



**e.santé**  
Occitanie  
Connecter pour mieux soigner



**Cyber**  
sécurité

# AMI CYBERSECURITE DE L'ARS

---

**Présentation des actions du centre de ressources mutualisées porté par le GRADeS sur lesquelles vous devez vous positionner**

Le 25/11/2022





# Support contractuel régional

Audits & Exercices de continuité d'activité

Afin de faciliter l'atteinte d'exigences portant sur la réalisation d'audits et d'exercices de continuité d'activité, le GRADeS propose de mettre en place un accord cadre régional permettant aux établissements bénéficiaires de recourir à des prestations externes dans des conditions négociées au niveau régional.



# Support contractuel régional



## OBJECTIFS

- **Faciliter l'accès à un socle de prestations « prioritaires »** permettant aux établissements d'Occitanie d'augmenter la sécurisation de leur SI, de mieux se préparer à faire face aux risques croissants de cybersécurité, de faciliter l'atteinte des pré-requis sur lesquels ils sont attendus, notamment dans le cadre du Ségur.
- **Générer un effet « booster »** en mutualisant un certain nombre de ressources au niveau du GRADeS:
  - Animation / évolution de l'offre
  - Pilotage de l'accord cadre et suivi de l'exécution
  - Conseil / Orientation des établissements
  - Organisation de benchmarking et retours d'expériences



## PERIMETRE

### AUDITS

- Audits de tous types : Test d'intrusion, Infrastructure, de code, analyse de risque, Scan de vulnérabilité, audit organisationnel, audit conformité (guide d'hygiène de l'ANSSI, instruction 309, ISO 27 001, ISO 27 002, NIS, HDS)

### EXERCICES DE CONTINUITÉ D'ACTIVITÉ

- Accompagnement à la réalisation d'exercices de crises sur la base des scénarios fournis par l'ANS (débutant, intermédiaire, confirmé)
- Formation d'animateurs d'exercices de crises sur la base des kits fournis par l'ANS
- Accompagnement à la réalisation d'exercices de crise sur mesure



## BENEFICIAIRE CIBLE

1. Etablissements sanitaires
2. e-santé Occitanie besoins internes

# Support contractuel proposé et technique d'achat associée

---

- **Accord cadre :**

- Permet de répondre aux besoins d'accompagnement des établissements afin de répondre aux exigences nationales
- Permet une massification en incluant des structures bénéficiaires de l'accord cadre
- Permet une relation directe avec les opérateurs économiques :
  - Permet un pilotage maîtrisé (gouvernance, choix et respect des délais et de la qualité des prestations, pénalités, modalités de paiement, reporting et retour d'expérience)
  - Pas de coût de mark-up additionnel

- **Allotissement :** selon la nature des prestations

- Permet d'ouvrir à la concurrence, en permettant à des opérateurs économiques spécialisés de se positionner
- Permet d'envisager de demander des certifications adaptées à l'objet de lot
- Permet aux bénéficiaires de se positionner sur les lots pour lesquels ils ne disposent pas de support contractuels

- **Multi-attributaire par lot :**

- Permet d'obtenir le meilleur de chaque société autant sur les plans techniques que financiers, sur chacun des besoins et dans un calendrier compatible avec les calendriers projets contraints
- Permet de maîtriser le risque portant sur la concurrence à l'achat (tissu économique tendu face au nombre de demandes)
- Permet de pallier aux défaillances fournisseurs éventuelles

