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 2
Niveau de maturité cyber peu avancée – Ressources cyber (en partie) dédiées

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 2 de la phase exploratoire de l'appel à projets médico-social destiné aux entités ayant un niveau de maturité cyber peu avancé et disposant de ressources cyber en partie dédiées.
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 3 (Maturité cyber moyennement avancée).

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.P2.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.P2.O2.1 - Elaborer une charte de sécurité des SI et la diffuser auprès de l'ensemble du personnel	Le candidat doit élaborer une charte de sécurité informatique, précisant les règles et bonnes pratiques pour la protection des SI, et assurer sa diffusion et application par les utilisateurs.
POC.P2.O2.2 - Définir et appliquer une politique globale de sécurisation des modalités d'authentification	Le candidat doit fournir une politique de sécurisation des modalités d'authentification adaptée aux usages et aux risques, et mettre en œuvre les mesures techniques et organisationnelles permettant son application effective sur les systèmes concernés.
POC.P2.O2.3 - Définir et appliquer une procédure formalisée 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.
POC.P2.O2.4 - Mettre en place une comitologie cyber récurrente	Le candidat doit organiser des réunions régulières dédiées à la gouvernance de la cybersécurité, impliquant les parties prenantes clés. Il doit assurer le suivi des actions, l'évaluation des risques et la prise de décisions pour piloter efficacement la stratégie de sécurité informatique.
Mise en œuvre d'actions de sensibilisation à la cybersécurité	
POC.P2.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.P2.O3.2 - Mettre en œuvre des actions de sensibilisation *applicative* auprès de la Direction et du personnel	Le candidat doit identifier et mettre en œuvre au moins une action de sensibilisation applicative auprès de la Direction et de l'ensemble du 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.P2.O4.A - Réaliser un inventaire des composants du SI à l'aide d'un outil automatisé et retirer/remplacer tous les composants obsolètes	Le candidat doit réaliser un inventaire exhaustif et à jour de son parc informatique, couvrant l'ensemble des équipements matériels et logiciels utilisés par la structure. Cet inventaire, réalisé à l'aide d'un outil automatisé, vise à disposer d'une vision globale des actifs du système d'information afin d'en faciliter

	la gestion. Il doit *a minima* porter sur les postes de travail, serveurs, imprimantes, systèmes d'exploitation et logiciels installés. Sur la base de cet inventaire, le candidat doit identifier les éléments obsolètes, puis planifier et exécuter leur retrait ou remplacement afin de garantir la sécurité et la performance du SI.
POC.P2.O4.B - Réaliser une cartographie des applications et technologies utilisées	Le candidat doit élaborer une cartographie détaillée des applications métiers et des technologies associées afin de visualiser les relations, les flux et les composants techniques.
POC.P2.O4.C - Sécuriser le réseau Internet professionnel	Le candidat doit sécuriser son réseau internet professionnel, notamment par l'installation et le paramétrage d'équipements de sécurité réseau actifs et par la mise en place de dispositifs de filtrage et de supervision adaptés.
POC.P2.O4.D - Définir une politique de gestion des identités et des comptes à privilèges	Le candidat doit définir et formaliser une politique encadrant la gestion des identités et des comptes à privilèges afin de maîtriser l'attribution des droits élevés et de limiter les risques liés aux accès administrateurs au sein du système d'information.
POC.P2.O4.E - Mettre en place au moins une mesure identifiée comme prioritaire suite au diagnostic initial	Le candidat doit mettre en place au moins une mesure de cybersécurité identifiée à l'issue du diagnostic d'entrée dans les parcours. L'action retenue doit être sélectionnée 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 l'objectif sélectionné ne soit en aucun cas similaire ou redondant avec ceux déjà spécifiés dans le cadre du présent appel à projets.
POC.P2.O4.F - Définir une politique de sauvegarde et de restauration des données cohérentes avec les besoins métiers, à valider avec la direction	Le candidat doit fournir sa politique de sauvegarde et de restauration validée par la direction. Elle doit pouvoir 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.
POC.P2.O4.G - Rédiger une fiche « processus métier » en suivant la méthodologie de construction du PCRA, et la diffuser auprès du personnel concerné	Le candidat doit rédiger une fiche processus métier en appliquant la méthodologie du kit PCRA ESMS[1]. Une fois rédigée, le candidat devra assurer sa diffusion auprès du personnel concerné pour garantir la compréhension et l'application du processus.

