AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

MINISTÈRE DU TRAVAIL, DE LA SANTÉ, DES SOLIDARITÉS ET DES FAMILLES
Liberté
Égalité
Fraternité

Délégation ministérielle au numérique en santé

Financé par l'Union européenne
NextGenerationEU

Webinaire thématique Domaine 2 : Atteinte des objectifs de sauvegarde

2 avril 2026

Programme CaRE : Cybersécurité accélération et Résilience des Etablissements

LA E-SANTÉ FRANÇAISE CaRE Cybersécurité accélération Résilience des Etablissements

Webin-aire

Nos webinaires pour construire la e-santé de demain !

Nos intervenants

Christophe MATTLER
Directeur de programme

MINISTÈRE DU TRAVAIL DE LA SANTÉ ET DES SOLIDARITÉS
Liberté
Égalité
Fraternité

Délégation au numérique en santé

Steven GARNIER
Directeur de domaine

Estelle NICAUD
Responsable de mission

Ange HIRSCH
Expert sécurité

AGENCE DU NUMÉRIQUE EN SANTÉ

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Webinaire, les bonnes pratiques

Le micro et la caméra sont automatiquement coupés sauf pour les intervenants.

Je pose mes **questions** dans **l'espace Questions/Réponses.**

Je ne pose **pas mes questions dans l'espace conversation.** Celles-ci ne seront pas traitées.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Déroulé du webinaire

1. Rappels sur le domaine 2 - Stratégie de continuité et de reprise d'activité
2. Objectifs de sauvegarde, preuves attendues et outils mis à la disposition des candidats
3. Trame et documents attendus au titre de la justification des coûts
4. Ressources mises à disposition des candidats

Webin-aire
Nos webinaires pour construire la e-santé de demain !

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

Gouvernance et résilience

Structurer la gouvernance de la cybersécurité dans le secteur de la santé en impliquant les niveaux nationaux, régionaux et locaux.

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 des appels à projets).

L'axe 4 du programme CaRE, consacré à la **sécurité opérationnelle**, est décliné en plusieurs domaines spécifiques.
Chacun de ces domaines vise à **traiter une problématique technique précise** et **à combler les lacunes existantes en matière de cybersécurité**, afin de renforcer la protection des systèmes d'information des établissements de santé.

Les domaines de financement

- **Domaine « Annuaire techniques et exposition internet »**
- **Domaine « Stratégie de continuité et de reprise d'activité »**
- **Domaine « Sécurisation des accès distants »**
- **Domaine « Supervision des postes de travail »**
- **HospiConnect**

Le deuxième domaine de financement du programme CaRE a été lancé le 16 juillet 2025. Il porte sur une thématique à la frontière entre la technique et la qualité : la stratégie de continuité et de reprise d'activité.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

1. Rappels sur le domaine 2 - Stratégie de continuité et de reprise d’activité

Lors d'une attaque par rançongiciel — l'une des principales menaces actuelles — les cyberattaquants visent à chiffrer non seulement les données des établissements ciblés, mais également leurs sauvegardes. Cette double compromission complique la reprise et la continuité d'activité, entraînant des pertes de données massives et souvent critiques.

Le domaine 2 « stratégie de continuité et reprise d'activité » se structure autour de 2 grandes thématiques complémentaires

1

Assurer la continuité et la reprise d'activité

Capacité des établissements à se préparer, s'organiser et à réagir dans le cadre d'une cyberattaque

Thème abordé dans un précédent webinaire

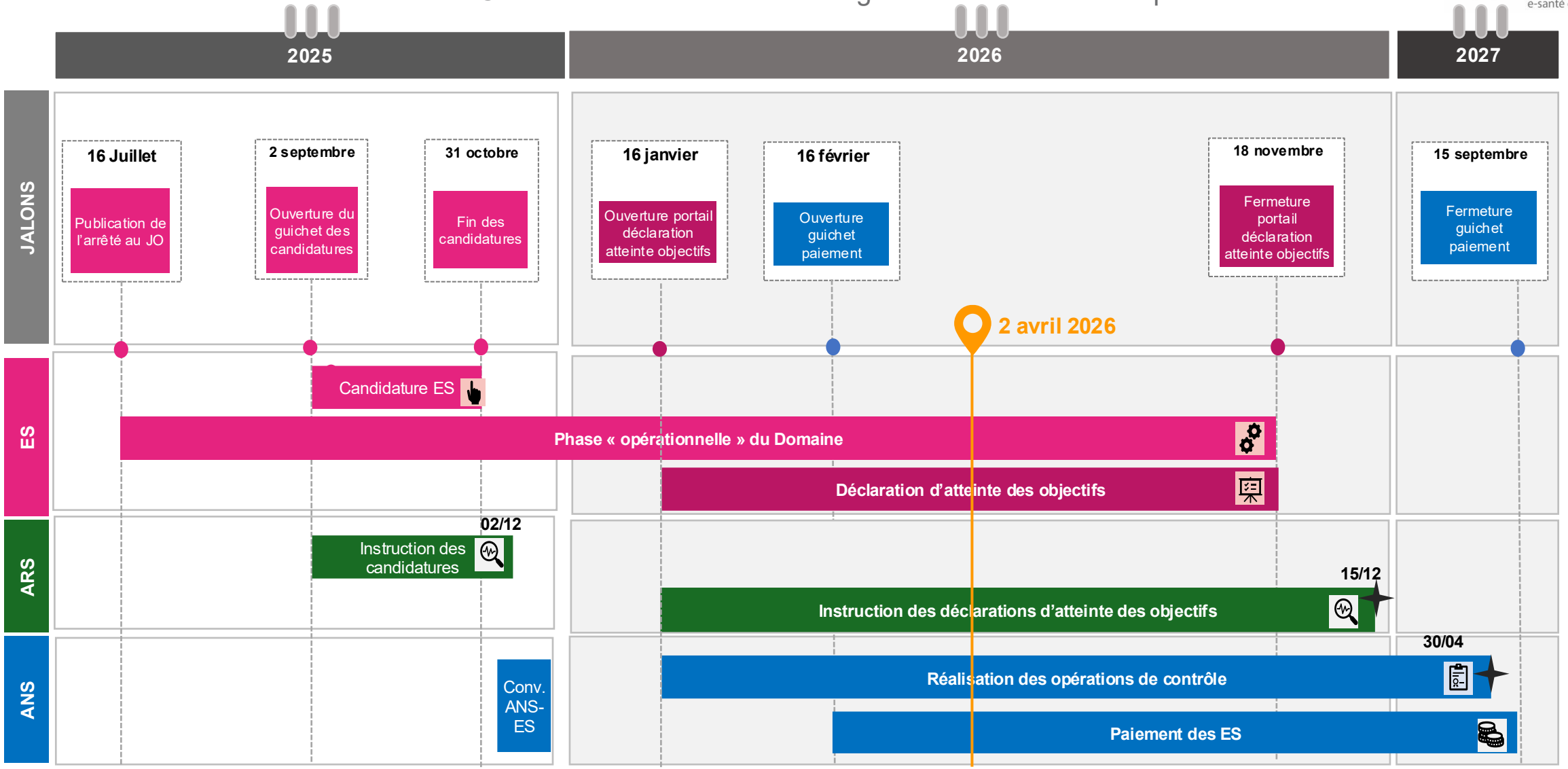
2

Construire une sauvegarde sécurisée

Mise en place de sauvegardes non contaminables et restaurables pour toutes les applications critiques

