Appel à Candidature

Renforcement de la Cybersécurité des Organismes Gestionnaires médico-sociaux de la région Auvergne-Rhône-Alpes

18 novembre 2024

GCS Sara
Parc technologique de la Pardieu
24 allée Evariste Galois – 63170 Aubière
Mail : contact@sante-ara.fr
www.sante-ara.fr

Sommaire

1 Contexte national

La transformation numérique du secteur social et médico-social, s'accompagne d'une exposition croissante au risque cyber. **Le risque est avéré** pour les ESMS et les personnes accompagnées.

Au premier semestre 2023, le chantier national **cybersécurité social et médico-social** a permis de mener :

- Une concertation auprès **de 60 organismes gestionnaires**
- **8 ateliers de co-construction** avec les acteurs du secteur
- Un **plan d'action 2023/2027 ambitieux, adapté, et cohérent** avec la feuille de route sanitaire.

Parallèlement à ceci**, l'observatoire des SI MS** a établi une grille pour évaluer la maturité numérique des établissements. Sur la base de différentes questions et de facteurs de pondérations, un score est produit qui détermine un niveau de maturité et les actions nécessaires pour améliorer sa maturité numérique. A terme, cette grille devra être remplie par l'ensemble des organismes gestionnaires.

Ces différents ateliers et travaux ont mené à la construction d'un plan d'action pour renforcer la cybersécurité des établissements de santé et des structures médico-sociales. Ce plan d'actions, appelé **CaRE** (Cybersécurité accélération et Résilience des Etablissements), vise à accélérer la mise à niveau des systèmes d'informations hospitaliers face à l'état de la menace et à renforcer durablement la résilience des structures de soins. Le programme doté de **250 M€ jusqu'en 2025**, sur un objectif d'investissement total de **750 M€ d'ici 2027**, poursuit le double objectif :

- Eviter que les attaques aboutissent ;
- Permettre aux établissements de s'en relever le plus rapidement possible.

L'un des objectifs du Ségur Numérique est de contribuer au renforcement de la cybersécurité. Les cyberattaques visant les établissements de santé et du médico-social se multiplient depuis plusieurs années. Il y a donc une réelle nécessité de sensibilisation et de préparation de tous les acteurs du secteur (directions, métiers, DSI, etc.) aux risques cybersécurité dans leurs contextes particuliers.

2 Stratégie régionale pour les établissements et services médico-sociaux

Le GCS SARA, missionné par l'ARS d'Auvergne-Rhône-Alpes, s'est engagé depuis plusieurs années dans le déploiement de la eSanté auprès des acteurs médico-sociaux.

L'année dernière, l'ARS a porté un appel à candidature afin de :

- Déterminer la capacité des établissements à pouvoir renseigner eux-mêmes des grilles d'évaluation
- Evaluer d'un point de vue méthodologique l'accompagnement à réaliser auprès des établissements dans leur diagnostic et mise en œuvre de plan d'action pour améliorer leur maturité en matière de cybersécurité.

Cet appel à candidature 2023 avait pour objectifs de :

- Procéder à la sélection d'une dizaine d'organismes gestionnaire dans la perspective de faire réaliser par un prestataire un audit de maturité numérique

- Financer la mise en œuvre d'actions de remédiations de vulnérabilités évaluées comme critiques.

Suite à la réussite du précédent appel à candidature, le GCS SARA propose une seconde vague d'accompagnement avec un nouvel appel à candidature qui a pour objectifs de renforcer la cybersécurité dans les établissements sociaux et médicaux sociaux.

Les projets retenus seront financés dans le cadre du programme CARE, via la délégation de moyens en région au Centre Régional de Ressources en Cybersécurité (CRRC) opéré par le GCS SARA.

3 Objet du financement de l'AAC

Le financement prévu dans cet appel à candidature aura pour but de réaliser un exercice de crise **ou** un diagnostic cyber selon la maturité de l'établissement. Le choix d'attribution d'un exercice de crise ou d'un diagnostic cyber sera fait suite à la candidature par le GCS SARA.

Critères d'éligibilité aux différents projets :

- Projet de diagnostic cyber : être un organisme gestionnaire/établissement du secteur médico-social et social.
- Projet d'exercice de crise : être un organisme gestionnaire du secteur médico-social et social et avoir participé au programme ESMS Numérique.

Les établissements les plus matures se verront plutôt proposer l'exercice de crise. Pour les deux projets, il faudra avoir déposé toutes les pièces de candidatures demandées.

4 Calendrier de l'appel à candidature

L'appel à candidature est ouvert jusqu'au **31 décembre 2025.**

Les candidatures seront instruites au fil de l'eau tout au long de l'année avec un premier cut off en janvier/février 2025. Ce premier cut off permettra de lancer une première vague de projets en février 2025.

Tout dossier déposé après la date de clôture de l'appel à candidature sera considéré comme non recevable.

5 Comment déposer sa candidature ?

La personne morale gestionnaire qui souhaite candidater doit remplir le questionnaire suivant et joindre les pièces complémentaires pour que sa candidature soit recevable.

Les pièces à fournir concernant cet appel à projet sont les suivantes :

- Une note de présentation expliquant la motivation de l'organisme gestionnaire à présenter sa candidature (obligatoire).
- Une lettre d'engagement signée, précisant que l'organisme gestionnaire s'engage à se rendre disponible (ainsi que les professionnels identifiés) pour la bonne réalisation de

l'exercice de crise ou des étapes de diagnostic, sous respect d'un délai de prévenance de 15 jours à minima par le prestataire (obligatoire).