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.

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

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.P2.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. Rôle et périmètre d'intervention du CRRC et du GRADeS : 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.P2.O2.1 : Elaborer une charte de sécurité des SI et la diffuser auprès de l'ensemble du personnel

1. Définition de l'objectif	
Définition	Mettre en place une charte de sécurité des systèmes d'information visant à encadrer les usages numériques au sein de la structure et à formaliser les règles de sécurité applicables aux utilisateurs (personnel, intervenants, prestataires le cas échéant). Cette charte contribue à rappeler notamment : • la gestion et confidentialité liées à la gestion des identités et des accès ; • les conditions dans lesquelles les SI doivent être utilisés ; • les règles de sécurité applicables lors de l'accès au système d'information depuis l'extérieur ; • les comportements attendus des utilisateurs afin de limiter les risques pour le système d'information. • les conséquences possibles en cas de non-respect des règles définies, conformément au cadre réglementaire et applicable dans l'établissement le cas échéant. Elle participe ainsi à une utilisation responsable et sécurisée des SI par les utilisateurs.
Valeur cible / seuil d'éligibilité	La structure dispose d'une charte de sécurité des SI formalisée, diffusée aux utilisateurs. Cette charte doit être : • soit annexée au règlement intérieur ; • soit, à titre transitoire, signée par le personnel en attendant son intégration formelle dans le règlement intérieur.
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	• Règlement intérieur intégrant la charte *pu* • Charte avec un document décrivant la procédure de diffusion et de prise de connaissance de la charte par le

	personnel (modalités de communication, de signature ou d'accusé de réception)
Opération de contrôle	Contrôle sur pièces

POC.P2.O2.2 : Définir et appliquer une politique globale de sécurisation des modalités d'authentification

1. Définition de l'objectif	
Définition	Mettre en œuvre une politique globale de sécurisation des modalités d'authentification, visant à garantir un accès sécurisé aux systèmes d'information, notamment par la gestion des mots de passe et/ou la mise en place d'un dispositif d'authentification multifacteur (MFA).
Valeur cible / seuil d'éligibilité	La structure a défini et applique une politique d'authentification formalisée, intégrant sur : • des règles de gestion des mots de passe ; (et/ou) • un dispositif d'authentification multi-facteur (MFA) conforme au Référentiel d'Identification Electronique v2. La politique d'authentification doit couvrir l'intégralité du SI, avec des mesures adaptées aux différents types d'applications et risques associés.
Textes de référence	Le référentiel d'identification électronique v2 de la 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	Politique d'authentification formalisée
Opération de contrôle	Contrôle sur pièces

POC.P2.O2.3 : Définir et appliquer une procédure formalisée 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 2 services critiques dont le DPI.
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* 2 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