Thème abordé dans ce webinaire

Calendrier du domaine « Stratégie de continuité et de reprise d'activité »



Objectifs relatifs à la continuité d'activité abordés dans un précédent webinaire

D2.O1 - Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements

D2.O1.A	• Mettre en place une gouvernance pour la Continuité et de Reprise d'activité
D2.O1.B	• Décrire les procédures de réponse à la gestion de la crise cyber
D2.O1.C	• Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA)
D2.O1.D	• Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain

Objectifs relatifs à la sauvegarde abordés dans ce webinaire

D2.O2 - Définir, documenter et tenir à jour la politique et le(s) plan(s) de sauvegarde et de restauration

D2.O2.A	• Définir une politique de sauvegarde et de restauration et la maintenir à jour
D2.O2.B	• Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour

D2.O3 - Construire un système de sauvegarde sécurisé

D2.O3.A	• Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde
D2.O3.B	• S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde
D2.O3.C	• S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1
D2.O3.D	• Mettre en place une supervision des sauvegardes

D2.O4 - Tester la sauvegarde et la restauration

D2.O4	• Tester la sauvegarde et la restauration

Webin-aire
Nos webinaires pour construire la e-santé de demain !

Modèle économique et conditions de financement

- Le **montant plafond** de financement a été fixé, préalablement à votre candidature, via la base des ES éligibles (sur la base d'un forfait « activité combinée » associé à un plancher et un maximum)
- Seules les **dépenses nouvelles** engagées **durant la phase opérationnelle** (soit depuis le 16 juillet 2025) sont éligibles
- Les financements sont alloués **sous réserve de l'atteinte des objectifs** et de la **soumission des justificatifs** des dépenses engagées (dont l'éligibilité sera analysée)

Principes clés et vigilance pour l'atteinte des objectifs

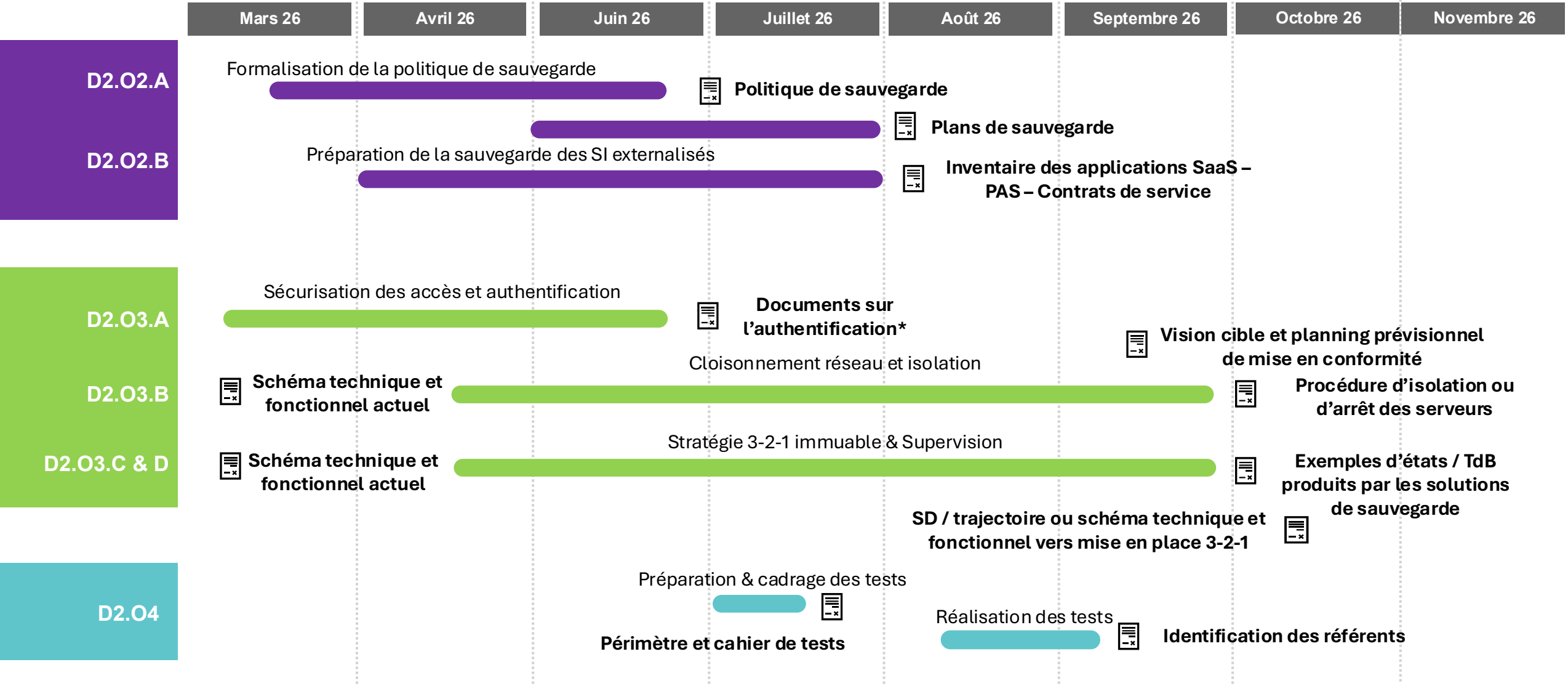
- Pour bénéficier d'un financement, les candidats doivent **atteindre l'ensemble des objectifs** définis pour le domaine, et transmettre les éléments financiers justificatifs
- Sauf mention contrainte (i.e. D2.O1.C) **l'ensemble des structures** (juridiques ou géographiques) composant le candidat **doivent atteindre les cibles** définies pour permettre la validation de l'objectif

