MARDI 3 décembre 2024
de 9h à 17h30
Centre de congrès d'Angers

JOURNEE REGIONALE E-SANTE

Pour les professionnels du social et du médico-social des Pays de la Loire

Quels outils numériques pour quels usages ?

RÉPUBLIQUE FRANÇAISE
ars Agence Régionale de Santé Pays de la Loire
l'Assurance Maladie
e-santé GRADeS Pays de la Loire
Collectif SI Médico-Social Pays de la Loire
CaRE Cybersécurité accélération Résilience des Etablissements
Financé par l'Union européenne NextGenerationEU

Atelier Cybersécurité

« Crise cyber : se préparer pour mieux la traverser »

Mehdi ZINE, *Agence du Numérique en Santé*

Bastien LE HYARIC, *ADAPEILA*

Emilie PRIOUX, *GRADeS Pays de la Loire*

Fabien APPRIOU, *GRADeS Pays de la Loire*

Financé par l'Union européenne NextGenerationEU

Sommaire

Financé par l'Union européenne NextGenerationEU

Les principaux impacts d'une crise cyber

Quels peuvent être, selon-vous, les **principaux impacts** d'une crise cyber sur une structure sociale ou médico-sociale ?

Les impacts d'une crise cyber sur la structure victime

Organisation et accompagnement des usagers

Finances

Crise cyber

Dommages sur la réputation

Juridique & légal

Qu'est-ce qu'une crise cyber ?

- Ce type de crise se caractérise par :

Sa **temporalité**
impacts immédiats vs remédiation longue

Son **absence d'unicité**
propagation possible due à la forte interconnexion des réseaux

Son **adaptabilité**
menace s'adaptant aux mesures d'endiguement ou remédiation

Son **incertitude**
périmètre touché, durée, ...

Un évènement à **fort impact**, survenant **sur le SI** et qui **ne pourrait être traité par les processus habituels** ou dans le cadre du **fonctionnement normal de l'organisation**.

Anticiper et se préparer

La mise en place au sein de l'établissement d'une organisation opérationnelle et stratégique en amont de la survenue d'un incident peut permettre de réduire les impacts potentiels d'une crise cyber.

Mettre en situation sa cellule de crise

Gagner en réactivité / efficacité dans la gestion et la communication de crise cyber

Vérifier la complétude de ses Plan de Continuité et Plan de Reprise de l'Activité (PCRA)

Assurer la continuité des activités de la structure

Tester la mise en œuvre de ses dispositifs de secours / crise

Gagner en adaptabilité et veiller au bon fonctionnement des process définis.

Sensibiliser

Impliquer les utilisateurs du SI

Formaliser la cartographie de son SI

Faciliter l'identification des impacts potentiels, la prise de décision et la reprise d'activité

Démarche régionale – Focus sur l'exercice de crise cyber

Webinaires techniques

- Sécuriser mon AD
- Protéger mes réseaux, mon Wifi
- Détecter les menaces
- Sécuriser ma messagerie

Journées régionales

- Partager les actualités, nouvelles réglementations et expériences avec les acteurs en région

Appui à la gestion des incidents

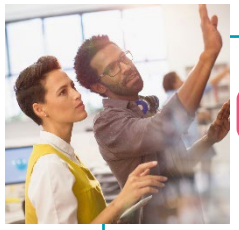
- Soutien en cas d'incident

Veille technologique et réglementaire

- https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-168.html

Base documentaire régionale

- Modèles de documents
- Mémos thématiques
- Base documentaire en ligne



Préparation à la crise cyber

- Soutien à la réalisation d'exercices de crise cyber (ES et ESMS)
- Centre de ressources SSI mutualisées accessible aux ESMS

Outils de sensibilisation

- Affiches
- Fonds d'écran
- Escape game
- Badges métalliques
- e-learning
- Vidéos de sensibilisation
- Flyer de sensibilisation des entrepreneurs
- Datablockers
- Faux phishing

Financé par l'Union européenne NextGenerationEU

Pourquoi réaliser un exercice de crise cyber ?

