-à-vis de la nome ISO27001.

Identifiant	Libellé de la mesure
17	L'organisation de la sécurité du système d'information fait l'objet, tous les trois ans, d'un audit organisationnel de la SSI dans l'esprit de l'ISO 27001

[5] ADS : Active Directory Security

3 SECURISATION – MISE EN CONFORMITE :

3.1 Mise en place d'un plan d'action de sécurité des SI

Un plan d'action de sécurité des SI pluriannuel budgété, hiérarchisé sera établi (par exemple : plans d'actions issus des actions de mise en conformité (règlementaires notamment), des actions issues des analyses de risques et des audits (techniques et organisationnels).
En priorisant les actions à entreprendre et la progression du niveau de maturité, il s'agit de se prémunir des risques et augmenter la résilience de l'établissement et de son offre de soins.

Ce plan d'action est à intégrer dans la démarche globale de maîtrise des risques de l'établissement. Son suivi sera également effectué dans le cadre des audits de certification, des programmes d'accompagnement ministériels (HOP'EN et SUN-ES), ainsi que de la mise en conformité de l'établissement.

Identifiant	Libellé de la mesure
18	L'établissement a mis en place un plan d'action de sécurité des SI annuel hiérarchisé et budgété pour la mise en conformité, la réduction des vulnérabilités et la couverture des risques.
19	Le plan de sécurité des SI annuel de réduction des vulnérabilités et de couverture des risques est intégré dans la démarche globale de maîtrise des risques de l'établissement.

3.2 Sécurité des communications :

3.2.1 Management de la sécurité des réseaux : gestion des accès aux réseaux

Il convient d'adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles ainsi que pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.

Identifiant	Libellé de la mesure
20	L'établissement met en œuvre des réseaux wifi cloisonnés : wifi patient, wifi pour le système d'information, wifi pour les intervenants extérieurs.
21	Une politique régissant les conditions et restrictions liées au télétravail est validée par l'établissement
22	Le télétravail est réalisé depuis un poste de l'entreprise (poste professionnel) ou un dispositif d'ouverture de sessions à distance type VDI[6] avec accès VPN et authentification multi facteurs.
23	Un tunnel VPN pour tous les flux est mis en place pour le télétravail
24	Une application de « mobile device management » (MDM) est utilisée et déployée pour administrer les appareils mobiles.
25	La séparation des accès télétravail et des accès télémaintenance (ex : bastion d'administration) au travers d'identification/authentification forte (OTP[4], CPS, etc.) est privilégiée
26	Les contrats de télémaintenance prévoient un mode dégradé en cas de coupure des flux Internet (exemple la cyberattaque du CHU : mesure de cloisonnement avec l'extérieur ne permettant pas à des éditeurs d'intervenir à distance sur les premiers jours).
27	Un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système d'information sont mis en place (exemple : zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, etc.).

[6] virtual desktop infrastructure (VDI), infrastructure de bureau virtuel

3.3 Sécurité liée à l'exploitation du SI

3.3.1 Sauvegarde des informations

La sécurisation des sauvegardes constitue une action prioritaire immédiate (sauvegardes déconnectés ou sécurisation des processus de sauvegarde).
Un guide spécifique sera mis à disposition rapidement sur le site du CERT Santé

28	Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques sont réalisées
29	Des sauvegardes régulières et fréquentes sont effectuées, elles permettent de disposer de copies déconnectées du réseau. Il est vérifié régulièrement qu'elles sont opérantes.
30	La revue périodique des comptes d'accès au serveur de sauvegarde est réalisé.
31	Des tests de restauration a minima sur échantillons représentatifs sont réalisés.

4 SENSIBILISATION AU RISQUE CYBER :

Déclinaison de la campagne nationale 2021 sur la cybersécurité en santé
Une campagne nationale sur la cybersécurité en santé : « Tous cyber vigilants », a été lancée par le ministère des solidarités et de la santé au printemps 2021. L'objectif de cette campagne de grande ampleur est de favoriser la prise de conscience et l'adoption de nouveaux comportements, individuel et collectif, dans les structures de santé par l'ensemble du personnel.
Les ARS déclinent cette campagne au niveau régional, jusqu'au niveau des structures de santé, en s'appuyant notamment sur les supports fournis par le MSS

4.1 Sensibiliser et former aux enjeux de la cybersécurité et aux principes d'hygiène numérique

Il appartient à chaque structure de santé de mettre en place un dispositif permanant de sensibilisation : Des campagnes régulières de sensibilisation / formation interne auprès de l'ensemble de son personnel et ciblé sur les risques cybers de l'organisme.