Prochaines échéances relatives au domaine 2

- Les candidats sont invités à réaliser au plus tôt une **analyse des coûts** pour **maximiser le montant de leurs dépenses éligibles** (en réalisant le cas échéant des investissements complémentaires)
- Le guichet de dépôt des preuves est **ouvert depuis le 16 janvier 2026** : les candidats peuvent désormais déclarer l'atteinte des objectifs
- Le guichet de dépôt des preuves **fermera le 18 novembre 2026** : les candidats ont **jusqu'à cette échéance** pour **déposer leurs justificatifs**

- L'Agence du Numérique en Santé met à disposition des candidats un **riche corpus documentaire** pour les accompagner dans leur démarche d'atteinte des objectifs
- **Plusieurs webinaires seront** organisés d'ici à l'été 2026 pour accompagner les candidats et répondre à leurs questions

Planning type pour la réalisation des travaux jusqu'à la fin de la phase opérationnelle



** Documents détaillés dans le guide des prérequis et objectifs*

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

2. Objectifs de sauvegarde, preuves attendues et outils mis à la disposition des candidats

Les objectifs relatifs à la sauvegarde nécessitent des travaux anticipés de la part des candidats, avec une vigilance relative aux attentes et preuves à fournir.

D2.O2.A
Définir une politique de sauvegarde et de restauration, et la maintenir à jour

- Le candidat doit transmettre un **inventaire complet des applications en mode SaaS** (précisant pour chacun si un PAS a été recueilli) ainsi que deux PAS à titre d'exemple
- La transmission d'un contrat de prestation HDS ne remplace par la transmission d'un PAS

D2.O2.B
Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour

- Les plans de sauvegardes de restauration doivent couvrir **l'ensemble des systèmes d'information critiques du candidat. L'ensemble des entités** (juridiques ou géographiques selon la typologie du candidat) doivent être **couvertes** par les plans de sauvegarde.

D2.O3.A
Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde

- Le candidat doit **opérationnellement disposer** d'une authentification sécurisée et anticiper les d'éventuelles actions de remédiation
- Les conditions spécifiques de sauvegarde de l'établissement doivent être analysées pour apporter les documents justificatifs associés

D2.O3.B
S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde

- Les attendus portent sur **l'ensemble du périmètre du candidat** – si plusieurs infrastructures de sauvegarde sont mises en œuvre, toutes devront être cloisonnées.

D2.O3.D
Mettre en place une supervision des sauvegardes

- Les procédures proposées par le candidat doivent couvrir **l'ensemble des sauvegardes** faisant l'objet d'une supervision
- Un **candidat GHT** doit avoir une procédure formalisée pour **traiter les alertes non résolues** par un ou plusieurs établissements.

D2.O4
Tester la sauvegarde et la restauration

- Au moins un des tests menés doit concerner les **données de production**.
- Les tests techniques doivent porter sur la restauration d'une machine virtuelle ou d'une base de données sur un périmètre d'un SI concourant à une des **activités critiques** (cf. D2.O1.C)

D2.O2.A Définir une politique de sauvegarde et de restauration, et la maintenir à jour

Valeur cible / seuil d'éligibilité

- Transmettre la politique de sauvegarde et de restauration intégrant à minima
  - Les types de données à sauvegarder
  - La hiérarchisation des données et la fréquence des sauvegardes selon leur criticité
  - Le délai de rétention en fonction de la typologie
  - La planification de sauvegardes en fonction de l'activité
  - Les responsabilités des personnels impliqués dans le processus de sauvegarde
  - Les exigences de conformité légale et réglementaire
  - Les procédures de mise à jour de la politique de sauvegarde
  - Les mesures de sécurisation des sauvegardes
  - Les mesures sur la confidentialité et l'intégrité des données

Pièces justificatives attendues

- Politique de sauvegarde et de restauration conforme à la cible
- Si un prestataire pour la sauvegarde en cas de SI métier externalisé et/ou sauvegarde externalisée :
  - Contrat de service avec le prestataire
  - Plan d'Assurance Sécurité (PAS) ou attestation du candidat

  ou le motif de non-présentation du document et le nom du prestataire

Points d'attention et information

- La politique de sauvegarde doit avoir été mise à jour entre le 16 juillet 2022 et la date de dépôt du dossier d'atteinte des objectifs.
- Les candidats multi-établissements (juridiques ou géographiques) disposant de SI mutualisés doivent proposer une stratégie d'harmonisation des sauvegardes sur les 18 mois suivant la clôture de la phase opérationnelle
- La politique doit porter une harmonisation de la sauvegarde indépendamment des dispositifs techniques. Elle n'exige pas pour autant l'unification du système de sauvegarde.

Points de vigilance

- Le candidat doit transmettre un **inventaire complet des applications en mode SaaS** (précisant pour chacun si un PAS a été recueilli) ainsi que **deux PAS à titre d'exemple**
- **La transmission d'un contrat de prestation HDS ne remplace par la transmission d'un PAS**
- Les candidats peuvent se référer au clausier de sécurité numérique du Club RSSI Santé – cliquez ici

D2.O2.A Définir une politique de sauvegarde et de restauration, et la maintenir à jour

Questions

Réponses

La politique de sauvegarde peut-elle comporter des exceptions pour certains domaines fonctionnels (à l'exemple de l'imagerie) en réponse au D2.O2.A?

Il est attendu dans le D2.O2.A que le candidat transmette une politique de sauvegarde couvrant l'ensemble de son système d'information. La politique de sauvegarde énumère les règles de sauvegarde s'appliquant à chaque type de données.

Par conséquent, si un type de donnée (par exemple données d'imagerie) fait l'objet de règles spécifiques, cette politique doit en faire mention.

Le PAS du prestataire doit-il contenir les mêmes éléments que ceux demandés dans le cadre d'une politique interne de sauvegarde dans le cadre du D2.O2.A ?

Non, le PAS du prestataire n'a pas à contenir l'intégralité des éléments composant une politique interne de sauvegarde. En revanche, il est indispensable de vérifier que le PAS couvre bien les exigences attendues (disponibilité, intégrité, sécurité, modalités de restauration) et qu'il répond aux besoins définis par l'établissement.

