RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Financé par l'Union européenne
NextGenerationEU

Renforcement de la cyber sécurité dans les établissements sociaux et médico-sociaux

Bonnes pratiques de cyber sécurité

- 18/10/2022-

Avec la participation de :

Ordre du jour

Informations pratiques

Bonnes pratiques de participation au webinaire

Bienvenue !

- **Nom d'utilisateur** : « Etablissement ou Service – Nom Prénom »
- Pour poser des questions / réagir :
  - **Par écrit :** <u>module "Questions Réponses" / "Q et R."</u> en bas de l'écran pour rebondir, poser des questions ou commenter. Une réponse concise/synthétique sera effectuée à l'oral lors des temps de questions/réponses :

  - **De vive voix :** <u>lors des temps de questions/réponses</u>, levez la main et la parole vous sera donnée.

Mise en ligne de l'enregistrement vidéo de la session : suivez ce lien

Informations pratiques

Qui sommes-nous ?

Le Groupement Régional d'Appui au Développement de la E-Santé (GRADeS) en Ile de France. Les GRADeS ont pour rôle de:

- Promouvoir l'usage des services numériques en santé dans les territoires
- Veiller à l'urbanisation, l'interopérabilité et la sécurité des Systèmes d'information (SI) à l'échelle régionale
- Animer et fédérer les acteurs de la région autour de la stratégie régionale d'eSanté

Intervenants - Département Sécurité des systèmes d'information


Emilie SAINZ


Didier DEMANTE


Tania MAC-LUCKIE


Adile DRAME

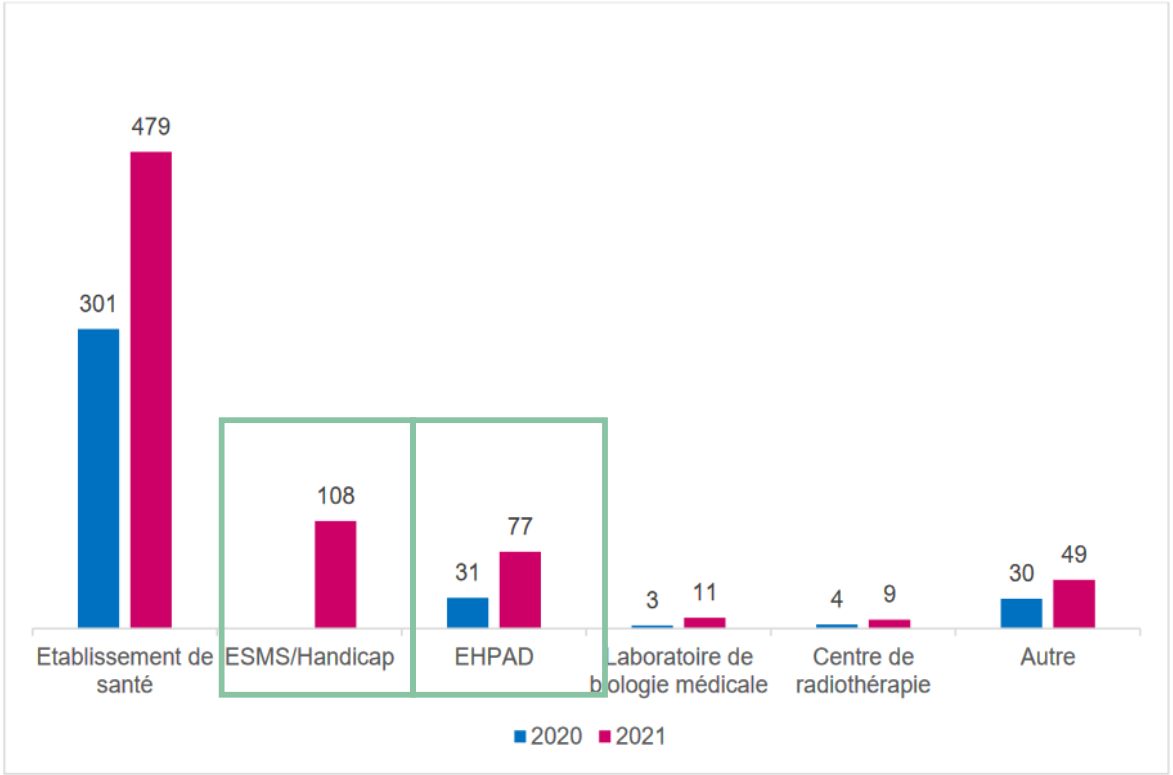
Contexte de la cybersécurité pour les ESMS

