TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Introduction de la journée

Nina PRUNIER

Directrice adjointe de l'innovation de la recherche et de la transformation numérique - ARS IDF

Naïma MEZAOUR

Directrice du GIP SESAN

sesan
Groupement d'Intérêt Public eSanté
ÎLE-DE-FRANCE

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle
ESMS

Guillaume CREPIN
Délégué ANSSI pour l'Île-de-France

Margaux BUGUET
Responsable de mission – ESMS – ANS

Mohcine EL OUBNANI
Référent Filière ESMS – SESAN

sesan
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle
ESMS

Guillaume CREPIN
Délégué ANSSI pour l'Île-de-France

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars
Agence Régionale de Santé
Île-de-France

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

REVUE NATIONALE STRATÉGIQUE ET STRATÉGIE NATIONALE CYBER

Nous entrons dans une nouvelle ère, celle d'un risque particulièrement élevé d'une guerre majeure de haute intensité en dehors du territoire national en Europe, qui impliquerait la France et ses alliés en particulier européens, à l'horizon 2030, et verrait notre territoire visé en même temps par des actions hybrides massives.

Il est vital de se préparer à cette hypothèse : la France et les Européens doivent être capables de mieux se défendre et de dissuader toute nouvelle agression russe sur le continent.

Revue nationale stratégique 205 – 2030 p.8

Une RNS déclinée en 11 objectifs stratégiques

OS 1 Une dissuasion nucléaire robuste et crédible

OS 2 Une France unie et résiliente : contribuer au réarmement moral de la Nation pour faire face aux crises

OS 3 Une économie qui se prépare à la guerre

OS 4 Une résilience cyber de premier rang

OS 5 La France, allié fiable dans l'espace euro-atlantique

OS 6 La France, un des moteurs de l'autonomie stratégique européenne

OS 7 La France, partenaire fiable de souveraineté et pourvoyeuse crédible de sécurité

OS 8 Une autonomie d'appréciation et une souveraineté décisionnelle garanties

OS 9 Une capacité à agir dans les champs hybrides

OS 10 La capacité d'emporter la décision dans les opérations militaires

OS11 Une excellence académique, scientifique et technologique au service de la souveraineté française et européenne

Une RNS déclinée en 11 objectifs stratégiques

OS 1 Une dissuasion nucléaire robuste et crédible

OS 2 Une France unie et résiliente : contribuer au réarmement moral de la Nation pour faire face aux crises

OS 3 Une économie qui se prépare à la guerre

OS 4 Une résilience cyber de premier rang

OS 5 La France, allié fiable dans l'espace euro-atlantique

OS 6 La France, un des moteurs de l'autonomie stratégique européenne

OS 7 La France, partenaire fiable de souveraineté et pourvoyeuse crédible de sécurité

OS 8 Une autonomie d'appréciation et une souveraineté décisionnelle garanties

OS 9 Une capacité à agir dans les champs hybrides

OS 10 La capacité d'emporter la décision dans les opérations militaires

OS11 Une excellence académique, scientifique et technologique au service de la souveraineté française et européenne

Une SNC s'appuyant sur 5 piliers

PILIER 1 Faire de la France le plus grand vivier de talents cyber d'Europe
orienter et former

PILIER 2 Renforcer la résilience cyber de la Nation
élever le niveau, réagir, financer

PILIER 3 Entraver l'expansion de la cybermenace
anticiper, entraver, partager

PILIER 4 Garder la maitrise de la sécurité de nos fondements numériques
maitriser les technologies, développer de nouvelles solutions

PILIER 5 Soutenir la sécurité et la stabilité du cyberespace en Europe et à l'international
coopérer, influence

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

L'ETAT DE LA MENACE 2025

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LE CONSTAT

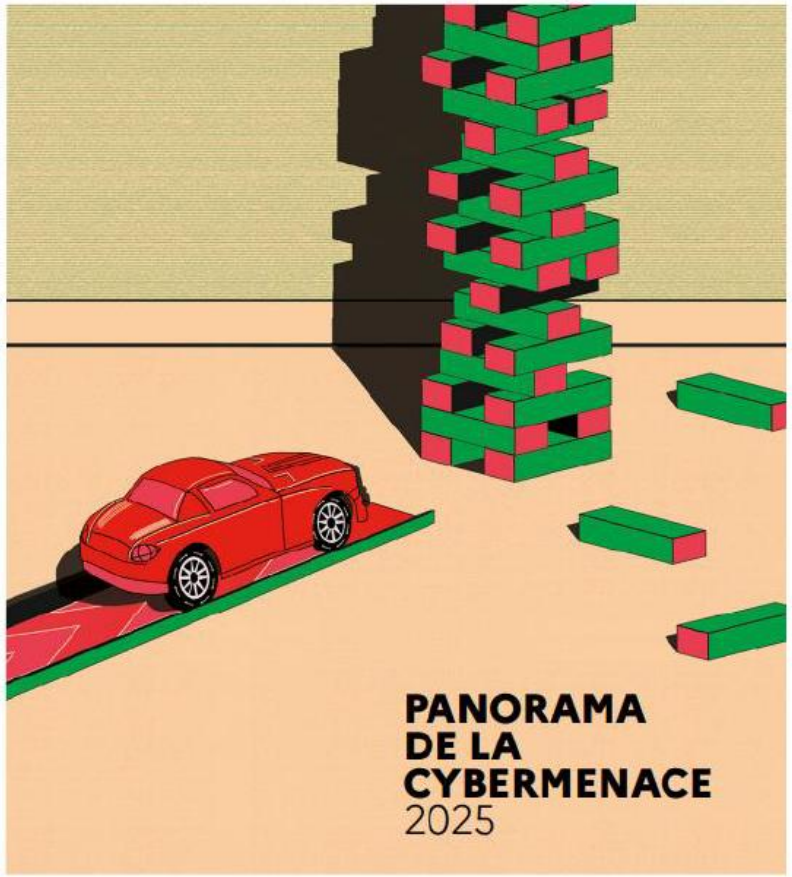
En 2025, la menace cyber se stabilise à un niveau particulièrement élevé, posant une pression constante sur l'Etat et le tissu économique et social français

2025 EN BREF

1. La menace cyber reste à un niveau élevé et s'inscrit dans un contexte d'aggravation des tensions géopolitiques mondiales

2. Il est plus difficile d'y voir clair dans le brouillard technologique et organisationnel des écosystèmes d'attaquants

3. L'écosystème cybercriminel se tourne de façon croissante vers le vol de données



https://www.cert.ssi.gouv.fr/cti/CERTFR-2026-CTI-002/

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES OUTILS ET SERVICES DE L'ANSSI

