# Agora

## Programme CaRE : point d'étape, actions à venir

21 mai 2026

# Les intervenants

## Direction programme

**Christophe MATTLER**
Directeur de Projet
MINISTÈRE DU TRAVAIL, DE LA SANTÉ, DES SOLIDARITÉS ET DES FAMILLES

**Estelle NICAUD**
Directrice de Programme
AGENCE DU NUMÉRIQUE EN SANTÉ

**Ange HIRSCH**
Expert cybersécurité
AGENCE DU NUMÉRIQUE EN SANTÉ

**Laure HELENE-DUHESME**
Chargée de mission
ANSSI Agence nationale de la sécurité des systèmes d'information

**Gilles LAROCHE**
Chef de projet cybersécurité
GIP e-santé Bretagne

1. Bilan global 2025-2026 du programme CaRE
2. NIS2
3. Focus Axe 2 – Les CRRC
4. Focus Axe 4 – Les domaines de sécurité opérationnelle
5. Les prochains travaux du programme CaRE

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

# BILAN GLOBAL 2025-2026 DU PROGRAMME CaRE

19 AU 21 MAI 2026

SANTEXPO 2026

# Rappel sur le plan d'action du programme

## Gouvernance et résilience

Renforcer la gouvernance et la résilience en cybersécurité dans le secteur de la santé, en articulation avec les niveaux national, régional et local

## Ressources et mutualisation

Prise en compte de la pénurie de talents et de ressources dans les établissements, et mise en avant du besoin de mutualiser et de pérenniser les ressources humaines.


## Sensibilisation

Encourager un engagement fort de chacune des parties prenantes de la cybersécurité dans les établissements de santé.

## Sécurité opérationnelle

Soutenir financièrement les investissements jugés prioritaires via des « Domaines » (via des appels à financements et/ou appels à projets).


*Le plan d'action du programme CaRE se décline autour de 4 axes*

# Réalisations 2025 - 2026

## AXE 1
## Gouvernance et résilience

***Préparation de la réponse aux crises cyber***

- Portage des actions d'élaboration des **PCRA**, de leurs **tests** et de l'**intégration** d'un **volet numérique** au plan blanc au **domaine 2**

***Démarche d'auto-évaluation de la maturité par les ES et ESSMS***

- **Publication d'une nouvelle version de l'OPSSIMS** destiné aux ESSMS
- Evaluation de la **maturité sur l'identification électronique intégrée à HospiConnect**

## AXE 2
## Ressources et mutualisation

***Catalogue des offres cyber mis à jour mensuellement***

- **493** offres publiques et **549** offres d'industrielles recensées (ouvert aux industriels depuis 2024)

***CRRC***

- **Montée en puissance** des CRRC lancés en 2024 et soutenus à hauteur de **26 M€** dont **8 M€** dédiés au secteur médico-social

## AXE 3
## Sensibilisation

***Etude de perception des risques cyber dans les ES***

- **Publication** de l'étude menée auprès de **700 directeurs hospitaliers**

***Témoignages***

- **Partage** de plusieurs **RETEX** d'établissements sur **la gestion de cyberattaques**

## AXE 4
## Sécurité opérationnelle

***Domaines prioritaires***

- **Atteinte des cibles du Domaine 1** « Annuaires techniques et exposition sur internet » par 939 candidats sur 1181
- **Lancement du Domaine 2** « Stratégie de continuité et de reprise d'activité »
- **Lancement de la généralisation HospiConnect,** portant sur les thématiques d'identification électronique
- **Lancement du POC de l'AAP médico-social** avec 3 parcours déclinés selon la maturité des ESSMS

# Etude de perception sur les risques cyber

## Contexte

Une enquête nationale a été réalisée auprès de 719 directeurs d'établissements de santé afin de comprendre comment les établissements perçoivent les risques cyber et les leviers d'amélioration. De cette étude émerge quelques enseignements :

- **La cybersécurité : une compétence technique à une compétence stratégique au cœur des arbitrages des Directeurs des établissements de santé**
- **La continuité des soins, priorité des Directeurs d'établissements de santé en cas de cyber attaque : un atout pour renforcer la confiance des usages**
- **La coopération et la mutualisation des expertises territoriales considérées comme levier de performance par les directeurs d'établissements de santé**
- **Le soutien financier du programme considéré comme nécessaire et à pérenniser**

Pour plus d'informations sur cette étude, n'hésitez pas à visiter le site de l'ANS !