D2.O2.B Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour

Valeur cible / seuil d'éligibilité

- Transmettre le(s) plan(s) de sauvegarde des systèmes d'information critiques contenant à minima :
  - Les logiciels, matériels.
  - Supports utilisés (Serveurs de sauvegarde, stockage dédié, cloud (préciser les types de flux utilisés), bande, ...).
  - Les types de sauvegardes (complète, incrémentielle, différentielle, ...).
  - La fréquence de réalisation des sauvegardes et les heures d'exécution.
  - Le délai de réplication.
  - Le délai de rétention détaillé lié aux plans de sauvegarde.
  - Les procédures à suivre en cas d'échec.
  - Les procédures de mise à jour des plans de sauvegardes

Pièces justificatives attendues

- Plan(s) de sauvegarde et procédure de mise à jour pour tous les éléments des SI critiques (identifiés à l'objectif D2.01.C)
- Projet d'harmonisation des plans de sauvegarde et de restauration pour les SI mutualisés

Points d'attention et information

- Les **candidats multi-établissements** (juridiques ou géographiques) disposant de **SI mutualisés** doivent proposer une stratégie d'harmonisation des sauvegardes sur les 18 mois suivant la clôture de la phase opérationnelle

Points de vigilance

- Les plans de sauvegardes de restauration doivent couvrir l'ensemble des systèmes d'information critiques du candidat. L'ensemble des entités (juridiques ou géographiques selon la typologie du candidat) doivent être couvertes par les plans de sauvegarde et de restauration

D2.O3.A Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde

Valeur cible / seuil d'éligibilité

- Disposer d'un système d'authentification indépendant pour ses infrastructures de sauvegarde
- Assurer une gestion fine des rôles pour l'accès à la sauvegarde
- Utiliser, lorsque cela est permis par la solution, une authentification à double facteurs pour accéder aux sauvegardes

Pièces justificatives attendues

- Document présentant le rôle de l'opérateur de sauvegarde et de l'administrateur
- Document décrivant la gestion des rôles pour l'accès à la sauvegarde
- Document décrivant la mise en œuvre de l'authentification à double facteur
- Cas spécifique d'un AD indépendant : score d'audit ORADAD (>=3) réalisé dans les 60 jours précédents le dépôt de la déclaration d'atteinte des objectifs.
- Cas spécifique d'une infrastructure externalisée : document décrivant les moyens d'accès aux sauvegardes fournis par le prestataire **et**
  - Extraits du PAS du prestataire relatif à la sauvegarde ou attestation du candidat de la présence du document
  - Ou, motifs de non-présence du document fournis par le prestataire, noms du prestataire et de la solution

Points d'attention et information

- Les motifs de non-présence du PAS doivent être des éléments de preuve (ex : email ou document signé par le prestataire)
- Pour la solution d'authentification à double facteurs :
  - Si l'interface d'administration permet une authentification forte, un document décrivant la mise en œuvre de l'authentification (procédure, impressions d'écran).
  - Si l'interface d'administration permet une authentification forte mais qu'elle n'est pas activée, un document justificatif des raisons de sa non mise en œuvre.
  - Si l'interface d'administration ne permet pas une authentification forte, un document précisant le nom de la solution de sauvegarde et sa version
- Des fiches pratiques du CERT Santé sur le schéma d'architecture (**cliquez ici**) et la matrice des flux (**cliquez ici**) sont disponibles, ainsi qu'un guide de l'ANSSI (**cliquez ici**)

Points de vigilance

- **Vérifier les conditions spécifiques de sauvegarde de l'établissement pour apporter les documents justificatifs associés**

D2.O3.A Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde

Questions

La mise en œuvre d'un Active Directory dédié pour les infrastructures de sauvegarde est-elle requise ?

Réponses

Non, l'atteinte de l'objectif repose sur la mise en œuvre d'un système d'authentification sécurisé et indépendant pour l'accès aux infrastructures de sauvegarde. Le candidat est libre du choix de la solution mise en œuvre pour atteindre cet objectif, qui peut reposer sur un Active Directory dédié comme sur des comptes locaux.

Dans le cas où un active directory dédié est mis en œuvre, un niveau supérieur ou égale à 3 doit être obtenu à l'audit ADS réalisé en fin de phase opérationnelle.

D2.O3.B S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde

Valeur cible / seuil d'éligibilité

- S'inscrire dans une démarche de cloisonnement des infrastructures de sauvegarde (comprenant l'isolation technique en cas d'incident)
- Positionner une fonction de filtrage autorisant uniquement les flux strictement nécessaires.

Pièces justificatives attendues

- Schéma technique et fonctionnel de l'architecture (actuelle ou cible) détaillant la matrice des flux techniques
- Un planning prévisionnel (inférieur à 3 ans) d'atteinte du schéma cible
- Procédure permettant l'isolation ou l'arrêt des serveurs de sauvegarde en cas d'incident
- Cas spécifique d'applications externalisées / infogérance / exploitation externalisée :
  - Extraits du PAS du prestataire relatif à la sauvegarde ou attestation du candidat de la présence du document
  - **Ou**, motifs de non-présence du document fournis par le prestataire, noms du prestataire et de la solution

Points d'attention et information

- Les investissements réalisés pour définir la démarche ou la mettre en œuvre (sur la base de factures reçues par la structure) sont valorisables même si la démarche n'est pas finalisée
- Les motifs de non-présence du PAS doivent être des éléments de preuve (ex : email ou document signé par le prestataire)

Points de vigilance

- Les attendus portent sur l'ensemble du périmètre du candidat – **si plusieurs infrastructures de sauvegarde sont mises en œuvre, toutes devront être cloisonnées.**

D2.O3.B S’inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde

Questions

Réponses

Le cloisonnement attendu de l’infrastructure de sauvegarde doit-il être un cloisonnement logique ou physique ?

Le choix du mode de cloisonnement mis en œuvre pour les infrastructures de sauvegardes est laissé au choix du candidat.

Le candidat devra soumettre le schéma technique et fonctionnel permettant de présenter la solution, qui devra garantir une capacité technique d’isolation en cas d’incident.

NIS2 supprime la notion de SIE spécifique par un SI critique global avec des exclusions. Est-ce que cet objectif s’inscrit dans la même démarche remplaçant un système SIE par un système de sauvegarde globale à tous le SI ?

Non. L’objectif D2.O3.B ne vise pas à instaurer un système de sauvegarde global pour l’ensemble du SI, mais à garantir la séparation et l’isolation des systèmes de sauvegarde. La logique est différente de celle de NIS2 : il ne s’agit pas de remplacer la sauvegarde par SIE par une sauvegarde unique couvrant tout le SI, mais de sécuriser les environnements de sauvegarde existants.