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

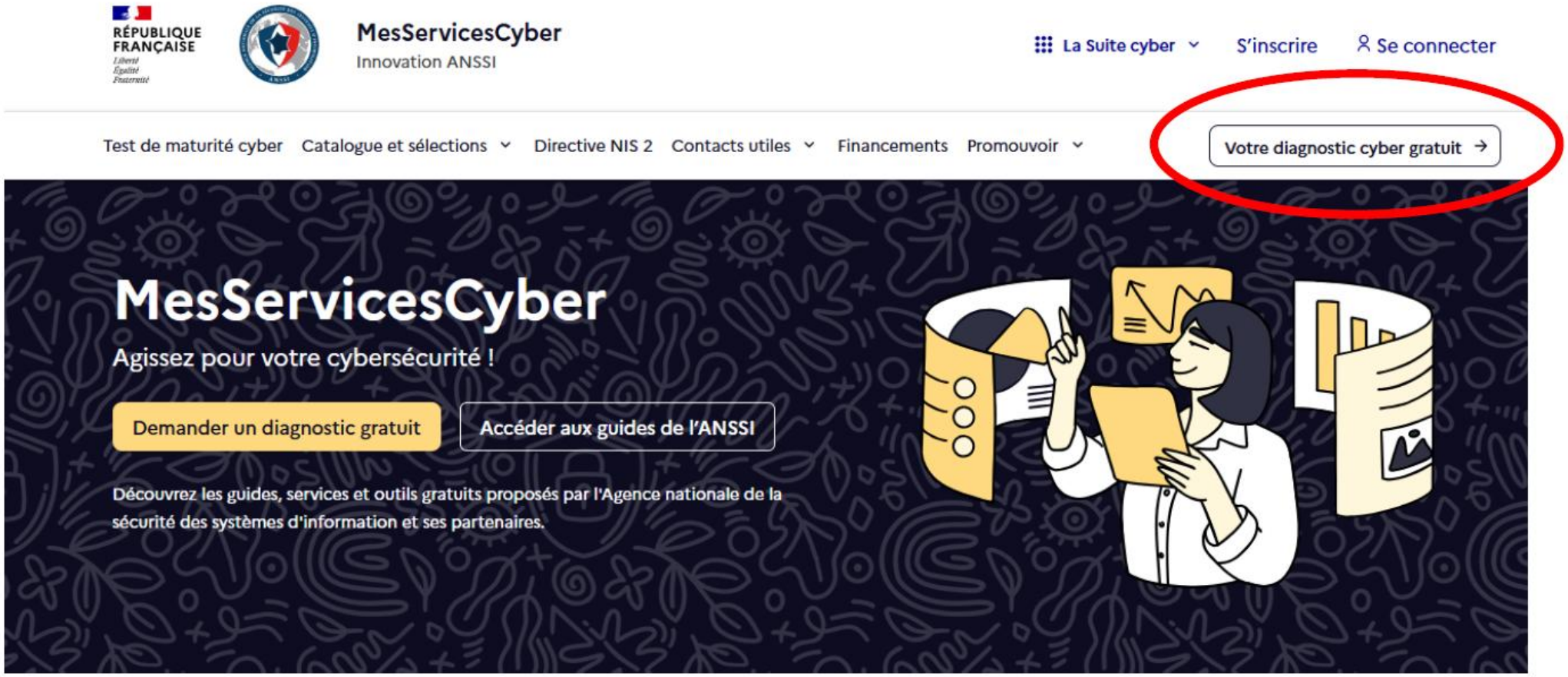
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

MesServicesCyber
Innovation ANSSI

La Suite cyber | S'inscrire | Se connecter

Test de maturité cyber | Catalogue et sélections | Directive NIS 2 | Contacts utiles | Financements | Promouvoir | Votre diagnostic cyber gratuit →

https://messervices.cyber.gouv.fr/



https://messervices.cyber.gouv.fr/

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

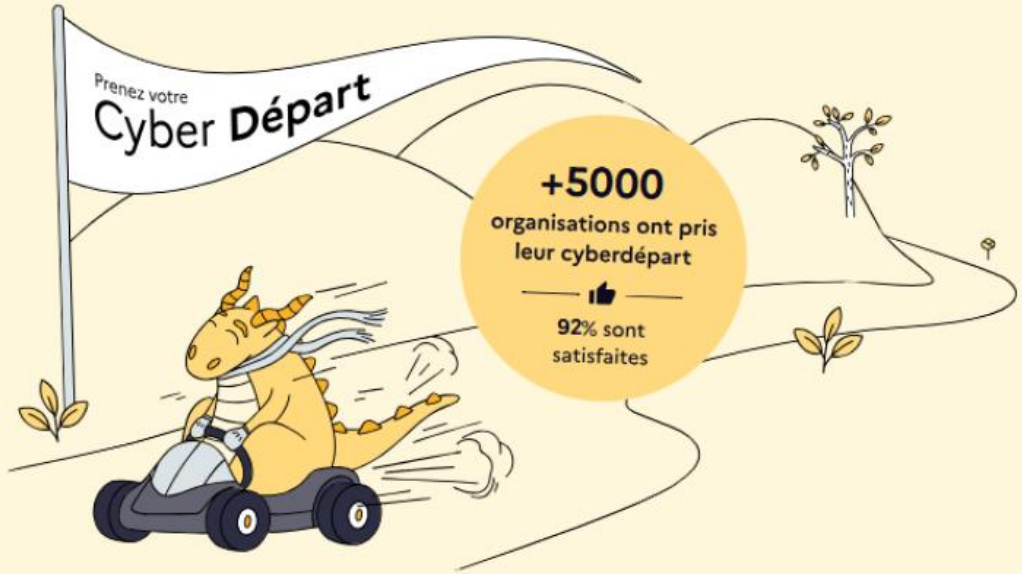
Retour

Vous souhaitez vous protéger contre les cyberattaques mais ne savez pas comment vous y prendre ?

Prenez votre cyberdépart ! Bénéficiez d'un **premier diagnostic gratuit accompagné d'un Aidant cyber** et recevez **6 recommandations prioritaires** à mettre en place pour améliorer la cybersécurité de votre organisation.

✓ Dans vos locaux ou en visio ✓ Rapide (1h30)

Ce diagnostic proposé par l'État n'est pas adapté aux particuliers et aux entreprises mono-salariées.



Recherchez votre organisation

ex : 13261762000010, Agglomération de Mansart, Société Y

https://messervices.cyber.gouv.fr/cyberdepart

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Accueil > Les services et ressources cyber > Réflexes Cyber

Outil

Réflexes Cyber

Simuler une crise cyber

Accéder au service

https://messervices.cyber.gouv.fr/ressources/reflexes-cyber.html

https://monespacenis2.cyber.gouv.fr/

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CERT-FR

Club SSI

Inscription FAQ EN

NIS 2 : Pré-enregistrer mon entité BETA

Anticiper l'obligation d'enregistrement

La directive européenne NIS 2 permet d'élever le niveau de cybersécurité des entités essentielles et entités importantes par l'application de règles harmonisées et simplifiées.
Dans le cadre de sa mise en œuvre, et dans l'attente de l'entrée en vigueur de l'obligation d'enregistrement qui interviendra avec la publication des textes réglementaires, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) met à disposition des entités un service de pré-enregistrement pour leur permettre d'anticiper cette étape.
Le pré-enregistrement constitue la première brique de l'entrée en vigueur de NIS 2 et un premier pas pour les entités dans le respect de leurs obligations.

- Pourquoi pré-enregistrer mon entité ?
- Comment s'assurer que mon entité est concernée ?
- Qui peut pré-enregistrer puis enregistrer mon entité ?
- Comment procéder au pré-enregistrement de mon entité ?

https://club.ssi.gouv.fr/#/nis2/introduction

RÉPUBLIQUE FRANÇAISE

Le présent outil de comparaison de référentiels est mis à disposition par l'Agence nationale de la sécurité des systèmes d'information (ci-après, l'Agence) à titre purement informatif et indicatif, afin de faciliter la compréhension par l'écosystème du référentiel NIS 2 qu'elle a élaboré.
Afficher la suite

Exigences applicables à NIS 2

Exporter le tableau

Télécharger les exigences
PDF - 965,8 ko

Télécharger le suivi des modifications
PDF - 1 383,4 ko

Comparaison entre référentiels d'exigence

Comparez les exigences issues du référentiel cyber français (ReCyF) applicables à NIS 2 à celles d'autres référentiels.

ReCyF (NIS 2) | Sélectionner

Type d'entité: Sélectionner une option

Objectif de sécurité: Sélectionner une option

Thématique: Sélectionner une option

https://messervices.cyber.gouv.fr/nis2#exigences

Merci pour votre attention

Guillaume CREPIN

Délégué ANSSI pour l'Ile de France

Ile-de-France@ssi.gouv.fr

Conférence Institutionnelle
ESMS

Margaux BUGUET
Responsable de mission – ESMS – ANS

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

La menace cyber dans le médico-social : une menace qui reste toujours prégnante

« La question n'est plus de savoir si mais quand nous allons être touchés »

DSI des PEP CBFC

204

déclarations d'incidents dans des ESSMS

113

incidents d'origine malveillante

Les missions du CERT Santé sont multiples : réponse à incidents (traitement des déclarations d'incidents de sécurité et intervention d'urgence à distance), veille proactive, sensibilisation et partage, audits d'exposition sur internet.

Quelles premières actions mettre en place ?