Contexte de la cybersécurité pour les ESMS

Quelques chiffres – incidents 2021

- Les déclarations d'incidents de sécurité informatique **en hausse de 400%** par rapport à 2021 pour les ESMS.
- L'Occitanie et **L'île-de-France** sont les régions les plus concernées par les signalements d'incidents.
- L'impact le plus important concerne la perte des données

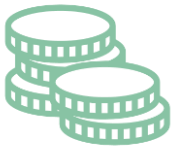
Répartition des signalements selon le type de structures



Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé - Rapport public 2021

Contexte de la cybersécurité pour les ESMS

Les menaces



- **La valeur des données de santé en constante augmentation**
  - Les données agrégées servent dans de domaine la recherche médicale et de l'IA.
  - Les données médicales individuelles peuvent servir divers activités malveillantes (chantage, prescription, usurpation,…)
- **Les établissements sanitaires et ESMS ont d'importants besoins**
  - Disponibilité
  - Intégrité
  - Confidentialité
- **Le manque de ressources dans le domaine de la SSI**
  - Peu de ressources allouées à la SSI dans les projets.
  - Manque de profils SSI sur le marché de l'emploi.

Contexte de la cybersécurité pour les ESMS

Les menaces

Le Parisien — S'ABONNER

Faits divers

Un Ehpad de l'Eure lui aussi victime d'une cyberattaque

L'établissement les Franches Terres installé à Beuzeville a vu son fichier patients chiffré par des pirates informatiques mercredi 24 août. Les dégâts ont été limités et une plainte contre X a été déposée.

Piratage informatique

Un établissement médico-social genevois victime d'une cyberattaque

L'EMS la Maison de Vessy a reçu une demande de rançon suite à une attaque informatique.

Fedele Mendicino
Publié: 20.09.2021, 17h38

HOSPIMEDIA — À la une

Système d'information

Le secteur médico-social est encore vulnérable face aux cyberattaques

Publié le 23/09/20 - 12h14

Fil d'information

Moins mature sur le volet numérique, le secteur médico-social est aussi moins protégé face aux cyberattaques. Les établissements et services sont d'ailleurs de plus en plus touchés, en particulier par des rançongiciels. Le futur plan ESMS numérique devrait permettre aux structures de rattraper leur retard en la matière.

Contexte de la cybersécurité pour les ESMS

Contexte règlementaire

- **Instruction 309, plan d'action SSI** – 2016

- **Signalement obligatoire des incidents de sécurité** – 2017
  - Etablissements de santé, Hôpitaux des armées, Centre de radiothérapie
  - Etablissements sociaux et médico-sociaux – 2020

- **Règlement Général sur la Protection des données** - 2018
  - Volet juridique
  - Volet technique

- **Programmes ESMS Numérique**– 2021 à 2025
  - La généralisation du dossier de l'usager informatisé (DUI)
  - L'atteinte d'un socle minimum de maturité de leurs systèmes d'information (sécurité, RGPD,..)

Contexte de la cybersécurité pour les ESMS

Acteurs régionaux

Décline la politique ministérielle en matière de cyber sécurité

- Facilite le partage des pratiques
- Intègre la sécurité dans les projets, objectifs, lettres...
- Suivi des incidents de sécurité

