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 Domaine 2 : Accompagnement des industriels

16 mars 2026

Programme CaRE : Cybersécurité accélération et Résilience des Etablissements

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 programme CaRE
2. Rappels sur le domaine 2 et calendrier
3. Zoom sur les objectifs, preuves attendues et dépenses éligibles/non éligibles
4. Synthèse des dépenses éligibles / non éligibles
5. Accompagnement industriel
6. Ressources mises à disposition des candidats
7. Questions/Réponses

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

1. Rappels sur le programme CaRE

Les 4 axes du plan d'action CaRE

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.

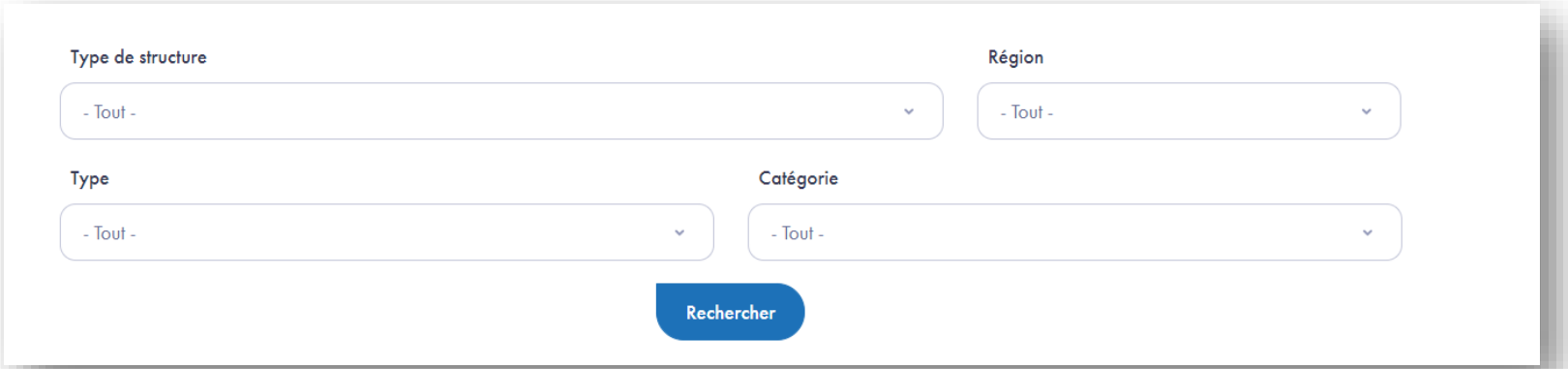
Sécurité Opérationnelle

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

L'axe 2 : Catalogue des offres cyber

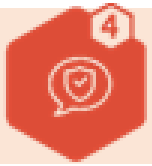
Dans le cadre de l'axe 2 du programme, l'ANS publie un « catalogue des offres cyber » qui collige plus de 900 offres proposées et diffusées par l'ANSSI, l'ANS, les GRADeS et les centrales d'achat (CAHPP, CAIH, RESAH) ainsi que plus de 450 offres d'industrielles, pour les établissements autour des thématiques : prévenir, contrôler, détecter, réagir et reconstruire.

- ✓ Une mise à jour **mensuelle**.
- ✓ Un catalogue basé sur **le déclaratif** et **accessible à tous** via le support du programme CaRE.



Catalogue des offres Cyber | Agence du Numérique en Santé

Les industriels souhaitant figurer dans ce catalogue sont invités à utiliser le support mis en place par l'ANS