D2.O3.C S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

Valeur cible / seuil d'éligibilité

- S'inscrire dans une démarche de mise en œuvre du 3-2-1 *(voir détail en page suivante)*
- Assurer l'intégrité et la disponibilité des informations critiques de l'établissement

Pièces justificatives attendues

Cas d'une infrastructure internalisée :

- Schéma technique et fonctionnel de l'architecture actuelle détaillant la matrice des flux techniques.
- Si applicable : un schéma directeur / trajectoire ou schéma technique et fonctionnel d'architecture cible vers une mise en place du 3-2-1 avec les principaux jalons identifiés

Cas d'un hébergeur tiers et sur le périmètre propre au candidat :

- Éléments contractuels explicitant les SLA en application
- Extraits du PAS du prestataire relatif à la sauvegarde ou attestation du candidat de la présence du document **ou** motifs de non-présence du document fournis par le prestataire, noms du prestataire et de la solution

Points d'attention et information

- Le candidat peut engager des dépenses permettant la mise en œuvre opérationnelle de sa stratégie 3-2-1. Auquel cas, les dépenses réalisées durant la phase opérationnelle sont considérées comme éligibles
- Une sauvegarde est considérée immuable si, une fois écrit, son contenu ne peut plus être modifié ni supprimé (volontairement ou involontairement) pendant une durée définie. (voir éléments détaillés en page suivante).

Points de vigilance

- **La démarche 3-2-1 porte sur l'ensemble des données nécessaires à la continuité des activités critiques (et non exclusivement sur les données de santé).**

D2.O3.C S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

La règle de sauvegarde 3-2-1 est une stratégie de protection des données visant à garantir l'intégrité et la disponibilité des informations critiques de l'établissement.

Trois copies de vos données

Il est essentiel de pouvoir disposer de trois copies des données sauvegardées : les données de production et deux copies supplémentaires. Cette redondance réduit le risque de perte de données en cas de défaillance d'un ou plusieurs supports

Deux types de supports différents

Les sauvegardes doivent être stockées sur au moins deux types de supports différents, comme une NAS ou un service de stockage en ligne en plus du stockage initial. L'utilisation de différents supports protège contre les défaillances spécifiques à un type de support

Une copie hors site ou hors ligne

Au moins une copie de sauvegarde doit être stockée dans un emplacement physique différent de celui des données originales, ou hors ligne, c'est-à-dire non connectée à un réseau. Cela protège les données contre les cyberattaques ou les catastrophes naturelles, comme les incendies ou les inondations

D2.O3.C S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

Illustration de solutions de copie « hors-ligne » / « hors-site » et de leurs principaux bénéfices

Sauvegarde sur bande magnétique

- **Serveur de sauvegarde** (connecté au serveur de production)
- **Bibliothèque de bandes** (stocke les bandes magnétiques)
- **Site distant** (bandes transportées physiquement vers un site sécurité)

Longue durée de vie
Protection contre les cyber-attaques et risques physiques

Sauvegarde sur disque dur

- **Disque dur externe** (connecté au serveur de production)
- **Site distant** (disques transportés physiquement vers un site sécurité, mais doit pas être remis en ligne sur le site distant – i.e. le site distant doit servir uniquement de lieu de stockage du disque)

Coût faible et facilité de stockage

Sauvegarde air-gap (isolation physique)

- **Serveur de sauvegarde** (connecté au serveur de production)
- **Stockage Air-Gap** (unité physiquement isolée du réseau principal)
- **Déconnexion physique** (déconnecté du réseau après la sauvegarde)
- **Sauvegarde initiale** (données copiées depuis le serveur de production) avant d'être **transférées** vers le stockage **Air-Gap**
- **Déconnexion** (du réseau, prévenant tout accès non autorisé)

Données intactes si sinistre du réseau
Protection contre les cyber-attaques

Sauvegarde cloud sans connexion physique

- **Serveur de sauvegarde** (connecté au serveur de production)
- **Cloud public/privé** (données ensuite transférées vers un service cloud)
- **Déconnexion physique** (données déconnectées du réseau après sauvegarde)

Accès rapide
Protection contre les sinistres locaux

D2.O3.C S’inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

Une sauvegarde est considérée immuable si, une fois écrit, son contenu ne peut plus être modifié ni supprimé (volontairement ou involontairement) pendant une durée définie. Cette immuabilité doit être garantie par la "technologie" (certifiée ou non / implémentation de mécanismes internes / produit déjà packagé), et non seulement par des procédures organisationnelles.

Exemples considérés comme immuables :

- Bandes WORM (Write Once Read Many),
- Stockage objet avec verrouillage (Object Lock / mode WORM),
- Snapshots ou systèmes de sauvegarde offrant un mode immuable intégré.

Exemples non immuables / "altérables" :

- Bandes réinscriptibles classiques,
- Copies externalisées sans mécanisme technique de verrouillage,
- Sauvegardes sur disque/NAS standards pouvant être écrasées ou effacées.

La stratégie du candidat doit inclure les dimensions technologiques empêchant toute modification ou suppression des données. *A titre d’exemple, définir une procédure organisationnelle sans justification technique (e.g. support en coffre-fort sans verrouillage, sauvegarde externalisée mais modifiable) ne permet pas de garantir l’immuabilité des sauvegardes.*

D2.O3.C S’inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

Questions

Comment distinguer une sauvegarde d'une réplication (SAN, NAS, mirroring), dans le cadre du 3-2-1, et quels sont les risques associés ?

Réponses

Une réplication n'est pas une sauvegarde dans la mesure où elle reproduit immédiatement toute modification ou corruption. Elle ne permet donc de revenir à un état antérieur.

Le 3-2-1, exige deux copies indépendantes du système de production, la possibilité de restaurer un état antérieur, d’être stockée sur un support distinct, d’être immuable et ne pas être automatiquement modifié par les opérations de production. Aussi, la mise en place d’un système de réplication ne permet pas de répondre aux objectifs du domaine et ne constitue pas une dépense éligible.

Dans le cadre de la mise en œuvre du 3-2-1, il est demandé d’avoir 3 copies sur 2 supports différents dont 1 support hors ligne / hors site. Est-ce que les données du serveur de production peuvent être comptées comme une copie ?

Oui, les données du serveur de production sont considérées comme une copie, et ce conformément aux recommandations de l’ANSSI considérant la sauvegarde initiale (i.e. données de l’environnement de production) comme une copie.

La stratégie « 3-2-1 » implique la réalisation de 2 copies de sauvegarde, sur 2 supports différents, dont 1 nécessairement hors-ligne.

Dans une architecture répartie sur plusieurs sites, la stratégie 3-2-1 est-elle respectée si plusieurs copies reposent sur la même technologie de stockage ?

La règle 3-2-1 repose sur 3 copies de vos données (les données de production et deux copies supplémentaires), 2 types de support différents, et 1 copie hors ligne ou hors site. Le candidat doit s’inscrire dans une trajectoire répondant à ces éléments.

Le candidat doit définir une trajectoire intégrant au moins 2 supports différents. Si une technologique unique est utilisée pour l’ensemble des copies, alors l’ensemble des copies sont exposées aux mêmes risques. La cible définie ne respecterait donc pas les conditions du 3-2-1.