Contacter votre CRRC

*« Nous invitons les ESMS à se faire accompagner **par leur CRRC** (centre régional de ressources cyber) car une cyberattaque, ça peut arriver à tout le monde. C'est important de pouvoir **se projeter** et **de connaitre les points où nous sommes en fragilité**. Ça permet également de rendre la cybersécurité **tangible** »*

Directeurs, L'Olivier Bleu

- Réalisez un **exercice de crise** et/ ou un **diagnostic de cybersécurité**
- Mettez en place des premières actions **concrètes, structurées et adaptées** à votre contexte* :
  - Limiter le nombre de postes administrateur et mettre régulièrement à jour l'inventaire du parc informatique
  - Mettre en place et tester les sauvegardes
  - Imposer une certaine complexité dans les mots de passes et déployer la double authentification lorsque cela est possible
  - Lister les activités et les informations dites « essentielles » à protéger en priorité
  - Faire des revues de compte de manière régulière
  - Documenter vos process et procédures, et prévoir un annuaire papier avec les contacts de la structure
  - Sensibiliser régulièrement les professionnels
- Disposez d'un suivi régulier afin de vous aider à mettre en place **votre plan d'action**

** Exemples d'actions mises en place par des ESMS à la suite d'un exercice de crise ou d'un diagnostic cyber, accompagnés par leur CRRC. Cette liste est non exhaustive et doit s'adapter à votre contexte*

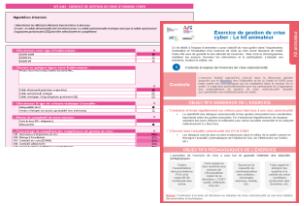
Où retrouver la documentation ?

Page Cybersécurité pour le médico-social

Cycle de webinaires dédiés au médico-social

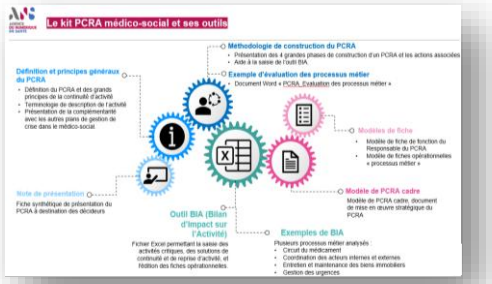
Guide cybersécurité en 13 questions

Kits Exercices de crise



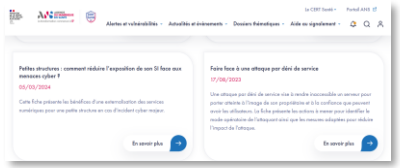
Pourquoi réaliser un exercice de crise ? RETEX de la Ligue Havraise

Le kit PCRA pour le médico-social



Modules sur la thématique cyber

Fiches thématiques – portail cyberveille



Offre de service des CRRC

L'OPSSIMS – Observatoire Permanent de la Sécurité des Systèmes d'Information dans le Médico-Social

Conférence Institutionnelle

ESMS:

Accompagner les ESMS pour augmenter la résilience du secteur médico-social face aux risques cyber

Mohcine EL OUBNANI

Chef de projet – Référent Filière ESMS – SESAN

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Le médico-social : une diversité de structures et de pratiques

Handicap

IME · ESAT · EAM/MAS/FAM · SESSAD

Transformation de l'offre · Dispositifs · Inclusion
75% d'équipement DUI

Protection De l'Enfance

MECS · Pouponnières · Services éducatifs

Mineurs protégés · Secret professionnel
Sensibilité des données · 50% d'équipement DUI

Personnes Âgées

EHPAD · Résidences autonomie · CRT

Perte d'autonomie · Turn-over
80% d'équipement DUI

Médico-social

Domicile

SSIAD · SAD · SAAD

Hors les murs · Mobilité
Outillage fragmenté · 35% d'équipement DUI

Accueil, Hébergement, Insertion

CHRS · CHU · Résidences sociales · FJT

Parcours d'insertion · Culture de l'oral
Hétérogénéité des pratiques · 30% d'équipement DUI

Personnes à Difficultés Spécifiques

LHSS · LAM · ACT · CAARUD · CSAPA

Publics complexes · Santé/social imbriqués
Variabilité des parcours · 40% d'équipement DUI

Un même organisme gestionnaire peut couvrir plusieurs de ces champs d'accompagnement simultanément.

Des réalités hétérogènes appellent des réponses différenciées.

Un contexte structurellement en tension dans les ESMS

Budget
- Pilotage serré
- Traçabilité renforcée
- Contrôles et indicateurs
- Marges limitées

RH
- Recrutement difficile
- Intérim encadré
- Exigence qualité accrue
- Risque juridique renforcé

Réformes
- Sérafin-PH
- Transformation de l'offre
- Logique de parcours
- Responsabilité gestionnaire

Sans appropriation du numérique
- Décider dans l'urgence
- Déployer pour « se couvrir »
- Déconnecter attentes et résultats
- S'exposer : cyber, juridique, continuité

= Instabilité structurelle

Le numérique n'est plus un projet. C'est un facteur de soutenabilité ou de fragilisation.

Quand la cyberattaque touche les personnes accompagnées

MDPH attaquée :

- 4 mois sans versement AAH
- Retards de loyer
- Ruptures de droits
- Familles sans réponse
- Salariés RQTH empêchés de travailler

Incidents sous-déclarés — ampleur réelle bien supérieure.

Échéances convergentes

- NIS2 (2028-2029)
- Ségur V2 (2027-2028)
- Sérafin-PH
- Évaluations HAS

Les enjeux pour SESAN avec les ESMS

1

Mieux connaître la situation du terrain

- Consolider l'état des lieux cyber, par couloir
- Repérer la sous-déclaration des incidents
- Identifier ce qui fonctionne et capitaliser

2

Adapter l'approche à la diversité des métiers

- Diversité des publics, des professionnels, des pratiques
- Expositions et usages différents par couloir
- Partir des réalités métier, pas seulement de la technique

3

Inscrire la cybersécurité à tous les niveaux

- Gouvernance des OG et projets d'établissement
- Encadrement, réunions d'équipe, formation continue
- Pratiques métier des professionnels
- **Construire une culture cyber – Sensibiliser dans la durée**

La cybersécurité devient une condition de pérennité pour les ESMS.

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

ESMS & structures de coordination :

Comment se préparer aux cyberattaques ?

Martine SOUPIN
Directrice – ASDMR SSIAD Melun

Florence BERNARD
Directrice de la Résidence Gabrielle D'Estrées – Fondation Partage et Vie

Audrey DEFRANCE
Infirmière Coordinatrice – ASDMR SSIAD Melun

Maître Marguerite BRAC DE LA PERRIERE
Avocate – Cabinet Charles Russell Speechlys

sesan Île-de-France
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

ESMS & structures de coordination :

Comment se préparer aux cyberattaques ?

Martine SOUPIN
Directrice – ASDMR SSIAD Melun
Audrey DEFRANCE
Infirmière Coordinatrice – ASDMR SSIAD Melun

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

ASDMR SSIAD DE MELUN : Qui sommes nous?

- Un service de soins infirmiers à domicile
- Une file active de 130 usagers
- 60 salariés

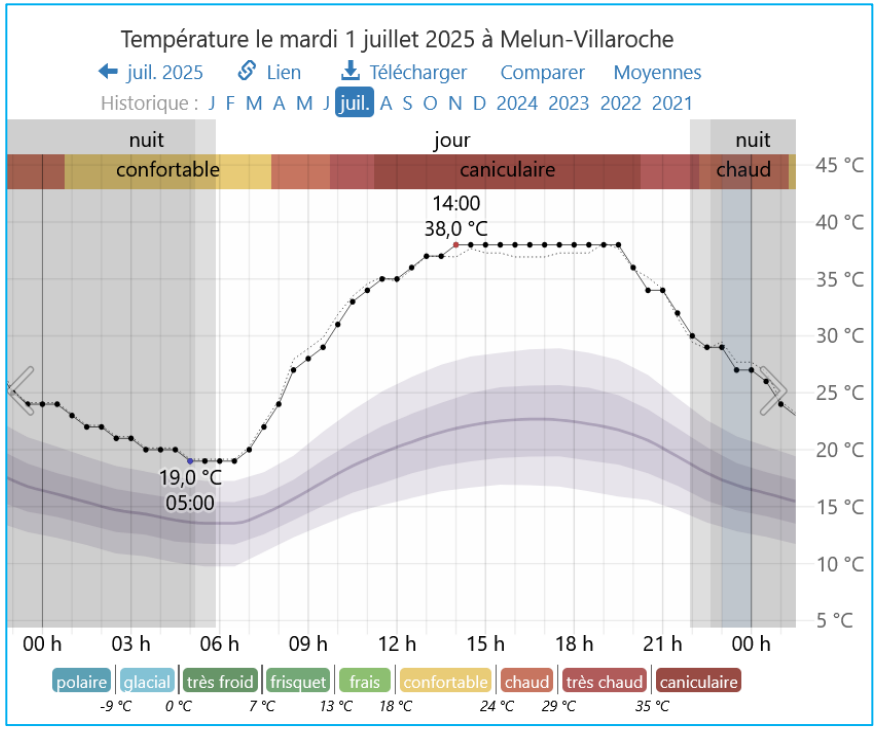
- Un prestataire informatique N.
- Un parc informatique : un serveur physique et des sauvegardes sur NAS et serveur virtuel
- Un VPN pour les connexions à distance