https://www.ars.sante.fr/securite-informatique-signaler-un-incident

Accompagne les acteurs du secteur dans la sécurité des systèmes d'information

- Gouvernance
- Détection et Protection
- Sensibilisation
- Gestion de crise

Anime un communauté régionale de référents sécurité

https://www.sesan.fr/services/ssi-conformite

Contexte de la cybersécurité pour les ESMS

Acteurs nationaux

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté
Égalité
Fraternité

l'Assurance Maladie
Agir ensemble, protéger chacun

cnsa
Caisse nationale de solidarité pour l'autonomie

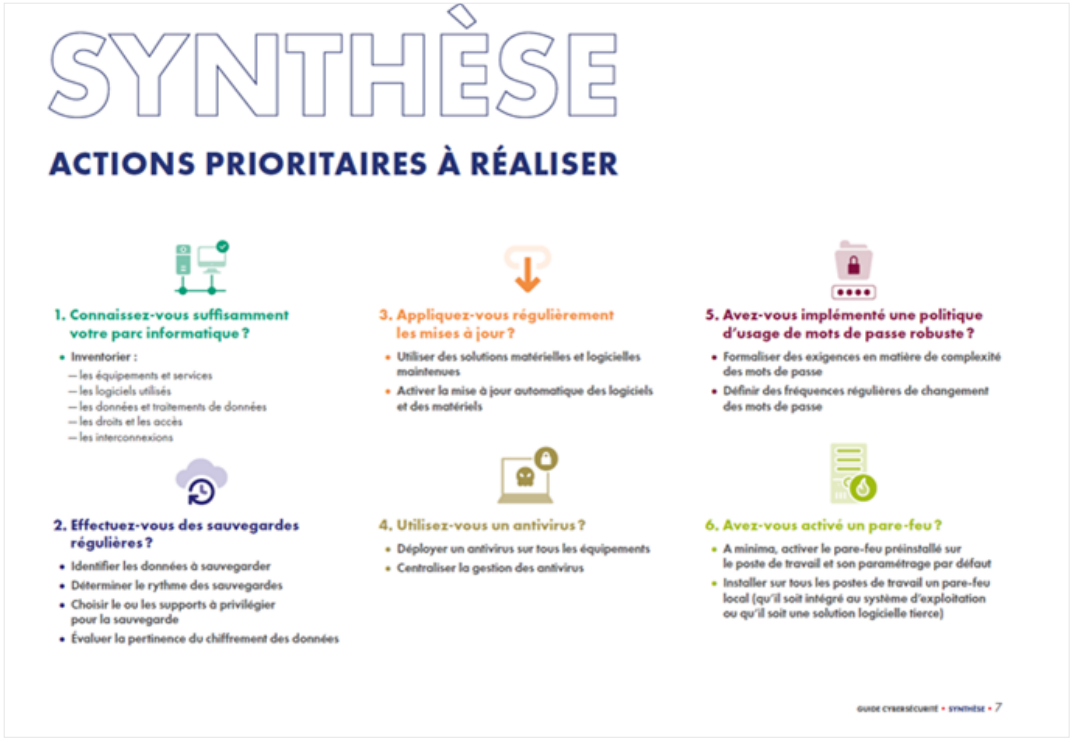
AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

- **Accompagne la transformation numérique** du système de santé aux côtés des acteurs concernés des secteurs.
- Traite les signalements d'incident
- Accompagne de façon préventives les structures (audit de cybersurveillance)
- Opère une veille sectorielle sur l'état de la menace

Contexte de la cybersécurité pour les ESMS

Guide cyber pour les ESMS

- Guide national "LA CYBERSÉCURITÉ POUR LES ESSMS EN 13 QUESTIONS" – *publication dans les prochains jours*


SYNTHÈSE

ACTIONS PRIORITAIRES À RÉALISER

1. Connaissez-vous suffisamment votre parc informatique ?
- Inventorier :
  - les équipements et services
  - les logiciels utilisés
  - les données et traitements de données
  - les droits et les accès
  - les interconnexions

2. Effectuez-vous des sauvegardes régulières ?
- Identifier les données à sauvegarder
- Déterminer le rythme des sauvegardes
- Choisir le ou les supports à privilégier pour la sauvegarde
- Évaluer la pertinence du chiffrement des données

3. Appliquez-vous régulièrement les mises à jour ?
- Utiliser des solutions matérielles et logicielles maintenues
- Activer la mise à jour automatique des logiciels et des matériels

4. Utilisez-vous un antivirus ?
- Déployer un antivirus sur tous les équipements
- Centraliser la gestion des antivirus

5. Avez-vous implémenté une politique d'usage de mots de passe robuste ?
- Formaliser des exigences en matière de complexité des mots de passe
- Définir des fréquences régulières de changement des mots de passe

6. Avez-vous activé un pare-feu ?
- A minima, activer le pare-feu préinstallé sur le poste de travail et son paramétrage par défaut
- Installer sur tous les postes de travail un pare-feu local (qu'il soit intégré au système d'exploitation ou qu'il soit une solution logicielle tierce)