S'interroger

- Sur les processus critiques
- Sur la pertinence des plans de secours

Sensibiliser

- En impliquant l'ensemble des acteurs concernés
- En s'appuyant sur une simulation

Progresser

- En identifiant des axes d'amélioration concrets pour assurer la continuité de l'activité

S'entraîner

- Pour gagner en réactivité et en efficience
- Pour apprendre à mesure les impacts d'une crise cyber

Formaliser

- Pour se préparer à faire face à un incident cyber
- Pour fluidifier la communication, le pilotage de crise, etc...

Créer une dynamique cyber

- En initiant une démarche d'amélioration continue de préparation à la crise cyber

Augmenter la résilience de l'offre médico-sociale

Financé par l'Union européenne NextGenerationEU

Retour d'expérience

- Partage de l'ADAPEILA sur la réalisation de son 1er exercice de crise cyber, réalisé le 28/11/24.

Par Bastien LE HYARIC, *Directeur des Systèmes d'Information & Transformation*.

La déclinaison régionale mise en œuvre

Appui sur la documentation nationale de référence

Un **kit** national proposant un **scénario adapté** au secteur social et médico-social

AGENCE DU NUMÉRIQUE EN SANTÉ

Une expérience éprouvée sur le secteur sanitaire

90 Etablissements sanitaires **accompagnés**

99% de participants **satisfaits ou très satisfaits**

Une organisation facilitée pour la structure bénéficiaire

Une démarche **clé en main** éprouvée depuis 2 ans

Financé par l'Union européenne NextGenerationEU

Modalités de réalisation de l'exercice de crise cyber

1 mois avant l'exercice

Réunion de lancement

Comprendre vos spécificités, organiser l'évènement et gérer la logistique

1h

1 référent de la structure

Distanciel

Jour J

Exercice de crise cyber

Réaliser l'exercice et conduire un retour d'expérience à chaud

3h

Cellule de crise décisionnelle

Dans vos locaux

1 mois après l'exercice

Restitution

Réaliser un bilan des bonnes pratiques et des axes d'amélioration

1h

Participants à l'exercice

Distanciel

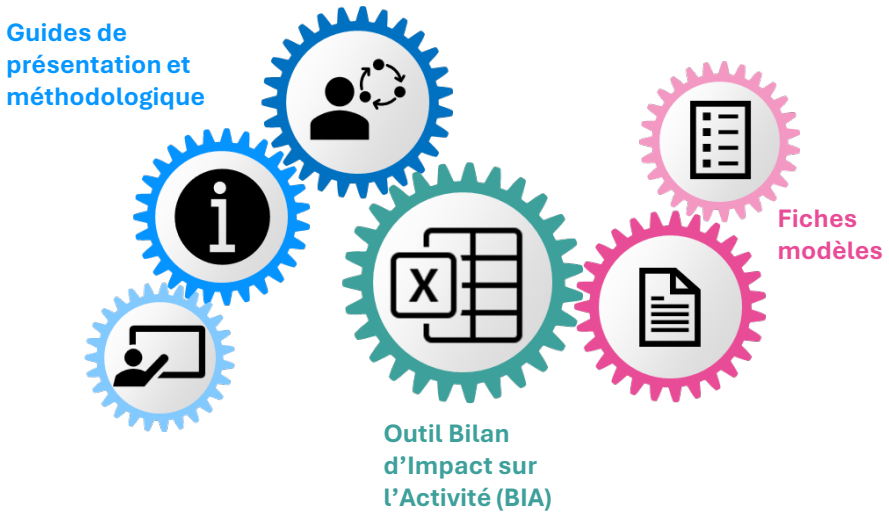
Focus sur le KIT PCRA pour les ESMS

- Présentation du Kit ANS

Par Mehdi ZINE, *Agence du Numérique en Santé*.