- **A bon de commande :**

- Facilité et rapidité d'exécution pour les établissements

# Support contractuel proposé et technique d'achat associée

---

- **Durée de l'accord-cadre : 2 ans ferme reconductible deux fois un an**
  - Justifié par le fait qu'il n'y a pas d'investissement lourd en début de marché de la part des prestataires
  - Permet de ne pas être enfermés dans le marché pendant 4 ans en cas de difficulté d'exécution.
  - Proche de la durée de Ségur ce qui laisse la possibilité aux établissements de ne plus être liés contractuellement s'ils le souhaitent
- **Engagement bénéficiaire**
  - **Durée d'engagement** : Les parties prenantes à l'accord-cadre sont liées par l'exclusivité et cela sur la durée de l'accord-cadre.
    - Une fois l'accord-cadre notifié, il n'est plus possible d'ajouter des bénéficiaires
    - Si un bénéficiaire souhaite sortir de l'accord-cadre, il faut soit l'inscrire dès le départ dans le périmètre de l'accord-cadre, soit le contractualiser par voie d'avenant en cours d'exécution.
  - **Positionnement**
    - L'estimation du besoin de l'établissement à date permet d'établir un modèle économique adapté et donne les moyens aux candidats d'optimiser leur offre technique et financière
    - L'estimation de CA est cumulée avec ceux des autres bénéficiaires et n'est pas engageante.

# FAQ « support contractuel régional »

---



- **Je bénéficie déjà d'un support contractuel sur ce type de marché (audit et/ou exercices de continuité d'activité), puis-je quand même me positionner sur le marché régional ?**
  - Oui, si l'établissement dispose d'ores et déjà d'un support contractuel, il suffit d'inscrire dans l'accord-cadre que « les établissements inscrits dans le périmètre de l'accord-cadre seront bénéficiaires à échéance de leur support contractuel existant ». De cette façon, ils rejoignent l'accord-cadre sans difficulté.
- **Je ne sais pas me positionner aujourd'hui, puis-je rejoindre l'accord cadre en cours de route ?**
  - Dans le cas où cette hypothèse se présente, nous essaierons d'y répondre, mais sans certitude à date.
- **Je souhaite quitter l'accord cadre en cours de marché, cela est-il possible ?**
  - Nous envisageons que les établissements bénéficiaires de l'accord cadre puissent s'engager uniquement sur une période ferme (sur la 1<sup>ère</sup> année uniquement par exemple).

# Souhaitez-vous bénéficier du support contractuel régional ?



- OUI sur le périmètre « audits »
- OUI sur le périmètre « exercices de crises »
- OUI sur le périmètre « audits » et « exercices de crises »
- NON

**QUESTIONS A REMPLIR DIRECTEMENT  
SUR DEMARCHES SIMPLIFIEES**

**Cette action permet de bénéficier du support contractuel régional. Les établissements commandent en direct et règlent directement leurs factures avec le(s) société(s) retenues. Les éventuels financements du national ou de l'ARS venant accompagner la mise en place de ces actions ne passent pas par le GRADeS.**

02

# Plate-forme Collaborative

RESANA

Afin de faciliter et stimuler l'échange entre les RSSI d'Occitanie et fédérer un réseau local, le GRADeS propose d'outiller la Communauté des RSSI régionale d'une plate-forme collaborative.



# Plate-forme Collaborative

- **Objectifs** : Stimuler l'échange entre les acteurs du territoire pour fédérer un réseau local
- **Cibles** : Accessible à tous les RSSI de la région (ES dans un 1er temps)
- **Fonctionnalités recherchées** : Partage de documents, forum, annuaire
- **L'outil choisi** : RESANA plateforme ouverte et administrée techniquement par la DINUM (direction interministérielle du numérique)
- **Les + :**
  - Sécurité :
    - Hébergement en France – Outscale (SecNim Cloud)
    - Échanges sécurisés – Certificat SSL
    - RGPD – Proportionnalité, propriété, confidentialité des données personnelles : outillage en place
    - La possibilité d'upgrader vers une offre RESANA SECURE pour le partage de données sensibles (chiffrement de bout en bout certifié CSPN par l'ANSSI)
  - Fonctionnalités en + :
    - Notifications, chacun décide de son niveau d'alerte.
    - Co-édition
    - Gestion des Evénements
    - Sondages