Les structures de santé pourront s'appuyer sur les supports nationaux et territoriaux (MSS, ANSSI, CNIL, cybermalveillance, CERT Santé, ARS, …) ; des travaux sont en cours pour recenser les supports disponibles – la liste correspondante sera mise à disposition sur le site du CERT Santé.

Identifiant	Libellé de la mesure
32	Les actions de formation et sensibilisation à la SSI sont identifiées.
33	Une campagne de sensibilisation aux risques cyber est menée (par exemple : des emails de rappels périodiques concernant les bonnes pratiques, des fiches reflexes à disposition, du contenu pédagogique dispensé sous forme de webinaires,…).
34	Une action de formation à la SSI au moins est inscrite dans le plan de formation annuel des personnes en charge de la SSI et des personnes en charge du SI (formation type sécurité des systèmes d'information).

5 ANTICIPATION : PREPARATION A FAIRE FACE AUX INCIDENTS

(participe à la mise en œuvre de la règle N°23 de la directive NIS)

5.1 Exercices de continuité d'activité en « mode numérique dégradé »

Au regard de l'accroissement des cyberattaques sur le secteur de la santé, il est demandé à chaque établissement d'organiser annuellement un exercice de continuité d'activité, avec la mise en place de procédures de travail en « mode dégradé » avec un compte rendu et des actions d'améliorations suivies par le RSSI.
Cet exercice devra aussi tester la chaine d'alerte de l'établissement qui doit être activable H24 – 7/7.
La réalisation de ces exercices s'inscrit dans une démarche d'amélioration continue des plans de continuité d'activité et de management des risques des établissements.
Un guide est disponible sur le site de l'ANSSI : https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/
Un guide spécifique sera mis à disposition sur le site du CERT Santé.

Identifiant	Libellé de la mesure
35	Un exercice de continuité des activités métiers est effectué annuellement (avec retour sur expérience et actions d'améliorations).
36	Les procédures de travail (métier) en mode dégradé sont rédigées.
37	Les procédures de travail dégradées donnent lieu à un plan d'améliorations, le cas échéant, à la suite de chaque exercice (retour sur expérience).
38	Les procédures de travail dégradées sont toujours accessibles (leurs supports sont protégés contre les risques cyber)

6 GESTION DES INCIDENTS :

6.1 Déclaration systématique des incidents de sécurité des SI

Depuis octobre 2017, les structures de santé sont tenues à la déclaration systématique des incidents de sécurité des SI qui les impactent (article L. 1111-8-2 du code de la santé publique).
Porté par le CERT-Santé, le dispositif de traitement des signalements des incidents de sécurité des SI constitue un élément clé de la stratégie d'amélioration du niveau de sécurité numérique du secteur santé portée par le ministère des solidarités et de la santé, en coordination étroite avec l'ANSSI.
Depuis 2020, les structures médico-sociales sont également concernées par ce dispositif.

Identifiant	Libellé de la mesure
39	L'établissement a défini et applique une procédure interne de remontée des incidents de sécurité SI qui associe les métiers concernés
40	Les incidents graves de sécurité des systèmes d'information sont systématiquement signalés, conformément à la Règlementation.
41	Le rôle du RSSI dans la procédure de remontée des incidents est défini et lui permet d'être informé en permanence sur le traitement de l'incident

6.2 Réponse aux incidents graves de sécurité

Les établissements doivent disposer d'un support contractuel permettant de pouvoir recourir à un spécialiste de la réponse à incidents de sécurité. Ce support contractuel peut être propre à l'établissement ou mutualisé à divers niveau (GHT, GRADeS, …).

Identifiant	Libellé de la mesure
42	L'établissement dispose d'un support contractuel permettant de pouvoir recourir à un spécialiste de la réponse à incidents de sécurité « De préférence, ce prestataire doit être qualifié PRESTATAIRES DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ (PRIS) ou en cours de qualification par l'ANSSI » .
43	La procédure de déclenchement de la réponse à incident, les informations contractuelles et de contact restent accessibles dans toutes les situations.

Les modalités de contrôle

Dans le cadre du programme HOP'EN, les ARS renforceront les contrôles des prérequis en matière de sécurité numérique (prérequis P2 et P3 en particulier), en vérifiant notamment la mise en place d'audits cyber et des plans de réductions des vulnérabilités afférents.

HAS – Certification pour la qualité des soins

Il s'agit pour les structures de santé de répondre aux exigences du « critère 3.06-02 : "les risques numériques sont maîtrisés" ».

DGOS – OPSSIES

Les résultats des audits cyber et de conformité aux exigences de sécurité (uniquement ceux du CERT Santé et de l'ANSSI) ont vocation à figurer dans l'onglet OPSSIES d'OSIS.