**Scannez-moi**

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

# ANSSI
# Point d’étape NIS 2

19 AU 21 MAI 2026

SANTEXPO 2026

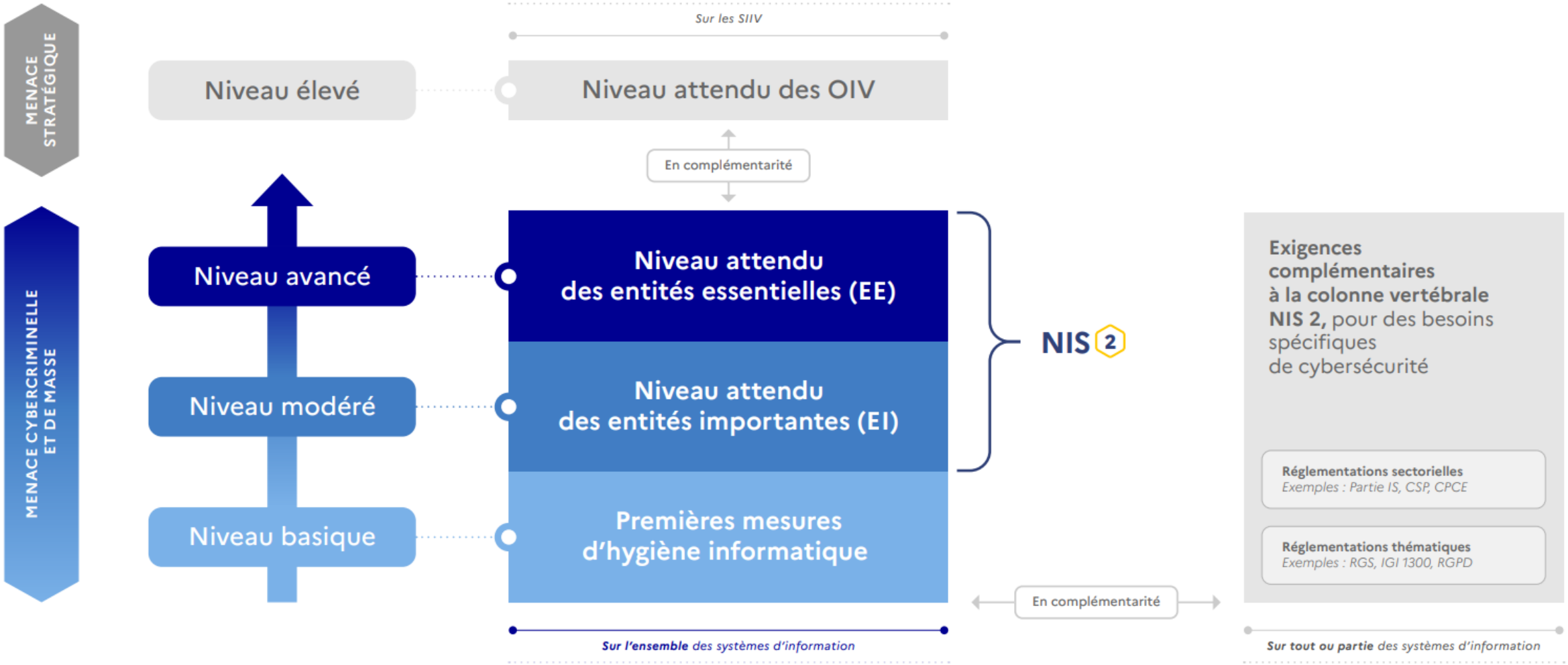
# NIS 2 : un changement de paradigme par rapport à NIS 1 pour faire face à une menace devenue systémique

| | |
|---|---|
| **Constat** | D'une menace principalement ciblée à une menace également opportuniste |
| **Cible** | Touche l'ensemble du tissu économique, y compris les plus petites structures (PME/ETI, collectivités territoriales, associations, etc.) |
| | Pour y répondre |
| **Changement d'échelle** | De quelques centaines d'entités **désignées** à plusieurs milliers d'entités majoritairement régulées selon une **logique de seuil** |
| **Niveau d'exigence** | Un niveau de sécurité imposé et adapté à la maturité et au profil de l'entité |
| **Sanctions** | Sanctions administratives proportionnées au type d'entité et à la gravité des manquements |

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

NIS 2

# NIS 2 : colonne vertébrale du cadre règlementaire de cybersécurité



# Pour les entreprises, 18 secteurs sont concernés dans 2 catégories

## Secteurs hautement critiques

- Administrations publiques
- Eaux potables
- Eaux non potables
- Énergies
- Espace
- Gestion des services Technologies de l'information et de la Communication (interentreprises)
- Infrastructures des marchés financiers
- Infrastructures numériques
- Santé
- Secteur bancaire
- Transport

## Autres secteurs critiques

- Fabrication, production et distribution de produits chimiques
- Fournisseurs numériques
- Gestion des déchets
- Industries manufacturières
- Production, transformation et distribution de denrées alimentaires
- Recherche
- Services postaux et d'expédition

| | | |
|---|---|---|
| **ETI et grandes entreprises** | **Entités essentielles (EE)** | **Entités importantes (EI)** |
| **Moyennes entreprises** | **Entités importantes (EI)** | |
| **Micro et petites entreprises** | **Entités non assujetties** | |

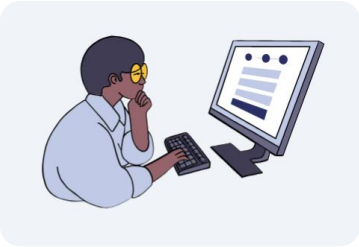
NB : Il existe certains cas particuliers pour lesquels l'assujettissement ne dépend pas d'un seuil (par exemple, les bureaux d'enregistrement et les agents agissant pour le compte d'un bureau).

# NIS 2 : les entités concernées dans le champ santé/social

- Présentation simplifiée basée sur la directive dans l'attente de l'aboutissement de la transposition

| | Grandes entités<br>~ ETP > 250 | Moyennes entités<br>~ 250 > ETP > 50 | Petites entités<br>~ ETP < 50 |
|---|---|---|---|
| **Périmètres spécifiques à la santé** | | | |
| **Prestataires de soins de santé** | Entités essentielles | Entités importantes | Hors périmètre NIS 2 |
| **Industrie pharmaceutique** | | | |
| **Fabricants de dispositifs médicaux** | | | |
| **Autres périmètres liés à la santé** | | | |
| **Administration publique** | Entités essentielles | | |
| **Infrastructures numériques et services TIC**<br>Périmètre soumis à un règlement d'exécution de la commission européenne | | Entités importantes | Hors périmètre NIS 2 |
| **Organismes de recherche** | | | |