- 45 téléphones avec applications métiers
- Un logiciel métier dans le Cloud
- Contrat d'assurance Cyberattaque

Tout a commencé en même temps que la canicule: le 30 juin 2025

- Contexte dégradé: congés + crise canicule
- Jour J 20h… : Découverte de l'attaque : Ransomware

(intrusion par le VPN)



- J+1 « Cellule de crise » :

La directrice et 2 IDEC : Répartition des tâches

Une directrice qui gère la cyberattaque et les IDEC qui gèrent la continuité des soins

SSIAD Melun

- 11h41 : l'expert désigné par l'assurance laure B. me contacte et me met en relation avec le CERT Almond (Computer Emergency Response Team)

  (je l'aurai au téléphone au moins 2 fois par jour pendant 15 jours)
- 12H10 à 16h30 : dépôt de plainte au commissariat
- 18h42 : J'informe le CERT Santé, ARS

J+2

- 7h32 :Information au CSE
- 8h35 : déclaration d'évènement indésirable grave sur le site de l'ARS.
- 11h30 à 12h30 : 1ere déclaration à la CNIL
- Les IDEC s'organisent avec la comptable, la secrétaire et l'assistante RH qui ne peuvent plus se connecter au serveur pour l'organisation des plannings de présence des salariés (pool de vacataires, interim en plein été, congés)
- Les informaticiens ont nettoyé un poste et permis l'accès au logiciel métier (1 poste pour 10 personnes: direction, IDEC, IDE, accueil) avec partage de connexion avec les téléphones pro et perso.
- Mise en place d'un planning d'accès à ce poste en fonction des horaires et missions de chacun
- Découverte du fonctionnement du service en mode papier

Un sprint suivi d'un marathon…

- Tous les soirs, pendant 2 semaines de 18h à 20h : visio avec le CERT et nos informaticiens : le CERT Almond guidera nos informaticiens pour la reconstruction et pour évite le nouveau piratage.
- **J+ 3** : Je suis contactée avec la Brigade de la Cybersécurité
- Certaines collègues sont éprouvées : la secrétaire est en arrêt maladie, la comptable rentre chez elle
- Les soignants comprennent la situation de crise et soutiennent/ préservent l'équipe administrative
- **J+8** : remise en fonctionnement de l'imprimante du service
- Mais les soins continuent et le service fonctionne pour les soins aux personnes âgées

Le marathon…

- **J+4** : Communication orale avec un texte fourni par le CERT Almond auprès des salariés
- **J+17** : déclaration modifiée à la CNIL
- **J+ 28** : communication aux usagers
- **J+30** : la reconstruction de la paie de juin 2025 et réalisation des paies de juillet dans l'urgence
- **De Aout à décembre 2025** : reconstruction de la comptabilité 2025 et reprise de tous les dossiers laissés en attente
- Saisir dans les logiciels toutes les informations prises sur papier durant 3 semaines
- Contractualisation avec un DPO externe
- Suivi de la mise en œuvre des préconisations du CERT Almond avec le DPO

ESMS & structures de coordination :

Comment se préparer aux cyberattaques ?

Florence BERNARD
Directrice de la Résidence Gabrielle D'Estrées
Fondation Partage et Vie

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars
Agence Régionale de Santé
Île-de-France

ESMS & structures de coordination :

Comment se préparer aux cyberattaques ?

Maître Marguerite BRAC DE LA PERRIERE
Avocate – Cabinet Charles Russell Speechlys

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

CRRC Ile-de-France
Centre Régional de Ressources Cybersécurité

Pitch SESAN :
Quelles actions pour les ESMS ?

sesan
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

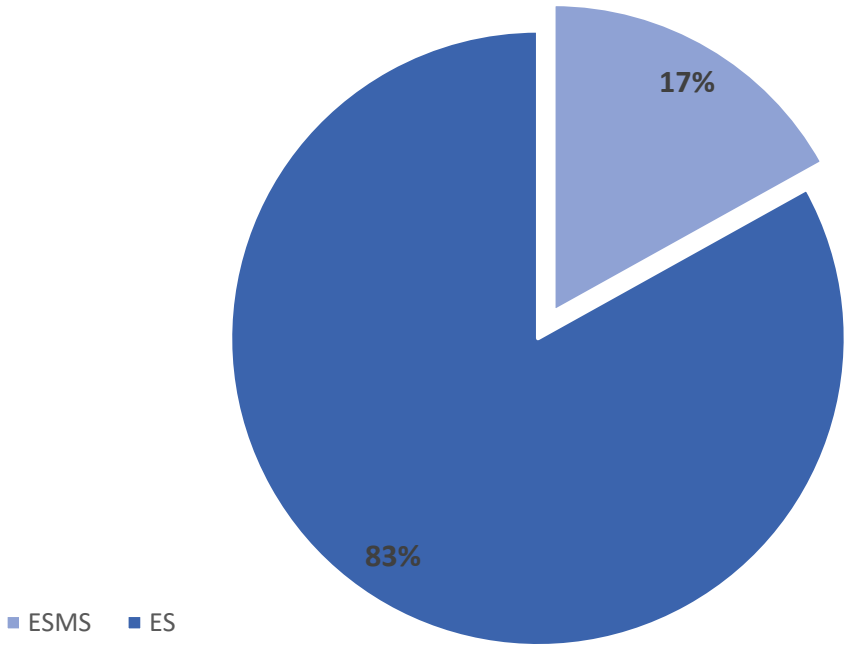
ars Agence Régionale de Santé Île-de-France

SESAN est le Groupement Régional d'Appui au Développement de l'eSanté (GRADeS) d'Île-de-France.

Le Département SSI de SESAN c'est :

- **7 Consultants** en SSI et RGPD,
- Plus de **130 adhérents**.

Répartition des Adhérents



Offre Cyber spéciale ESMS

Un large panel de services couvrant les principales thématiques cyber :

- Conformité
- Sensibilisation
- Détection
- Protection
- Résilience

CONFORMITE

Comment se conformer aux exigences de sécurité ?

RSSI

Resp. Sécurité des systèmes d'information)

Accompagnement par un RSSI ou consultant SSI dans vos missions cyber.

DPO

Délégué à la protection des données

Accompagnement par un DPO dans vos enjeux de conformité et de protection des données.

SENSIBILISATION

Comment sensibiliser les professionnels à la cybersécurité ?

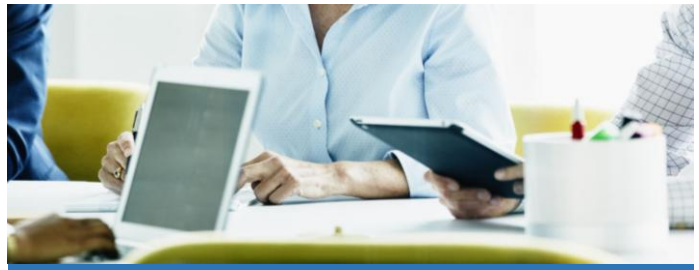
Campagne de sensibilisation

Sensibilisez vos collaborateurs aux bonnes pratiques SSI

- Vidéos
- Quizz
- Jeu de cartes

Test de Phishing

Testez la réaction de vos collaborateurs à une tentative de Phishing/hameçonnage.



Exercice de Cybercrise

Formez vos équipes à bien réagir en cas de cybercrise.

DETECTION

Comment détecter les vulnérabilités du SI de l'établissement ?