Ces informations constitueront le cœur de l'observatoire permanent du niveau de maturité en sécurité numérique des établissements de santé qui va être créé en 2022.

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité

7 ANNEXES

7.1 Annexe 1 : liste des mesures prioritaires

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
1	L'établissement dispose d'une cartographie des risques liés aux services numériques actualisée annuellement basée sur une méthodologie qui permette de comparer les résultats d'une itération à l'autre.	Oui datant de moins d'1 an	Oui datant de plus d'1 an	Non	Non renseigné		
2	La cartographie des risques liés aux services numériques est consolidée dans une cartographie globale des risques[7] portant sur l'établissement.	Oui	Non	Non renseigné	Non applicable		
3	Une analyse de risque, validée par les responsables métiers des services concernés, est réalisée lors de l'introduction d'un nouveau service numérique (application, matériel IT, équipement biomédical et technique, GTB/GTC) .	Oui, systématiquement	Oui, pas systématiquement	Non	Non renseigné		
4	Le plan d'action associé à l'analyse de risque est suivi et priorisé.	Oui	Non	Non renseigné	Non applicable		
5	Le principe de la réalisation d'une analyse de risques numériques est accepté par la Direction (acceptation des risques résiduels).	Oui	Non	Non renseigné	Non applicable		
6	Une personne en charge de la fonction sécurité du système d'Information (SSI) ou RSSI est nommée au sein de l'établissement.	Oui	Non	Non renseigné			

[7] La cartographie globale des risques : Intégrer les risques numériques aux risques métiers en reconnaissant le risque numérique comme impactant la gestion des ES

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
7	La personne prenant en charge la sécurité des systèmes d'information ou RSSI a au moins un rendez-vous semestriel formel avec le Directeur Général de l'établissement.	Oui	Non	Non renseigné	Non applicable		
8	Le rendez-vous a minima semestriel formel avec le Directeur Général de l'établissement donne lieu à un compte rendu (document de preuve).	Oui	Non	Non renseigné	Non applicable		
9	L'établissement calcule la part, en %, du budget global annuel de l'établissement consacrée au SI selon la méthodologie de l'enquête "charges et ressources" de la DGOS	Oui	Non	Non renseigné			
10	L'établissement calcule annuellement le ratio budget SI rapporté au poste de travail.	Oui	Non	Non renseigné			
11	Un inventaire des matériels et logiciels (matériel: postes de travail, serveurs, machines virtuelles, équipements réseau, biomédical, etc) est réalisé et publié annuellement	Oui datant de moins d'1 an	Oui datant de moins d'1 an mais non publié	Oui datant de plus d'1 an	Oui datant de plus d'1 an mais non publié	Non	Non renseigné
12	Une cartographie applicative est réalisée et tenue à jour (flux d'échange entre applications et ensemble des flux) sur la base de celles demandées par l'ANSSI (cartographie du systèmes d'information).	Oui datant de moins d'1 an	Oui datant de plus d'1 an	Non	Non renseigné		
13	L'audit d'exposition de vulnérabilité sur internet du CERT Santé est réalisé au moins annuellement. Il comprend les résultats suivants : • date audit de cybersurveillance (récent) • nombre de domaines (récent) • appréciation (récent) • total vulnérabilités (récent) • nombre de vulnérabilités critiques	Valeurs					

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
14	L'audit d'identification des vulnérabilités sur l'« Active Directory » (AD) de L'ANSSI est réalisé au moins annuellement. Il comprend les résultats suivants : • Date audit Active Directory (récent) • niveau de sécurité (récent) • progression totale (récent) • nombre d'utilisateurs (récent)	Valeurs					
15	Un plan d'actions urgentes issu des conclusions des audits des mesures 13 et 14 est validé et mis en œuvre par la direction de l'établissement .	Oui validé	Oui validé et mise en œuvre	Non	Non renseigné		
16	Des alertes sont en place pour surveiller la sécurité de l'annuaire AD.	Oui	Non	Non renseigné			
17	L'organisation de la sécurité du système d'information fait l'objet, tous les trois ans, d'un audit organisationnel de la SSI dans l'esprit de l'ISO 27001	Oui, annuel	Oui, plus d'une fois par an	Oui, moins d'une fois par an	oui, au moins tous les trois ans	Non	Non renseigné
18	L'établissement a mis en place un plan d'action de sécurité des SI annuel hiérarchisé et budgété pour la mise en conformité, la réduction des vulnérabilités et la couverture des risques.	Oui hiérarchisé	Oui hiérarchisé et budgété	Non			
19	Le plan de sécurité des SI annuel de réduction des vulnérabilités et de couverture des risques est intégré dans la démarche globale de maîtrise des risques de l'établissement.	Oui	Non				
20	L'établissement met en œuvre des réseaux wifi cloisonnés : wifi patient, wifi pour le système d'information, wifi pour les intervenants extérieurs.	Oui	Non	Non renseigné			
21	Une politique régissant les conditions et restrictions liées au télétravail est validée par l'établissement	Oui	Non	Non renseigné			