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

2. Rappels sur le domaine 2 et calendrier

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

Enveloppe budgétaire : 45 M€

Sanitaire public et privé

1

Assurer la continuité et la reprise d'activité

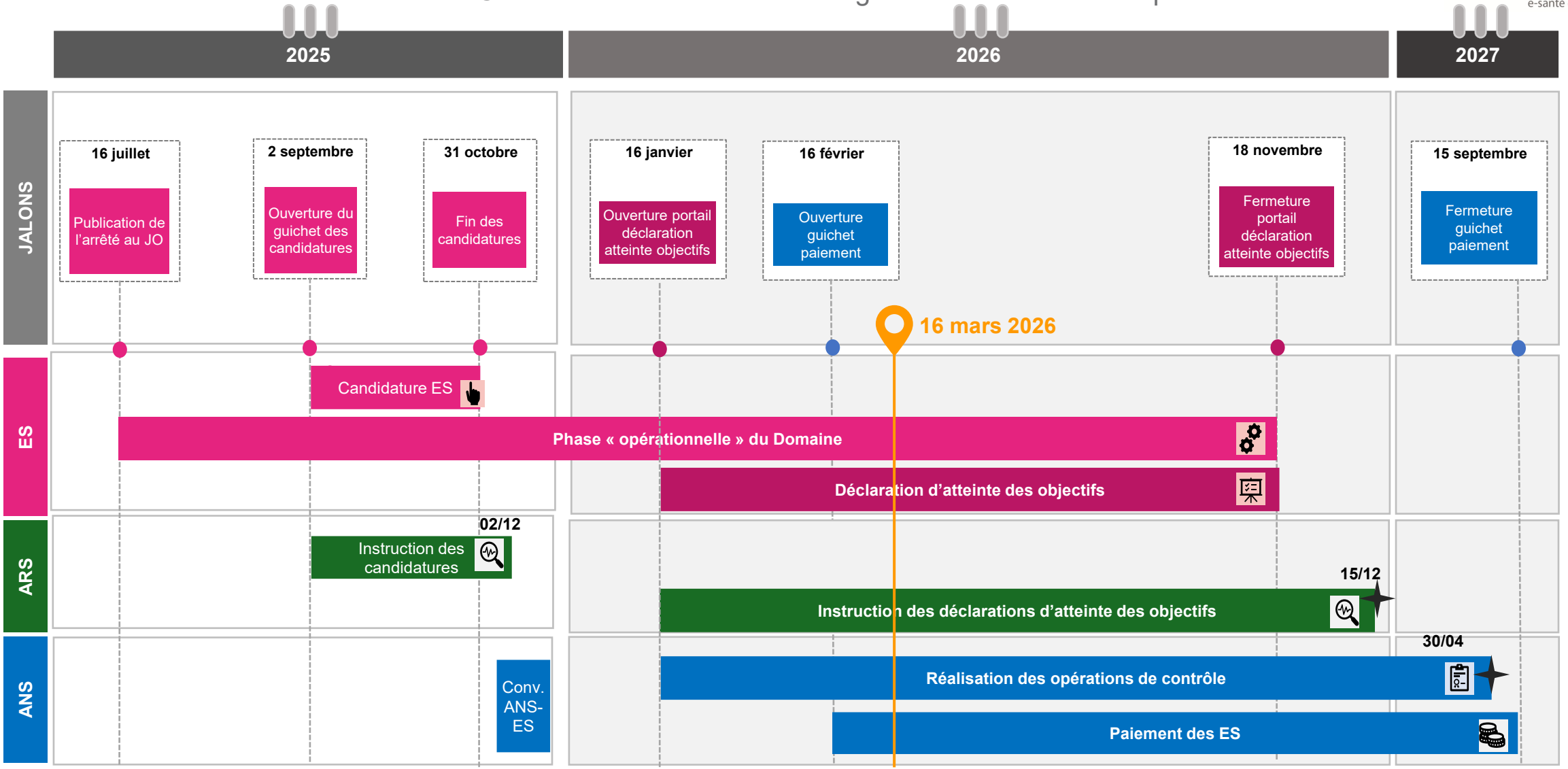
Capacité des établissements à se préparer, s'organiser et à réagir dans le cadre d'une cyberattaque