POC.P2.O2.4 : Mettre en place une comitologie cyber récurrente

1. Définition de l'objectif	
Définition	Structurer et piloter la gouvernance de la cybersécurité au sein de la structure, en instaurant une comitologie cyber récurrente permettant de suivre le niveau de sécurité des systèmes d'information, de coordonner les acteurs concernés et de piloter les actions de prévention et de traitement des risques cyber. La structure met en place une comitologie dédiée à la cybersécurité, organisée autour de comités réguliers, dont la fréquence et le périmètre sont définis. Cette comitologie a pour objectifs de : • partager un état des lieux du niveau de sécurité du système d'information, • suivre les incidents de sécurité et les événements significatifs, • piloter les plans d'actions et les mesures correctives, • suivre l'avancement des projets et des actions de sécurisation, • sensibiliser et mobiliser les parties prenantes sur les enjeux de cybersécurité.
Valeur cible / seuil d'éligibilité	La structure doit avoir une comitologie cyber formalisée, mise en œuvre et opérationnelle. Elle doit être réaliser à fréquence définie (a minima annuelle), disposant d'un périmètre clair et d'objectifs formalisés
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 validé par la direction, décrivant l'organisation du comité cyber mis en place pour la sécurisation du système d'information, incluant *a minima* : - les acteurs impliqués (Direction, DSI, Coordonnateur SSI, métiers, etc.) - les rôles et responsabilités des acteurs mobilisés - les modalités de fonctionnement (périmètre, instances, fréquence, circuits de validation) • Compte-rendu de la première occurrence de ce comité
Opération de contrôle	Contrôle sur pièces

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

POC.P2.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.P2.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-SOCIAL

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.P2.O4.A : Réaliser un inventaire des composants du SI à l'aide d'un outil automatisé et retirer/remplacer tous les composants obsolètes

1. Définition de l'objectif	
Définition	La réalisation d'un inventaire des composants du système d'information, à l'aide d'un outil automatisé, vise à disposer d'une vision exhaustive, fiable et à jour des éléments constituant le SI. Cet inventaire permet notamment d'identifier les composants matériels et logiciels, leurs versions, leur niveau de support, ainsi que leur rôle au sein du système d'information. Cet inventaire permet de faciliter l'analyse des risques, prioriser les actions de mise à jour, de remplacement ou de retrait des composants obsolètes, et de renforcer durablement le niveau de sécurité du système d'information.
Valeur cible / seuil d'éligibilité	Le candidat doit disposer d'un inventaire formalisé et automatisé des composants du système d'information, couvrant l'ensemble du périmètre de la candidature. Cet inventaire doit : • être réalisé et maintenu à jour à l'aide d'un outil automatisé, selon des modalités définies par le candidat ; • permettre d'identifier les composants obsolètes, non supportés ou en fin de vie. L'inventaire doit couvrir *a minima* : • postes de travail, • serveurs, • imprimantes, • systèmes d'exploitation, • logiciels installés Le candidat doit formaliser les principes de maintien à jour de cet inventaire, précisant notamment : • les acteurs (équipe ou fonction) responsables de son maintien à jour ; • les événements déclenchant sa mise à jour (ajout, modification, retrait ou remplacement d'un composant) ; • la périodicité de revue de l'inventaire. L'inventaire doit permettre d'identifier et de piloter les actions de retrait, de mise à jour ou de remplacement des composants

	obsolètes, dans une logique de réduction des risques de sécurité. Pour les groupements, l'inventaire peut être réalisé au niveau du groupement ou au niveau des entités juridiques, sous réserve de couvrir l'ensemble du périmètre de la candidature.
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	• Inventaire automatisé des composants du SI • Document décrivant le maintien à jour de l'inventaire • Tableau de suivi des composants obsolètes et des actions associées
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.B : Réaliser une cartographie des applications et technologies utilisées