# 3 obligations principales pour les EE et EI



**Enregistrer son organisation auprès de l'autorité nationale compétente. En France, l'ANSSI.**

**Notifier ses incidents importants et ses vulnérabilités critiques à l'ANSSI.***

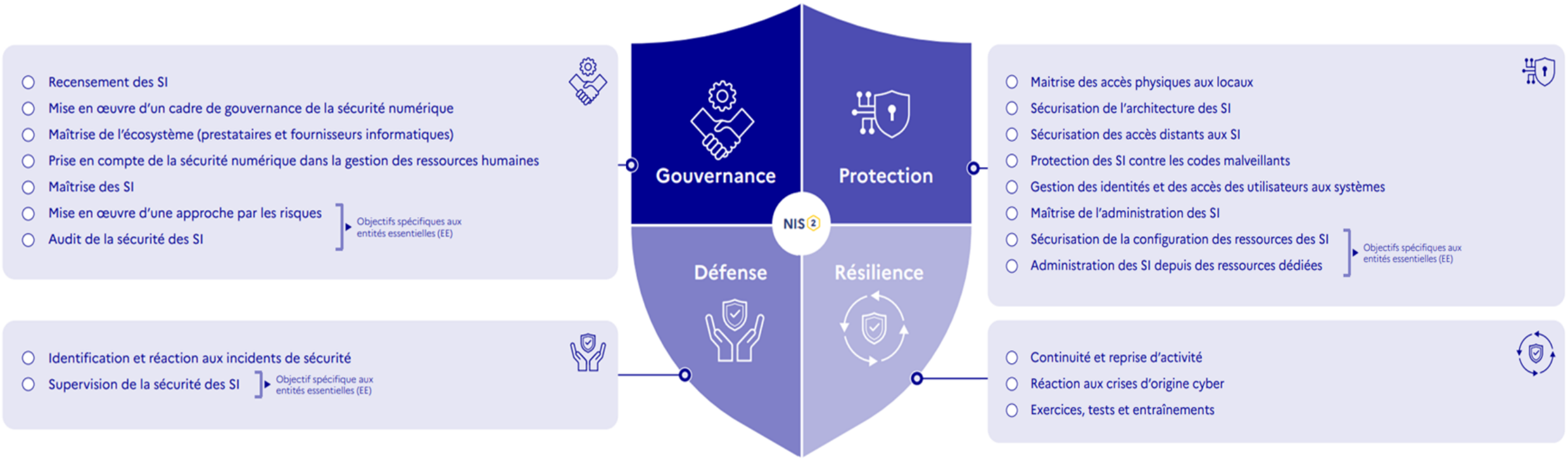
*** Pour les entités déjà concernées par une obligation de déclaration au CERT Santé, il est prévu que la notification NIS 2 puisse être faite au travers de la même démarche**

**Mettre en œuvre des mesures de gestion des risques, par le respect des objectifs de sécurité fixés par la transposition de la directive NIS 2.**

# Réduire ses risques cyber

## Le Référentiel Cyber France (ReCyF) applicable à NIS2

Le référentiel des exigences de sécurité (ReCyF) de l'ANSSI. 20 objectifs de sécurité obligatoires pour les EI et EE. Les objectifs 16 à 20 sont réservés aux EE.



# MesServicesCyber

- S’adresse à **toutes les entités publiques et privées souhaitant renforcer leur cybersécurité**.
- **2 cibles prioritaires** auxquelles est **réservé l’accès à certains services numériques** : les entités régulées **(i.e NIS 2**) ainsi que les **entités publiques** (État, collectivités territoriales)
- ***La plateforme est destinée à évoluer et proposer de nouveaux services***.


## Catalogue général

- Des ressources pour débuter en cybersécurité

- Des ressources pour approfondir ses connaissances

## Services NIS 2

- S’informer
- Se pré-enregistrer dès maintenant
- Ressources et outils **pour aider à réduire ses risques cyber**
- Déclarer un incident

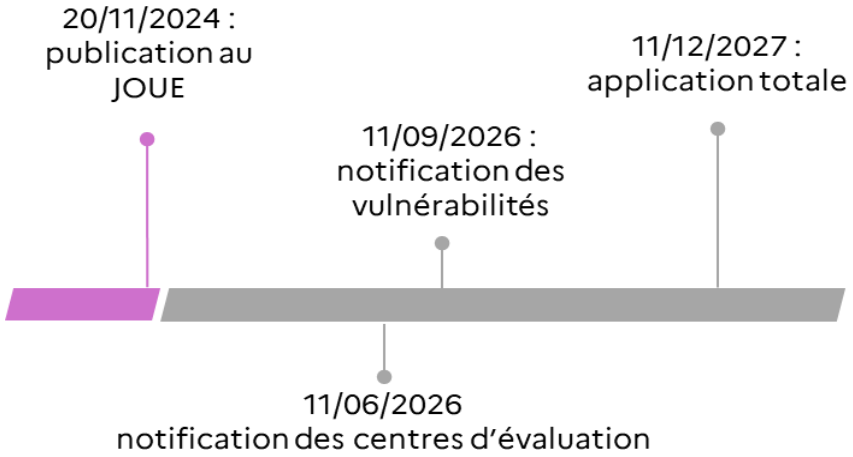
# En complément de NIS 2 : l'arrivée du Cyber Resilience Act (CRA)

Le règlement CRA prévoit des **exigences essentielles de cybersécurité sur les produits et sur la gestion des vulnérabilités**, et établit des **procédures d'évaluation de la conformité**.