- 
- Espaces
- Contacts
- Documents
- Dialogues
- Agenda
- Projets
- Tâches

Documents

Aide Liens Infos 1

## Avec nouveauté

## Sans nouveauté

Communauté RSSI Occitanie

Aucune nouvelle information

Personnalisez votre niveau d'alerte

- Priorité basse**  
Avertir une fois par mois des nouvelles publications.
- Priorité moyenne**  
Permet d'être informé régulièrement, chaque semaine vous recevez un mail synthétisant les informations non lues dans vos espaces.
- Priorité haute**  
Permet d'être informé à tout moment, à chaque nouvelle information dans l'espace vous recevez une notification par mail.
- Archivé**  
Les espaces archivés sont placés dans les archives.

Nouveau message (1)

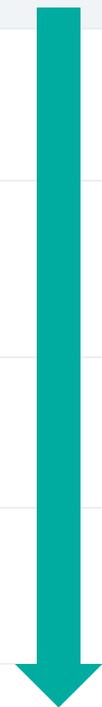
# Un espace collaboratif



-  Support Atelier Cartographier son SI\_20221125  
Taille : 1.32 Mo
-  La cybersécurité pour les ESMS en 13 questions (V\_Octobre 2022)  
ANS\_GUIDECYBER\_PHASE 1-EXE -V2.pdf (esante.gouv.fr)
-  Kits d'exercices de crise  
La grille d'auto-évaluation + le kit débutant + kit intermédiaire en téléchargement au lien ci-dessous :  
Exercice de crise cyber | Portail du CERT Santé (cyberveille-sante.gouv.fr)
-  CR-rencontres-SSI-Santé-APSSIS-sept-2022  
Taille : 3.33 Mo
-  CERTSante\_presentation-activités  
Taille : 0.09 Mo
-  Recueil centralisé de la documentation réglementaire, des recommandations et bonnes pratiques en matière de cyber\_mars-2022\_VF  
Taille : 0.20 Mo



Plus récent



Plus ancien

Alexandra LEPRINCE il y a 4 h  
ajouter un commentaire 4 lus 0 J'aime

Alexandra LEPRINCE il y a 7 h  
3 commentaires 25 lus 0 J'aime

Alexandra LEPRINCE 3 jour(s)  
ajouter un commentaire 8 lus 0 J'aime

Alexandra LEPRINCE 1 semaine(s)  
0 lus 0 J'aime

Alexandra LEPRINCE 1 semaine(s)  
ajouter un commentaire 0 lus 0 J'aime

Alexandra LEPRINCE 1 mois  
ajouter un commentaire 8 lus 0 J'aime

Les informations s'affichent par ordre chronologique (les plus récentes en haut). Pour accéder au contenu d'un document, il suffit de cliquer dessus

# La gestion documentaire



**Dossiers** + Ajouter

A classer

- Divers documents d'intérêt
- Guides bonnes pratiques**
- Offre CERT Santé
- Outils et méthodes indispensables

**Guides bonnes pratiques** Sélectionner plusieurs Importer un document Créer un document

Nom Recherche Type Dernière modification Dernier contributeur

	La cybersécurité pour les ESMS en 13 questions (V_Octobre 2022)	pub	25/11/2022 à 11:27	Alexandra LEPRINCE
	Recueil centralisé de la documentation réglementaire, des recommandations et bonnes pratiques en matière de cyber_mars...	.pdf	21/10/2022 à 14:27	Alexandra LEPRINCE

**Une arborescence de dossiers, constituant un centre de ressources documentaires pour la communauté des RSSI. Une gestion des droits fine qui permet de définir avec qui on souhaite partager.**

2 Documents

- Annuaire
- Dialogues
- Evènements
- Documents
- Sondages
- Publications
- Formulaires
- Contributions
- Statistiques



# Souhaitez vous rejoindre la communauté des RSSI d'Occitanie sur RESANA ?



- OUI
- NON

Si oui coordonnées de la ou des personnes à inscrire sur la plate-forme :