D2.O3.D Mettre en place une supervision des sauvegardes

Valeur cible / seuil d'éligibilité

- Instaurer une organisation pour assurer le suivi efficace des sauvegardes, incluant un plan d'actions pour vérifier leur bonne exécution et des procédures à suivre en cas d'échec

Pièces justificatives attendues

En cas d'internalisation :

- Exemple d'états produits ou générés par les solutions de sauvegarde / tableaux de bord produits par les outils de sauvegarde
- Procédures pour le contrôle des incidents de sauvegarde et le plan de traitement des alertes décrites dans la politique de sauvegarde.

Pour un GHT : documents décrivant la gouvernance de contrôle de la réalisation des sauvegardes.

En cas d'externalisation :

- Les procédures pour la gestion des incidents remontés par la supervision et à défaut éléments contractuels explicitant les Contrats de Niveau de Service (CNS/SLA) en application.

Points d'attention et information

- Un candidat GHT doit avoir une procédure formalisée pour traiter les alertes non résolues par un ou plusieurs établissements.
- Un candidat GHT doit mettre en œuvre une gouvernance de contrôle, centraliser les alertes et permettre au RSSI d'effectuer les contrôles nécessaires (cf. D2.02.A).
- Il n'existe aucune exigence imposant le déport des journaux d'accès et d'administration des solutions de sauvegarde vers un puits de logs ou un SIEM

Points de vigilance

- **L'organisation mise en œuvre doit porter sur l'ensemble des sauvegardes du candidat**

D2.O3.D Mettre en place une supervision des sauvegardes

Questions

Est-ce que l'intégration des rapports de sauvegardes dans un outil de monotoring via API, avec création d'une alerte automatiquement remplit le critère D2.O3.D

Réponses

L'intégration, via API, des rapports de sauvegarde dans un outil de supervision avec génération automatique d'alertes répond à ces attendus : il s'agit bien d'une supervision centralisée et automatisée des sauvegardes

D2.O4 Tester la sauvegarde et la restauration

Valeur cible / seuil d'éligibilité

- Réaliser des tests techniques de : (i) bon fonctionnement des sauvegardes, et (ii) remise en marche du système suite à la restauration
- Identifier au minimum un référent ou correspondant métier sur les applications métier critiques telles qu'identifiées dans le sous-objectif D2.O1.C.

Pièces justificatives attendues

- Document précisant le périmètre des tests
- Cahier de tests de l'opération de restauration (contenant à minima la vérification du bon démarrage pour une VM ou l'exécution d'au moins une requête basique pour une BDD)
- Identification (non nominative) des référents ou correspondants métiers pour la réalisation des tests sur les applications métier sur les systèmes critiques

Points d'attention et information

- Les référents métier sont identifiés en prévision de la conduite de tests fonctionnels (qui ne sont pas demandés dans cet objectif).
- Un établissement ayant rencontré un évènement en production l'ayant amené à restaurer les données d'une sauvegarde
  - sur le périmètre d'un SI critique
  - durant la phase opérationnelle
  - avec la formalisation d'un RETEX

  peut valoriser cette expérience en lieu et place de l'exercice attendu

Points de vigilance

- Au moins un des **tests menés doit concerner un environnement de production**. Celui-ci doit concerner un système dont la criticité pour l'activité de l'établissement est établie
- Dans le cadre de services centralisés (groupes nationaux) la **réalisation d'un test central embarquant l'ensemble des établissements du groupe** est acceptée. Le justificatif soumis devra préciser le périmètre d'applicabilité du test
- Les tests techniques doivent porter sur la **restauration d'une machine virtuelle ou d'une base de données** sur un **périmètre** d'un SI concourant à une des **activités critiques identifiées dans l'objectif D2.O1.C.**

D2.O4 Tester la sauvegarde et la restauration

Modalités pratiques pour la réalisation du test de restauration sur un environnement de production

Conditions attendues pour la réalisation du test

Réalisation de tests techniques portant sur la restauration d'une VM ou d'une base de données

Au moins un test conduit sur des données de production

Le test de restauration doit être réalisée sur un SI soutenant une activité critique identifiée dans l'objectif D2.O1.C

Axes de vigilance

Le test ne doit pas impacter la production : il s'agit de réaliser un test de restauration avec des données de production sur un environnement connexe

La plus grande vigilance est à apporter dans la préparation du test – notamment sur les scripts et fichiers de paramétrage – pour ne pas avoir d'impact sur l'environnement de production du système ou de systèmes connexes

Bonnes pratiques

La réalisation d'une recette métier et/ou d'un test terrain est recommandée (bien que seul l'identification d'un référent métier soit requis pour la conduite des tests fonctionnels)

L'utilisation d'un environnement reflétant au plus proche l'état de l'environnement de production

La simulation de la perte d'une salle machine pour tester la capacité à restaurer les données sur un site distant peut être pertinente

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

3. Trame et documents attendus au titre de la justification des coûts

Versement des financements

1. Sous-réserve de l'atteinte de l'ensemble des objectifs du domaine
2. D'un montant maximal correspondant au montant plafond défini dans le cadre du domaine
3. Sur la base des **justificatifs de dépenses réellement engagées durant la phase opérationnelle**, (i.e. bon de commande et facture émis durant cette phase ; charges humaines mobilisées durant cette phase). La phase opérationnelle court du 16 juillet 2025 jusqu'au dépôt du dossier d'atteinte des objectifs.
4. **Suite aux contrôles réalisés par les équipes en charge du contrôle de conformité financière** de l'ANS, qui sont souverain dans l'attribution d'un montant de financement. La **remise de l'ensemble des pièces exigées** par ces derniers constitue un **engagement** des candidats.

Maximisation des dépenses éligibles

Il est recommandé aux candidats, selon les dépenses effectivement engagées durant la phase opérationnelle, de **soumettre des justificatifs pour l'ensemble des dépenses réalisées en vue de l'atteinte des objectifs**

Pour les objectifs portant « l'inscription dans une démarche » (i.e. D2.O3.B et D2.O3.C), les **dépenses** mises en œuvre pour permettre **l'atteinte opérationnelle de la cible définie sont éligibles**.

Les candidats sont invités à réaliser une **analyse préalable des dépenses estimées** pour l'atteinte des cibles du domaine, et ce afin de pouvoir le cas échéant **engager des dépenses complémentaires** durant la phase opérationnelle afin de **maximiser leur financement.**

Le guide des dépenses éligibles mis à disposition sur le site de l'ANS apporte une lecture détaillée de l'éligibilité des dépenses par sous-objectif. Il précise également les modalités de contrôle des justificatifs financiers mise en œuvre. Pour y accéder, cliquez ici

Dépenses éligibles pour le domaine n°2 :

- Prestations externes pour la production des documents attendus ;
- Investissements logiciels (nouvelles licences, système de supervision des sauvegardes, …) contribuant à l'atteinte des objectifs ;
- Coûts internes (mobilisation de personnel) ;
- Coûts de formation sur la méthodologie de réalisation du PCRA ;
- Acquisition d'un SMCA ;
- Mise en œuvre d'un nouveau système de sauvegarde ;
- Evolution du système de sauvegarde dans une stratégie 3 – 2 – 1 ;
- Evolution de la solution d'authentification pour l'accès aux sauvegardes ;
- Nouveaux abonnements dans le cadre de l'atteinte des objectifs.