Le CRA **vise à** :

- renforcer la **cybersécurité des produits comportant des éléments numériques** en établissant un cadre juridique uniforme ,
- imposer des obligations de cybersécurité aux **fabricants, importateurs et distributeurs**, dès la conception et tout au long du cycle de vie des produits ;
- renforcer la **transparence pour les utilisateurs.**

**Le règlement entrera en application progressivement entre juin 2026 et décembre 2027.**




**A noter :** les dispositifs médicaux **sont hors champ d'application** et traités dans le cadre des règlements européens dédiés aux dispositifs médicaux

# FOCUS AXE 2 – LES CRRC

# LES CRRC

## Contexte

Dans le cadre de l'axe 2 du plan d'action CaRE (Ressources et mutualisation), il est demandé aux ARS de mettre en place des **centres de ressources cyber (CRRC),** en charge de développer une offre de services répondant aux besoins prioritaires des établissements. Ces CRRC se sont vus attribuer plusieurs missions et **objectifs tant généraux que spécifiques**, propres au secteur du médico-social.

## Les enjeux

- Les CRRC poursuivent leur dynamique de structuration et sont de mieux en mieux identifiés par les établissements sanitaires, mais la mobilisation du secteur médico-social est à accélérer.
- Les CRRC développent de plus en plus d'initiatives de mutualisation (groupements d'achat, formations régionales, postes à déployer en cas d'incident…)

## Objectifs portés par les CRRC

- Animer la communauté cyber de la région
- Accompagnement aux exercices de crise cyber
- Renforcement de la maturité
- Sensibiliser les acteurs sanitaires et médico-sociaux en région
- Promouvoir les domaines CaRE auprès des ES/ESMS
- Diagnostic cyber
- Favoriser l'émergence d'initiatives autour de la cybersécurité
- Accompagner les établissements dans le déploiement du PCRA « CaRE »
- Soutenir les ES/ESMS dans l'atteinte des objectifs des différents domaines
- Accompagner la formation cyber des professionnels informatiques)
- Construire un échelon de réponse régional lors des incidents cyber (hors CERT)

Pour plus d'informations, n'hésitez pas à visiter le site de l'ANS !

**Scannez-moi**

*Mai 2026*

# Programme Care D2 « Stratégie de continuité et de reprise d'activité »

## Accompagnement en région Bretagne

# Une offre de services et des partenaires

GROUPEMENT RÉGIONAL e-santé BRETAGNE

Cyberdefense

Daspren

WaToo

ANOZR WAY

AIRBUS CYBERSECURITY


Cyberdefense

alcyconie

pwc

Crisalyde

Lexfo

PÔLE D'EXCELLENCE CYBER

# Phase préparatoire au D2 CaRE

**Mars 2025**

AMI pour le projet de co-construction d'une offre d'accompagnement pragmatique PCRA auprès des ES bretons

Sélection du prestataire pour l'accompagnement au projet

**Avril 2025**

GT n°1 du recueil des besoins d'accompagnement régional à Care D2

**Juillet 2025**

Parution du programme Care D2

**Septembre 2025**

GT n°2 du recueil des besoins d'accompagnement régional à Care D2

**Octobre 2025**

Groupes de travail pour la co-construction du jeu de cartes PCRA accompagnés par PWC Crisalyde