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
22	Le télétravail est réalisé depuis un poste de l'entreprise (poste professionnel) ou un dispositif d'ouverture de sessions à distance type VDI[8] avec accès VPN et authentification multi facteurs.	Oui	Non	Non renseigné			
23	Un tunnel VPN pour tous les flux est mis en place pour le télétravail	Oui	Non	Non renseigné			
24	Une application de « mobile device management » (MDM) est utilisée et déployée pour administrer les appareils mobiles.	Oui	Non	Non renseigne			
25	La séparation des accès Télétravail et des accès Télémaintenance (ex : bastion d'administration) au travers d'identification/authentification forte (OTP[4], CPS, etc.) est privilégiée	Oui	Non	Non renseigné			
26	Les contrats de télémaintenance prévoient un mode dégradé en cas de coupure des flux Internet (ex cyberattaque du CHU : mesure de cloisonnement avec l'extérieur ne permettant pas à des éditeurs d'intervenir à distance sur les premiers jours).	Non	Oui à 20%	Oui à 40%	Oui à 60%	Oui à 80%	Oui à 100%
27	Un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système d'information sont mis en place (exemple : zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, etc.).	Oui	Non	Non renseigné			
28	Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques sont réalisées	Oui, au moins une fois par jour	Oui, périodiquement	Non	Non renseigné		

[8] virtual desktop infrastructure (VDI), infrastructure de bureau virtuel

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
29	Des sauvegardes régulières et fréquentes sont effectuées, elles permettent de disposer de copies déconnectées du réseau. Il est vérifié régulièrement qu'elles sont opérantes.	Oui	Non	Non	Non renseigné		
30	La revue périodique des comptes d'accès au serveur de sauvegarde est réalisé.	Oui	Non	Non	Non renseigné		
31	Des tests de restauration a minima sur échantillons représentatifs sont réalisés.	Oui, au moins une fois par an	Oui, périodiquement	Non	Non renseigné		
32	Les actions de formation et sensibilisation à la SSI sont identifiées.	Oui	Non	Non renseigné			
33	Une campagne de sensibilisation aux risques cyber est menée (par exemple : des mails de rappels périodiques concernant les bonnes pratiques, des fiches reflexes à disposition, du contenu pédagogique dispensé sous forme de webinaires,…).	Oui	Non	Non renseigné			
34	Une action de formation à la SSI au moins est inscrite dans le plan de formation annuel des personnes en charge de la SSI et des personnes en charge du SI (Formation type Sécurité des Systèmes d'Information).	Oui	Non	Non renseigné			
35	Un exercice de continuité des activités métiers est effectué annuellement (avec retour sur expérience et actions d'améliorations).	Oui	Non	Non renseigné			
36	Les procédures de travail (métier) en mode dégradé sont rédigées.	Oui	Non	Non renseigné			
37	Les procédures de travail dégradées donnent lieu à un plan d'améliorations, le cas échéant, à la suite de chaque exercice (retour sur expérience).	Oui	Non	Non renseigné			

Mesures Prioritaires	Libellé	Réponse possible 1	Réponse possible 2	Réponse possible 3	Réponse possible 4	Réponse possible 5	Réponse possible 6
38	Les procédures de travail dégradées sont toujours accessibles (leurs supports sont protégés contre les risques cyber)	Oui	Non	Non renseigné			
39	L'établissement a défini et applique une procédure interne de remontée des incidents de sécurité SI qui associe les métiers concernés	Oui totalement	Oui en partie	Non	Non renseigné		
40	Les incidents graves de sécurité des systèmes d'information sont systématiquement signalés, conformément à la Règlementation.	Oui	Non	Non renseigné			
41	Le rôle du RSSI dans la procédure de remontée des incidents est défini et lui permet d'être informé en permanence sur le traitement de l'incident	Oui	Non	Non renseigné			
42	L'établissement dispose d'un support contractuel permettant de pouvoir recourir à un spécialiste de la réponse à incidents de sécurité « De préférence, ce prestataire doit être qualifié PRESTATAIRES DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ (PRIS) ou en cours de qualification par l'ANSSI » .	Oui	Non	Non renseigné			
43	La procédure de déclenchement de la réponse à incident, les informations contractuelles et de contact restent accessibles dans toutes les situations.	Oui	Non	Non renseigné			