1. Définition de l'objectif	
Définition	La cartographie attendue doit permettre d'identifier, pour chaque métier, les applications mises en œuvre, leur environnement technique (par exemple : type d'hébergement, base de données), ainsi que les principales relations et flux existants entre les applications. Elle vise à offrir une vision structurée du paysage applicatif, facilitant la compréhension des dépendances, l'analyse des impacts en cas d'incident et le pilotage des évolutions du système d'information.
Valeur cible / seuil d'éligibilité	Une cartographie des applications et des technologies est formalisée et documentée. Elle permet d'identifier les principales applications et technologies composant le système d'information, leurs usages métiers, ainsi que les dépendances existantes entre les processus métiers et les applications qui les supportent. Cette cartographie met en évidence les interconnexions majeures entre les applications et offre une vision structurée du paysage applicatif, facilitant l'analyse des impacts en cas d'incident, de dysfonctionnement ou d'évolution du système d'information. Le lauréat devrait maintenir cette cartographie à jour dans le temps, selon des modalités définies. Il est préconisé que cette mise à jour soit réalisée *a minima* une fois par an, et à l'occasion des changements significatifs du système d'information.
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	• Cartographie ou extrait issu de l'outil utilisé • Document attestant de l'engagement de mise à jour annuelle de la cartographie
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.C : Sécuriser le réseau Internet professionnel

1. Définition de l'objectif	
Définition	Le réseau internet professionnel constitue un point d'entrée privilégié pour les attaques cyber. Sa sécurisation vise à protéger le système d'information contre les accès non autorisés, les intrusions, les logiciels malveillants et les usages inappropriés, tout en garantissant la continuité des activités.
Valeur cible / seuil d'éligibilité	Le candidat doit disposer de mesures de sécurité permettant de protéger le réseau internet professionnel et de contrôler les échanges entre le système d'information interne et internet. A minima, le dispositif mis en place permet : • de filtrer et contrôler les flux réseau entrants et sortants ; • de protéger le système d'information contre les menaces courantes issues d'internet (intrusions, logiciels malveillants, accès non autorisés) ; • de définir des règles d'accès et d'usage du réseau internet professionnel. Les équipements et solutions de sécurité déployés (pare-feu, proxy, VPN, etc) sont configurés et maintenus selon des règles définies. Le candidat devrait maintenir ces dispositifs dans le temps, notamment par leur mise à jour et leur adaptation aux évolutions du système d'information et des menaces.
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 ou schéma de l'architecture réseau • Description des mesures de sécurité déployées • Document interne encadrant l'usage et la sécurité du réseau internet professionnel
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.D : Définir une politique de gestion des identités et des comptes à privilèges

1. Définition de l'objectif	
Définition	La politique de gestion des identités et des comptes à privilèges formalise l'organisation des identités numériques, les principes de gestion des comptes à privilèges ainsi que la séparation des rôles et des droits, notamment entre comptes utilisateurs et comptes administrateurs.
Valeur cible / seuil d'éligibilité	Le candidat dispose une politique de gestion des identités et des comptes à privilèges formalisée et appliquée au sein du système d'information. Cette politique intègre *a minima* : • le choix et le paramétrage d'une solution d'annuaire (ex. Active Directory) ; • la séparation des comptes et des privilèges entre comptes administrateurs et comptes utilisateurs. Le candidat devrait maintenir cette politique dans le temps et à la faire évoluer en fonction des besoins, des usages et des risques identifiés.
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 d'identification et d'authentification
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.E : Mettre en place au moins une mesure identifiée comme prioritaire suite au diagnostic initial

1. Définition de l'objectif	
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 une mesure identifiée comme prioritaire à l'issue du diagnostic initial. L'action retenue est sélectionnée en concertation avec le GRADeS/CRRC, afin d'assurer sa pertinence et sa faisabilité. Il est impératif que l'action sélectionnée ne soit en aucun cas similaire ou redondante 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) : • Mettre en place un système d'enregistrement des logs de connexion internet, et de surveillance quotidienne du réseau et des équipements ; • Réaliser un test d'intrusion ; • Etc.
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 l'action sélectionnée • Description de la mesure réalisée • Livrables ou éléments attestant de sa mise en œuvre
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.F : Définir une politique de sauvegarde et de restauration des données cohérentes avec les besoins métiers, à valider avec la direction