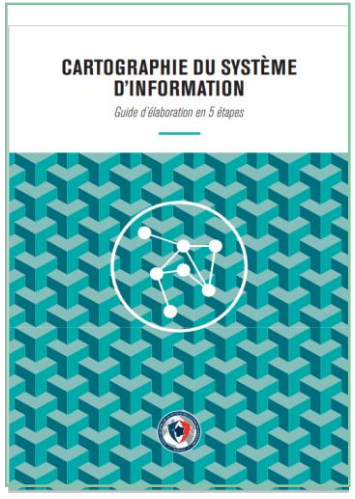
Les bons reflexes

Cybersécurité

Les bons reflexes

1. Connaitre son parc informatique

- Equipements
- Logiciels
- Données / Traitements
- Accès
- Interconnexions



https://www.ssi.gouv.fr/uploads/2018/11/guide-cartographie-systeme-information-anssi-pa-046.pdf

2. Sauvegarder régulièrement

- Modalité en fonction de la criticité des données
- Déconnecté du réseau
- Test des sauvegardes

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Cybersécurité

Les bons reflexes

3. Appliquer les mises à jour

- Matériel sous contrat de maintenance
- Solutions logicielles maintenues
- Appliquer de manière régulière
- Réaliser une veille des vulnérabilités et menaces

4. Utiliser un antivirus

- Sur tous les équipements
- Mise à jour régulière
- Gestion centralisée

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/ mises-a-jour

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

Cybersécurité

Les bons reflexes

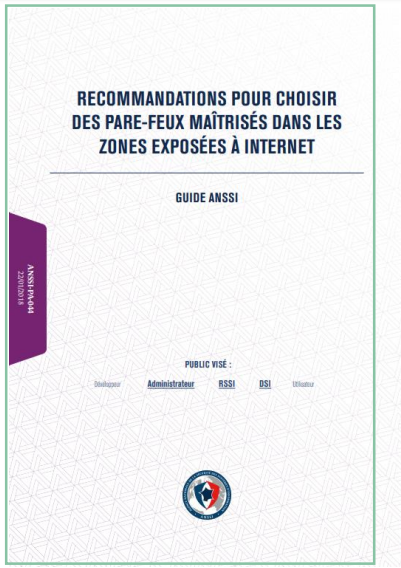
5. Politique des mots de passe robuste

- Formaliser des exigences
- Définir la fréquence de changement

https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_sécurité_mot_passe.pdf

6. Activer le pare-feu

- Sur le poste de travail
- Sur l'accès internet



https://www.ssi.gouv.fr/uploads/2018/01/guide_preconisations-pare-feux-zone-exposee-internet_anssi_pa_044_v1.pdf

Cybersécurité

Les bons reflexes

7. Sécuriser la messagerie

- Sensibiliser les professionnels
- Système d'analyse antivirus
- Anti-SPAM

8. Séparer les usages

- Compte utilisateur dédié sans privilège administrateur
- Révoquer les accès en cas de départ

CERT Santé

Service de test de la messagerie

https://esante.gouv.fr/produits-services/cert-sante

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

Cybersécurité

Les bons reflexes

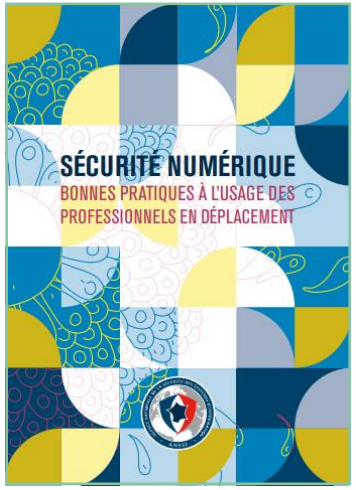
9. Sécuriser le nomadisme

- Sauvegarde
- Pas d'enregistrement des mots de passe
- VPN
- Supprimer l'utilisation des clés USB

10. Sensibiliser

- Aux bonnes pratiques
- A la déclaration des incidents
- Rédiger une Charte Informatique

FOCUS



https://www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable/

Cybersécurité

Les bons reflexes

11. Gérer la cyberattaque

- Identifier des prestataires spécialisés
- Portails de déclaration des incidents
- Organiser des exercices de Cybercrise FOCUS

12. Sécuriser les relations avec les tiers

- Clauses RGPD
- Exigences de sécurité annexées au contrat
- S'assurer de la solidité/solvabilité du prestataire

CNIL.

Notification d'une violation de données personnelles

https://notifications.cnil.fr/notifications/index

CNIL.