2

Construire une sauvegarde sécurisée

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

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



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

Arrêté du 16/07/2025

Phase de candidature
02 septembre – 02 décembre 2025

Phase d'atteinte des objectifs et paiement
16 janvier 2026 – 15 septembre 2027

La phase opérationnelle court depuis la publication de l'arrêté, jusqu'à la fermeture du portail de déclaration des objectifs

16 janvier 2026 — **Ouverture du portail de déclaration d'atteinte des objectifs**

- Les structures peuvent débuter la complétion des documents et déposer les justificatifs attendus

16 février 2026 — **Ouverture du guichet de paiement**

- Le versement des subventions débutera pour les établissements ayant atteint les objectifs du domaine.

18 novembre 2026 — **Fermeture du portail de déclaration d'atteinte des objectifs**

- Date limite de dépôt de l'ensemble des éléments justificatifs attendus pour valider l'atteinte des objectifs du domaine.

15 septembre 2027 — **Fermeture du guichet de paiement**

- Date limite de paiement des fonds alloués, sous réserve de l'atteinte des objectifs.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

3. Zoom sur les objectifs, preuves attendues et dépenses éligibles/non éligibles

Objectifs concernant le PCRA

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 concernant la sauvegarde

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

D2.O1.A Mettre en place une gouvernance pour la Continuité et de Reprise d'activité

Valeur cible / seuil d'éligibilité

- Formaliser le schéma de gouvernance décrivant la démarche mise en pace pour la continuité et la reprise d'activité – présentant notamment le comité de pilotage retenu, l'organisation du suivi du projet, et les équipes mobilisées

Pièces justificatives attendues

- Le schéma de gouvernance **signé** par la direction de l'établissement / GHT explicitant la démarche mise en place pour la continuité et la reprise d'activité
- Compte-rendu d'une instance de direction du candidat où le schéma de gouvernance a été présenté et validé (CODIR, COSTRAT, ...).

Points d'attention et information

- Le schéma de gouvernance doit être signée par le représentant légal du candidat
- Le schéma de gouvernance doit expliciter la démarche mise en place pour la continuité et la reprise d'activité *(contexte, prérequis, objectifs, bénéfices attendus, portée / périmètre, équipe / responsables et leurs rôles, comitologie, macro-planning, processus et méthodologie, communication, indicateurs de suivi, etc)*

Points de vigilance

- Le schéma de gouvernance doit être signé par le responsable juridique du candidat :
  - Le directeur de l'établissement support dans le cas d'un GHT ;
  - Le directeur de l'entité juridique candidate dans le cas d'un établissement seul (y-compris dans le cas où il s'agit d'une politique de groupe).

Dépenses éligibles

- ✓ Prestation externe : Accompagnement à la structuration de la gouvernance PCRA

D2.O1.B Décrire les procédures de réponse à la gestion de la crise cyber

Valeur cible / seuil d'éligibilité

- Intégrer les risques numériques dans le plan blanc
- Formaliser ou revoir les procédures de crise cyber – incluant l'organisation de la ou des cellules de crise et des modalités de signalement

Pièces justificatives attendues

- Plan blanc (ou extrait du plan blanc) intégrant : (i) les modalités de gestion des risques numériques, (ii) l'organisation de la ou des cellules de crise
- Procédure décrivant les modalités de signalement (montante et descendante) mise en place

Points d'attention et information

- Pour des structures multisites, le plan blanc peut être défini à l'échelle du candidat dans son ensemble, ou à l'échelle de chacune des entités composant le candidat

Points de vigilance

- **L'intégration des risques numériques dans le plan blanc n'est pas suffisante pour valider l'objectif D2.01.C** : le PCRA est un plan de réponse stratégique en cas d'évènement perturbateur entraînant une indisponibilité de ressource(s) critique(s), qui est complémentaire au Plan Blanc. Le PCRA est donc complémentaire au Plan Blanc, même si les deux documents peuvent intégrer des procédures communes.