1. Définition de l'objectif	
Définition	La politique de sauvegarde est un ensemble de directives et de règles établies au sein d'un établissement pour protéger l'ensemble de ses données. Elle vise à garantir que toutes les données importantes soient sauvegardées régulièrement et de manière sécurisée, en fonction de la criticité des activités qu'elles soutiennent.
Valeur cible / seuil d'éligibilité	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, 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, ...). • 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, CNIL, ...). • 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. **Spécificités pour les SI mutualisés** : • les candidats multi-établissements doivent élaborer une politique de sauvegarde et de restauration visant à harmoniser les pratiques avec un planning prévisionnel sur les 18 mois post appel à projet. Il est entendu par le terme « harmonisation » une stratégie de sauvegarde cohérente entre établissements pour les SI sous-tendant une même activité, un cadre documentaire partagé, etc. Il n'est pas attendu une unification du système de sauvegarde par exemple.
Textes de référence	Guide d'élaboration et de mise en œuvre de PSSI

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 de sauvegarde et de restauration conforme aux exigences de la cible. **Spécificités pour les SI mutualisés :** • Un planning prévisionnel sur 18 mois post appel à projet. • Politique de sauvegarde et de restauration conforme aux exigences de la cible. ***Documents à fournir par le prestataire pour la sauvegarde en cas de SI métier externalisé ou sauvegarde externalisée sur le périmètre propre au candidat :*** • inventaire complet des applications en mode SaaS, précisant pour chaque application si un PAS a été obtenu • contrat de service : Document définissant les niveaux de services attendus, les responsabilités de chaque partie, les délais de récupération des données, notamment. • plan d'Assurance Sécurité (PAS) du prestataire pour deux des applications inventoriées : Si ce document est disponible : • PAS ou attestation du candidat de la présence de ce document. Si ce document est non disponible : • motif(s) de non-présence du document : élément(s) de preuve du refus du prestataire ou de l'absence du document. • nom du prestataire et de la solution.
Opération de contrôle	Contrôle sur pièces

POC.P2.O4.G : Rédiger une fiche « processus métier » en suivant la méthodologie de construction du PCRA, et la diffuser auprès du personnel concerné

1. Définition de l'objectif	
Définition	Rédiger une fiche « processus métier », également appelée Fiche Service (FS), en s'appuyant sur la méthodologie du kit de construction du Plan de Continuité et de Reprise d'Activité (PCRA) ESMS[2]. La fiche service est un document unique et synthétique qui recense les points clés nécessaires pour assurer la continuité et la reprise de l'activité à l'échelle d'un service ou d'un processus métier. Elle synthétise l'ensemble des informations recueillies et analysées lors des entretiens métiers et du Bilan d'Impact sur l'Activité (BIA), notamment les activités critiques, les dépendances, les impacts et les modalités de fonctionnement en situation dégradée. La fiche est ensuite diffusée auprès du personnel concerné, afin de garantir une compréhension partagée du processus et des rôles à tenir en cas de crise, notamment cyber.
Valeur cible / seuil d'éligibilité	Une ou plusieurs Fiches Service (FS) sont formalisées pour au moins un processus métier critique, conformément à la méthodologie PCRA. La fiche service : • Constitue un document de synthèse (format court, type une page recto-verso) issu des travaux de BIA ; • Décrit le processus métier ou le service, ses missions et ses activités essentielles ; • Identifie les ressources nécessaires à son fonctionnement (ressources humaines, outils SI, données, infrastructures, prestataires) ; • Précise les impacts en cas d'indisponibilité, les délais de reprise attendus et les priorités ; • Définit les modalités de continuité et de reprise de l'activité en situation dégradée. La ou les fiches service sont validées par les responsables métiers concernés et diffusées aux équipes impliquées.
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

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

3. Restitution de l'objectif	
Remontée de l'information	Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Fiche Service (FS) formalisée • Preuve de validation et de diffusion de la Fiche Service (ex : mail de validation par le responsable, compte rendu de réunion, etc.)
Opération de contrôle	Contrôle sur pièces