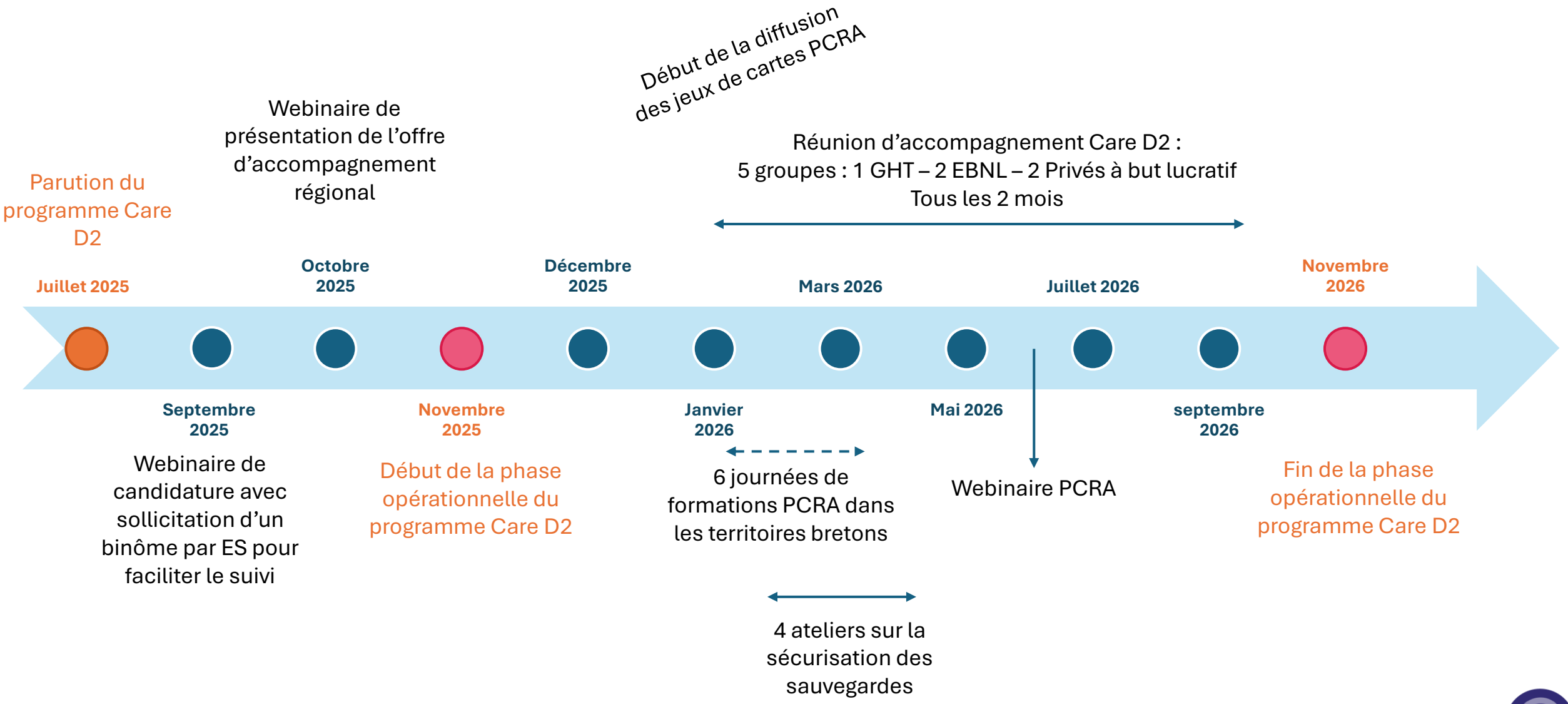
**Novembre 2025**

Début de la phase opérationnelle du programme Care D2

**Décembre 2025**

Sollicitation des trois prestataires du marché régional cyber résilience pour l'ajout de nouvelles UO pour l'atteinte des objectifs Care D2 – objectif

# Phase d'accompagnement au D2 CaRE



# Zoom sur la méthodologie PCRA (1)

Elaboration de
15 jeux de cartes

La méthode pragmatique c'est d'abord un jeu de carte, comprenant :

## Cartes « Contexte »

**C0 – Absence d'informatique**

**C1 – Bureautique et internet**

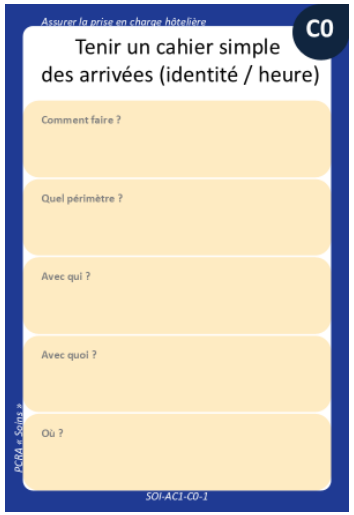
**C2 – Informatique de base**

**C3 – Retour progressif d'un SI**

## Cartes « activités »


Chaque carte comprend une activité de l'unité fonctionnelle choisie.

## Cartes « objectifs »




Chaque carte représente un objectif avec des solutions de continuité ou de reprise d'activité à décrire

# Zoom sur la méthodologie PCRA (2)

La méthode pragmatique, c’est ensuite JOUER !!

- ❑ Adhésion immédiate des participants
- ❑ Réflexion collaborative et émulation de groupe
- ❑ Forcer la synthèse par le format
- ❑ Gain de temps ET gain qualitatif

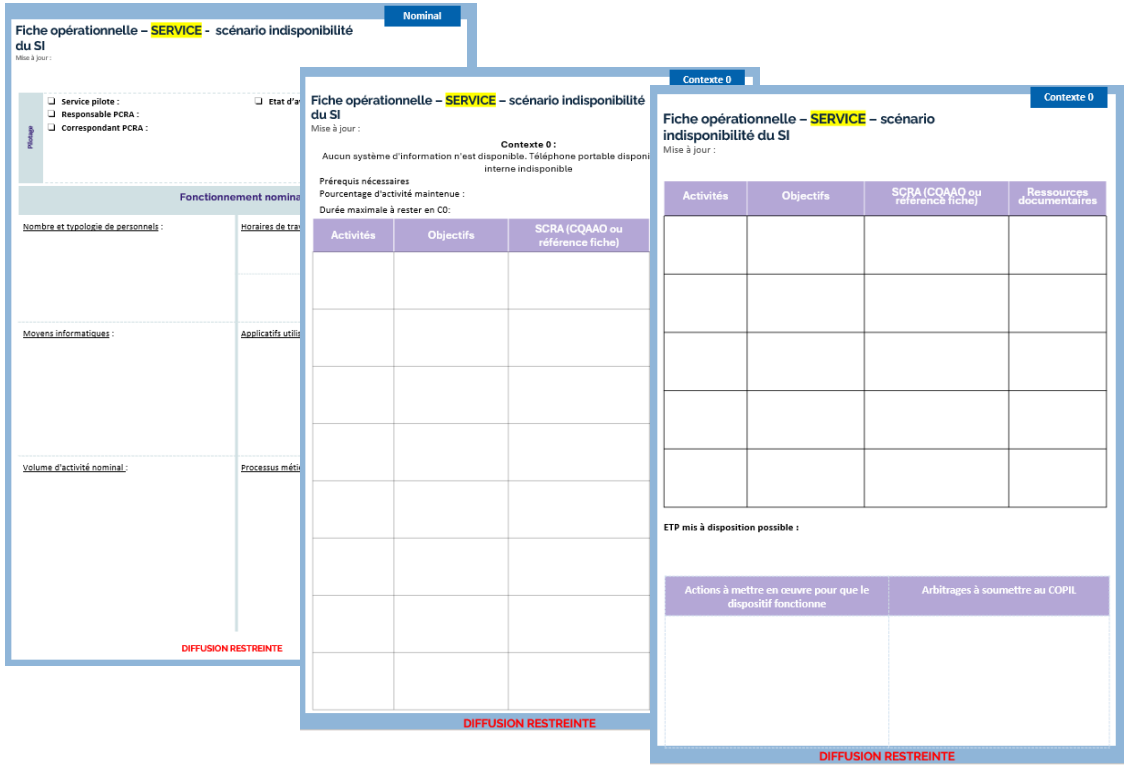
➔ Les cartes restent une modalité d’animation, pas un livrable