Préparer et accompagner les établissements à réagir et à faire face à la cybermenace

Mettre en œuvre des Plans de Continuité et de Reprise d'Activité (PCRA) dans les établissements (ES et ESSMS)



Anticiper la survenue de crise pouvant amener à une **indisponibilité des ressources, dont les SI**, dans le but de sécuriser la continuité des activités critiques au fonctionnement de l'ESSMS

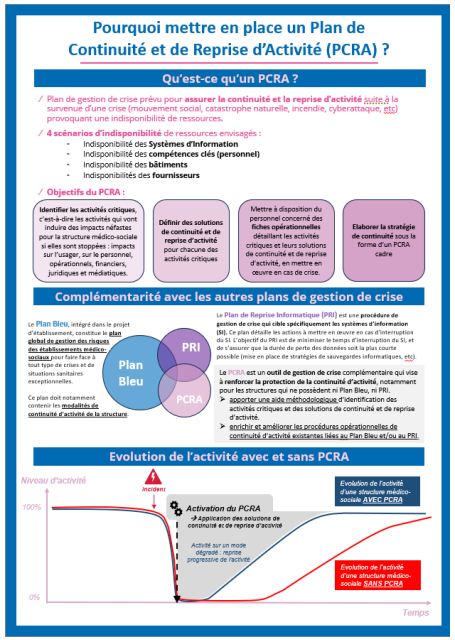
Construction d'un **kit PCRA adapté au secteur médico-social** en collaboration avec des acteurs du secteur médico-social (handicap, domicile et personne âgée) :

- *guide méthodologique de mise en place d'un PCRA*
- *outil « BIA » d'identification des activités critiques et de définition de solutions de continuité et de reprise d'activité*
- *modèles documentaires : fiches opérationnelles, PCRA cadre*

Kit en cours de finalisation : publication prochaine sur le site de l'ANS

Kit PCRA médico-social

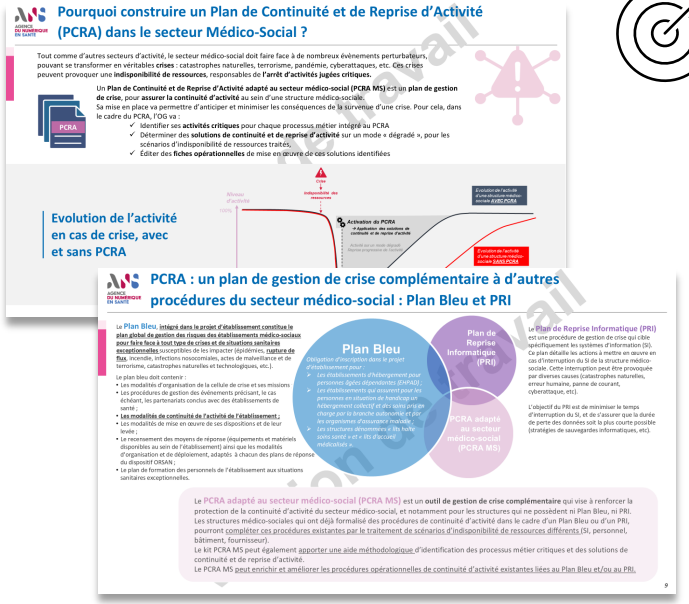
Note de présentation



Présenter de manière synthèse aux décideurs :

- Ce qu'est un PRCA à destination du secteur médico-social
- La complémentarité du PCRA avec les autres plans de gestion de crise
- L'impact de la mise en place d'un PCRA sur l'activité

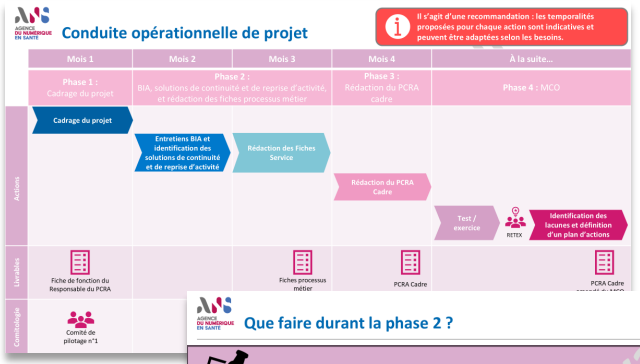
Définition et principes généraux du PCRA