7.2 Annexe 2 : liste des mesures prioritaires croisement avec les référentiels de sécurité

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
1	L'établissement dispose d'une cartographie des risques liés aux services numériques actualisée annuellement basée sur une méthodologie qui permette de comparer les résultats d'une itération à l'autre.	6.1.2 Appréciation des risques de sécurité de l'information	Règle 1 Gouvernance Analyse de risques	**INT-REX-AR** : analyse de risques. **INT-HOMOLOG-SSI** Homologation de sécurité des systèmes d'information	P2.4 Existence d'une analyse des risques détaillée	**P2-ORG** Etablissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI **P3-ORG** Réalisation et tenue à jour d'une analyse de risque SI de la structure ;	R41-R Mener une analyse de risques formelle	PS2.1 Existence d'une analyse des risques détaillée
2	La cartographie des risques liés aux services numériques est consolidée dans une cartographie globale des risques[9] portant sur l'établissement.	6.1.2 Appréciation des risques de sécurité de l'information	Règle 1 Gouvernance Analyse de risques		P2.4 Existence d'une analyse des risques détaillée	**P2-ORG** Etablissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI	R41-R Mener une analyse de risques formelle	PS2.1 Existence d'une analyse des risques détaillée
3	Une analyse de risque, validée par les responsables métiers des services concernés, est réalisée lors de l'introduction d'un nouveau service numérique (application, matériel IT, équipement biomédical et technique, GTB/GTC) .	6.1.2 Appréciation des risques de sécurité de l'information	Règle 1 Gouvernance Analyse de risques		P2.4 Existence d'une analyse des risques détaillée	**P2-ORG** Etablissement d'une procédure formelle d'appréciation du risque avant toute mise en production d'un SI	R41-R Mener une analyse de risques formelle	PS2.1 Existence d'une analyse des risques détaillée
4	Le plan d'action associé à l'analyse de risque est suivi et priorisé.	6.1.3 Traitement des risques de sécurité de l'information (Plan)	Règle 3. Homologation de sécurité	INT-HOMOLOG-SSI Homologation de sécurité des systèmes d'information	P2.4 Existence d'une politique de sécurité, d'une analyse des risques détaillée, d'un plan d'action associé	P3-ORG Définition et mise en œuvre du plan d'action associé à l'analyse de risque	R41-R Elaboration d'un plan de traitement du risque	PS2.1 Existence d'un plan d'action associé à l'analyse de risque

[9] La cartographie globale des risques : Intégrer les risques numériques aux risques métiers en reconnaissant le risque numérique comme impactant la gestion des ES

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
5	Le principe de la réalisation d'une analyse de risques numériques est accepté par la Direction (acceptation des risques résiduels).	6.1.3 Traitement des risques de sécurité de l'information (Plan)	Règle 3. Homologation de sécurité	INT-HOMOLOG-SSI Homologation de sécurité des systèmes d'information	P2.4 Existence d'une politique de sécurité, d'une analyse des risques détaillée, d'un plan d'action associé	P3-ORG Analyse de risque et mise en œuvre du plan d'action associé validés par les instances de gouvernance de la structure	R41-R Elaboration d'un plan de traitement du risque à faire valider par une autorité désignée à plus haut niveau.	PS2.1 Existence d'une analyse des risques détaillée, d'un plan d'action associé
6	Une personne en charge de la fonction Sécurité du Système d'Information (SSI) ou RSSI est nommée au sein de l'établissement.	5.3 Rôles, responsabilités et autorités au sein de l'organisation	Règle 2. Politique de sécurité (Equivalence)	ORG-RSSI : désignation du responsable SSI.	P2.4 Positionnement du RSSI en dehors de la DSI, par exemple rattaché à la cellule qualité. Existence d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement pour point de situation.	P1-RH La fonction sécurité des systèmes d'information est identifiée et prise en charge par la direction	R39S	PS2.1 Existence d'une fonction de responsable sécurité
7	La personne prenant en charge la sécurité des systèmes d'information ou RSSI a au moins un rendez-vous semestriel formel avec le Directeur Général de l'établissement.	5.3 Rôles, responsabilités et autorités au sein de l'organisation			P2.4 idem	P1-RH La fonction sécurité des systèmes d'information est identifiée et prise en charge par la direction		PS2.1 Existence d'une fonction de responsable sécurité