Contact 1 :

- Nom
- Prénom
- Fonction
- Mail

Contact 2 :

- Nom
- Prénom
- Fonction
- Mail

**QUESTIONS A REMPLIR DIRECTEMENT  
SUR DEMARCHES SIMPLIFIEES**

**Cette action est 100 % prise en charge  
(aucun reste à charge pour l'établissement)**

03

## Plate-forme de sensibilisation

Campagne de sensibilisation régionale

Afin de développer la sensibilisation aux bonnes pratiques cybersécurité dans vos établissements et en nous appuyant sur une plate-forme de sensibilisation régionale, le GRADeS vous propose de réaliser vos campagnes de sensibilisation et de vous benchmarker.



# La plate-forme régionale de sensibilisation



- **Une plate-forme de sensibilisation**, solution logicielle « Sensiwave » conçue et développée par Conscio technologies proposant 3 types de contenus :
  - Questionnaires d'évaluation de la maturité cyber
  - Capsules de e-learning
  - Faux tests de phishing
- **L'équipe cyber du GRADeS :**
  - Paramétrage et administration des campagnes de sensibilisation
  - Mise à disposition des statistiques des campagnes et d'éléments de benchmarking
- **Un Club utilisateurs « santé »** permettant d'assurer un renouvellement des contenus



- Diversité des modules de sensibilisation (format, durée, contenu...), personnalisation possible et certains contenus spécifiques au secteur de la santé
- Accès web des modules à travers un portail avec comme pré-requis : adresse de messagerie par utilisateur pour diffusion & accès (import des utilisateurs via fichier csv ou excel)
- Adresses IPs et noms de domaine à whitelister pour la réception des emails
- Export des modules possible au format SCORM pour diffusion sur votre intranet

# Les contenus de sensibilisation

- **Chaque mois**, les utilisateurs que vous avez sélectionnés reçoivent un mail les renvoyant vers **une activité (vidéo quizz ou chat bot) inférieure à 3 minutes** envoyée par notre plate-forme.



Bonjour,

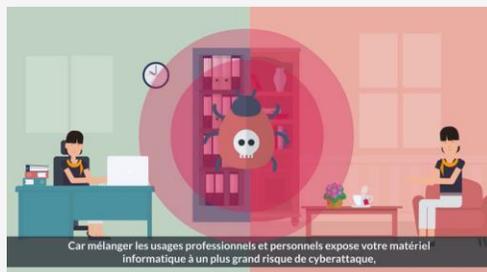
Dans le cadre d'une campagne régionale de sensibilisation à la cybersécurité, votre établissement et le GRADeS e-santé Occitanie vous proposent une courte vidéo (1 min 30) pour vous expliquer les dangers du phishing (ou hameçonnage) et les bonnes pratiques pour ne pas vous faire piéger. Ces techniques couramment utilisées par les pirates informatiques représentent une vraie menace pour nos SI.

Pour y accéder et en savoir plus, veuillez cliquer sur le lien ci-dessous :

**COMMENCER**

Nous comptons sur vous car la protection du système d'information est l'affaire de chacun(e) d'entre-nous.

Merci.



Car mélanger les usages professionnels et personnels expose votre matériel informatique à un plus grand risque de cyberattaque.

Quelle(s) erreur(s) a commis le professionnel de santé ?