Dépenses éligibles

- ✓ Prestation d'accompagnement à la formalisation / mise à jour du volet numérique du plan blanc
- ✓ Acquisition / abonnement à un outil de gestion de crise

Dépenses non éligibles

- × Acquisition / abonnement à un système de détection des intrusions
- × Acquisition / abonnement à des canaux de veille des failles et vulnérabilités pour la gestion des alertes descendantes

D2.O1.C Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) (1/2)

Valeur cible / seuil d'éligibilité

- Formaliser un Plan de Continuité et de Reprise d'Activité PCRA)
- Réaliser un Bilan d'Impacts sur les Activités (BIA) pour identifier les systèmes critiques sur les trois périmètres suivants :
  - un **service de soins** ayant un impact majeur sur la prise en charge
  - un **plateau technique** en lien avec le parcours
  - le **processus administratif le plus critique** pour la structure

Pièces justificatives attendues

- Bilan d'Impacts sur les Activités (BIA) établi sur un périmètre de structures couvrant au moins 66% de l'activité combinée du candidat
- Document énumérant les activités critiques à minima de chaque établissement
- PCRA sur les activités critiques identifiées
- Si un ou plusieurs BIA non réalisés : Motif(s) de non-présence du document.

Points d'attention et information

- L'attendu minimal porte sur la formalisation **du PCA de chaque activité critique** ayant fait l'objet d'un BIA.
- Le PCA et le PRA portent sur les **aspects métiers et organisationnels** de l'établissement, au-delà de l'aspect informatique seul.

Points de vigilance

- Parmi les 4 scénarios d'indisponibilité définis dans le kit PCA / PRA (ressources humaines, bâtiments, fournisseurs, informatique) : **le scénario d'indisponibilité des systèmes d'information et un 2nd scénario** au choix de l'établissement doivent être traités obligatoirement.
- **La charge relative à cet objectif doit être anticipée, et notamment car elle nécessite une forte mobilisation des équipes métier et qualité pour la réalisation du BIA.**
- **L'intégration des risques numériques dans le plan blanc n'est pas suffisante pour valider l'objectif D2.01.C** : le PCRA est un plan de réponse stratégique en cas d'évènement perturbateur entraînant une indisponibilité de ressource(s) critique(s), qui est complémentaire au Plan Blanc. Le PCRA est donc complémentaire au Plan Blanc, même si les deux documents peuvent intégrer des procédures communes

D2.O1.C Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) (2/2)

Dépenses éligibles

- ✓ Assistance à la réalisation des BIA (sur les périmètres critiques a minima et des périmètres idoines)
- ✓ Acquisition / abonnement à un SMCA (Système de Management de la Continuité d'activité)
- ✓ Coûts de mise en œuvre technique d'une brique de PCA (ex : solution de secours cloud)
- ✓ Coûts d'acquisition du matériel informatique nécessaire à la continuité d'activité (poste de travail « hors réseau », imprimantes, bornes d'accès 5G, etc.)
- ✓ Coûts associés à la formation des collaborateurs à l'utilisation des solutions de PCRA mises en œuvre

D2.O1.D Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain

Valeur cible / seuil d'éligibilité

- Effectuer un test pour la mise en œuvre d'au moins un PCA dans le cadre d'un exercice terrain
- Planifier la réalisation des autres exercices terrain du PCA

Pièces justificatives attendues

- PCA utilisés dans le cadre de l'exercice de terrain sur une des activités critiques, sur un périmètre de structures couvrant au moins **66% de l'activité du candidat**
- Scénario de test du PCA
- RETEX élaboré suite à l'exercice, et incluant un plan d'amélioration du PCA
- Planning de réalisation des autres exercices terrain

Points d'attention et information

- Le test doit nécessairement être réalisé durant la phase opérationnelle de l'appel à financement ;
- Il n'est pas nécessaire que les documents soient signés
- Il est possible de mutualiser ce test avec un exercice de cyber-crise (qui constituent deux tests distincts).