Sécurité : Gérer la sous-traitance

Encadrer la sécurité des données avec les sous-traitants.

https://www.cnil.fr/fr/securite-gerer-la-sous-traitance

FOCUS
La sensibilisation

La sensibilisation

Tous Cybervigilants

Kit de communication tous Cybervigilants pour le secteur médico-social

https://esante.gouv.fr/sites/default/files/media_entity/documents/kit-de-com-medico-social.zip

- Affiche A4
- Bannière-Visuel Réseaux Sociaux
- Dossier d'information (Stratégie Nationale, Panorama des incidents, rôle du CERT Santé, Campagne d'information)
- Triptyque : La sécurité numérique, socle de la "Transformation du numérique en santé" (règles clés à respecter, …)

TOUS CYBER VIGILANTS

La sensibilisation

CyberMalveillance

Kit de sensibilisation https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation

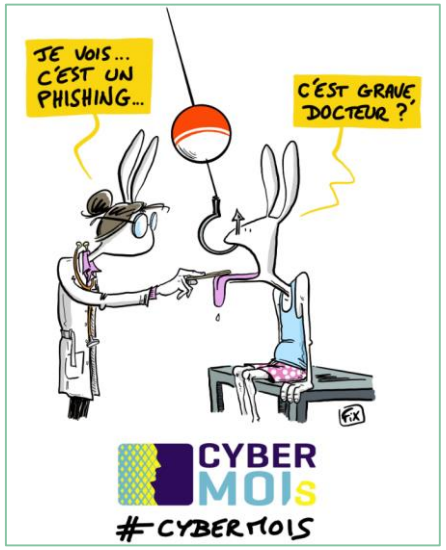
- Fiches pratiques et réflexes,
- mémos,
- affiche A2,
- BD,
- vidéos, ...

La sensibilisation

ANSSI – Cybermoi/s

Kit de sensibilisation

- Fiches pratiques et réflexes,
- vidéos, ...



https://www.ssi.gouv.fr/agence/cybersecurite/cybermois-2021-les-mots-de-passe/
https://www.ssi.gouv.fr/agence/cybersecurite/le-cybermois/cybermois-2022-tous-ensemble-face-aux-rancongiciels-et-au-hameconnage/

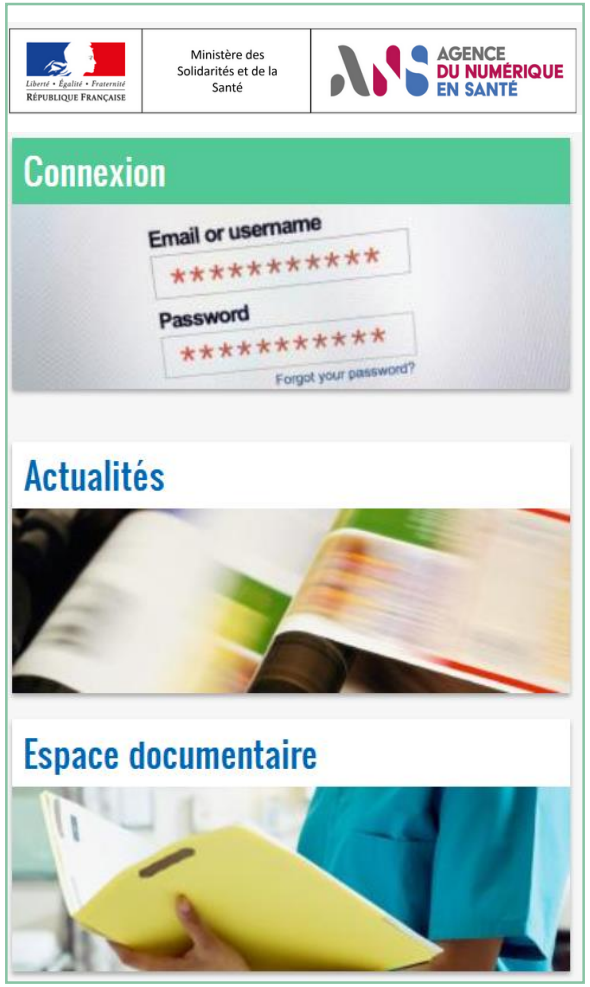
La sensibilisation

Cyberveille santé

Site relais de la communication du Cert-santé

- **Veille et alerte** sur les vulnérabilités et menaces critique ou relatif à la SSI santé
- Evènements et webinaire de l'ANS
- Espace documentaire
  - Guides de bonnes pratiques
  - Instructions ministérielles et PGSSIS

https://cyberveille-sante.gouv.fr/



La sensibilisation

SEGUR Numérique

https://segurnumerique.sante-idf.fr/docutheque/

La sensibilisation

Newsletter

Utilisez la newsletter mensuelle de SESAN pour vos sensibilisations

https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/

Veille réalisée auprès de sites institutionnels (ANS, CNIL, ANSSI…) et de sites spécialisés.