- Aucune
- Il a connecté un périphérique personnel sur du matériel professionnel
- Il a utilisé une clé USB de provenance non fiable,
- Il est interdit de brancher une clé USB sur du matériel professionnel

**Valider**



Des capsules de sensibilisation et certaines spécifiques au domaine de la santé vous seront proposées :

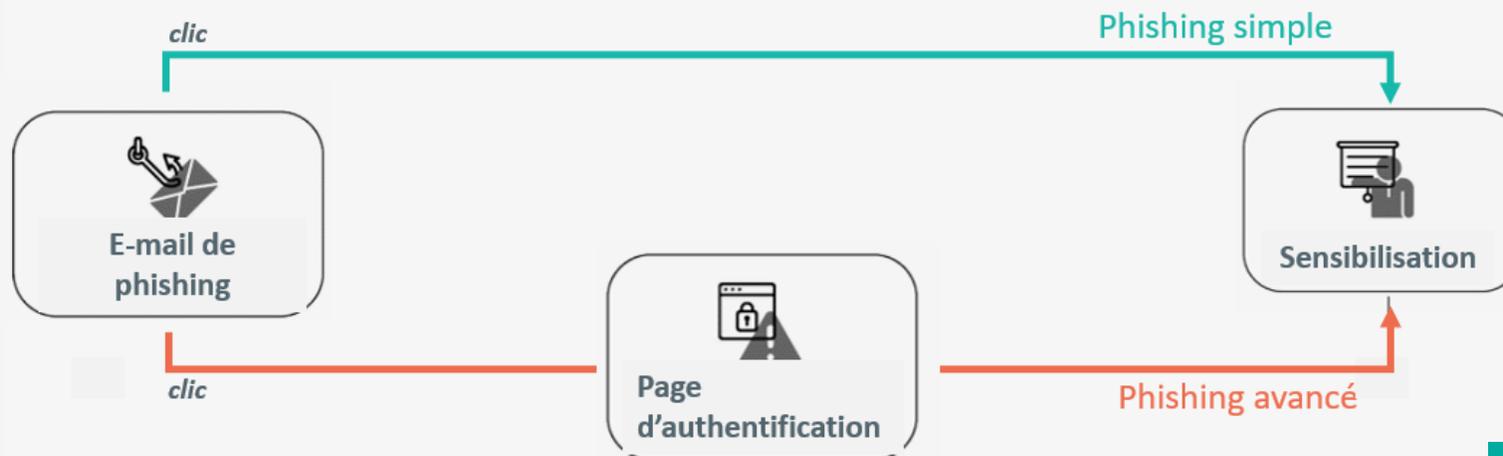
- Différents **formats** : saynètes (PPT à dérouler), vidéos interactives / vidéos quiz (vidéos sous-titrées se concluant par un quiz), chatbot
- Différents **thèmes** : codes malveillants, phishing, mot de passe, ingénierie sociale, protection de l'information, mobilité, poste de travail, usage pro/perso.

Un portail comprenant un large panel de contenus disponibles a été réalisé pour que vous puissiez les consulter.

N'hésitez pas à demander votre accès en envoyant un mail à : [cybersecurite@esante-occitanie.fr](mailto:cybersecurite@esante-occitanie.fr)

# Les fausses campagnes de phishing

- Le phishing est le **point d'entrée de nombreuses tactiques de cyberattaques** : vol d'informations personnelles, voire confidentielles (données de santé, identifiants), installation de codes malveillants, ou ingénierie sociale.
- Le phishing permet de cibler l'ensemble des utilisateurs d'un établissement, multipliant ainsi les chances de réussite d'une attaque. **Il est donc important d'évaluer le risque autour du phishing** dans son établissement en réalisant des campagnes de tests et en reproduisant ce type d'exercice après sensibilisation des utilisateurs.
- Des campagnes de faux tests de phishing seront organisées **plusieurs fois dans l'année** ou **à la demande\*** (*Demande effectuée au moins un mois avant la campagne via le formulaire dédié, modèles à choisir dans notre catalogue*)



NB : Informations non sauvegardées

N'hésitez pas à demander le catalogue reprenant l'ensemble des modèles de phishing disponibles en envoyant un mail à : [cybersecurite@esante-occitanie.fr](mailto:cybersecurite@esante-occitanie.fr)