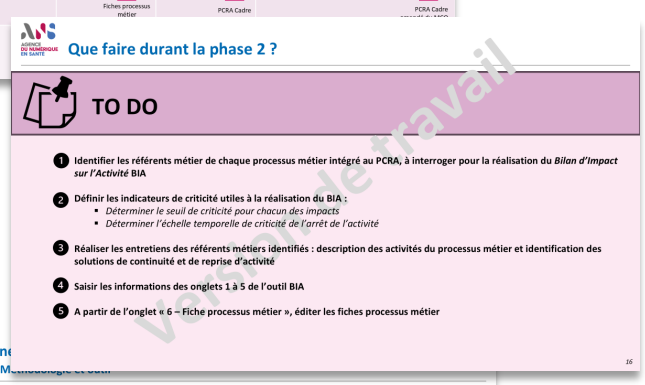


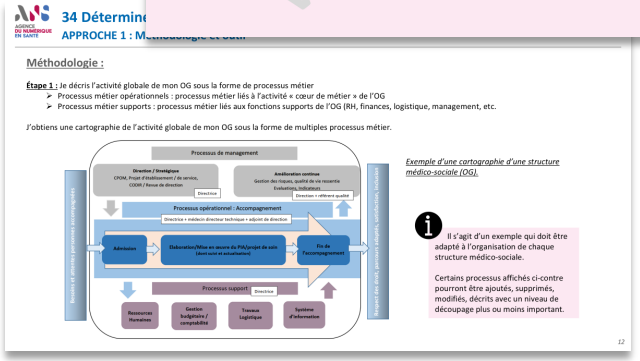
- Communiquer des éléments facilitants pour mener à bien les travaux
- Répondre à la question « Pourquoi mettre en place un PCRA » ?
- Définir le Système de Management de la Continuité d'Activité (SMCA)
- Présenter les scénarios d'indisponibilité à traiter dans un PCRA
- Expliquer comment décrire l'activité d'une structure médico-sociale
- Aborder la complémentarité du PCRA avec les autres plans de gestion crise dans le médico-social (Plan bleu et plan de reprise informatique)
- Définir les termes spécifiques de la continuité d'activité dans un glossaire

Kit PCRA médico-social

Méthodologie de construction du PCRA

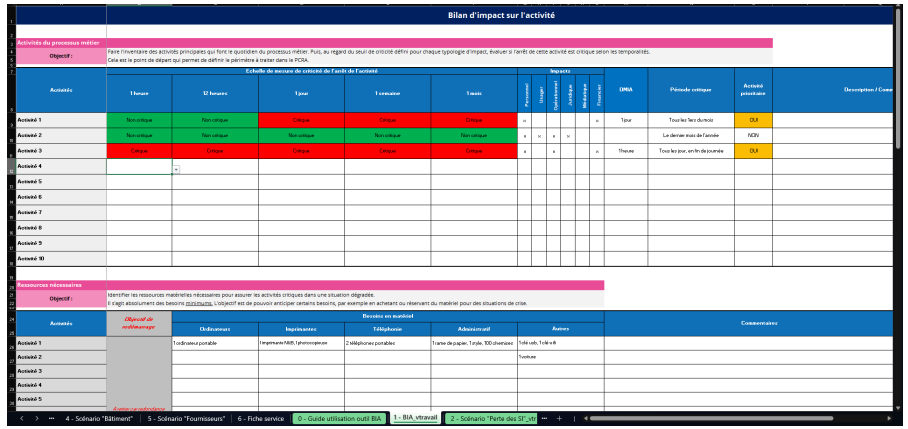






Dans une logique « pas à pas », guider l'équipe en charge de mener les travaux de construction du PCRA au sein de l'OG :

- Proposition d'un calendrier de conduite opérationnelle des travaux à mener
- Pour chacune des 4 grandes phases de construction du PCRA :
  - Actions à réaliser sous forme de « To do list »
  - Outils et modèles documentaires à utiliser



Pour aller plus loin : Que faire en cas d'incident cyber ?

(signalements et déclarations)

Dispositif de signalement des incidents de sécurité des SI dans le secteur santé – Art. 110.

Mission de soutien et d'appui aux structures dans la gestion de leurs incidents confiée par l'ARS au GRADeS Pays de la Loire, depuis 2016.

- **Facilitation des échanges entre la structure, le CERT Santé et le prestataire infor matique de la structure (éventuellement)**
- **Conseils techniques et organisationnels**

Incident cyber ESMS

Etablissements de santé
Organismes et services exerçant des activités de prévention, de diagnostic ou de soins

Si violation données personnelles suspectée ou avérée

Démarches de notification à la CNIL

Déclaration sans délai

https://signalement.social-sante.gouv.fr

Si origine malveillante

***Fiche mémo** Dépôt de plainte à la suite d'un incident d'origine malveillante*

Agence Régionale de Santé des Pays de la Loire (**SSI-PDL@ars.sante.fr**)

Equipe régionale Sécurité des SI (GRADeS Pays de la Loire) (**ssi@esante-paysdelaloire.fr**)

Cellule d'Accompagnement Cybersécurité des Structures de Santé

(CERT-Santé – Agence du numérique en santé)

24h/7j - 09 72 43 91 25
cyberveille@esante.gouv.fr

Pour aller plus loin : Sensibilisation

- Sensibilisation aux bonnes pratiques d'hygiène numérique via la plateforme de e-learning / faux-phishing du GRADeS, à destination de ses adhérents :

Exemple de e-learning

Bonjour,

Nous tenons à vous informer de la nouvelle réglementation en matière d'acquisition des congés payés en cas d'arrêt maladie, entrée en vigueur dernièrement suite à l'adaptation du Code du Travail français au droit de l'Union Européenne.

Les changements décrits dans le document toucheront les membres du personnel travaillant à temps plein et à temps partiel, ainsi que ceux ayant droit à des prestations sociales.

Il est donc fortement RECOMMANDE que tous les employés consultent cette nouvelle politique applicable dès à présent, via le lien ci-dessous :

Veuillez cliquer ici

Bien Cordialement.
Les Ressources Humaines.

Faux-phishing partagé à l'été 2024

Adresse pour toute demande d'un accompagnement cyber au GCS e-santé PdL :
cyber.esms@esante-paysdelaloire.fr

Pour aller plus loin : Programme CaRE et RETEX

- Programme CaRE - Cybersécurité accélération et Résilience des Etablissements.

- **Retours d'expérience de structures victimes d'une cyberattaque** :
  - 3 établissements victimes d'une cyberattaque en 2023 pour lesquels le CERT-Santé est intervenu en appui technique dans la réponse à incident : leurs retours d'expérience.
    - Dont l'association Handi Val de Seine, victime d'une cyberattaque le 23/02/23 (lien direct vers le support).
  - Vidéos de témoignage de structures victimes d'une cyberattaque :

Directeur Général du GHT Cœur Grand Est

Directeur Général du CH de Versailles

Pour aller plus loin : Veille cybersécurité

- Veille GCS e-santé Pays de la Loire

- **Documentation ANSSI** :
  - Crise d'origine cyber - Les clés d'une gestion opérationnelle et stratégique – guide
  - Anticiper et gérer sa communication de crise cyber (ANSSI) – guide

- **Partager, rappeler** régulièrement les **bonnes pratiques et conseils d'hygiène numérique** avec ses confrères/consœurs.

Financé par l'Union européenne NextGenerationEU

Merci pour votre attention

« Gérer la crise est d'un certain point de vue une contradiction dans les termes. On ne gère pas le tourment, le trouble ; on s'efforce d'éviter qu'il se produise, d'en minimiser les effets ou de rétablir l'ordre. »

Simone EIKEN & Olivier VELIN

Financé par l'Union européenne NextGenerationEU