La sensibilisation

Conclusion

1/ Sensibilisez tout au long de l'année

2/ Alternez les modes de sensibilisation

- **Affiche,**
- **Signature de mail,**
- **Présentation physique,**
- **Évènement majeur...**

FOCUS
Les exercices de cybercrise

La sensibilisation

Organiser un exercice de Cybercrise

Comment Sensibiliser au risque Cyber ?

- Exercice de cyber crise : une démarche d'anticipation des risques
- Un kit "Débutant" mis à disposition par l'ANS

Objectif :

- Prendre conscience de sa dépendance aux SI
- Définir un plan d'action pour prendre en compte le risque Cyber dans son PCA

https://www.cyberveille-sante.gouv.fr/index.php/exercice-crise

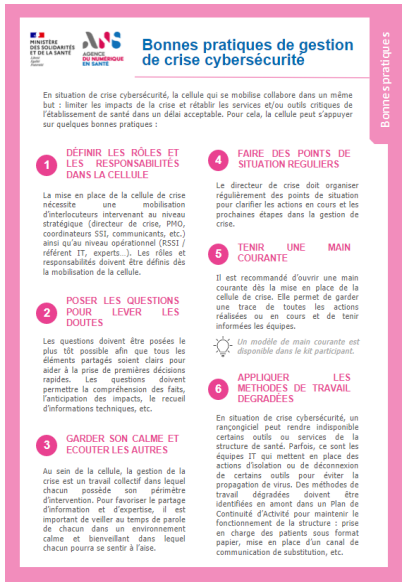
La sensibilisation

Organiser un exercice de Cybercrise

Contenu du Kit :

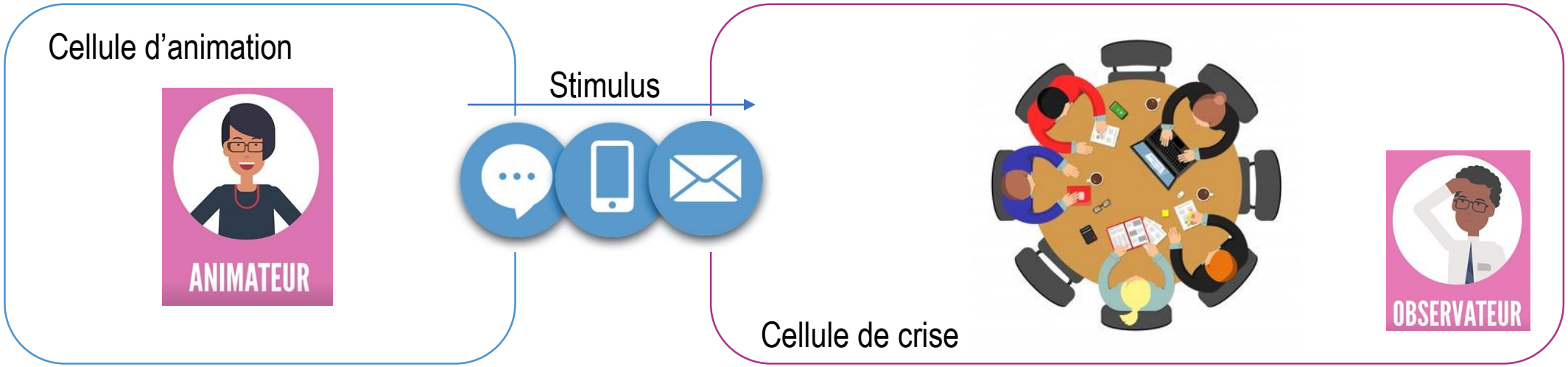
- **Livret Animateur** (bonnes pratiques d'animation, scénario, organisation de l'exercice, animation du briefing, animation de l'exercice, animation du débriefing, le rôle de l'observateur...)
- **Livret Participant** (règles du jeu, bonnes pratiques de communication en situation de crise, bonnes pratiques de gestion de crise Cyber, …)

En toute autonomie



La sensibilisation

Organiser un exercice de Cybercrise



L'**animateur** met en action le scénario en envoyant les stimuli à la cellule de crise sous forme de simulations d'appels ou de mails pour susciter une réaction / action des joueurs.