Test d'intrusion

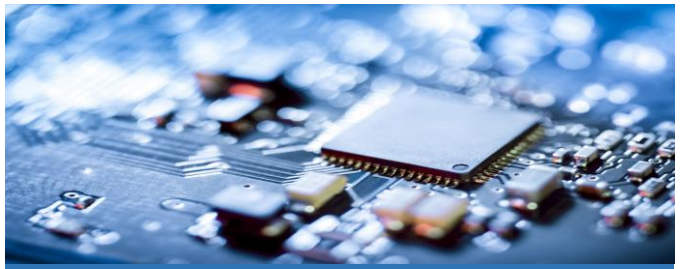
Testez la sécurité de votre système d'information par simulation des actions d'attaquants et découvrez les failles de votre SI.

Cybersurveillance

Surveillez en continu votre exposition sur Internet.

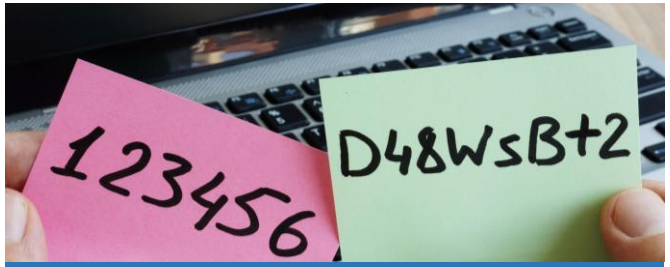
PROTECTION

Comment protéger les informations ?



Expertise Technique

- Sécurisation serveur
- Sécurisation AD
- Sécurisation réseau



Gestionnaire de Mots de Passe

Solution centralisée de coffre-fort à mots de passe.

Echanges sécurisés

Solution d'échange sécurisé de messages et de documents.

RESILIENCE

Comment se préparer et réagir en cas d'incident majeur ?

Experts en Continuité d'Activité

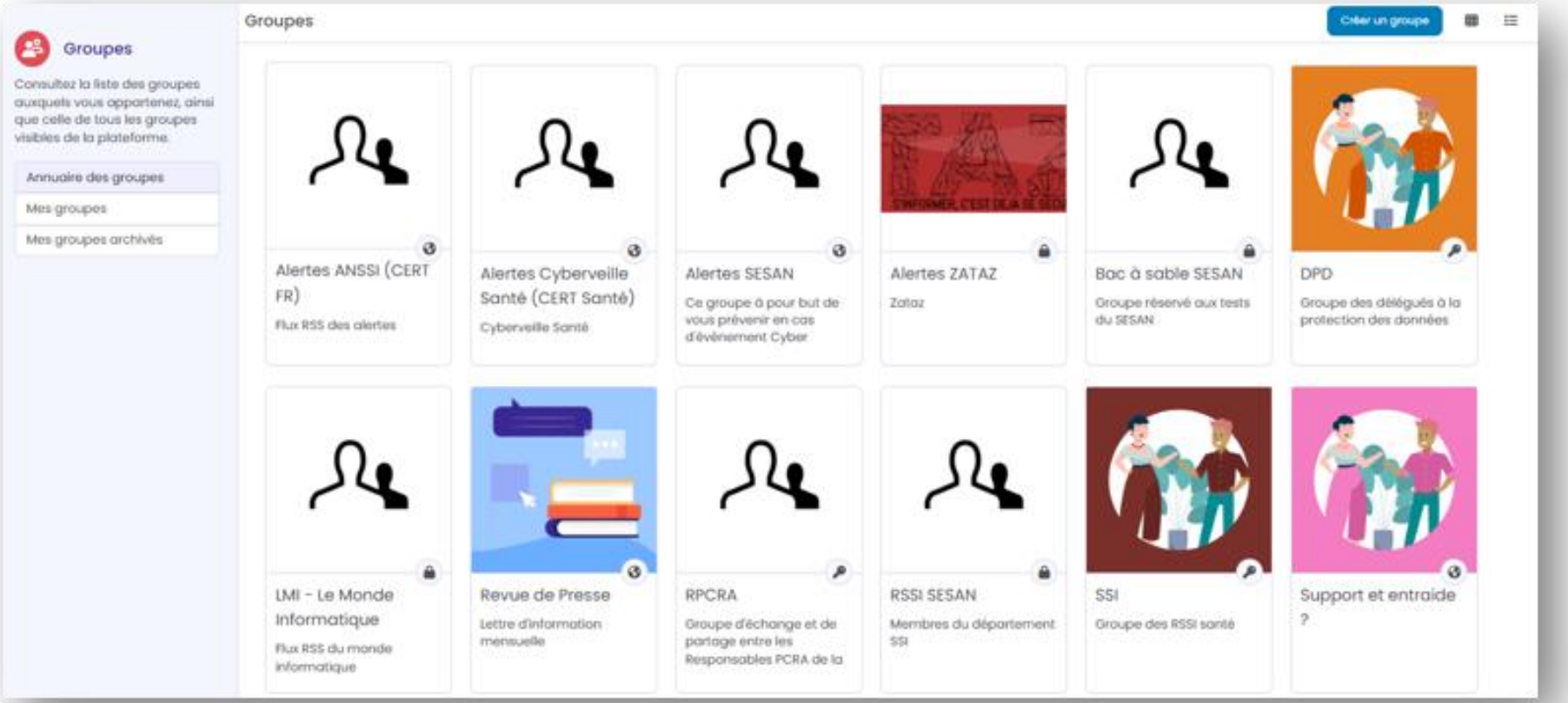
Accompagnement pour la rédaction de vos Plans de Continuité d'activité (PCA)

Solution de Continuité d'Activité

Sauvegardez vos données essentielles pour continuer l'activité en cas de crise.

Forum d’échanges : Jamespot

Un réseau social communautaire piloté par le GRADeS à destination des référents sécurité des structures de santé de la région.



Retours de nos adhérents (* enquête de satisfaction 2024)

Disponibilité

Accompagnement

Réactivité

Dynamisme

Rapide

Sympathique

Maitrise le sujet de la sécurité

Satisfaction de nos adhérents

95% satisfaction sur l'ensemble des services SSI en 2025

96% satisfaction sur la réactivité de l'équipe SSI à vous répondre à vos questions.

Pourquoi pas vous ?

Pause networking & visite des stands

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

ESMS & structures de coordination :

→ Se mettre en ordre de marche

Maud TISNE
Consultante SSI – SESAN

Docteur Sothea SAR
Présidente – CPTS PARIS 6 et 7

Virginie GOURRAUD
Consultante Formind

Christophe DOUESNEAU
Directeur Général – HOVIA

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

ESMS & structures de coordination :

→ se mettre en ordre de marche

Maud TISNE
Consultante SSI – SESAN

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Guichet Unique d'accompagnement pour les ESMS

Le Centre Régional de Ressources Cyber (CRRC) Île-de-France, porté par l'ARS Île-de-France et le GIP SESAN, propose depuis 2024 aux ESMS publics et privés de la région (Entité Juridique), un dispositif d'accompagnement gratuit pour renforcer leur cybersécurité, intitulé : « Guichet Unique d'accompagnement pour les ESMS ».

Le guichet unique d'accompagnement comporte initialement 3 actions :

Un diagnostic MonAideCyber

Réalisation du diagnostic de maturité cyber gratuit d'environ **1h30** par l'équipe CRRC-SESAN au sein de votre entité ou en visio avec :

- ✓ **Le responsable informatique et/ou le prestataire informatique**
- ✓ **Un membre de la direction**

Une mesure corrective

Financement et mise en œuvre d'une des 6 actions prioritaires identifiées lors du diagnostic MonAideCyber.

Ne sont financées que les **prestations réalisées avec SESAN ou via le marché SESAN** (hors matériel), dans **les limites du budget du CRRC disponible**

Exercice de crise

Un exercice de simulation de crise cyber conçu à partir des kits fournis par l'ANS et adapté à leur structure, et animé par un prestataire spécialisé.

