



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 ?



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*



Sommaire

- 1. Les principaux impacts d'une crise cyber***
- 2. Anticiper et se préparer***
- 3. Démarche régionale – Focus sur l'exercice de crise cyber***
- 4. Focus sur le KIT PCRA pour les ESMS***
- 5. Pour aller plus loin***



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





Qu'est-ce qu'une crise cyber ?

- Ce type de crise se caractérise par :



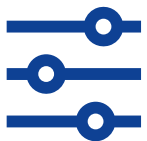
Sa **temporalité**

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



Wanna Decryptor
 Une campagne d'attaques de type ransomware est actuellement en cours dans plusieurs pays, particulièrement au niveau de l'Union Européenne. Le fonctionnement de certains établissements de santé hospitaliers a été affecté par ce type d'attaque. Aucune alerte n'est identifiée actuellement dans les établissements français. Le virus concerné serait Wanna Decryptor (autre nom : Jaff, Wanna, wjff). Il semble exploiter une vulnérabilité corrigée par le correctif Microsoft MS17-016. Il est demandé la plus grande vigilance et de diffuser largement cette information.

Appui à la gestion des incidents

- Soutien en cas d'incident



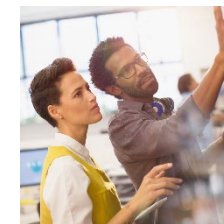
Veille technologique et réglementaire

- <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

Pourquoi réaliser un exercice de crise cyber ?

S'interroger

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

Progresser

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

Formaliser

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

Sensibiliser

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

S'entraîner

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

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




Retour d'expérience

- Partage de l'ADAPEILA sur la réalisation de son 1^{er} 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



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



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)



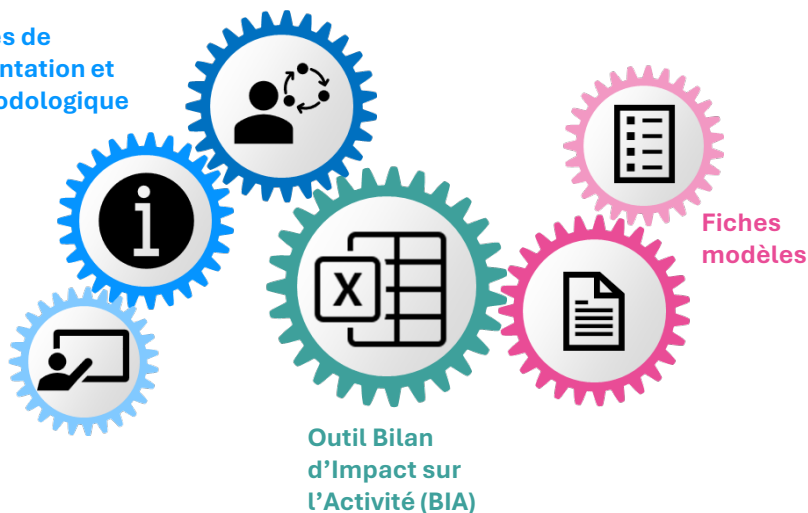
Anticiper la survenue de crise pouvant amener à une **indisponibilité des ressources, dont les SI**, dans le but de sécuriser la continuité des activités critiques au fonctionnement de l'ESSMS



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*

Guides de présentation et méthodologique



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



Kit PCRA médico-social



Note de présentation

Pourquoi mettre en place un Plan de Continuité et de Reprise d'Activité (PCRA) ?

Qu'est-ce qu'un PCRA ?

- Plan de gestion de crise prévu pour assurer la continuité et la reprise d'activité **avant** la survenue d'une crise (mouvements sociaux, catastrophe naturelle, incendie, cyberattaque, etc.) provoquant une indisponibilité de ressources.
- 4 scénarios d'indisponibilité de ressources envisagés :
 - Indisponibilité des **Systèmes d'Information**
 - Indisponibilité des **Compétences clés (personnel)**
 - Indisponibilité des **Bâtiments**
 - Indisponibilité des **Fournisseurs**
- Objectifs du PCRA :
 - Identifier les **activités critiques**, c'est-à-dire les activités qui vont induire des impacts néfastes pour la structure médico-sociale si elles sont stoppées. Impacts sur l'usage, sur le personnel, opérationnels, financiers, juridiques et médiatiques.
 - Définir des solutions de continuité et de reprise d'activité pour chacune des activités critiques.
 - Mettre à disposition du personnel concerné des **feuilles opérationnelles** décrivant les activités critiques et leurs solutions de continuité et de reprise d'activité, en mettre en œuvre en cas de crise.
 - Elaborer la **stratégie de continuité** sous la forme d'un PCRA **cadre**.

Complémentarité avec les autres plans de gestion de crise

Le Plan de Reprise Informatique (PRI) est une procédure de gestion de crise qui cible **spécifiquement** les systèmes d'information (SI). Ce plan décrit les actions à mettre en œuvre en cas d'indisponibilité du SI. L'objectif du PRI est de minimiser le temps d'interruption du SI, et de l'assurer que le durée de perte des données est la plus courte possible (mise en place de stratégies de sauvegarde informatiques, etc.).