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
8	Le rendez-vous a minima semestriel formel avec le Directeur Général de l'établissement donne lieu à un compte rendu (document de preuve).	5.3 Rôles, responsabilités et autorités au sein de l'organisation			P2.4 Existence d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement pour point de situation.			PS2.1
9	L'établissement calcule la part, en %, du budget global annuel de l'établissement consacrée au SI selon la méthodologie de l'enquête "charges et ressources" de la DGOS	5.1 Leadership et engagement						
10	L'établissement calcule annuellement le ratio budget SI rapporté au poste de travail.	5.1 Leadership et engagement						
11	Un inventaire des matériels et logiciels (matériel: postes de travail, serveurs, machines virtuelles, équipements réseau, biomédical, etc) est réalisé et publié annuellement	A8.1.1 Inventaire des actifs	Règle 6. Cartographie	GDB-INVENT	P2.4	**P1-ORG**	R4-S	PS2.1

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
12	Une cartographie applicative est réalisée et tenue à jour (flux d'échange entre applications et ensemble des flux) sur la base de celles demandées par l'ANSSI (cartographie du systèmes d'information).	A8.1.1 Inventaire des actifs	Règle 6. Cartographie	GDB-INVENT	P2.4	**P1-ORG**	R4-S, R17-S	PS2.1
13	L'audit d'exposition de vulnérabilité sur internet du CERT Santé est réalisé au moins annuellement. Il comprend les résultats suivants : • date audit de cybersurveillance (récent) • nombre de domaines (récent) • appréciation (récent) • total vulnérabilités (récent) • nombre de vulnérabilités critiques	A12.7.1 Mesures relatives à l'audit des systèmes d'information	Règle 5. Audits de la sécurité		P.25		R38-R	P2.2
14	L'audit d'identification des vulnérabilités sur l'« Active Directory » (AD) de L'ANSSI est réalisé au moins annuellement. Il comprend les résultats suivants : • date audit Active Directory (récent) • niveau de sécurité (récent) • progression totale (récent) • nombre d'utilisateurs (récent)	A12.7.1 Mesures relatives à l'audit des systèmes d'information			P.25		R38-R	P2.2

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
15	Un plan d'actions urgentes issu des conclusions des audits mesures 13 et 14 est validé et mis en œuvre par la direction de l'établissement	A12.7.1 Mesures relatives à l'audit des systèmes d'information	Règle 5. Audits de la sécurité				R38-R	
16	Des alertes sont en place pour surveiller la sécurité de l'annuaire AD.	A12.7.1 Mesures relatives à l'audit des systèmes d'information						
17	L'organisation de la sécurité du système d'information fait l'objet, tous les trois ans, d'un audit organisationnel de la SSI dans l'esprit de l'ISO 27001	A18.2.1 Revue indépendante de la sécurité de l'information	Règle 5. Audits de la sécurité	CONTR-SSI : contrôles locaux, CONTR-BILAN-SSI : bilan annuel. EXP-CI-AUDIT : audit/contrôle.	P2.5		R38-R Procéder à des contrôles et audits de sécurité réguliers	PS2.2
18	L'établissement a mis en place un plan d'action de sécurité des SI annuel hiérarchisé et budgété pour la mise en conformité, la réduction des vulnérabilités et la couverture des risques.	9.3 Revue de direction	Règle 5. Audits de la sécurité		P2.4	P3-ORG	R38-R appliquer les actions correctives associées	P2.1
19	Le plan de sécurité des SI annuel de réduction des vulnérabilités et de couverture des risques est intégré dans la démarche globale de maîtrise des risques de l'établissement.	8.3 Traitement des risques de sécurité de l'information (Do)			P2.4	P3-ORG	R38-R Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées	P2.1

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
20	L'établissement met en œuvre des réseaux wifi cloisonnés : wifi patient, wifi pour le système d'information, wifi pour les intervenants extérieurs	A13.1.3 Cloisonnement des réseaux	Règle 8 : Segmentation / cloisonnement	PDT-NOMAD-DESACTIV	P2.4	**P2-RES**	R20-S, R37-S	P2.1
21	Une politique régissant les conditions et restrictions liées au télétravail est validée par l'établissement	A6.2.2 Télétravail	Règle 9. Accès distant			P1-RH		
22	Le télétravail est réalisé depuis un poste de l'entreprise (poste professionnel) ou un dispositif d'ouverture de sessions à distance type VDI[10] avec accès VPN et authentification multi facteurs	A6.2.2 Télétravail				P2-RES	R32-S	
23	Un tunnel VPN pour tous les flux est mis en place pour le télétravail	A6.2.2 Télétravail	Règle 9. Accès distant			P2-RES	R32-S	