- **Pour plus d'information** : https://cyberservices.sante-idf.fr/crrc-idf/guichet-esms/
- **Pour toute demande contacter :** crrc@sesan.fr

Guichet Unique d'accompagnement pour les ESMS : Bilan 2025-2026

40

MonAide Cyber
INNOVATION ANSSI

Diagnostics MonAideCyber

réalisés auprès d'ESMS

9

Mesures de sécurité personnalisées financées

12

Exercices de crise cyber financés

Guichet Unique d'accompagnement pour les ESMS

RENFORCÉ

Depuis le 1er Janvier 2026, le Centre Régional de Ressources Cyber (CRRC) Île-de-France, porté par l'ARS Île-de-France et le GIP SESAN, renforce le guichet unique ESMS en y intégrant des actions complémentaires :

Le guichet unique d'accompagnement s'étoffe avec l'ajout de 5 actions complémentaires :

1. **Journées d'accompagnement RSSI**
2. **Journées d'accompagnement DPO**
3. **Audit d'exposition internet**
4. **Cartographie du SI**
5. **Espace de stockage pour la continuité d'activité**

La phase pilote du guichet unique renforcé est complète et réservée aux 20 premiers candidats au S1 2026.
Une phase de généralisation, ouverte à tous, est prévue au S2 2026.

- **Pour candidatez, complétez le formulaire :** https://forms.office.com/
- **Pour plus d'information** : https://cyberservices.sante-idf.fr/crrc-idf/guichet-esms/
- **Pour toute demande contacter :** crrc@sesan.fr

ESMS & structures de coordination :

→ se mettre en ordre de marche

Docteur Sothea SAR
Présidente – CPTS PARIS 6 et 7
Virginie GOURRAUD
Consultante Formind

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Lancement de la démarche de mise en conformité RGPD – CPTS Paris 6 & 7

Contexte :

- Règlement Général sur la Protection des Données en vigueur depuis mai 2018
- CPTS Paris 6 & 7amenée progressivement à traiter des données de santé
- Augmentation des risques liés à ces traitements
- Besoin d'être conseillée et d'engager les actions de remédiation nécessaire

Enjeux :

- Protection des données personnelles
- Confiance clients & partenaires
- Réduction des risques juridiques

Objectifs de l'accompagnement :

- Évaluer le niveau de conformité actuel
- Identifier les écarts et risques
- Définir un plan d'actions priorisé

Périmètre de la mission :

- Missions portées par la CPTS Paris 6 & 7
- Types de données traitées (clients, RH, prospects…)
- Outils & systèmes (CRM, SI, outils SaaS…)
- Acteurs impliqués

Méthodologie proposée

1. Cadrage & collecte d’informations
2. Cartographie des traitements
3. Analyse de conformité RGPD
4. Plan d’actions & recommandations

👉 **Approche pragmatique, adaptée à la taille de la CPTS Paris 6 & 7 et aux enjeux**

Couvrir les risques

Identification et priorisation des risques

Risques juridiques :
• Non-respect des obligations (registre, exhaustivité de l'information et recueil du consentement des personnes, …)

Risques sécurité :
• Fuite / violation de données
ex : réception en clair de documents comportant des données de santé > cas récent

Risques réputationnels :
• Perte de confiance des usagers

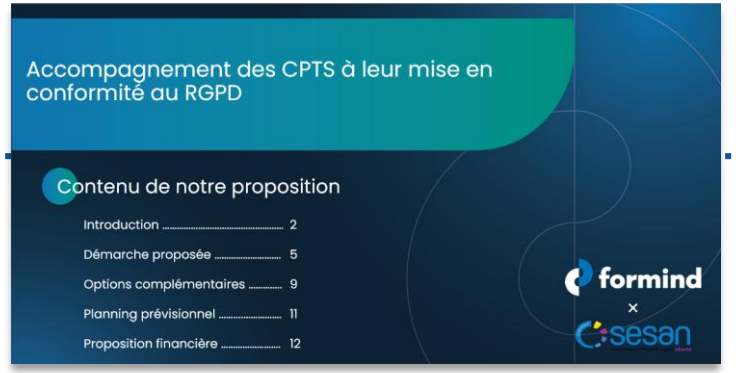
Risques opérationnels :
• Mauvaise gestion des droits (accès, suppression, limitation, …)
• Absence de règles de gestion du cycle de vie des données

Méthode d'analyse :
• Critères :
  • Probabilité d'occurrence
  • Impact (financier, juridique, image)

• Outils :
  • Matrice de criticité
  • Analyse d'impact (AIPD si nécessaire)

• Priorisation :
  • Risques critiques → traitement immédiat
  • Risques modérés → planifiés

Une offre sur-mesure pour les CPTS



L'accompagnement repose sur le modèle PDCA (Planifier, Déployer, Contrôler, Améliorer) pour assurer une amélioration continue de la conformité

Phase 1 : Diagnostic initial

- Cadrage, analyse de l'existant et évaluation de la maturité RGPD
- Initialisation du plan d'actions priorisé
- Sensibilisation

Phase 2 : Élaboration du registre des traitements

- Animation d'ateliers avec les acteurs métiers pour cartographier les données
- Assistance à la rédaction des fiches de traitement (en tant que Responsable de Traitement)

Phase 3 : Mise en Conformité Opérationnelle

- Déploiement du kit documentaire (politiques, procédures, mentions d'information, recueil du consentement, registres de suivi des demandes d'exercice de droits et des violations …)
- Réalisation d'une AIPD (Analyse d'Impact relative à la Protection des Données) pour les traitements sensibles

Livrables

- Registre des traitements
- Cartographie des traitements
- Analyse des écarts de conformité
- Plan d'actions priorisé
- Recommandations organisationnelles & techniques

Facteurs clés de succès

- Implication des équipes
- Sensibilisation des collaborateurs
- Suivi régulier des actions
- Amélioration continue

ESMS & structures de coordination :

→ se mettre en ordre de marche

Christophe DOUESNEAU
Directeur Général – HOVIA

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

HOVIA en quelques données

+ 3 000 personnes accompagnées

+ 60 établissements & services répartis sur
4 régions et 10 départements

50 sites géographiques

5 pôles : EHPAD, Handicap Bretagne, Handicap Hauts-de-France et Normandie, Handicap Île-de-France et Protection de l'enfance

+ de 1 300 salariés

100 M€ de budget annuel

Un contexte nécessaire à rappeler

Un sous-investissement ancien sur le numérique dans le secteur social et médico-social… et encore plus contraint sur certaines activités (ex. : protection de l'enfance…)

Des exigences identiques à toutes les entreprises et organismes gestionnaires… voir supérieures du fait des contraintes liées au secteur de la Santé

Ce que nous tentons de mettre en place à HOVIA (1 / 2)

Nous sommes aujourd'hui équipés d'une plateforme de cybersécurité Trend Micro qui couvre tous les points sensibles :

- les postes de travail
- les identités
- les services cloud
- la détection des attaques avancées

C'est un dispositif global qui renforce la sécurité de l'association et protège notre mission au quotidien

Ce que nous tentons de mettre en place à HOVIA (2 /2)

Une approche technique :

- La double authentification / MFA (pour le tenant Office 365)
- Un durcissement des mots de passe
- Des serveurs à jour avec des correctifs mensuels
- Une protection avec une suite de sécurité avec EDR
- Un pentest et un audit sécurité tous les 2 ans (en mécénat)
- Une procédure direction générale en cas de cybercrise
- Des exercices de cybercrise

Une approche pédagogique :

- Un mail mensuel du directeur général aux directeurs sur les risques cyber avec le calendrier SESAN
- Une newsletter tous les 3 mois de la DSI sur des trucs et astuces
- Une campagne régulière de test phishing
- Un projet de MOOC
- Une PSSI formalisée
- Une charte informatique et IA

Une approche à inscrire dans une démarche globale

Une gestion du numérique qui doit s'inscrire dans une logique organisme gestionnaire / taille critique… et de maitrise de son SI

Une tendance à l'externalisation

L'inscription dans une veille régulière (groupe de DSI, partenaires experts externes…)

Une veille sur les mises à jour et les nouveaux enjeux (NIS2 par exemple)

Un risque cyber à relativiser avec l'activité…

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Conférence

Madame Odile DUTHIL

Directrice Cybersécurité – Groupe Caisse des Dépôts,
Présidente du CLUSIF
(Club de la Sécurité Informatique Français)

ILE-DE-FRANCE sesan
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Cybersécurité dans le domaine de la santé
Quels risques émergents et quelles solutions pour les RSSI ?