Dépenses non-éligibles pour le domaine n°2 :

- Frais de déplacement ;
- Formations générales en cybersécurité (ISO 27001, 27002, etc.) ;
- Dépenses liées à l'organisation d'évènements ou de la communication ;
- Achat de matériel informatique courant (ordinateur, téléphone, etc...) ;
- Frais récurrent de fonctionnement (abonnement internet, etc.) ;
- Audit de l'Active Directory ;
- Système de détection d'intrusion (caméra, alarme, etc.) ;
- Dépenses de travaux portant sur les locaux du candidat.

Conformément aux dispositifs européens, **seuls des « coûts nouveaux » sont éligibles** à un financement (qu'ils portent sur des prestations de services, de systèmes d'information ou des coûts internes) :

- **Les frais récurrents** d'hébergement d'applicatifs et d'abonnement ne **sont pas éligibles** si elles constituent des **dépenses préexistantes** au lancement du domaine.
- La création et la signature de **lettres de missions est recommandée** pour les agents particulièrement mobilisés dans l'atteinte des objectifs du domaine, bien qu'elles **ne fassent pas l'objet de contrôle de la part de l'ANS.**

La **trame de justification des coûts** est mise à disposition **sur le site de l'ANS** : elle doit être **obligatoirement renseignée** par tout candidat soumettant un dossier d'atteinte des objectifs (en sus des documents justificatifs exigés dans cette dernière).
Pour y accéder, cliquez ici

Une trame structurée autour de 3 volets :

Etape n°1 - pour les dépenses externes | **Pour les dépenses internes** | **Pour les recettes**

Eléments à renseigner :

- Type de coût (coût d'investissement, coût récurrent, etc.)
- Date de commande et date de facture
- Numéro de commande et de facture
- Tiers de la facture (fournisseur / prestataire)
- Intitulé de la prestation
- Montant de la facture
- Contribution de la dépense à l'atteinte de l'objectif

Coûts externes (prestations) et autres coûts (licences, montée de version ...)									
Type de coûts*	Date commande*	N° de commande*	Date facture*	N° facture*	Tiers de la facture*	Intitulé de la prestation externalisée*	Montant total facturé (€ TTC)*	Coûts engagés (€ TTC)	D2.01 - Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements
A renseigner	A renseigner	A renseigner	A renseigner	A renseigner	A renseigner	A renseigner	A renseigner	Ne pas renseigner	Coûts engagés (€ TTC)
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	
								0,00 €	

Le candidat doit transmettre l'ensemble des factures mentionnées aux équipes de l'ANS, et les factures doivent impérativement avoir été émise durant la période opérationnelle.

La **trame de justification des coûts** est mise à disposition **sur le site de l'ANS** : elle doit être **obligatoirement renseignée** par tout candidat soumettant un dossier d'atteinte des objectifs (en sus des documents justificatifs exigés dans cette dernière).
Pour y accéder, cliquez ici

Une trame structurée autour de 3 volets :

Pour les dépenses externes | **Etape n°2 - pour les dépenses internes** | Pour les recettes

Eléments à renseigner :

- Salaire brut
- Charges patronales *(séparément les éléments éligibles ou non)*
- Nombre d'heures productives annuelles
- Nombre d'heures effectives consacrées à l'atteinte d'objectifs
- Objectif de référence associé avec contribution à l'atteinte

		2025	2026	TOTAL (€)
[Matricule du salarié]	SALAIRE BRUT ANNUALISE (sans prorata)*			0,00
	CHARGES PATRONALES (sans prorata)*			0,00
	dont paiement des éléments non éligibles (sal brut)**			0,00
	dont paiement des éléments non éligibles (charges patronales)	0,00	0,00	0,00
	SALAIRE BRUT (hors éléments non éligibles)**	0,00	0,00	0,00
	CHARGES PATRONALES (hors éléments non éligibles)**	0,00	0,00	0,00
	S/TOTAL SALAIRES BRUTS + CHARGES PATRONALES	0,00	0,00	0,00
	NOMBRE D'HEURES PRODUCTIVES ANNUELLES			
	TAUX HORAIRE	0,00	0,00	
	NOMBRE D'HEURES EFFECTIVES CONSACREES A L'ACTION			0,00
	CHARGES DE PERSONNEL IMPUTABLES SUR L'ACTION	**0,00**	**0,00**	0,00
[Matricule du salarié]	SALAIRE BRUT ANNUALISE (sans prorata)*			0,00
	CHARGES PATRONALES (sans prorata)*			0,00
	dont paiement des éléments non éligibles (sal brut)**			0,00
	dont paiement des éléments non éligibles (charges patronales)	0,00	0,00	0,00
	SALAIRE BRUT (hors éléments non éligibles)**	0,00	0,00	0,00
	CHARGES PATRONALES (hors éléments non éligibles)**	0,00	0,00	0,00
	S/TOTAL SALAIRES BRUTS + CHARGES PATRONALES	0,00	0,00	0,00
	NOMBRE D'HEURES PRODUCTIVES ANNUELLES			
	TAUX HORAIRE	0,00	0,00	
	NOMBRE D'HEURES EFFECTIVES CONSACREES A L'ACTION			0,00
	CHARGES DE PERSONNEL IMPUTABLES SUR L'ACTION	**0,00**	**0,00**	0,00

En complément des éléments renseignés, le candidat devra fournir un récapitulatif annuel de paye 2025 et/ou 2026.

La **trame de justification des coûts** est mise à disposition **sur le site de l'ANS** : elle doit être **obligatoirement renseignée** par tout candidat soumettant un dossier d'atteinte des objectifs (en sus des documents justificatifs exigés dans cette dernière).
Pour y accéder, cliquez ici

Une trame structurée autour de 3 volets :

Pour les dépenses externes | Pour les dépenses internes | **Etapes n°3 - pour les recettes**

Eléments à renseigner :

- Nature / provenance des recettes perçues
- Montant des recette perçues

/!\ ces éléments doivent être renseignés séparément pour chaque objectif

Le dernier onglet de la trame « Synthèse des frais engagés » doit être soumis au format .pdf et dument signé par l'ordonnateur et le trésorier payeur / agent comptable.