Les **joueurs** s'adaptent à la situation de crise fictive déroulée par l'animateur en utilisant des moyens de communication et procédures opérationnelles habituellement utilisées dans la structure (si elles existent).

L'**observateur** apporte un regard extérieur à l'exercice et relève les points positifs et axes d'amélioration selon les objectifs de l'exercice. Il n'intervient pas dans le déroulement de l'exercice.

La sensibilisation

Organiser un exercice de Cybercrise

Vidéo disponible dans le kit

SESAN POUR VOUS ACCOMPAGNER

SESAN pour vous accompagner

Campagne de sensibilisation

- **Parcours de sensibilisation interactifs dédiés au secteur sanitaire et médico-social**
  - Quizz, vidéos,
  - Durée d'1m30 en moyenne
  - Sensibilisation personnalisée et contextualisée (contact ESMS, charte graphique,…)

Logos et charte graphique personnalisables

SESAN pour vous accompagner

Escape Game

- **Sensibilisation ludique à la sécurité numérique**

Une équipe de journaliste s'introduit dans une salle de réunion laissée sans surveillance dans le but de retrouver le dossier médical du célèbre Johnny Jackson.

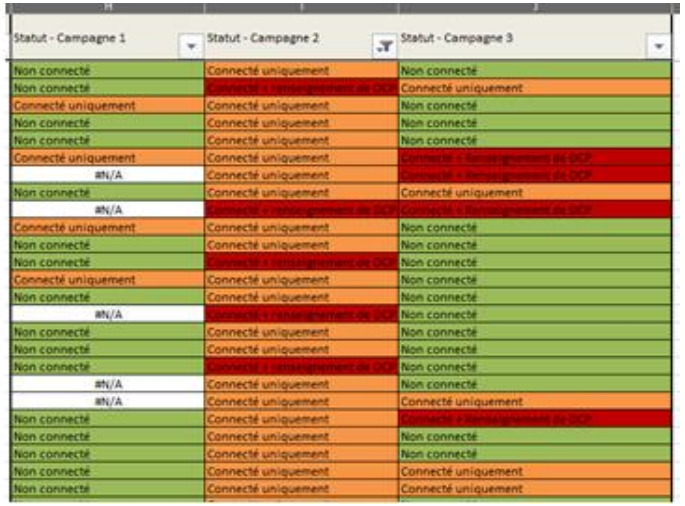
Objectif :

- Démontrer la dangerosité des mauvaises pratiques
- Apporter des solutions concrètes à chaque problématique
- Souligner l'importance de la sécurité numérique par chaque acteur
- Favoriser la cohésion des équipes

SESAN pour vous accompagner

Test de Phishing

- Nombre d'adresses mail illimité
- Possibilité d'ajouter un portail de saisie d'informations personnelles
- Portail de sensibilisation pour les personnes "piégées"
- Statistiques de la campagne



SESAN pour vous accompagner

Autres supports de sensibilisation

- Multiplier les canaux de sensibilisation

Affiches complémentaires

Ecrans de veille

E-mailing

Calendrier SSI

SESAN pour vous accompagner

Autres offres

- Gouvernance
- Détection et protection
- Gestion de crise
- Formation

- Communauté régionale de référent sécurité et protection des données

TÉMOIGNAGE

Témoignage

Centre de la Gabrielle

Le Centre de la Gabrielle et **les Ateliers du Parc de Claye** sont composés de 12 établissements et services médico-sociaux privés à but non lucratif.

Le Centre de la Gabrielle propose une offre de service destinée à répondre aux besoins des enfants, adolescents et adultes en situation de handicap mental.