6 Déroulé du projet de diagnostic

A. Diagnostic de l'organisme gestionnaire

Les candidats retenus dans le cadre de cet appel à candidature seront contactés par un prestataire dans l'objectif de réaliser une journée de diagnostic sur site à partir d'outils préétablis (grille Maturin SMS et guide de maturité cyber en 13 questions[1]).

Un entretien préalable sera réalisé afin d'identifier les documents et procédures existantes puis déterminer les personnes à rencontrer et le(s) site(s) à visiter sur cette journée.

Le diagnostic ne dépassera pas 1 journée et demie.

Au terme de ce diagnostic, le prestataire émettra un rapport ainsi qu'un plan d'actions à mettre en œuvre par l'organisme gestionnaire afin de pallier aux risques ou failles considérées comme les plus critiques. Ces éléments seront présentés lors d'un entretien à l'organisme gestionnaire qui sera amené à se positionner sur sa capacité à mettre en œuvre les actions préconisées. Suite à cet entretien, des points de suivi auront lieux pour suivre la mise en place du plan d'action.

B. Prestataires

Les audits et l'accompagnement à la mise en œuvre des actions seront réalisés par des prestataires spécialisés en cybersécurité et certifiés PASSI.

Ils sont retenus dans le cadre d'un marché public dont le GCS SARA est le pouvoir adjudicateur.

7 Déroulé du projet d'exercice de crise

A. Exercice de crise

Les candidats retenus dans le cadre de cet appel à candidature se verront contacter par un prestataire dans l'objectif de réaliser, selon la taille de l'organisme gestionnaire un exercice de crise adapté avec l'utilisation d'outils préétablis (kit ANS).

Un entretien préalable de « cadrage » sera réalisé afin d'identifier l'établissement sur lequel sera joué l'exercice, les personnes présentes ainsi que la difficulté de l'exercice de crise et la version du kit qui sera utilisé.

[1] La Cybersécurité pour le social et le médico-social en 13 questions - Agence du Numérique en Santé https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

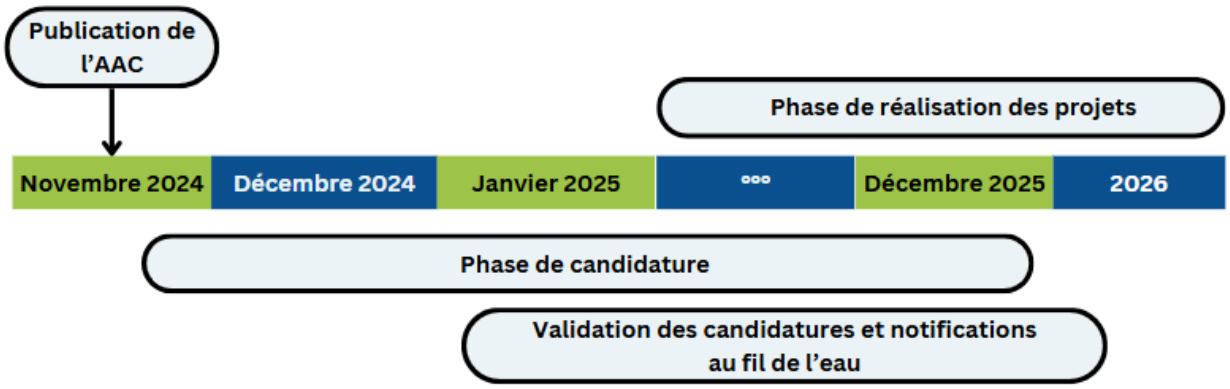
Au terme de l'exercice de crise, le prestataire émettra un rapport d'exercice qui sera transmis à l'OG avec des recommandations. Suite à cela, des points de suivi seront organisé avec l'OG pour suivre la mise en place d'actions en lien avec les recommandations reçues.

B. Prestataires

Les exercices de crises seront réalisés par des prestataires spécialisés en cybersécurité.

Ils sont retenus dans le cadre d'un marché public dont le GCS SARA est le pouvoir adjudicateur.

8 Planning



9 Priorisation des projets

Le GCS SARA priorisera les dossiers à l'issue de l'évaluation des éléments remplis dans le dossier de candidature. Les dossiers seront priorisés en fonction du niveau de risque de la structure et des motivations de l'établissement présenté dans la note. Le niveau de risque est évalué grâce aux réponses présentes dans le questionnaire et basé sur une grille des risques proposée par l'ANS.

Le GCS SARA attribuera un projet de diagnostic ou d'exercice de crise en fonction des critères de recevabilité et de la maturité de l'organisme gestionnaire. La préférence de l'établissement sera prise en compte.

10 Contacts

Pour toute information complémentaire, veuillez contacter :

Priscilla OHLING, Responsable programmes ESMS
priscilla.ohling@sante-ara.fr

Elodie Picano, Cheffe de projet SI-MS
elodie.picano@sante-ara.fr

GCS Sara
la santé connectée

Parc technologique de la Pardieu
24 allée Evariste Galois
63170 Aubière
Mail : contact@sante-ara.fr

www.sante-ara.fr