[10] virtual desktop infrastructure (VDI), infrastructure de bureau virtuel

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
24	Une application de « mobile device management » (MDM) est utilisée et déployée pour administrer les appareils mobiles.	A6.2.1 Politique en matière d'appareils mobiles					R33-S	
25	La séparation des accès télétravail et des accès télémaintenance (ex : bastion d'administration) au travers d'identification/authentification forte (OTP[4], CPS, etc.) est privilégiée	A6.2.2 Télétravail				P2-RES	R32-R	
26	Les contrats de télémaintenance prévoient un mode dégradé en cas de coupure des flux Internet (ex cyberattaque du CHU : mesure de cloisonnement avec l'extérieur ne permettant pas à des éditeurs d'intervenir à distance sur les premiers jours).	A15.1.2 La sécurité dans les accords conclus avec les fournisseurs				P3-PRESTA P2-RES	R3-S	
27	Un ou plusieurs dispositifs de filtrage permettant un cloisonnement entre les différentes zones réseaux plus ou moins critiques du système d'information sont mis en place (exemple : zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, etc.).	A13.1.3 Cloisonnement des réseaux	Règle 8 : Segmentation / cloisonnement	RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes.		P2-RES	R28-S Utiliser un réseau dédié et cloisonné pour l'administration du système d'information, R32-S	

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
28	Des sauvegardes régulières de l'ensemble des données, y compris celles présentes sur les serveurs de fichiers, d'infrastructure et d'applications métier critiques sont réalisées	A12.3.1 Sauvegarde des informations		ARCHI-STOCKCI	P2.4	P1-SAUV	R37-S, R37-R Définir et appliquer une politique de sauvegarde des composants critiques	P2.1
29	Des sauvegardes régulières et fréquentes sont effectuées, elles permettent de disposer de copies déconnectées du réseau. Il est vérifié régulièrement qu'elles sont opérantes.	A12.3.1 Sauvegarde des informations		ARCHI-STOCKCI	P2.4	**P1-SAUV**	R37-S, R37-R Définir et appliquer une politique de sauvegarde des composants critiques	P2.1
30	La revue périodique des comptes d'accès au serveur de sauvegarde est réalisé.	A12.3.1 Sauvegarde des informations		ARCHI-STOCKCI	P2.4	P1-SAUV	R37-S, R37-R Définir et appliquer une politique de sauvegarde des composants critiques	PS2.1
31	Des tests de restauration a minima sur échantillons représentatifs sont réalisés.	A12.3.1 Sauvegarde des informations		ARCHI-STOCKCI	P2.4	P1-SAUV	R37-S, R37-R Définir et appliquer une politique de sauvegarde des composants critiques	PS2.1

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
32	Les actions de formation et sensibilisation à la SSI sont identifiées.	A7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information	Règle 2. Politique de sécurité	RH-UTIL	P2.4	**P2-RH Gestion des ressources humaines**	R1-S	PS2.1
33	Une campagne de sensibilisation aux risques cyber est menée (par exemple : des emails de rappels périodiques concernant les bonnes pratiques, des fiches reflexes à disposition, du contenu pédagogique dispensé sous forme de webinaires,…).	A7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information		RH-UTIL		**P2-RH**	R2-S	
34	Une action de formation à la SSI au moins est inscrite dans le plan de formation annuel des personnes en charge de la SSI et des personnes en charge du SI (formation type Sécurité des Systèmes d'Information).	A7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information		RH-UTIL	P2.4	P2-RH	R1-S	PS2.1
35	Un exercice de continuité des activités métiers est effectué annuellement (avec retour sur expérience et actions d'améliorations).	A17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information		PCA-EXERC	P2.1 Continuité d'activité			

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
36	Les procédures de travail (métier) en mode dégradé sont rédigées.	A17.1.1 Organisation de la continuité de la sécurité de l'information	Règle 2. Politique de sécurité (pour partie)	PCA-LOCAL	P2.1			
37	Les procédures de travail dégradées donnent lieu à un plan d'améliorations, le cas échéant, à la suite de chaque exercice (retour sur expérience).	A17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information		PCA-MISAJOUR				
38	Les procédures de travail dégradées sont toujours accessibles (leurs supports sont protégés contre les risques cyber)	A17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information						
39	L'établissement a défini et applique une procédure interne de remontée des incidents de sécurité SI qui associe les métiers concernés	A16.1.2 + A16.1.3 Signalement des failles liées à la sécurité de l'information		TI-OPS-SSI : chaînes opérationnelles SSI.	P2.4	P1-ORG	R40-S	PS2.1
40	Les incidents graves de sécurité des systèmes d'information sont systématiquement signalés, conformément à la Règlementation.	A16.1.2 + A16.1.3 Signalement des failles liées à la sécurité de l'information			P2.4	P1-ORG	R40-S	PS2.1

