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 1
Niveau de maturité peu avancé – Absence de ressource cyber dédiée

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 1 de la phase exploratoire de l'appel à projets médico-social destiné aux entités ayant un niveau de maturité cyber peu avancé et ne disposant pas de ressource cyber interne, externe ou mutualisée dédiée.

Deux autres guides sont également mis à disposition par l'ANS pour les parcours 2 (Maturité cyber peu avancée - Ressources cyber en partie 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.P1.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).
POC.P1.O1.2 - Désigner un Correspondant SSI	Le candidat doit désigner une personne responsable de la sécurité des systèmes d'information. Il s'agit d'une fonction ou mission et non nécessairement d'un poste dédié (la fonction peut être externalisée).
Construction d'un cadre de référence pour la cybersécurité	
POC.P1.O2.1 - Élaborer une charte informatique et l'annexer au règlement intérieur	Le candidat doit rédiger une charte informatique, précisant les règles d'utilisation des outils numériques, et l'annexer au règlement intérieur afin d'en assurer la diffusion et l'application par les utilisateurs.
POC.P1.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.P1.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.
Mise en œuvre d'actions de sensibilisation à la cybersécurité	
POC.P1.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.P1.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 (2 au choix)	
POC.P1.O4.A - Réaliser un inventaire du parc informatique et formaliser un plan de renouvellement des équipements 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 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 formaliser un plan de renouvellement du parc, permettant d'anticiper le remplacement des équipements et logiciels obsolètes ou à risque.
POC.P1.O4.B - Réaliser une cartographie applicative et fonctionnelle	Le candidat doit réaliser une cartographie applicative et fonctionnelle de son système d'information. Cette cartographie vise à représenter les processus métiers de la structure ainsi que les applications qui les supportent. Elle doit permettre d'identifier, pour chaque métier, les applications utilisées, ainsi que les principales interconnexions existantes entre les applications.
POC.P1.O4.C - Disposer d'un accès internet délivré par une offre professionnelle	La structure doit disposer d'une offre d'accès internet professionnelle, administrée par le prestataire ou par un administrateur en interne.
POC.P1.O4.D - Rédiger une procédure formalisée de signalement et d'alerte en cas d'accident cyber, et la diffuser auprès de l'ensemble du personnel	Le candidat doit formaliser une procédure pour le signalement et la gestion des incidents cyber et la diffuser auprès de l'ensemble du personnel. Cette procédure a pour objectif de clarifier les actions à mener, les circuits d'alerte et les interlocuteurs à mobiliser en cas d'événement cyber. Elle doit être testée dans le cadre d'un exercice de gestion de crise, notamment en lien avec les actions de sensibilisation applicative mises en œuvre auprès des directions et du personnel (POC.P1.O3.2).
POC.P1.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 initial. 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.

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.P1.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	INSTRUCTION N° DNS/2024/54 du 2 juillet 2024 relative aux missions des centres régionaux

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

POC.P1.O1.2 : Désigner un Correspondant SSI

1. Définition de l'objectif	
Définition	Désignation d'un correspondant en Sécurité des Systèmes d'Information (SSI) chargé de porter la fonction SSI au sein de la structure, lorsque celle-ci ne dispose pas d'un Responsable Sécurité des Systèmes d'information (RSSI). Il s'agit d'une fonction ou mission, pas nécessairement rattachée à un poste dédié, pouvant le cas échéant être externalisée.
Valeur cible / seuil d'éligibilité	La structure lauréate doit avoir désigné un correspondant SSI, lorsque la désignation d'un RSSI n'est pas possible. Il doit disposer, *a minima*, des compétences suivantes : • une connaissance générale des enjeux de cybersécurité et de protection des systèmes d'information ; • une compréhension de l'organisation et des activités de l'entité juridique ; • une capacité à coordonner les actions SSI, à relayer les consignes et à sensibiliser les acteurs internes. Remarque : aucune certification spécifique n'est exigée, mais une expérience ou une formation dans le domaine du numérique et/ou de la sécurité des systèmes d'information est recommandée. La désignation doit : • être formalisée (note de service, lettre de mission, contrat) ; • préciser le périmètre d'intervention et les responsabilités associées. Lorsque la fonction est externalisée, le rôle de correspondant SSI peut être assuré par un prestataire externe. Dans ce cas, le cadre contractuel doit préciser *a minima* : • le périmètre exact de la mission confiée ; • les livrables attendus ; • les modalités d'intervention (fréquence, présence sur site ou à distance) ; • les engagements en matière de confidentialité et de protection des données ; • la durée de la mission et les conditions de résiliation.
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	• Décision ou note de désignation du Correspondant SSI • Lettre de mission précisant les responsabilités • En cas d'externalisation, contrat ou convention avec le prestataire désigné
Opération de contrôle	Contrôle sur pièces

2.2 Construction d'un cadre de référence pour la cybersécurité

POC.P1.O2.1 : Élaborer une charte informatique et l'annexer au règlement intérieur