# L'offre « Programme de sensibilisation à la Cybersécurité régionale »

**POUR QUOI FAIRE ?**  
VOUS SIMPLIFIER LA SENSIBILISATION DE VOS COLLABORATEURS

**UNE OFFRE QUI S'APPUIE SUR**  
La plate-forme SENSIWAVE de CONSCIO TECHNOLOGIES

**Vous êtes**

Établissement sanitaire

**Nos services**

Réalisation de campagne de sensibilisation

- **Diffuser** chaque mois, une vidéo courte ciblant une problématique cyber.
- > Des contenus qui répondent aux enjeux cyber propres aux établissements de santé

Test de phishing trimestriel

- **Réaliser** des campagnes de phishing pour l'ensemble de vos collaborateurs tous les trois mois

Sensibilisation ciblée sur les collaborateurs piégés

- **Identifier les collaborateurs piégés pendant les campagnes de phishing** et leur adresser une sensibilisation « rappel » sur le phishing/ransomware

Questionnaire de fin de parcours

- A l'issue du programme, possibilité de réaliser **un quiz** via la plateforme afin d'évaluer les connaissances acquises

**REPORTING**  
Un reporting trimestriel anonyme sera adressé à l'établissement (phishing + sensibilisation)

**Le groupement vous propose, en parallèle de cette offre régionale**

- La possibilité de réaliser des tests de phishing ciblés « à la carte » à condition de respecter un **délai de prévenance d'un mois minimum** et de **rester sur des modèles du catalogue**.
- La mise à disposition d'un **kit communication** pour outiller votre rôle de sponsor et relais interne

# Programme régional de sensibilisation à la cybersécurité



Année 2023

T1

T2

T3

T4

Campagnes mensuelles de sensibilisation et phishing trimestriel



Questionnaire de fin de programme



Capsule micro-learning



Sensibilisation ciblée pour les personnes piégées



Tests phishing



La sensibilisation n'est pas qu'un projet, c'est un processus. Pour obtenir des résultats durables et significatifs, il convient de s'inscrire dans la durée et de recommencer le cycle



# Concrètement, qui fait quoi ?

Grandes étapes d'un cycle	e-santé Occitanie	Établissement
Segmentation de la population à sensibiliser		✓
Réaliser des tests avant le lancement du programme régional	✓	✓
Définition du programme de sensibilisation (e-learning) et envoi des campagne de sensibilisation	✓	<b>Une réunion de concertation sera organisée avec les ES partenaires</b>
Mise en œuvre des campagnes de phishing	✓	<b>Rôles de « sponsor » et « relais » nécessaires</b>
Identification des collaborateurs piégés et mise en œuvre de sensibilisation spécifique	✓	<b>Rôles de « sponsor » et « relais » nécessaires</b>
Reporting trimestriel	✓	
Information des utilisateurs sur l'utilisation de leurs données dans le cadre de programmes de sensibilisation organisés avec le GRADeS		✓

# Souhaitez vous adhérer à l'offre de sensibilisation régionale du GRADeS ?



- OUI
- NON

Au-delà des campagnes de phishing prévues dans le cadre de la campagne régionale, souhaitez-vous également bénéficier de campagnes de phishing à la demande (nécessite de prendre le temps de préparation avec l'équipe du GRADeS et de planifier)

- OUI
- NON

A terme, nous envisageons de pouvoir aussi personnaliser à la demande les campagnes de sensibilisation et diffusion de contenus e-learning. Ce sujet vous intéresse t-il ?

- OUI
- NON

**QUESTIONS A REMPLIR DIRECTEMENT  
SUR DEMARCHES SIMPLIFIEES**

**Cette action est 100 % prise en charge par l'ARS Occitanie sur 2023 (aucun reste à charge pour l'établissement)**

**Merci  
pour votre attention.**

**Pour toute question, merci d'adresser un  
mail à : [cybersecurite@esante-occitanie.fr](mailto:cybersecurite@esante-occitanie.fr)**