Objectifs du domaine 2		Recettes perçues pour l'atteinte de l'objectif	
N°	Intitulé	Nature / provenance de la recette	Montants perçus (€ TTC)
		A renseigner	*A renseigner*
D2.O1.A	Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements		
D2.O2	Définir, documenter et tenir à jour la politique et le(s) plan(s) de sauvegarde et de restauration		
D2.O3	Construire un système de sauvegarde sécurisé		
D2.O4	Tester la sauvegarde et la restauration		

Contrôle exhaustif de 97 dossiers pilotes d'un montant inférieur à 50k€.
Ces analyses permettront de déterminer le taux d'erreur.

Tx : ∑(Mrevu – Minit)/ ∑Minit*100

Le taux d'erreur retranscrit l'écart (en %) entre (i) le montant attribué aux dossiers suite aux contrôles exhaustifs réalisés par les équipes de conformité financière, et (ii) le montant qui aurait été versé en l'absence de contrôle

- *Mrevu désigne le montant de financement préconisé par la direction des affaires financières à la suite du contrôle exhaustif*
- *Minit désigne le montant de financement qui aurait été versé par l'Agence du Numérique en Santé en l'absence de contrôle*

Le taux d'erreur est **inférieur à 2%**

Contrôle par sondage

Un contrôle **exhaustif a priori** est réalisé pour :

- **5%** des dossiers dont le montant de subventionnement demandé est **< 50 000€**
- **100%** des dossiers dont le montant de subventionnement demandé est **>= 50 000€**

Un contrôle **exhaustif a posteriori** est réalisé pour 5% des dossiers n'ayant pas déjà fait l'objet d'un contrôle *a priori*

Le taux d'erreur est **supérieur à 2%**

Contrôle exhaustif

Un contrôle **exhaustif a priori** est réalisé pour **100% des dossiers soumis**

Les candidats sont appelés à faire preuve de vigilance dans la transmission des justificatifs financiers, et notamment en (i) vérifiant préalablement l'éligibilité des dépenses, (ii) renseignant exhaustivement et correctement la trame de l'état financier, et (iii) assurant la transmission des justificatifs attendus *(commandes, factures, journaux de paye, …)*

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

4. Ressources mises à disposition des candidats

Webin-aire
Nos webinaires pour construire la e-santé de demain !

Une sélection de ressources documentaires est mise à disposition des candidats dans le cadre du domaine 2 du programme CaRE

- Arrêté du 3 juillet 2025
- Arrêté du 8 septembre 2025 modifiant l'Arrêté du 3 juillet 2025
- Replay du webinaire du 11/09
- Base des ES éligibles
- Guide des prérequis et objectifs du domaine 2
- Glossaire du domaine 2
- Trame de l'état financier pour la déclaration d'atteinte des objectifs du domaine 2
- Guide des dépenses éligibles du domaine 2
- Liste des preuves à vérifier avant le dépôt d'atteinte des objectifs
- Kit PCA/PRA
- Guide de la continuité d'activité du SGDSN
- Formation PCRA disponible sur la plateforme e-learning de l'ANS
- Catalogue des offres cyber

Les CRRC (Centres Régionaux de Ressources Cyber) proposent des services mutualisés et personnalisables, pour mieux prévenir et gérer la cybersécurité des établissements de santé

- **Aider** les structures sanitaires et médico-sociales à renforcer leur cybersécurité
- **Concevoir des services** pour prévenir et réagir aux cyberattaques
- **Proposer des formations** et **sensibiliser** aux bonnes pratiques en cybersécurité
- **Mobiliser** les capacités de soutien nécessaires en cas d'incident cyber

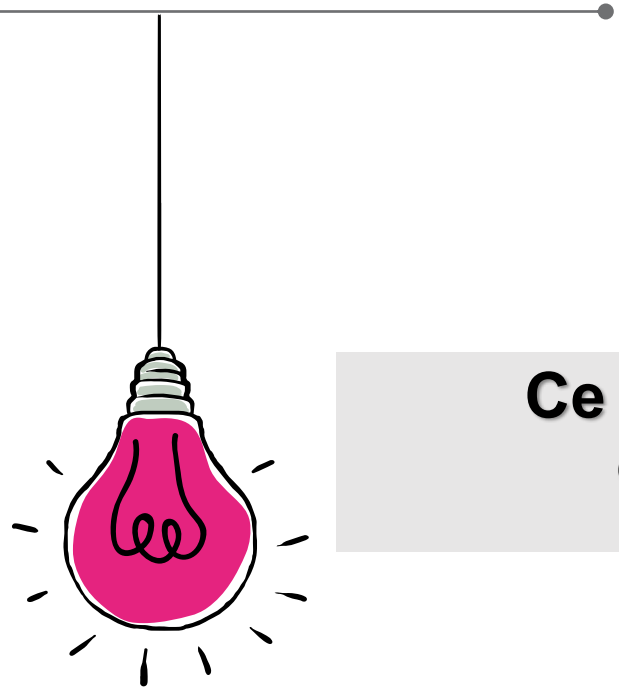
Cartographie des GRADeS

Prenez contact avec votre CRRC pour vous accompagner dans le renforcement de votre cybersécurité

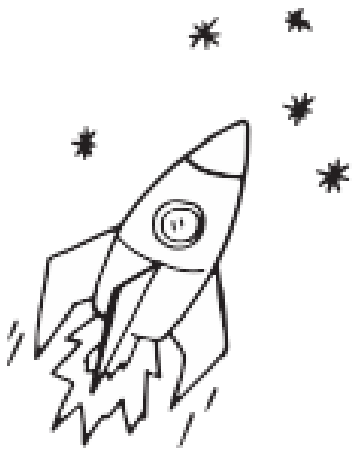
Webin-aire
Nos webinaires pour construire la e-santé de demain !

Pour toute demande autour du programme, les établissements sont invités à utiliser le support mis en place par l'ANS.

Page web dédiée au Programme CaRE sur le site de l'ANS : https://esante.gouv.fr/strategie-nationale/cybersecurite



Ce webinaire est enregistré et le replay sera mis à disposition sur la chaine Youtube de l'ANS

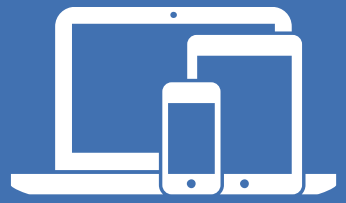


MERCI POUR VOTRE ATTENTION

ET A BIENTÔT SUR LE PROGRAMME

AGENCE DU NUMÉRIQUE EN SANTÉ

La transformation commence ici



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante