Guide des objectifs

Appel à projets relatif à un programme de financement destiné à renforcer la sécurité Numérique des entités juridiques de santé social et médico-social

Parcours 3
Niveau de maturité cyber moyennement avancé

Historique du document – Suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V1	15/04/2026	Équipe programme CaRE	Version finale

SOMMAIRE

1. OBJECTIF DE CE GUIDE

L'objectif de ce guide est de détailler les objectifs du parcours 3 de la phase exploratoire de l'appel à projets médico-social destiné aux entités ayant un niveau de maturité cyber moyennement avancée.
Deux autres guides sont également mis à disposition par l'ANS pour les parcours 1 (Maturité cyber peu avancée – absence de ressources dédiées) et parcours 2 (Maturité cyber peu avancée - Ressources cyber en partie dédiées)).
En complément, un guide dédié aux prérequis est également disponible sur le site de l'ANS.

Pour rappel et conformément au cahier des charges relatif à la mise en œuvre de mesures de cybersécurité pour les établissements et services du secteur social et médico-social (ESSMS) - phase exploratoire (Proof Of Concept - POC) :

- Sont éligibles, les ESSMS relevant de l'article L.312-1 du Code de l'Action Sociale et des Familles (CASF).
  Les structures hybrides, exerçant à la fois des activités sanitaires et médico-sociales, sont bien éligibles à cet appel à projets. Toutefois, deux règles s'appliquent :
  - seules les activités relevant du champ médico-social peuvent bénéficier d'un financement dans le cadre de cet appel à projets ;
  - lorsque certains objectifs ont déjà été atteints par des structures médico-sociales dans le cadre de réponses à d'autres dispositifs du programme CaRE, leur réalisation n'est pas éligible à un nouveau financement dans le cadre de cet appel à projet.

- Sont acceptés tous types de regroupements d'ESSMS, notamment :
  - organismes gestionnaires (OG) ;
  - grappes d'établissements formées dans le cadre du programme ESSMS numérique (en incluant tous les établissements composant la grappe) ;
  - groupements de coopération sociale ou médico-sociale (GCSMS) ;
  - groupements territoriaux sociaux ou médico-sociaux (GTSMS) ;
  - tout groupement constitué par une convention de partenariat spécifiquement signée dans le cadre de l'appel à projets médico-social.

  A noter :
  - les différents types de groupements peuvent porter une candidature, cependant, seuls les entités juridiques et services du périmètre concerné sont éligibles au financement et pris en compte au titre du dispositif ;
  - les candidatures mono-entité juridique (mono-EJ) sont acceptées.

Notion de porteur du projet :

Dans le cadre d'un groupement ou d'un organisme gestionnaire, le projet est porté collectivement par l'ensemble des établissements et services sociaux et médico-sociaux constituant le groupement.
Une entité est désignée comme porteuse de projet, agissant pour le compte de l'ensemble des entités du groupement. Le porteur de projet assure la responsabilité administrative du dépôt de la candidature, de la contractualisation et de la gestion des subventions attribuées, sans préjudice de l'implication et de la responsabilité de chacun des établissements membres dans la mise en œuvre du projet.

De manière générale (et pas uniquement pour les groupements), le candidat s'appuiera sur sa propre organisation pour la mise en œuvre du projet et, s'il en a le besoin, sur un ou plusieurs fournisseurs de services numériques et de cybersécurité, ainsi qu'éventuellement sur des prestataires de services publics ou privés (expertise technique, pilotage de projet, conduite du changement, support, etc.).

Ci-dessous, le tableau récapitulatif des objectifs :
A noter : Les objectifs fixés dans le cadre de ce domaine doivent être traités, sauf mention contraire, par l'entité juridique candidate, ou par l'ensemble des entités juridique parties du groupement selon le cas.
La mention candidat constitue donc une mention générique qui traite les deux cas précités.

Objectifs	Description
Formalisation de la collaboration avec l'écosystème cyber (CRRC , GRADeS)	
POC.P3.O1.1 - Signer un acte de partenariat avec le GRADeS / CRRC	Le candidat doit formaliser un acte de partenariat (format juridique libre) précisant les modalités de collaboration avec le GRADeS (Groupement Régional d'Appui à la e-Santé) / CRRC (Centre Régional de Ressources en Cybersécurité).
Construction d'un cadre de référence pour la cybersécurité	
POC.P3.O2.1 - Elaborer une PSSI	Le candidat doit élaborer et fournir sa politique de sécurité des systèmes d'information (PSSI).
POC.P3.O2.2 - Elaborer des procédures de sécurité des SI	Le candidat doit définir, formaliser et maintenir à jour un ensemble de procédures de sécurité des systèmes d'information permettant de décliner opérationnellement les règles de sécurité définies dans la Politique de Sécurité des Systèmes d'Information (PSSI).
POC.P3.O2.3 - Formaliser et appliquer une procédure de gestion des comptes utilisateurs nominatifs et mettre en place une matrice d'habilitation	Le candidat doit fournir : • une procédure de gestion des comptes utilisateurs nominatifs couvrant l'ensemble du cycle de vie des comptes ; • une matrice d'habilitation, précisant les droits d'accès aux outils et applications en fonction des profils métiers, afin de garantir un accès aux ressources numériques strictement nécessaire aux missions exercées.
Mise en œuvre d'actions de sensibilisation à la cybersécurité	
POC.P3.O3.1 - Mettre en œuvre des actions de sensibilisation *informative* auprès de la Direction et du personnel	Le candidat doit identifier et mettre en œuvre au moins une action de sensibilisation informative auprès de la Direction et de l'ensemble du personnel. Les actions informatives ont pour objectif de développer une culture de base en cybersécurité, de sensibiliser aux risques numériques et de diffuser les bonnes pratiques essentielles en matière d'hygiène informatique. Le format des listes des actions est laissé au libre choix de la structure.
POC.P3.O3.2 - Mettre en œuvre des actions de sensibilisation	Le candidat doit identifier et mettre en œuvre au moins une action de sensibilisation applicative auprès de la Direction et de l'ensemble du

applicative **auprès de la Direction et du personnel**	personnel. Le format des listes des actions est laissé au libre choix de la structure. Les actions applicatives visent à ancrer les bonnes pratiques dans les usages quotidiens des professionnels, à travers des mises en situation, des cas pratiques ou des supports adaptés aux réalités métiers. Le format des actions de sensibilisation est laissé au libre choix de la structure.
Objectifs à atteindre « à la carte » par les structures (3 au choix)	
POC.P3.O4.A - Utiliser un réseau dédié et cloisonné pour l'administration	Le candidat doit mettre en place un réseau dédié et cloisonné réservé aux usages d'administration du système d'information, afin de renforcer la sécurité des accès sensibles et de limiter les risques de propagation d'incidents ou de compromission.
POC.P3.O4.B – Mettre en place un système d'enregistrement des logs de connexion internet, et de surveillance quotidienne du réseau et des équipements	Le candidat doit déployer un dispositif permettant l'enregistrement des journaux de connexion internet et assurer une surveillance régulière du réseau et des équipements, afin de détecter les événements de sécurité, les comportements anormaux et les tentatives d'intrusion.
POC.P3.O4.C - Réaliser un audit de la surface exposée sur internet, à renouveler annuellement	Le candidat doit réaliser un audit de la surface exposée sur internet, afin d'évaluer son niveau de résistance face à des tentatives d'attaque.
POC.P3.O4.D - Mettre en place au moins deux mesures identifiées comme prioritaire suite au diagnostic initial	Le candidat doit mettre en place au moins deux mesures de cybersécurité identifiées à l'issue du diagnostic initial. Les actions retenues doivent être sélectionnées à la suite d'un échange avec le GRADeS/CRRC, afin de garantir sa pertinence au regard du niveau de maturité de la structure, de ses priorités et des risques identifiés. Il est impératif que les actions à réaliser ne soient en aucun cas similaires ou redondant aux objectifs déjà spécifiés dans le cadre du présent appel à projets.
POC.P3.O4.E - Mettre en place un système de sauvegarde intègre et immuable *	Le candidat doit mettre en place un système de sauvegarde garantissant l'intégrité et l'immutabilité des données sauvegardées, afin de les protéger contre toute altération, suppression ou chiffrement malveillant.
POC.P3.O4.F - Instaurer une organisation et des procédures pour assurer le suivi efficace des sauvegardes ainsi qu'un plan d'action pour gérer les alertes *	Le candidat doit instaurer et documenter 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'incident.
POC.P3.O4.G - Mettre en œuvre la politique de sauvegarde et de restauration des données et tester les sauvegardes et les restaurations à fréquence régulière (tests techniques et fonctionnels) *	Le candidat doit fournir sa politique de sauvegarde et de restauration validée. Elle doit pouvoir s'appliquer aux prestations externalisées et aux applications gérées en mode SaaS par le biais de clauses contractuelles avec le prestataire. Le candidat doit aussi réaliser au moins un test technique de bon fonctionnement des sauvegardes et de remise en ligne des restaurations dans le système pendant la phase opérationnelle sur un périmètre d'un SI concourant à une activité critique.
POC.P3.O4.H - Elaborer un PCRA sur le scénario	Le candidat doit élaborer un Plan de Continuité et de Reprise d'Activité (PCRA) portant sur le scénario d'indisponibilité des systèmes

d'indisponibilité des Systèmes d'Information	d'information, couvrant au moins un processus métier critique (service de soin) et intégrant la prise en compte des risques numériques.

* *Précision relative aux objectifs de sauvegarde :*

Les objectifs de sauvegarde POC.P3.O4.E ; POC.P3.O4.F et POC.P3.O4.G sont indissociables dans leur mise en œuvre.
Ainsi, lorsqu'un candidat choisit de s'engager sur l'un de ces objectifs, il doit s'engager sur l'ensemble des trois, afin de garantir la cohérence, l'efficacité et la pérennité du dispositif de sauvegarde et de restauration des données.
Toutefois, lorsque le candidat a d'ores et déjà atteint un ou plusieurs de ces objectifs, le candidat peut sélectionner un objectif relevant du périmètre de la sauvegarde, complété par un ou plusieurs objectifs d'une autre nature, parmi les objectifs « à la carte » proposés.

Dans la suite du document, les objectifs sont décrits dans des fiches synthétiques composées :

- d'une définition ;
- de la méthode de production de l'indicateur associé à l'objectif ;
- des modalités de restitution de l'indicateur permettant de vérifier la bonne atteinte de l'objectif.

La phase opérationnelle est la période comprise entre :

- la date de publication du cahier de charges : 31 mars 2026 ;
- la date du dépôt de la déclaration d'atteinte des objectifs par le candidat sur le guichet dédié.

2. OBJECTIFS OBLIGATOIRES DE L'APPEL A PROJETS MEDICO-SOCIAL

Pour les organismes gestionnaires et les groupements : le pilotage de la réponse au présent appel à projet et le suivi de l'atteinte de ses objectifs par toutes les entités juridiques doivent être réalisés par la structure porteuse de la candidature. Une gouvernance transverse du projet permettant d'atteindre les objectifs doit être mise en place pour l'ensemble de l'organisme ou du groupement.

2.1 Formalisation de la collaboration avec l'écosystème cyber

POC.P3.O1.1 : Signer un acte de partenariat

1. Définition de l'objectif	
Définition	Signature d'un acte de partenariat entre la structure lauréate et le CRRC/GRADeS précisant les engagements respectifs des parties dans le cadre du projet soutenu par l'appel à projets.
Valeur cible / seuil d'éligibilité	La structure lauréate doit avoir signé un acte de partenariat avec le CRRC ou le GRADeS. Cette démarche devrait s'inscrire dans une logique de pérennité au-delà du présent domaine et être engagée dès le début des travaux de l'appel projets. En fonction de l'organisation du candidat, l'acte de partenariat doit être : • porté au niveau de l'entité juridique ou de l'organisme gestionnaire ; • établi au niveau de l'entité juridique porteuse de la candidature pour le groupement. Lorsque la candidature concerne plusieurs entités juridiques, l'acte de partenariat doit couvrir et mentionner l'ensemble des entités juridiques concernées. Remarque : aucun modèle type d'acte de partenariat n'est fourni dans le cadre du présent appel à projets. Chaque région est libre de proposer un acte de partenariat dans un format correspondant à son accompagnement. <u>Rôle et périmètre d'intervention du CRRC et du GRADeS</u> : le CRRC / GRADeS assure un accompagnement global des structures lauréates, en cohérence avec les objectifs médico-sociaux fixés dans l'instruction CRRC, et en s'appuyant le cas échéant sur les catalogues de services déjà en place. Dans le cas d'une candidature multi-régions, l'entité juridique porteuse de la candidature devra : • identifier une ou plusieurs régions référentes ; • fournir un ou des actes de partenariat correspondants.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	Acte de partenariat signé par l'ensemble des parties prenantes ou une convention / accord de partenariat formalisé précisant le périmètre et les engagements du projet
Opération de contrôle	Contrôle sur pièces

2.2 Construction d'un cadre de référence pour la cybersécurité

POC.P3.O2.1 : Elaborer une PSSI

1. Définition de l'objectif	
Définition	L'objectif consiste à formaliser une Politique de Sécurité des Systèmes d'Information (PSSI), définissant le cadre de référence de la cybersécurité au sein de la structure. La PSSI précise les objectifs de sécurité, les principes directeurs, ainsi que les règles organisationnelles et techniques applicables à l'ensemble des systèmes d'information, utilisateurs et partenaires de la structure. La PSSI doit couvrir *a minima* : • les objectifs de sécurité ; • le périmètre d'application ; • la gouvernance SSI et les responsabilités ; • le cadre règlementaire ; • les grands principes de protection du SI. La PSSI doit être diffusée aux acteurs concernés et sert de référence pour la mise en œuvre des mesures de sécurité.
Valeur cible / seuil d'éligibilité	Le candidat doit disposer d'une PSSI rédigée ou mise à jour entre la date de publication du cahier des charges (31 mars 2026) et la date de dépôt du dossier d'atteinte des objectifs. En fonction de son organisation, ce document peut être fourni par candidat ou par chaque établissement constituant le candidat. Si l'entité juridique ou groupement ne fournit pas une PSSI unique, l'établissement porteur de la candidature doit s'assurer que chaque établissement dispose de sa propre PSSI, signée par le directeur de l'établissement.
Textes de référence	• Guide d'élaboration de PSSI (ANSSI) • Guide pratique organisationnel PGSSI-S

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	La PSSI validée ou revue - entre la date de publication du cahier des charges (31 mars 2026) et la date de dépôt du dossier d'atteinte des objectifs - par le représentant légal du candidat ou, le cas

	échéant, par chaque établissement du groupement ou un document de présentation de la PSSI (et non la PSSI complète) selon un formalisme laissé à leur appréciation. Le document de présentation devra néanmoins présenter (i) la date de mise à jour, (ii) le signataire de la PSSI (iii) le périmètre des entités juridiques et/ou géographiques appliquant cette politique et doit être signé par le référent de cette politique.
Opération de contrôle	Contrôle sur pièces.

POC.P3.O2.2: Elaborer des procédures de sécurité des SI

1. Définition de l'objectif	
Définition	Définir et formaliser des procédures de sécurité des systèmes d'information afin de décliner opérationnellement les règles et principes définis dans la PSSI. Ces procédures décrivent les actions concrètes à mettre en œuvre pour prévenir les incidents de sécurité, détecter les événements anormaux et réagir efficacement en cas d'incident.
Valeur cible / seuil d'éligibilité	Un ensemble de procédures de sécurité formalisées est disponible, cohérent avec la PSSI et adapté au contexte de la structure. Ces procédures doivent couvrir *a minima* les thématiques suivantes : • la gestion des incidents de sécurité ; • la gestion des sauvegardes et restaurations ; • la gestion des mises à jour et correctifs ; • la gestion des accès et des habilitations.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	Ensemble de procédures de sécurité des SI formalisées, cohérentes avec la PSSI de la structure ou un document de synthèse des procédures SSI existantes, avec leur périmètre d'application
Opération de contrôle	Contrôle sur pièces

POC.P3.O2.3 : Formaliser et appliquer une procédure de gestion des comptes utilisateurs nominatifs et mettre en place une matrice d'habilitation

1. Définition de l'objectif	
Définition	La structure définit et applique une procédure formalisée de gestion des comptes utilisateurs nominatifs, couvrant : • la création des comptes lors de l'arrivée d'un collaborateur ; • l'évolution des habilitations en cas de changement de fonctions; • la suppression ou la désactivation des comptes lors du départ. Le service Ressources humaines (RH) joue un rôle central dans ce dispositif. Il est notamment chargé de notifier, dans des délais définis, les arrivées, départs et changements de situation des collaborateurs aux acteurs en charge de la gestion des comptes, afin de garantir la mise à jour effective des habilitations. Cette organisation est complétée par une matrice d'habilitation précisant les droits d'accès pour 3 services critiques, dont le DUI.
Valeur cible / seuil d'éligibilité	La structure dispose, pour tous les utilisateurs : • de procédures écrites décrivant l'organisation mise en place pour la gestion des comptes et des habilitations ; • d'une matrice d'habilitation. Le périmètre d'application de cet objectif couvre *a minima* 3 services critiques. L'entité juridique peut étendre ce périmètre à d'autres applications ou systèmes sensibles, en fonction de son organisation et de son niveau de maturité.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Procédure(s) de gestion des comptes utilisateurs, • Matrice d'habilitation (ou extrait).
Opération de contrôle	Contrôle sur pièces

2.3 Mise en œuvre d'actions de sensibilisation à la cybersécurité

POC.P3.O3.1: Mettre en œuvre des actions de sensibilisation informative auprès de la Direction et du personnel

1. Définition de l'objectif	
Définition	Développer une culture de cybersécurité au sein de la structure, auprès de la Direction comme du personnel, par des actions de sensibilisation à visée informative.
Valeur cible / seuil d'éligibilité	La structure formalise et met en œuvre au moins une action de sensibilisation à destination de la Direction et/ou du personnel. Le format des actions est laissé au libre choix de la structure, afin de s'adapter à son organisation, à ses moyens et à ses publics. À titre d'exemples, les actions de sensibilisation peuvent prendre les formes suivantes (liste non exhaustive) : • sessions de formation en présentiel ou en distanciel ; • modules e-learning, avec parcours adaptés aux profils métiers ; • webinaires (interventions d'experts cybersécurité, retours d'expérience) ; • quiz, défis ou auto-évaluations de connaissances ; • diffusion de supports pédagogiques (infographies, fiches réflexes, guides, newsletters) ; • campagnes de communication internes (affiches, écrans dynamiques) ; • podcasts ou vidéos courtes (témoignages, interviews) ; • etc. Les actions de sensibilisation peuvent être mutualisées ou externalisées, notamment au niveau régional, en s'appuyant sur les dispositifs existants tels que le Centre régional de ressources cyber (CRRC). Cette mutualisation vise en particulier à faciliter l'accès aux actions de sensibilisation pour les structures disposant de ressources humaines, techniques ou financières limitées. Il est fortement recommandé de prioriser les actions proposées dans le cadre du CRRC. A noter : même s'il est recommandé de réaliser 2 niveaux de sensibilisation en fonction du public ciblé (Direction et personnel), cela n'est pas exigé pour répondre à cet objectif.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Supports de sensibilisation utilisés ou diffusés *ou* • Programme ou compte rendu de session / webinaire *ou* • Attestations de participation, statistiques de diffusion ou de complétion, ou tout élément permettant d'attester de la mise en œuvre de l'action pendant la phase opérationnelle de l'appel à projets
Opération de contrôle	Contrôle sur pièces

POC.P3.O3.2 : Mettre en œuvre des actions de sensibilisation applicative auprès de la Direction et du personnel

1. Définition de l'objectif	
Définition	Renforcer les réflexes opérationnels de la Direction et du personnel face aux risques cyber, par des actions de sensibilisation à caractère pratique et expérientiel. Par sensibilisation applicative, on entend des actions permettant aux participants de se confronter concrètement à des situations à risque ou à des scénarios réalistes, afin de développer des réflexes opérationnels et des comportements adaptés face aux menaces cyber.
Valeur cible / seuil d'éligibilité	La structure doit formaliser et mettre en œuvre au moins une action de sensibilisation applicative à destination de la Direction et/ou du personnel. Le format des actions est laissé au libre choix de la structure, afin de s'adapter à son contexte et à son niveau de maturité. À titre d'exemples, les actions de sensibilisation applicative peuvent prendre les formes suivantes (liste non exhaustive) : • campagnes de phishing simulé, avec analyse des résultats et actions de feedback ; • exercices de gestion de crise cyber ; • ateliers pratiques dédiés à des thématiques cybersécurité ; • jeux pédagogiques (serious games, escape games), • capture the flag (CTF) ; • audits internes participatifs impliquant les collaborateurs dans l'identification des risques ; • etc. Les actions de sensibilisation peuvent être mutualisées ou externalisées, notamment au niveau régional, en s'appuyant sur les dispositifs existants tels que le Centre régional de ressources cyber (CRRC). Cette mutualisation vise en particulier à faciliter l'accès aux actions de sensibilisation pour les structures disposant de ressources humaines, techniques ou financières limitées. Il est fortement recommandé de prioriser les actions proposées dans le cadre du CRRC.

	A noter : même s'il est recommandé de réaliser 2 niveaux de sensibilisation en fonction du public ciblé (Direction et personnel), cela n'est pas exigé pour répondre à cet objectif.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Supports utilisés et livrables produits (scénarios, restitutions, analyses), *ou* • Résultats ou retours d'expérience (le cas échéant) *ou* • Attestations de participation, statistiques de diffusion ou de complétion, ou tout élément permettant d'attester de la mise en œuvre de l'action pendant la phase opérationnelle de l'appel à projets
Opération de contrôle	Contrôle sur pièces

3. OBJECTIFS FACULTATIFS DE L'APPEL A PROJETS MEDICO-SOCIA

Les objectifs présentés ci-après sont proposés à la carte. Les lauréats ne sont pas tenus de mettre en œuvre l'ensemble des objectifs listés.

Dans le cadre de l'appel à projets, il est toutefois demandé aux entités juridiques de **s'engager *a minima* sur la réalisation de trois objectifs**. Ces objectifs doivent être **choisis en concertation avec le CRRC/GRADeS** en fonction du contexte et des priorités opérationnelles.

POC.P3.O4.A : Utiliser un réseau dédié et cloisonné pour l'administration

1. Définition de l'objectif	
Définition	L'objectif consiste à mettre en place un réseau dédié et cloisonné, spécifiquement réservé aux opérations d'administration du système d'information. Ce réseau d'administration est distinct des autres réseaux de la structure et vise à isoler les usages et les accès sensibles afin de réduire la surface d'attaque et de renforcer la protection des composants critiques du système d'information. Le réseau d'administration repose sur une segmentation stricte, permettant de limiter les communications aux seuls flux nécessaires aux opérations d'administration. Il intègre un contrôle des accès renforcé, réservé à des profils autorisés, et prévoit l'interdiction des connexions croisées non justifiées entre le réseau d'administration et les autres réseaux (réseau utilisateur, réseau métier, etc.). Par ailleurs, l'objectif inclut une limitation de l'accès à internet depuis les postes ou serveurs utilisés pour l'administration, afin de réduire les risques d'exposition aux menaces externes et de compromission des comptes ou outils d'administration.
Valeur cible / seuil d'éligibilité	Pour atteindre l'objectif, le candidat doit disposer : • d'un réseau d'administration dédié et opérationnel, distinct des autres réseaux ; • d'une segmentation effective permettant d'isoler les flux d'administration ; • de règles de contrôle des accès limitant l'utilisation du réseau d'administration aux seuls utilisateurs et équipements autorisés ; • de mécanismes interdisant les connexions croisées non justifiées entre le réseau d'administration et les autres réseaux ; • de mesures restreignant l'accès à internet depuis les postes ou serveurs utilisés pour l'administration, conformément aux besoins strictement nécessaires.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	Document décrivant le réseau d'administration mis en place mettant en évidence le cloisonnement et les règles d'accès
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.B : Mettre en place un système d'enregistrement des logs de connexion internet, et de surveillance quotidienne du réseau et des équipements

1. Définition de l'objectif	
Définition	La journalisation des connexions internet et la surveillance régulière du réseau et des équipements constituent un élément essentiel de la détection des incidents de sécurité. Cet objectif vise à disposer d'une visibilité suffisante sur les événements affectant le système d'information afin d'identifier les comportements anormaux, analyser les incidents et réagir de manière appropriée.
Valeur cible / seuil d'éligibilité	Pour atteindre l'objectif, le candidat doit disposer : • d'un système d'enregistrement des logs de connexion internet couvrant le périmètre du système d'information concerné ; • de journaux centralisés et exploitables, permettant l'analyse des événements de sécurité ; • d'une organisation assurant une surveillance quotidienne du réseau et des équipements (postes, serveurs, équipements réseau, solutions de sécurité).
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Description du dispositif d'enregistrement des logs et de surveillance mis en place • Extrait ou exemple de journaux collectés • Document décrivant l'organisation de la surveillance quotidienne et la gestion des alertes
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.C : Réaliser un audit de la surface exposée sur internet, à renouveler annuellement

1. Définition de l'objectif	
Définition	Un audit de la surface exposée sur internet permet d'en évaluer le niveau de sécurité et de détecter d'éventuelles vulnérabilités concourant ainsi à une démarche d'amélioration continue de la sécurité.
Valeur cible / seuil d'éligibilité	Un audit de la surface exposée sur internet est réalisé via le service Cybersurveillance[1] mis à disposition par l'Agence du Numérique en santé. Un audit de ce type devrait être réalisé annuellement ou après des évolutions majeures du SI.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	Rapport d'audit de cyber-surveillance
Opération de contrôle	Contrôle sur pièces

[1] Les services | Portail du CERT Santé

POC.P3.O4.D Mettre en place au moins deux mesures identifiées comme prioritaires suite au diagnostic initial

Définition	Engager des actions concrètes d'amélioration de la cybersécurité, adaptées au niveau de maturité de la structure, en traduisant les résultats du diagnostic initial en premières mesures opérationnelles accessibles et réalistes. La structure met en œuvre au moins deux mesures identifiées comme prioritaires à l'issue du diagnostic initial. Les actions retenues sont sélectionnées en concertation avec le GRADeS/CRRC, afin d'assurer leurs pertinences et leurs faisabilités. Il est impératif que les actions sélectionnées ne soient en aucun cas similaires ou redondantes avec celles associées à des objectifs du présent parcours de l'appel à projets.
Valeur cible / seuil d'éligibilité	Cet objectif vise prioritairement la mise en place d'un socle minimal de mesures simples, constituant des premiers leviers d'amélioration de la posture de cybersécurité de la structure. À titre d'exemples, ce socle minimal peut inclure une ou plusieurs des mesures suivantes (liste non exhaustive) : • décrire l'organisation projet pour la mise en œuvre de la sécurisation des accès distants ; • disposer d'une liste des typologies des accès distants de ses prestataires et fournisseurs ; • disposer d'une liste des typologies des utilisateurs agents de l'établissement et partenaires et de leurs accès distants ; • déploiement ou renforcement d'un antivirus / EDR sur les postes ou serveurs critiques ; • mise en place de règles de filtrage réseau complémentaires sur un périmètre ciblé ; • etc. Ces mesures ne nécessitent pas de transformation technique lourde et doivent être adaptées aux capacités et aux ressources de la structure.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Attestation ou compte rendu d'un échange avec le CRRC, identifiant des actions à réaliser • Description de la mesure réalisée • Livrables ou éléments attestant de sa mise en œuvre
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.E : Mettre en place un système de sauvegarde intègre et immuable

Pour rappel, les objectifs relatifs à la sauvegarde (POC.P3.O4.E, POC.P3.O4.F et POC.P3.O4.G) sont indissociables dans leur mise en œuvre : l'engagement sur l'un de ces objectifs implique un engagement sur l'ensemble des objectifs de sauvegarde, sauf lorsque le candidat justifie avoir déjà atteint un ou plusieurs de ces objectifs.

1. Définition de l'objectif	
Définition	L'objectif consiste à déployer un système de sauvegarde garantissant l'intégrité et l'immutabilité des données, afin de protéger les informations critiques contre les risques de perte, d'altération ou de chiffrement malveillant, notamment en cas de cyberattaque. Le dispositif de sauvegarde repose sur des mécanismes techniques assurant l'immutabilité des données sauvegardées, tels que des solutions de stockage immuable (par exemple WORM, snapshots immuables, coffres-forts numériques) et non uniquement sur des mesures organisationnelles. Il intègre également des procédures régulières de vérification de l'intégrité des sauvegardes et de restauration, permettant de s'assurer de la fiabilité et de l'exploitabilité des données sauvegardées en cas d'incident. Le périmètre couvert inclut *a minima* le DUI.
Valeur cible / seuil d'éligibilité	Pour atteindre l'objectif, le candidat doit disposer : • d'un système de sauvegarde intégrant des mécanismes techniques d'immutabilité, garantissant l'intégrité des données sauvegardées sur un périmètre critique (*a minima* DUI), • de procédures de vérification et de restauration associées.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	Document décrivant les procédures de sauvegarde et précisant les périmètres couverts
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.F : Instaurer une organisation et des procédures pour assurer le suivi efficace des sauvegardes ainsi qu'un plan d'action pour gérer les alertes

Pour rappel, les objectifs relatifs à la sauvegarde (POC.P3.O4.E, POC.P3.O4.F et POC.P3.O4.G) sont indissociables dans leur mise en œuvre : l'engagement sur l'un de ces objectifs implique un engagement sur l'ensemble des objectifs de sauvegarde, sauf lorsque le candidat justifie avoir déjà atteint un ou plusieurs de ces objectifs.

1. Définition de l'objectif	
Définition	Le suivi des sauvegardes et la gestion des alertes associées reposent sur une organisation claire et des procédures formalisées. La sauvegarde des données est essentielle, mais la supervision de ces activités est tout aussi indispensable pour assurer la restauration des données, en particulier celles critiques, à la suite d'un incident, attaque ou perte informatique. La supervision doit s'appuyer *a minima* sur les outils de sauvegarde existants, permettant de générer des rapports de suivi de la réalisation des sauvegardes.
Valeur cible / seuil d'éligibilité	Le candidat doit 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.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Procédure de suivi et de contrôle des sauvegardes • Exemple de tableau de suivi ou de rapport de sauvegarde • Plan d'action ou procédure de gestion des alertes liées aux sauvegardes
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.G : Mettre en œuvre la politique de sauvegarde et de restauration des données et tester les sauvegardes et les restaurations à fréquence régulière (tests techniques et fonctionnels)

Pour rappel, les objectifs relatifs à la sauvegarde (POC.P3.O4.E, POC.P3.O4.F et POC.P3.O4.G) sont indissociables dans leur mise en œuvre : l'engagement sur l'un de ces objectifs implique un engagement sur l'ensemble des objectifs de sauvegarde, sauf lorsque le candidat justifie avoir déjà atteint un ou plusieurs de ces objectifs.

1. Définition de l'objectif	
Définition	La mise en œuvre de la politique de sauvegarde et de restauration des données s'accompagne de tests réguliers afin de vérifier l'efficacité des dispositifs en place. Ces tests, techniques et fonctionnels, permettent de s'assurer de la capacité réelle de restauration des données et de reprise des activités en cas d'incident.
Valeur cible / seuil d'éligibilité	Le candidat doit fournir sa politique de sauvegarde et de restauration validée. Elle doit pouvoir également s'appliquer aux prestations externalisées et aux applications gérées en mode SaaS par le biais de clauses contractuelles avec le prestataire, et doit avoir été rédigée ou mise à jour entre la date de publication du cahier des charges (31 mars 2026) et la date de dépôt du dossier d'atteinte des objectifs. La politique de sauvegarde et de restauration doit inclure, *a minima*, les éléments suivants : • les types de données à sauvegarder (base de données, applications, serveurs, documents, ...) ; • la hiérarchisation des données en fonction de leur criticité ; • la fréquence des sauvegardes en fonction de la criticité des données ; • le délai de rétention en fonction de la typologie des données ; • la planification des sauvegardes en fonction de l'activité ; • les responsabilités des personnels impliqués dans le processus des sauvegardes ; • les exigences de conformité légale et réglementaire (RGPD, LIL, ...) ; • les procédures de mise à jour de la politique de sauvegarde ;

	• les mesures de sécurisation des sauvegardes (chiffrement, contrôle d'accès, ...) ; • les mesures sur la confidentialité et l'intégrité des données. Le candidat doit aussi réaliser des tests techniques (restauration d'une machine virtuelle, d'une base de données, vérification du bon redémarrage) et fonctionnels (en lien avec les usages métiers des applications concernées) de : • bon fonctionnement des sauvegardes ; • remise en marche du système suite à la restauration. Les tests portent prioritairement sur un périmètre critique du système d'information, concourant à une activité essentielle de la structure. Les tests de sauvegarde et de restauration doivent être réalisés au moins une fois par an et documentés. Dans le cadre de services centralisés (groupements) la réalisation d'un test central embarquant l'ensemble des établissements du groupe est acceptée si les mesures de sauvegarde sont identiques dans l'ensemble des établissements. Le justificatif soumis devra préciser le périmètre d'applicabilité du test.
Textes de référence	N/A

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Politique ou procédure de sauvegarde et de restauration appliquée • Document précisant le périmètre des tests • Document précisant la planification des prochains tests • Cahier de tests de l'opération de restauration (contenant *a minima* la vérification du bon démarrage pour une VM ou l'exécution d'au moins une requête basique pour une BDD)
Opération de contrôle	Contrôle sur pièces

POC.P3.O4.H : Elaborer un PCRA sur le scénario d'indisponibilité des Systèmes d'Information

1. Définition de l'objectif	
Définition	Le Plan de Continuité et de Reprise d'Activité (PCRA) relatif au scénario d'indisponibilité des systèmes d'information vise à anticiper les impacts d'une interruption majeure du SI. Il permet d'identifier les activités critiques, d'organiser les priorités de reprise et de définir les modalités de continuité afin de limiter les conséquences sur le fonctionnement de la structure. Le PCRA est élaboré en s'appuyant sur les kits nationaux mis à disposition par l'ANS[2] et couvre *a minima* un processus métier critique (par exemple un service de soin ou un processus essentiel au fonctionnement de l'établissement). Il intègre la prise en compte des risques numériques dans la gestion globale des risques de la structure et formalise les rôles, responsabilités et instances de pilotage associées.
Valeur cible / seuil d'éligibilité	Pour atteindre l'objectif, le candidat doit disposer : • d'un PCRA formalisé, dédié au scénario d'indisponibilité des systèmes d'information couvrant au moins un processus métier critique, identifié comme prioritaire par la structure ; • de la constitution d'un comité de pilotage PCRA, chargé du suivi et de la mise en œuvre du plan ; • d'une organisation de réunions régulières de suivi du PCRA ; • d'une intégration explicite des risques numériques dans la démarche globale de gestion des risques de l'établissement. Le PCRA doit être validé par les responsables concernés (direction et métiers) et être cohérent avec l'organisation, les ressources et le niveau de maturité de la structure.
Textes de référence	KIT PCRA ESMS

2. Production de l'objectif	
Unité	Booléen
Modalité de calcul	N/A
Période	Sur la durée de l'appel à projets
Fréquence	Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• PCRA formalisé sur le scénario d'indisponibilité des SI • Preuve de constitution du comité de pilotage PCRA (composition, mandat, etc.) • Compte rendu ou calendrier de réunions de suivi du PCRA

[2] https://esante.gouv.fr/actualites/du-nouveau-pour-securiser-les-systemes-dinformation-de-vos-etablissements-dans-le-secteur-medico-social

	• Élément attestant de la prise en compte des risques numériques dans la gestion globale des risques
Opération de contrôle	Contrôle sur pièces