1. Définition de l'objectif	
Définition	Mettre en place une charte informatique visant à encadrer l'usage des outils et ressources informatiques par les utilisateurs (personnel, intervenants, etc.)
Valeur cible / seuil d'éligibilité	La structure dispose d'une charte informatique 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 informatique *ou* • Charte informatique 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.P1.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 *a minima* couvrir le DUI. Il est toutefois recommandé qu'elle s'applique à l'ensemble du SI, avec des mesures adaptées aux différents types d'applications et aux 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.P1.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	Sécuriser l'accès au Dossier Usager Informatisé (DUI) en encadrant les entrées, sorties et changements de fonctions des collaborateurs, par la mise en place de procédures claires et d'une matrice d'habilitation. 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 au DUI, en fonction des rôles et responsabilités.
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* le Dossier Usager Informatisé (DUI), ainsi que les comptes utilisateurs nominatifs permettant d'y accéder. 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.P1.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.P1.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 deux objectifs**. Ces objectifs doivent être **choisis en concertation avec le CRRC/GRADeS** en fonction du contexte et des priorités opérationnelles.

POC.P1.O4.A : Réaliser un inventaire du parc informatique et formaliser un plan de renouvellement des équipements obsolètes

1. Définition de l'objectif	
Définition	Disposer d'une vision exhaustive et à jour du parc informatique, afin de faciliter la gestion des actifs et la planification des renouvellements.
Valeur cible / seuil d'éligibilité	La structure réalise un inventaire des équipements matériels et logiciels et formalise un plan de renouvellement de ses équipements obsolètes. Il est recommandé de réaliser cet inventaire via un outil automatisé. L'inventaire doit couvrir *a minima* : • postes de travail ; • serveurs ; • imprimantes ; • systèmes d'exploitation ; • logiciels installés Le plan de renouvellement constitue un document de projection et de planification à moyen terme. Il vise à identifier les besoins prévisionnels de renouvellement du parc informatique, et n'est pas limité à la phase opérationnelle de l'appel à projets. Si le remplacement de matériel obsolète peut être pris en compte dans le cadre de l'appel à projets, les financements sont prioritairement destinés à d'autres types d'actions.
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	• Export ou restitution de l'outil d'inventaire • Plan de renouvellement
Opération de contrôle	Contrôle sur pièces

POC.P1.O4.B : Réaliser une cartographie applicative et fonctionnelle

1. Définition de l'objectif	
Définition	Comprendre et maîtriser les processus métiers et les applications qui les supportent, ainsi que leurs interconnexions. La cartographie attendue doit permettre d'identifier, pour chaque métier, les applications utilisées, ainsi que les principales interconnexions existantes entre les applications.
Valeur cible / seuil d'éligibilité	Une cartographie applicative et fonctionnelle est formalisée et permet d'identifier les dépendances entre processus métiers et applications. 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.P1.O4.C : Disposer d'un accès internet délivré par une offre professionnelle

1. Définition de l'objectif	
Définition	Garantir un niveau de service et de sécurité adapté aux usages professionnels et à la sensibilité des données traitées.
Valeur cible / seuil d'éligibilité	La structure doit disposer d'une offre d'accès internet professionnelle, administrée par le prestataire ou par un administrateur en interne. Pour gérer la continuité d'activité en cas d'indisponibilité de l'accès principal, les lauréats sont libres de mettre en place : • Deux accès distincts ; ou • Un accès en mode dégradé permettant de maintenir un niveau de service minimal.
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	Un contrat ou une facture de l'offre internet professionnelle ou une attestation du prestataire
Opération de contrôle	Contrôle sur pièces

POC.P1.O4.D : Rédiger une procédure formalisée de signalement et d'alerte en cas d'accident cyber, et la diffuser auprès de l'ensemble du personnel

1. Définition de l'objectif	
Définition	Permettre une réaction rapide et coordonnée en cas d'incident ou d'accident cyber.
Valeur cible / seuil d'éligibilité	La structure formalise une procédure de signalement et d'alerte en cas d'incident cyber et la diffuse auprès de l'ensemble du personnel. Cette procédure doit être testée dans le cadre de l'exercice de crise de l'objectif 3.2 : « Mettre en œuvre des actions de sensibilisation applicative auprès des Directions et du personnel ». En d'autres termes, si le lauréat sélectionne cet objectif à la carte, il devra forcément réaliser *a minima* l'action « Exercice de crise » de l'objectif obligatoire 3.2.
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 signalement et d'alerte cyber • Justificatif de diffusion (mail, intranet, support de communication, etc.) • Document attestant de l'utilisation de la procédure dans le cadre de l'exercice de crise
Opération de contrôle	Contrôle sur pièces

POC.P1.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) : • définir une politique de sauvegarde et de restauration des données cohérentes avec les besoins métiers, à valider avec la direction ; • rédiger une fiche « processus métier » en suivant la méthodologie du kit de construction du Plan de Continuité et de Reprise d'Activité (PCRA) ESMS[1], et la diffuser auprès du personnel concerné ; • 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	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

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

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