Le Clusif

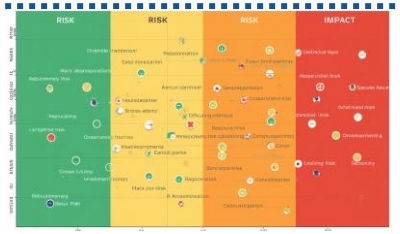
- Le Clusif est l'association de référence de la sécurité du numérique en France.
- Reconnue d'utilité publique le 28 novembre 2024, sa mission consiste à favoriser les échanges d'idées et de retours d'expérience à travers des groupes de travail, des conférences et publications.
- Il réunit tous les secteurs d'activité de l'économie autour de la cybersécurité et de la confiance numérique.
- Basé au Campus Cyber à la Défense, le Clusif relaie également ses actions en région et à l'international via les CLUSIR.
- 18 administrateurs
- 18 groupes de travail, 10 à 15 livrables par an, 6 conférences annuelles

Agenda

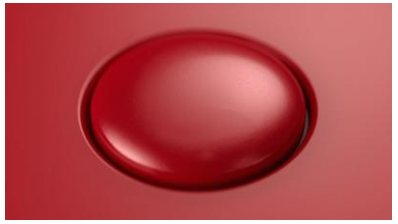
- Sommes-nous dans un monde plus risqué ?
- Les scénarios de risques
- Les risques liés aux ruptures technologiques
- Les risques liés à nos dépendances numériques

Sommes-nous dans un monde plus risqué ?

- Le risque cyber est le risque opérationnel le plus élevé, malgré nos DMR
- Le risque de Supply chain
  - 66 % des cyberattaques sont dues à un sous-traitant
  - Le SI d'une entreprise privée ou d'un établissement public est maintenant considéré dans sa globalité
  - C'est l'objet des réglementations NIS2/DORA
- Les risques liés aux ruptures technologiques
  - Hébergement dans le cloud
  - L'IA générative et l'IA agentique
  - Le quantique
- Le risque géopolitique
  - La dépendance numérique
  - Le kill switch

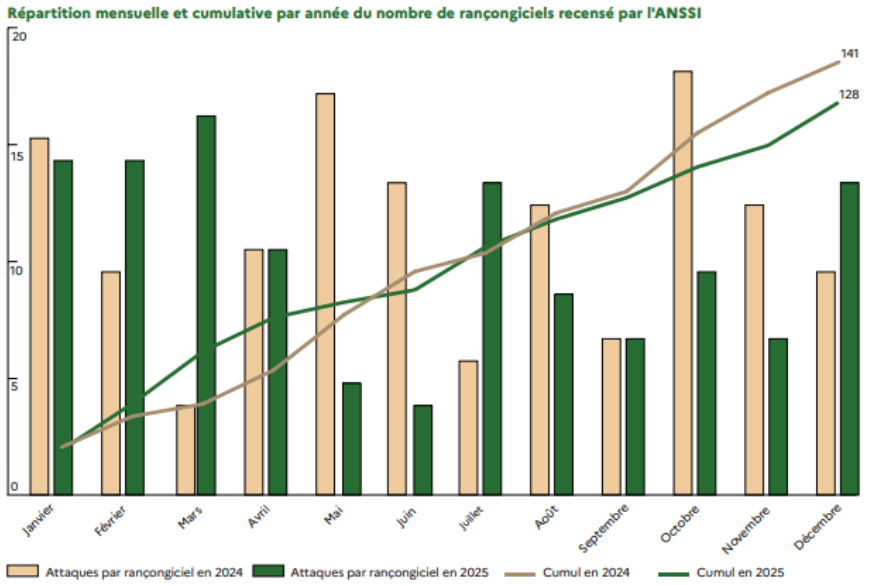


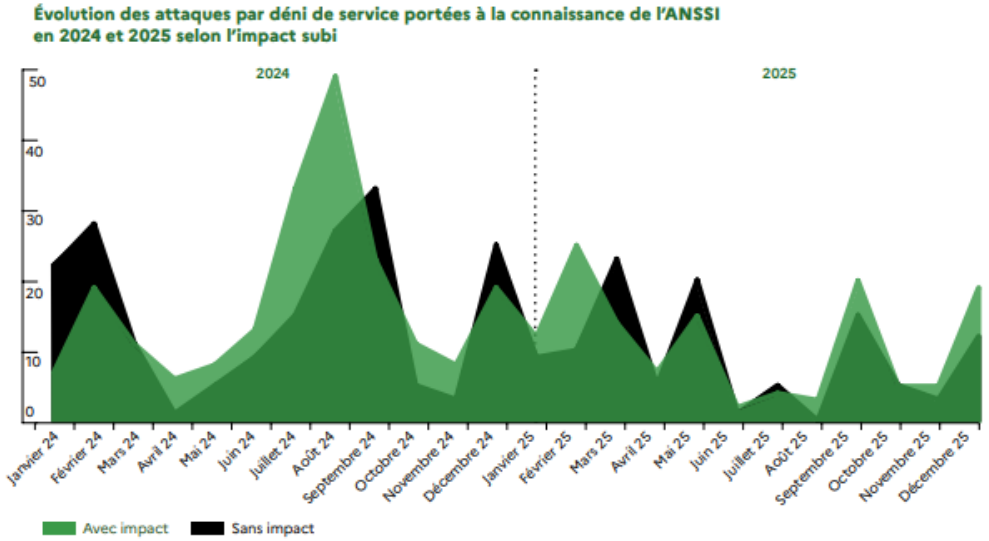
European Commission



Les scénarios de risques

- Ransomware avec perte totale ou partielle du SI
- Fuite de données
- DDoS
- Fraude au président





Les risques liés aux ruptures technologiques

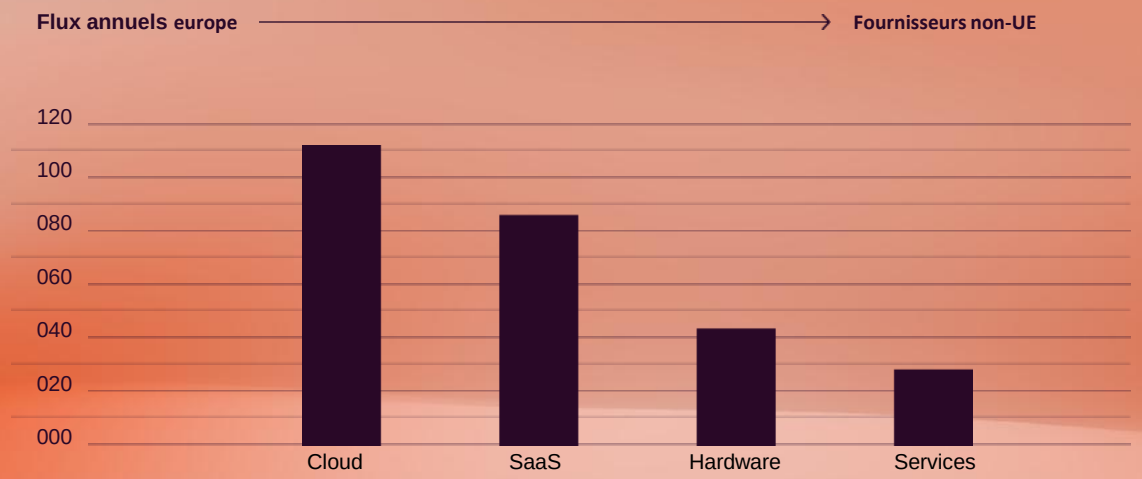
- Hébergement dans le cloud
  - Le Clusif a édité un livrable sur la souveraineté numérique dédié à l'hébergement dans le cloud
- L'IA générative et l'IA agentique
  - PSSI IA
  - Sécurisation de l'IA
- Le quantique
  - Replay de la conférence dédiée au quantique

La maitrise de nos dépendances numériques

À l'échelle macroéconomique

Chaque année, 265 Md€ de dépenses liées aux logiciels et services cloud à usage professionnel sortent de l'Union européenne – soit près de 80% du total des dépenses.

À trajectoire constante, ce montant pourrait atteindre 500 Md€ par an d'ici 2030.



Décomposition des flux financiers de l'Europe vers des fournisseurs extra-européens

265 Md€/an de dépenses numériques extra-européennes (≈1,5% du PIB de l'UE)

Sources : Cigref 2025 (Asterès), Commission Européenne Digital Decade 2025, Eurostat Cloud Services 2024, ECDPM Tech Sovereignty 2024

Une dépendance renforcée par l'évolution des modèles économiques

Le modèle de facturation des technologies s'est profondément transformé :

- D'un modèle de propriété (licences logicielles détenues par le client),
- À un modèle locatif (SaaS, y compris sur des infrastructures on-premise),
- Jusqu'à un modèle de consommation dynamique (Pay-As-You-Go, facturation à l'usage, à l'API ou au token, notamment en IA).