# Zoom sur la méthodologie PCRA (3)

Le tout en 1 journée

La méthode pragmatique, c'est enfin :

**des fiches opérationnelles** synthétiques,
par contexte, reprenant les solutions de continuité par activité




**un BIA :** outil de suivi de projet et de pilotage de crise

**Bilan d'impact sur l'activité (BIA)**

| | Processus : | C0 : Aucun système d'information n'est disponible. Téléphone portable disponible mais téléphonie interne indisponible | C1 : Mise en place d'un socle nominal. Nous remettons X PC, avec une connexion internet dégradée (clé 4G, satellite…), pas de connexion entre les PC (absence de réseau local) | C2 : Mise en place d'un socle minimal. Capacité à construire des réseaux locaux physiques et à installer des clients lourds sur les PC. | C3 : Retour progressif vers le mode nominal avec des connexions partielles |
|---|---|---|---|---|---|
| STRATEGIE | Stratégie globale *Décrire votre stratégie (priorisation, transfert, délestage…)* | | | | |
| N° | Activités | | | | |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| Au total, je peux tenir : | | | | | |
| | Avec quel prérequis | | | | |
| | Durée de viabilité tolérable (DVT) | | | | |
| | % d'activité maintenu | | | | |
| | Dépendance | Je dépends de… / Pour… | Je dépends de… / Pour… | Je dépends de… / Pour… | Je dépends de… / Pour… |
| | Arbitrages | | | | |

# Zoom sur les ateliers de sécurisation des sauvegardes

- Organisation de webinaires
  - #1 : Mettre en place le 3-2-1 + Cas particulier des SI et/ou sauvegardes externalisées
  - #2 : Construire une architecture de sauvegarde sécurisée
  - #3 : Supervision des sauvegardes et tests de restauration
  - #4 : Etat de l'art de la sauvegarde et RETEX
    - *Sauvegarde et soins, le contexte*
    - *Etat de l'art et concepts clés*
    - *Panorama de solutions*
    - *Sauvegarde et cybersécurité*
    - *Retours d'expérience d'établissements bretons*

- Fourniture de modèles de documents associés

AGENCE DU NUMÉRIQUE EN SANTÉ
LE VILLAGE DE LA E-SANTÉ

# FOCUS AXE 4 – DOMAINES DE SÉCURITÉ OPÉRATIONNELLE

# D1 - Annuaires techniques et exposition sur internet

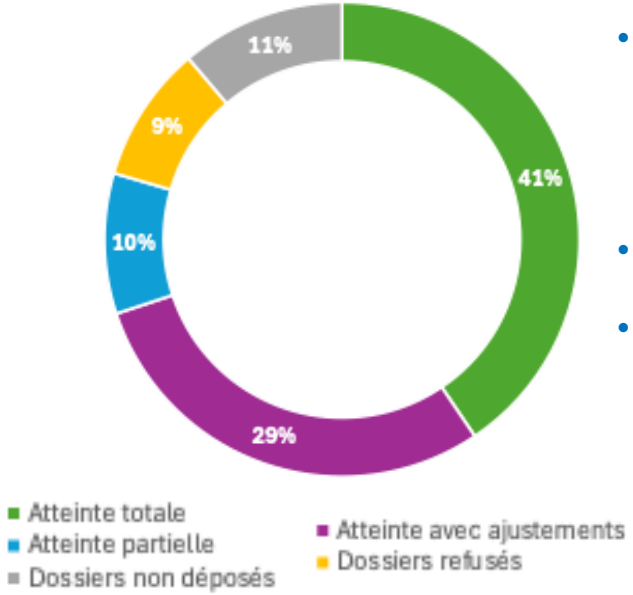
Le Domaine 1 visait à accompagner les établissements à **maitriser les risques d'exposition sur internet et la sécurisation de leurs annuaires**.

**65 M€**
dédiés au financement des ES dont **27,6 M€** validés pour paiement

**1 181**
candidats engagés soit **83%** des candidats éligibles

**939**
candidats ayant atteint les objectifs

## Bilan




- **Nette amélioration** des **niveaux de sécurisation des audits ADS et de la surface exposée** avec une **forte diminution** de la part d'établissements présentant des **vulnérabilités critiques**
- **Implication forte des régions** et l'accompagnement des candidats
- Poursuite **des contrôles financiers** permettant de **valider le montant de financement accordé** au regard de l'éligibilité des dépenses soumises

**Mars 2024**
Publication de l'arrêté

**Mars-Avril 2024**
Phase de candidature

**Juin 2025**
Fin de la phase de réalisation des travaux

**Juin 2026**
Fin des contrôles ANS

# D1 Bis - Annuaires techniques et exposition sur internet complémentaire

Le Domaine 1 bis vise à réintégrer des structures initialement non éligibles au D1 afin qu'elles puissent également **sécuriser** leurs **Active Directory** et limiter leur **exposition internet**.

**2 M€**
dédiés au financement des ES

**81**
candidats éligibles

**21**
candidatures validées

**Ce domaine ne constitue pas une nouvelle opportunité de recandidater ni un complément de financement par rapport au Domaine 1.**

Les objectifs portés dans le domaine 1 bis sont identiques au domaine 1 et intègrent nativement les ajustements des opérations de contrôle

## Prochaines actions

- **Accompagnement des candidats** au niveau **national et régional** dans l'atteinte des objectifs du domaine

**Janvier 2026**
Publication de l'arrêté

**Février-Mars 2026**
Phase de candidature

**29 octobre 2026**
Ouverture du guichet de dépôt des objectifs

**31 mars 2027**
Fermeture du guichet de dépôt des objectifs

**Novembre 2027**
Fin des contrôles ANS

# D2 - Stratégie de continuité et de reprise d'activité

Le domaine 2 porte sur l'amélioration de la résilience des établissements de santé au travers de la construction et du test de **leur stratégie de continuité et de reprise d'activité**, mais aussi au travers de **la sécurisation du système de sauvegarde**.