Points de vigilance

- Un test PCA ou exercice terrain **simule en temps réel l'indisponibilité d'une ou plusieurs ressources critiques** et teste la mise en œuvre des solutions de continuité d'activité à l'échelle des services de soins (niveau opérationnel)
- Le scénario de test doit porter sur **au moins l'un des scénarios d'indisponibilité** listés dans le kit PCA / PRA, bien qu'il soit recommandé de tester les 4 scénarios concomitamment.

Dépenses éligibles

- ✓ Prestation d'organisation d'un exercice PCA/PRA
- ✓ Appui à la rédaction du retour d'expérience

D2.O2.A Définir une politique de sauvegarde et de restauration, et la maintenir à jour (1/2)

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 se doit de porter une harmonisation des pratiques de sauvegarde indépendamment des dispositifs techniques. Elle n'exige pas pour autant l'unification du système de sauvegarde.

D2.O2.A Définir une politique de sauvegarde et de restauration, et la maintenir à jour (2/2)

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**

Dépenses éligibles

- ✓ Accompagnement à la rédaction / mise à jour de la politique

D2.O2.B Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour (1/2)

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

D2.O2.B Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour (2/2)

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.

Dépenses éligibles

- ✓ Prestation de formalisation / mise à jour des plans de sauvegarde / restauration

Dépenses non éligibles

- × Frais additionnels liés à l'évolution des contrats et/ou infrastructures de sauvegarde pour assurer le respect de la politique définie car cela ne contribue pas à l'atteinte du présent objectif. Ces dépenses sont éligibles et à déclarer en réponse à l'objectif D2.O3.C.

D2.O3.A Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde (1/2)

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**)

D2.O3.A Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde (2/2)

Points de vigilance

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

Dépenses éligibles

- ✓ Prestation d'audit et de cartographie de l'infrastructure de sauvegarde
- ✓ Frais associés à la mise en œuvre d'une authentification sécurisée : création d'un Active Directory distinct, achat de MIE dédiés, etc.
- ✓ Si applicable, dépenses engagées pour atteinte le niveau attendu de sécurité de l'Active Directory utilisé pour se connecter aux infrastructures de sauvegarde

Dépenses non éligibles

- × Si applicable, coûts de réalisation d'un audit pour l'AD dédié aux infrastructures de sauvegarde car cela ne contribue pas à l'atteinte de l'objectif qui requiert la réalisation d'un audit ADS (gratuit)

D2.O3.B S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde (1/2)

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)

Ressources utiles

- **Définition** : 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).

D2.O3.B S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde (2/2)

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.**
- 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).

Dépenses éligibles

- ✓ Achat d'équipements dédiés au cloisonnement du système de sauvegarde (ex : sous-réseau logique dédié (VLAN), pare-feu interne (filtrage des flux), serveurs ou machines virtuelles, logiciels de sauvegarde, chiffrement TLS des flux, …)
- ✓ Acquisition d'un outil de supervision du système de sauvegarde
- ✓ Définition de la trajectoire de cloisonnement et de supervision
- ✓ Paramétrage / intégration du cloisonnement et de la supervision
- ✓ Acquisition d'un pare-feu *quand cela contribue directement à l'atteinte de l'objectif, si et seulement si, le pare-feu est utilisé pour isoler et cloisonner le système de sauvegarde.*
- ✓ Achat d'un bastion d'administration uniquement si le bastion s'inscrit dans un projet plus large d'isolation de l'infrastructure qui doit inclure un cloisonnement du réseau (c'est-à-dire que le bastion apparaît dans le schéma d'architecture transmis)

Dépenses non éligibles

- × Mise en œuvre d'un pare-feu si cela correspond à des coûts de support, d'abonnement et de maintenance d'une solution de pare-feu déjà mise en place
- × Coûts humains ou de prestation permettant l'adaptation des locaux du candidat → Ces dépenses ne sont pas éligibles y compris pour la création et/ou rénovation de salles serveurs car les dépenses ne contribuent pas directement à l'atteinte des objectifs

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

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 (seuls les flux strictement nécessaires doivent circuler).
- 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

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).**

Ressources utiles

- **Définition** : 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).

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

Dépenses éligibles

- ✓ Mise en place d'un repository dimensionné pour accueillir la volumétrie de sauvegarde concernant les VM et bases de données critiques
- ✓ Achat de supports et équipements de sauvegarde supplémentaires (ex. disques, bandes WORM, coffre externe, stockage objet avec verrouillage, snapshots ou systèmes de sauvegarde offrant un mode immuable intégré)
- ✓ Achat d'un robot cassette
- ✓ Acquisition d'un pare-feu *quand cela contribue directement à l'atteinte de l'objectif, si et seulement si, le pare-feu est utilisé pour isoler et cloisonner le système de sauvegarde*
- ✓ Achat ou mise en place de solutions de sauvegarde immuables
- ✓ Prestation pour définir et/ou mettre en œuvre l'architecture 3-2-1
- ✓ Dépenses liées à l'évolution des salles de sauvegardes, à la création d'une 2nd salle de sauvegarde (redondance) ou à l'externalisation de la sauvegarde
- ✓ Frais additionnels liés à l'évolution des contrats et/ou infrastructures de sauvegarde pour assurer la mise en œuvre de la stratégie 3-2-1

Dépenses non éligibles

- × Mise en oeuvre d'un pare-feu si cela correspond à des coûts de support, d'abonnement et de maintenance d'une solution de pare-feu déjà mise en place
- × Coûts humains ou de prestation permettant l'adaptation des locaux du candidat → Ces dépenses ne sont pas éligibles y compris pour la création et/ou rénovation de salles serveurs car les dépenses ne contribuent pas directement à l'atteinte des objectifs

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

<u>En cas d'internalisation</u> :

- 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.

<u>Pour un GHT</u> : documents décrivant la gouvernance de contrôle de la réalisation des sauvegardes.

<u>En cas d'externalisation</u> :

- 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

Dépenses éligibles

- ✓ Implémentation d'un outil de centralisation des évènements (ex : par API) et de supervision

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.**

Dépenses éligibles

- ✓ Réalisation d'un test technique de restauration (VM ou base)
- ✓ Prestation d'accompagnement pour documenter le test
- ✓ Mise en place d'un environnement isolé de test

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

4. Synthèse des dépenses éligibles / non éligibles

Synthèse des dépenses éligibles

Prestations externes	• Ensemble des frais de prestations intellectuelles externes permettant d'accompagner le candidat dans l'atteinte des objectifs et la production des documents attendus.
Remédiation des niveaux de sécurité ou évolution de l'infrastructure de sauvegarde	• Ensemble des coûts mis en œuvre (prestations, acquisition de matériel ou investissement logiciel) pour soit (i) remédier à un niveau de sécurité inférieur aux objectifs fixés dans le domaine, ou (ii) mettre en œuvre les dispositifs de continuité d'activité et de stratégie de sauvegarde.
Investissement logiciel	• Ensemble des coûts d'investissement logiciel, y compris des frais d'abonnement, acquittés pour contribuer à l'atteinte des objectifs.
Coûts de formation des collaborateurs	• Ensemble des dépenses engagées pour assurer la formation des collaborateurs pour leur permettre de disposer des compétences attendues pour atteindre les objectifs du domaine.

Les dépenses sont éligibles **si et seulement si** :

> elles **contribuent directement** à l'atteinte d'un objectif du domaine
> elles sont **justifiées par des livrables** ou résultats concrets
> elles **constituent des dépenses nouvelles** engagées dans le cadre du dispositif

Les dépenses **préexistantes** ou **insuffisamment justifiées** ne sont **pas éligibles**.

Remarque : les dépenses réalisées durant la phase opérationnelle concourants à l'élaboration du PCRA sont éligibles, **y compris si le périmètre dépasse le périmètre minimal défini dans les objectifs** qui ne constitue pas une limite.

Remarque : pour les objectifs visant à « **s'inscrire dans une démarche »,** les investissements opérationnels réalisés **pour définir cette démarche ou la mettre en œuvre** sont bien valorisables au titre de l'AAF domaine 2.

Synthèse des dépenses **NON** éligibles

Frais de déplacement	• Frais liés aux déplacements des professionnels au sein des établissements du candidat : forfait kilométrique, ticket de péage, facture d'essence, note de restaurant, etc.
Formation des collaborateurs	• Frais associés à la réalisation de formations générales en cybersécurité (ex : ISO 27001, 27002, 27005 ou EBIOS) → ***Mais une formation** sur la méthodologie de **réalisation du PCRA** constituerait **une dépense éligible**.*
Dépenses diverses liées à l'organisation d'évènements et la communication	• Frais d'impression, de réalisation de campagnes de communication et/ou d'achats de prestation de restauration
Achat de matériel informatique courant	• Frais d'achats de matériel informatique courant : ordinateur, téléphone, borne wifi, imprimante, etc. → ***sauf** dans le cas spécifique où l'achat d'un matériel **permet directement** la mise en œuvre des **éléments formalisés dans le PCA/PRA**. Ces dépenses **ne sont pas à privilégier par le candidat.***
Frais récurent de fonctionnement	• Dépenses et abonnements récurrents permettant le fonctionnement nominal de la structure : abonnement internet, coûts d'électricité, etc.
Abonnements liés à la sauvegarde des applicatifs et des données	• Frais récurrents d'hébergement des applicatifs métiers et/ou abonnements à des solutions SaaS (à l'exception de solutions de SMCA) → ***Les nouvelles dépenses** concourant directement à l'atteinte d'un objectif) **sont éligibles**.*
Dépenses de travaux portant sur les locaux du candidat	• Coûts humains ou de prestation (par exemple, auprès d'entreprise de BTP) permettant l'adaptation des locaux du candidat
Numérisation des archives	• Coûts humains internes ou de prestations externes visant à la numérisation des archives médicales et/ou administratives

Chaque structure candidate doit renseigner et renvoyer à l'ANS une **trame de justification des dépenses,** et l'ensemble des pièces justificatives

Cette trame est structurée autour de 3 volets, avec un volet dédié aux **dépenses externes** :

Les structures candidates doivent renseigner les éléments suivants pour chaque dépense externe :

- 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

> Les industriels sont **invités à partager au plus tôt l'ensemble des informations nécessaires** à la complétion de la trame aux structures candidates (**factures et bons de commandes émis durant la phase opérationnelle** ..).

La complétude de la trame pouvant représenter un volume de travail conséquent, une saisie au fil de l'eau est recommandée aux structures.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

5. Accompagnement industriel

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

Rôle des industriels

Accompagner **les structures dans l'atteinte des objectifs du programme**, préférablement dans le cadre des **prestations éligibles à un financement.**

Fournir et transmettre en amont aux ES l'ensemble des **livrables nécessaires à la justification des objectifs et des coûts**, émises pendant la phase opérationnelle, afin de leur permettre de **finaliser leur dossier avant le 18 novembre 2026**.

Accompagner les structures **dans le cadre des demandes de documents complémentaires formulées par l'ANS**, afin de **faciliter le traitement collectif des dossiers** et de contribuer à la réduction des délais de paiement des subventions.

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

Synthèse des livrables attendus dans le cadre du domaine n°2 (1/3)

D2.O1.A

- **Le schéma de gouvernance** signé par la direction de l'établissement / GHT explicitant la démarche mise en place pour la continuité et la reprise d'activité
- **Compte-rendu d'une instance de direction** du candidat où le schéma de gouvernance a été présenté et validé (CODIR, COSTRAT, ...).

D2.O1.B

- **Plan blanc** (ou extrait du plan blanc) intégrant : (i) les modalités de gestion des risques numériques, (ii) l'organisation de la ou des cellules de crise
- **Procédure décrivant les modalités de signalement** (montante et descendante) mise en place

D2.O1.C

- **Bilan d'Impacts sur les Activités** (BIA) établi sur un périmètre de structures couvrant au moins 66% de l'activité combinée du candidat
- **Document énumérant les activités critiques**
- **PCRA sur les activités critiques identifiées**
- Si un ou plusieurs BIA non réalisés : **Motif(s) de non-présence du document.**

D2.O1.D

- **PCA utilisés dans le cadre de l'exercice de terrain** sur une des activités critiques, sur un périmètre de structures couvrant au moins 66% de l'activité du candidat
- **Scénario de test du PCA**
- **RETEX élaboré suite à l'exercice**, et incluant un plan d'amélioration du PCA
- **Planning de réalisation** des autres exercices terrain

D2.O2.A

- **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

D2.O2.B

- **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
- En cas de SI ou de sauvegarde externalisée : **calendriers des tests de sauvegarde** ou **éléments contractuels définissant les SLA fournis** par le prestataire.

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

Synthèse des livrables attendus dans le cadre du domaine n°2 (2/3)

D2.O3.A

- **Document présentant le rôle de l'opérateur** de sauvegarde
- **Document décrivant la gestion des rôles** pour l'accès à la sauvegarde
- **Document décrivant la solution de gestion 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 (preuve du refus du prestataire), noms du prestataire et de la solution

D2.O3.B

- **Schéma technique et fonctionnel de l'architecture** (actuelle ou cible) détaillant la matrice des flux techniques
- Le cas échéant, **un planning prévisionnel** (inférieur à 3 ans) d'atteinte du schéma cible quant au cloisonnement
- **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 (preuve du refus du prestataire) et noms du prestataire et de la solution

D2.O3.C

Cas d'une infrastructure internalisée :

- **Schéma technique et fonctionnel de l'architecture actuelle** détaillant la matrice des flux techniques (seuls les flux strictement nécessaires doivent circuler)
- Le cas échéant, 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

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

Synthèse des livrables attendus dans le cadre du domaine n°2 (3/3)

D2.O3.D

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

D2.O4

- **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

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

6. Ressources mises à disposition des candidats

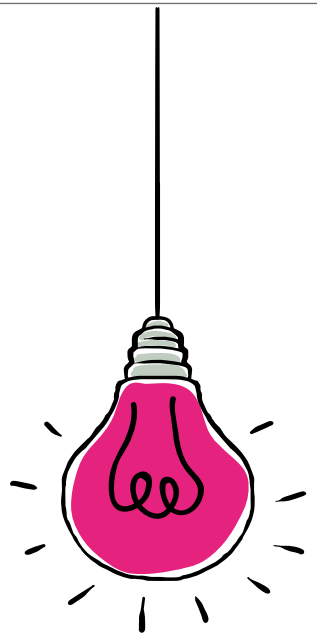
Webin-aire
Nos webinaires pour construire la e-santé de demain !

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 22/07
- Base des ES éligibles
- Guide des prérequis et objectifs du domaine 2
- Glossaire du domaine 2
- Kit ANS – Atelier PCRA service soins
- Kit PCA/PRA
- Guide de la continuité d'activité du SGDSN
- Formation PCRA disponible sur la plateforme e-learning de l'ANS
- Ressources méthodologiques relatives à l'organisation d'exercices de terrain
- Catalogue des offres cyber

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/CaRE



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

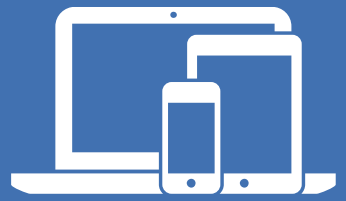
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

7. Questions / Réponses

Questions à poser dans l'onglet Q/R

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