Enfants et adolescents

Adultes

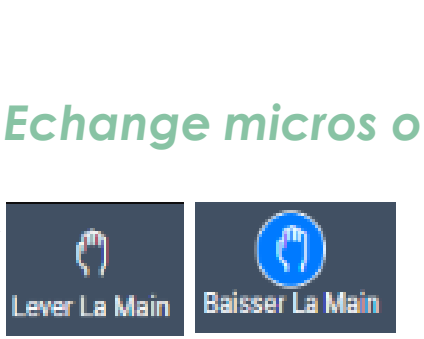
Actions et projets

CENTRE DE LA GABRIELLE
ATELIERS DU PARC DE CLAYE

Jean-Luc ANGOT
Responsable Système d'Information

Questions / Réponses

Echange micros ouverts



Contactez : ssi@sesan.fr

sesan
SERVICE NUMÉRIQUE DE SANTÉ

Journée E-santé

*La cyber-sécurité, une thématique incontournable de la **journée régionale de la eSanté** organisée par l'ARS-IF et SESAN*

Nous aurons plaisir à vous y retrouver le

8 novembre à la Cité Internationale Universitaire de Paris

ANNEXES

Votre accompagnement régional

ars-idf-si-esms@ars.sante.fr

- **Pilotage régional du programme ESMS Numérique**
- Organisation et gestion des **appels à projets régionaux**
- Analyse et sélection des projets soumis
- **Accompagnement et suivi,** dans les différentes phases du projet, des organismes gestionnaires retenus
- Communication autour du programme et du Ségur du numérique

segur@sesan.fr

- Expertise en **sécurité des systèmes d'information**
- Expertise dans le **déploiement du DUI** et les **services socles** (nationaux, régionaux).
- Appui à l'ARS Île-de-France dans l'**accompagnement** et **le suivi** des projets retenus
- Communication et **contenus pédagogiques** (Services socles, Ségur du Numérique)

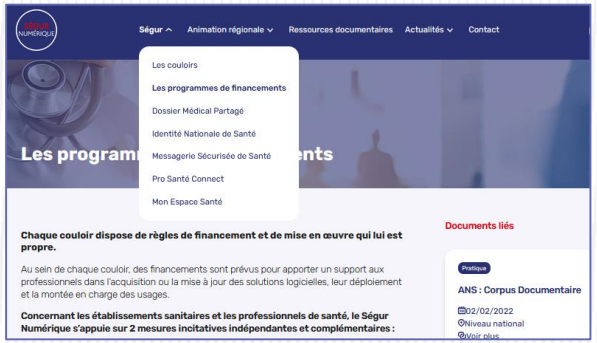
Idf-collectif-si@uriopss-idf.fr

- **Représentation** du secteur
- **Information et animation de réseau**
- **Soutien** à la c**oopération** des organismes gestionnaires et au partage de bonnes pratiques
- **Appui à la mutualisation des petits organismes gestionnaires**

Transmettez vos demandes de regroupement *en précisant quelques éléments :*
✓Activités déployées et publics accompagnés,
✓Sur quels aspects des AAP souhaiteriez-vous répondre ?
> Installation de DUI
> Mise en conformité (dans ce cas quel est votre éditeur actuel)

En savoir plus sur les financements et les services socles :

https://segurnumerique.sante-idf.fr



Prochains rendez-vous :

Retrouver la liste des événements

A ce lien

Page dédiée au Collectif SI MS IDF

A ce lien

GESTION DE CRISE

Liens utiles

Synthèse des ressources disponibles

- Kit "Débutant": https://www.cyberveille-sante.gouv.fr/index.php/exercice-crise

- Support du webinaire du 16 juin consacré au kit ANS : https://segurnumerique.sante-idf.fr/wp-content/uploads/2022/06/20220616_Segur-Numerique-Q.R-Fenetre-1-SUN-ES_KitANS.pdf

- Replay du webinaire du 16 juin consacré au kit ANS : Webinaire IDF - Renforcement de la Cybersécuritédanslesétablissements Sanitaires -16 juin2022 - YouTube

- Retex d'une cyberattaque dans un EHPAD: https://cyberveille-sante.gouv.fr/sites/default/files/2019-10/7%20-%204%20TR%20JB%20Rouffet%20-%20Les%20lecons%20d%20une%20cyberattaque%20-%20%20EHPAD%20les%203%20sources%20-%203%2010%202019.pdf

SENSIBILISATION

Liens utiles

Synthèse des ressources disponibles

- Kit de sensibilisation : https://esante.gouv.fr/sites/default/files/media_entity/documents/kit-de-com-medico-social.zip
- Kit de sensibilisation CyberMalveillance : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation
- CyberveilleSanté : https://cyberveille-sante.gouv.fr/
- Newsletter SESAN : https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/
- Affiches SESAN : https://segurnumerique.sante-idf.fr/docutheque/

- Autres liens utiles :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales
https://www.ssi.gouv.fr/particulier/precautions-elementaires/dix-regles-de-base/
https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/