**45 M€**
dédiés au financement des ES

**1457**
candidats éligibles

**1147**
candidats engagés soit un taux de candidature de **79%**

## Avancement

- **Accompagnement national** autour des thématiques **PCRA** et de **sauvegarde** auprès des candidats sous forme de webinaires et d'un RETEX disponible sur le site de l'ANS
- **Offre régionale fournie par les CRRC** pour soutenir les établissements dans l'atteinte des objectifs et particulièrement sur le volet PCRA

**Juillet 2025**
Publication de l'arrêté

**Sept-Oct 2025**
Phase de candidature

**16 janvier 2026**
Ouverture du guichet de dépôt des objectifs

**18 novembre 2026**
Fermeture du guichet de dépôt des objectifs

**Juin 2027**
Fin des contrôles ANS

Retrouvez les ressources documentaires du D2 ici

# Domaines 3 et 4 à venir

## Domaine 3 - Sécurisation des accès distants

Il vise à sécuriser l'ensemble des accès distants, couvrant à la fois les accès des fournisseurs et ceux du personnel des établissements. Il porte à la fois sur :

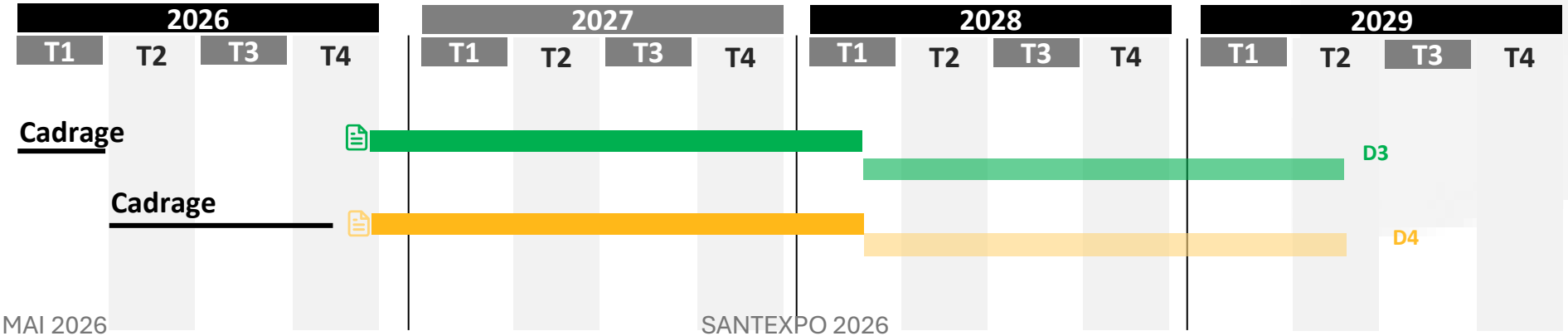
- Des améliorations techniques des **accès du personnel et des fournisseurs de l'établissement**
- Des améliorations organisationnelles au travers de la formalisation de **politiques de gestion des accès**

## Domaine 4 - Sécurisation des postes de travail

Il vise à renforcer la supervision des postes de travail afin de détecter au plus tôt les tentatives d'intrusion et les compromissions, notamment lors des phases de propagation et de prise de contrôle du système d'information. Il repose sur :

- La définition d'une **gouvernance et d'un cadre de sécurité**
- La **sécurisation technique des postes de travail** (LAPS, durcissement des configurations, etc.)
- **La supervision des postes**

Hypothèse de lancement : Les domaines 3 et 4 seraient lancés conjointement. Les ES pourront choisir l'ordre dans lequel ils aborderont ces domaines.



# Appel à projet spécifique au secteur médico-social

Afin de soutenir les **ESSMS** dans le renforcement de leur cybersécurité et pour prendre en compte leurs spécificités **technologiques et organisationnelles**, des appels à projets sont lancés en plusieurs itérations :

- **Une 1ère itération**, sous forme de POC permet **de tester ce dispositif avant sa généralisation** à l'ensemble du secteur. Ce **POC a été lancé le 31 mars 2026.**
- Dans un second temps, suite au RETEX du POC et après ajustements, **plusieurs itérations seront déployées sur un périmètre élargi**

**3 parcours**
conçus selon la maturité cyber

**21**
lauréats

**Près de 1,8 M€**
prévus pour le POC de l'AAP

## Principes

- **3 parcours au choix** s'adaptant à la maturité des candidats :
  - Parcours 1 : Maturité cyber faible, ESSMS sans ressources cyber dédiées
  - Parcours 2 : Maturité cyber faible, ESSMS avec potentiellement des ressources cyber dédiées
  - Parcours 3 : Maturité cyber intermédiaire
- Chaque parcours contient des prérequis, des objectifs obligatoires et des objectifs à la carte

**Mars 2026** – Publication du cahier des charges

**Mai-Juin 2026** Phase de candidature AAP POC

**T1 2027** Fin de la phase de réalisation des travaux

**T1 2027** – Lancement de l'itération suivante

# HospiConnect CaRE

HospiConnect vise à **sécuriser la chaîne d'identification électronique** au sein des établissements et s'appuie sur 2 programmes de financement : **HOP'EN 2** et **CaRE**.

Le dispositif **HospiConnect CaRE** porte sur le **financement des moyens d'identification électronique** afin de permettre la **mise en œuvre d'une authentification à deux facteurs (2FA)**, en conformité avec le RIE.