Mesures Prioritaires	Libellé	ISO 27001/27002	NIS V1	PSSI MCAS	HOP'EN	IM 309	Guide d'Hygiène ANSSI	SUN-ES
41	Le rôle du RSSI dans la procédure de remontée des incidents est défini et lui permet d'être informé en permanence sur le traitement de l'incident	A16.1.2 * Signalement des événements liés à la sécurité de l'information						
42	L'établissement dispose d'un support contractuel permettant de pouvoir recourir à un spécialiste de la réponse à incidents de sécurité « De préférence, ce prestataire doit être qualifié PRESTATAIRES DE RÉPONSE AUX INCIDENTS DE SÉCURITÉ (PRIS) ou en cours de qualification par l'ANSSI » .	A16.1.5 Réponse aux incidents liés à la sécurité de l'information					R40-S	
43	La procédure de déclenchement de la réponse à incident, les informations contractuelles et de contact restent accessibles dans toutes les situations.	A16.1.5 Réponse aux incidents liés à la sécurité de l'information						

7.3 Glossaire

Acronyme	Signification
ANSSI	Agence nationale de la sécurité des systèmes d'information
AQSSI	L'autorité qualifiée pour la sécurité des systèmes d'information (AQSSI)
PASSI	Prestataires d'audit de la sécurité des systèmes d'information qualifiés par l'ANSSI
PRIS	Prestataires de réponse aux incidents de sécurité qualifiés par l'ANSSI
Guide d'hygiène informatique ANSSI	42 règles de sécurité simples proposées par l'ANSSI Version 1.0 - Janvier 2013
Directives NIS-V1	Règles de sécurité applicables aux réseaux et systèmes d'information mentionnés à l'article 7 du décret no 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
PSSI-MCAS	Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS). Déclinaison de la politique de sécurité des systèmes d'information de l'Etat (PSSI-E), approuvée par arrêté ministériel du 1er octobre 2015.
PGSSI-S	Politique de sécurité des systèmes d'information de santé (PGSSI-S)
Instruction 309	INSTRUCTION N°SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information (« Plan d'action SSI ») dans les établissements et services concernés
ISO/CEI 27001:2013	NORME INTERNATIONALE Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences
OPSSIES	OPSSIES : l'observatoire permanent de la maturité SSI des établissements (OPSSIES) sera l'outil de déclaration de conformité des ES aux différentes mesures.
Plateforme OSIS V2	Observatoire des Systèmes d'Information de Santé (oSIS)
RUMS	Référentiel unique des mesures de sécurité (RUMS). Le RUMS a l'ambition de reprendre l'ensembles des mesures de sécurité SI relatives aux ES et définies à des fins de : Evaluation de la conformité à des exigences de sécurité SI, Evaluation de la maturité en matière de sécurité SI.
Service ADS : Outil de collecte ORADAD	le service ADS (Active Directory Security) développé par l'ANSSI met à disposition des opérateurs Règlementés et de la sphère publique une capacité d'audit des annuaires AD (Active Directory) visant à leur donner de la visibilité sur le niveau de sécurité de leur annuaire et à les accompagner dans son durcissement par l'application progressive de mesures adéquates, avec un suivi dans le temps.
MSS	Ministère des Solidarités et de la Santé
EBIOS RM	EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement des risques numériques publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI)
Cartographie globale des risques	La cartographie globale des risques : Intégrer les risques numériques aux risques métiers en reconnaissant le risque numérique comme impactant la gestion des ES
CDP ou Continuous Data Protection	Sauvegarde en continu (CDP ou Continuous Data Protection)
Données sensibles	Données sensibles : utilisé dans le Guide Hygiène de l'ANSSI, PSSI-MCAS
VDI	virtual desktop infrastructure (VDI), infrastructure de bureau virtuel
HOP'EN	Le programme HOP'EN pour « Hôpital numérique ouvert sur son environnement » fixe le nouveau plan d'action national des systèmes d'information hospitaliers à 5 ans, dans la continuité du programme hôpital numérique.
SUN-ES	Programme SUN-ES pour « Ségur Usage Numérique en Établissements de Santé » qui s'adresse plus particulièrement aux établissements de santé. Le suivi opérationnel du programme SUN-ES a été confié à la DGOS.

MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION

Liberté
Égalité
Fraternité

Direction générale
de l'offre de soins