Cette évolution entraîne une perte de maîtrise des actifs numériques, des coûts difficilement prévisibles et une dépendance accrue aux fournisseurs en position dominante.

Des impacts multiples et systémiques

Ces dépendances ne sont pas uniquement techniques. Elles génèrent des risques :

- Économiques (volatilité des coûts, verrouillage fournisseur),
- Juridiques et contractuels,
- Géopolitiques et stratégiques,
- Opérationnels et de continuité d'activité.

Malgré l'ampleur de ces enjeux, les entreprises
ne disposaient jusqu'ici d'aucun instrument structuré pour mesurer et piloter leur niveau de dépendance numérique.

Objectif

Mettre à disposition des dirigeants :

- Un outil de pilotage stratégique global des risques IT et IA
- Des clés de lecture claires, consolidées et actionnables pour les Comex et les conseils d'administration

Clarifier les concepts

La démarche permet de distinguer et d'articuler :

- Souveraineté
- Dépendances
- Résilience

L'approche est globale, transverse et orientée business, couvrant l'ensemble du système d'information et des usages critiques.

L’IRN, un bien commun qui repose sur une démarche de co-construction

Une construction collaborative

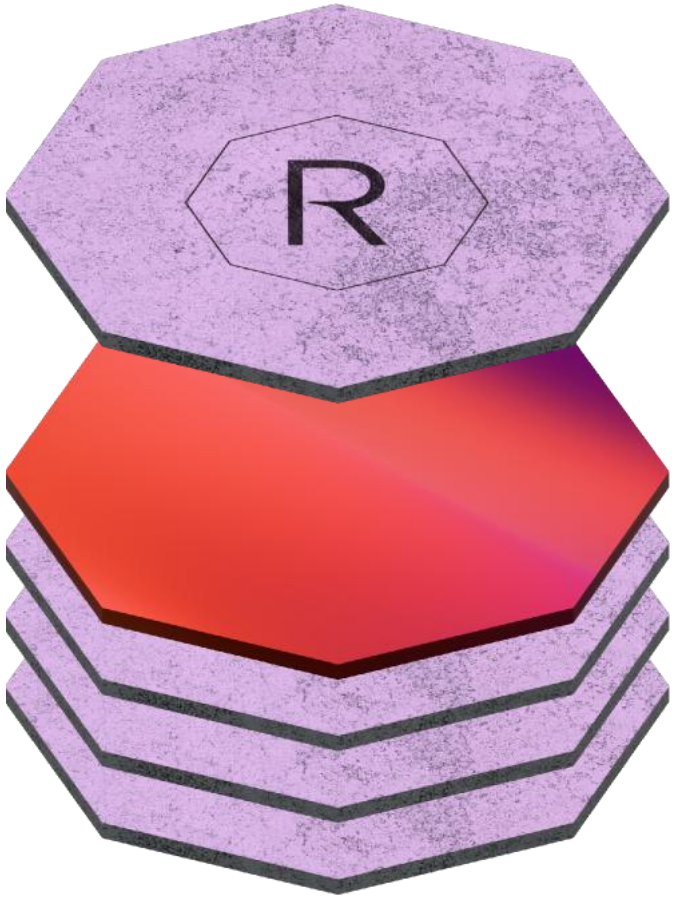
- 10 design partners issus de grands groupes et d’organisations de référence
- Contribution active du Cesin et du Cigref
- Supervision par un comité méthodologique indépendant

Un référentiel ouvert

- Logique de bien commun
- Licence Creative Commons
- Favorisant l’adoption, la transparence et l’amélioration continue

Une approche par les métiers vitaux

- Point de départ : les métiers et processus critiques de l'entreprise
- Reconstruction des systèmes critiques qui les supportent
- Décomposition en assets



Couche applicative (software)

Regroupe les modèles d'intelligence artificielle et d'apprentissage automatique chargés de l'analyse, de la prédiction et de l'automatisation intelligente.

Data

Plateforme

Infrastructure

Compétences

Une analyse structurée des dépendances

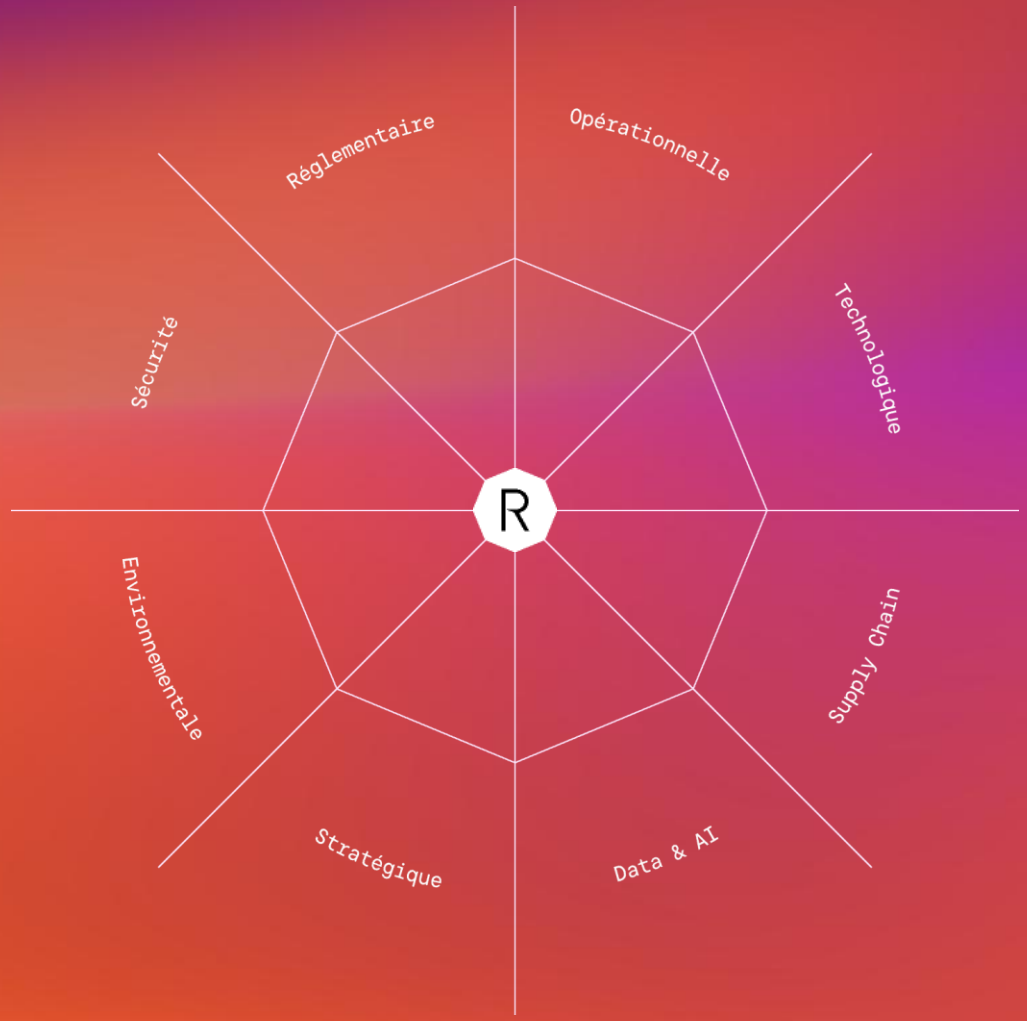
Identification de 8 grandes catégories de dépendances, inspirées notamment du Cloud Sovereignty Framework, enrichies par des dimensions complémentaires :

- Stratégique & géopolitique (killswitch)
- Économique & juridique (contrats et conformité)

- Opérationnelle (continuité d'activité)
- Sécurité & continuité (cyber)
- Environnementale

- Technologique
- Données & IA
- Supply Chain

Les 8 piliers de la résilience numérique



Questions/Réponses

Merci

Groupement d'Intérêt Public eSanté

TOUS CYBER VIGILANTS

07 Avril 2026 JOURNÉE DE LA CYBERSÉCURITÉ

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Régionale de Santé Île-de-France