**27,3 M€**
dédiés au financement des MIE

**1445**
candidats éligibles

**1335**
candidatures validées soit un taux de participation de **92%**

## Avancement

- **Accompagnement national renforcé sous la bannière unifiée HospiConnect** (HOP'EN 2 et CaRE)
- Mise à disposition d'un **questionnaire d'auto-évaluation de la maturité des ES en termes d'identification électronique**
- **Ouverture prochaine de la 1ère phase de relève** de l'atteinte des objectifs

**Il s'agit de la généralisation de l'AAP Alpha dont les retours ont été pris en compte pour construire l'accompagnement autour de ce dispositif**

**Janvier 2026**
Publication de l'arrêté

**Janvier-Février 2026**
Phase de candidature

**S2 2026**
1ère relève de l'atteinte des objectifs

**Mi juin-mi juillet 2027**
2ème relève de l'atteinte des objectifs

**Mi juin-mi juillet 2028**
Dernière relève de l'atteinte des objectifs

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

# TRAVAUX EN COURS ET A VENIR

# Travaux en cours et à venir

## Gouvernance et résilience

- Travaux sur la certification HAS
- Publication d'une instruction cyber à destination des établissements mise à jour dans le contexte de NIS 2

## Ressources et mutualisation

- Pérennisation des Centres Régionaux de Ressources Cyber (CRRC)

## Sensibilisation

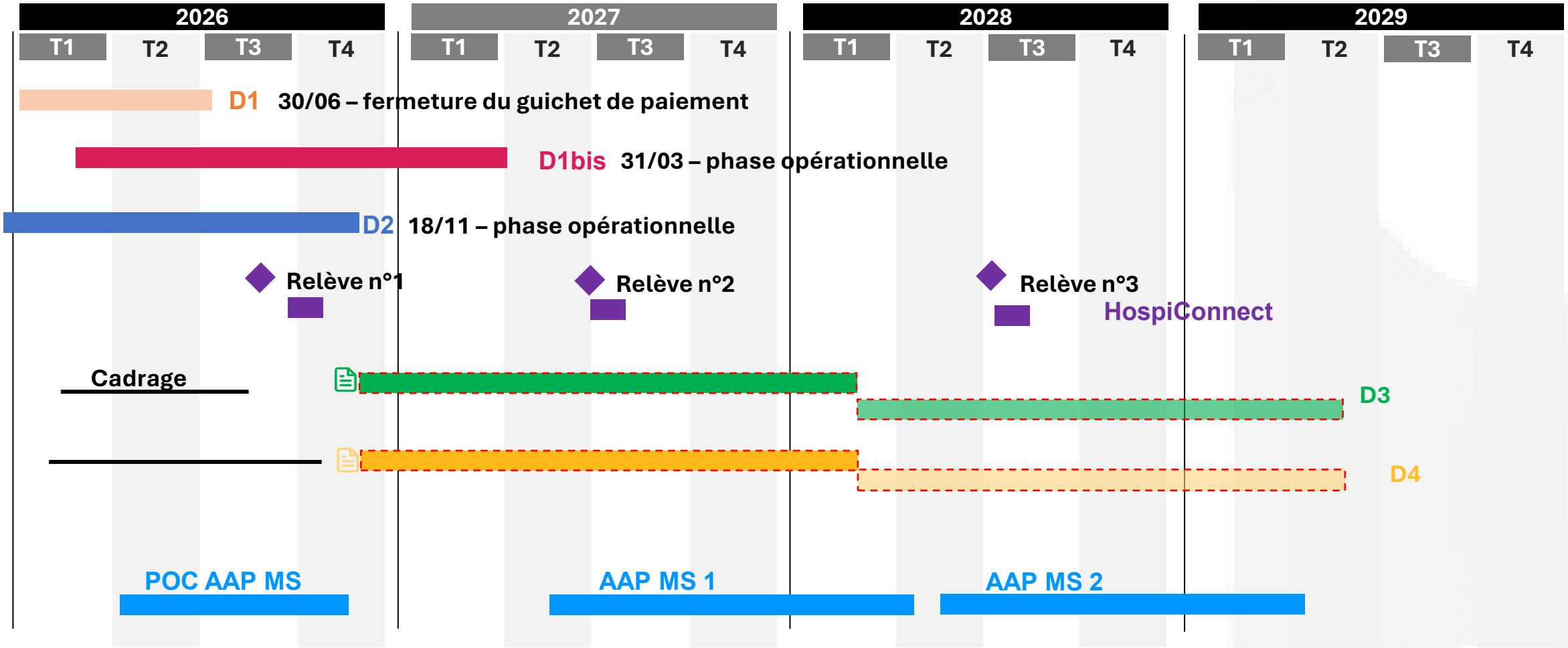
- Partage de RETEX sur les impacts d'une cyberattaque
- Appui à la structuration de l'offre de formation cyber

## Sécurité opérationnelle

- Cadrage des domaines 3 et 4
- Cadrage du Socle cyber destiné à pérenniser le financement en ES
- Cadrage des prochaines itérations de l'AAP MS

**Préparation de la poursuite du programme au-delà de 2027**

# Calendrier prévisionnel des domaines engagés et à venir 2026 - 2027




**Légende :**

- Publication d'arrêté
- Phase opérationnelle ES
- Contrôle ANS et paiement
- Domaine 1
- Domaine 1b
- Domaine 2
- Domaine 3
- HospiConnect
- Socle
- Domaine 4
- AAP MS

AGENCE DU NUMÉRIQUE EN SANTÉ

LE VILLAGE DE LA E-SANTÉ

# Pour plus d'information retrouvez nous sur esante.gouv.fr