Le Plan Bleu, intégré dans le projet d'établissement, constitue le **Plan de Continuité et de Reprise d'Activité (PCRA)** des établissements médico-sociaux. Ce plan vise à assurer la continuité et la reprise d'activité en cas de crise et de situations similaires exceptionnelles.

Le PCRA est un outil de gestion de crise complémentaire qui vise à renforcer la protection de la continuité d'activité, notamment pour les structures qui ne possèdent ni Plan Bleu, ni PRI.

Le PCRA permet également d'identifier des processus métier critiques et des solutions de continuité et de reprise d'activité.

Evolution de l'activité avec et sans PCRA



Présenter de manière synthétique aux décideurs :

- Ce qu'est un PCRA 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

Pourquoi construire un Plan de Continuité et de Reprise d'Activité (PCRA) dans le secteur Médico-Social ?

Tout comme d'autres secteurs d'activité, le secteur médico-social doit faire face à de nombreux événements perturbateurs, pouvant se transformer en véritables crises : catastrophes naturelles, terrorisme, pandémie, cyberattaques, etc. Ces crises peuvent provoquer une indisponibilité de ressources, responsables de l'arrêt d'activités jugées critiques.

Un Plan de Continuité et de Reprise d'Activité adapté au secteur médico-social (PCRA MS) est un plan de gestion de crise, pour assurer la continuité d'activité au sein d'une structure médico-sociale.

Si mis en place au préalable, il permet d'anticiper et minimiser les conséquences de la survenue d'une crise. Pour cela, dans le cadre du PCRA, l'ONG va :

- ✓ Identifier les **activités critiques** pour chaque processus métier intégré au PCRA.
- ✓ Déterminer des **solutions de continuité et de reprise d'activité** sur un mode « dégradé », pour les scénarios d'indisponibilité de ressources traités.
- ✓ Éditer des **feuilles opérationnelles** de mise en œuvre de ces solutions identifiées.

Evolution de l'activité en cas de crise, avec et sans PCRA

PCRA : un plan de gestion de crise complémentaire à d'autres procédures du secteur médico-social : Plan Bleu et PRI

Le Plan Bleu, intégré dans le projet d'établissement constitue le **plan de gestion de crise** des établissements médico-sociaux pour faire face à toute situation de crise (catastrophes naturelles, terrorisme, pandémie, cyberattaques, etc.).

Le plan vise à assurer la continuité et la reprise d'activité en cas de crise et de situations similaires exceptionnelles.

Le Plan de Reprise Informatique (PRI) est une procédure de gestion de crise qui cible spécifiquement les systèmes d'information (SI). Ce plan détaille les actions à mettre en œuvre en cas d'indisponibilité du SI de la structure médico-sociale. Cette intervention peut être groupée par domaines (sauvegarde informatique, serveur, erreur humaine, panne de courant, cyberattaque, etc.).

L'objectif du PRI est de minimiser le temps d'interruption du SI, et de l'assurer que le durée de perte des données est la plus courte possible (stratégies de sauvegarde informatiques, etc.).

Le PCRA adapté au secteur médico-social (PCRA MS) est un outil de gestion de crise complémentaire qui vise à renforcer la protection de la continuité d'activité du secteur médico-social, et notamment pour les structures qui ne possèdent ni Plan Bleu, ni PRI.

Les structures médico-sociales qui ont déjà formalisé des procédures de continuité d'activité dans le cadre d'un Plan Bleu ou d'un PRI, pourront compléter ces procédures existantes par le traitement de scénarios d'indisponibilité de ressources (SI, personnel, bâtiment, fournisseur).

Le kit PCRA MS peut également apporter une aide méthodologique d'identification des processus métier critiques et des solutions de continuité et de reprise d'activité.

Le PCRA MS peut servir à améliorer les procédures opérationnelles de continuité d'activité existantes liées au Plan Bleu et/ou au PRI.



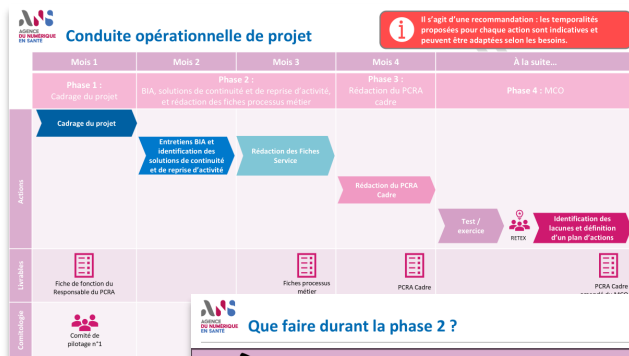
- Communiquer des éléments facilitants pour mener à bien les travaux
- Répondre à la question « Pourquoi mettre en place un PCRA » ?
- Définir le Système de Management de la Continuité d'Activité (SMCA)
- Présenter les scénarios d'indisponibilité à traiter dans un PCRA
- Expliquer comment décrire l'activité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



Que faire durant la phase 2 ?

TO DO

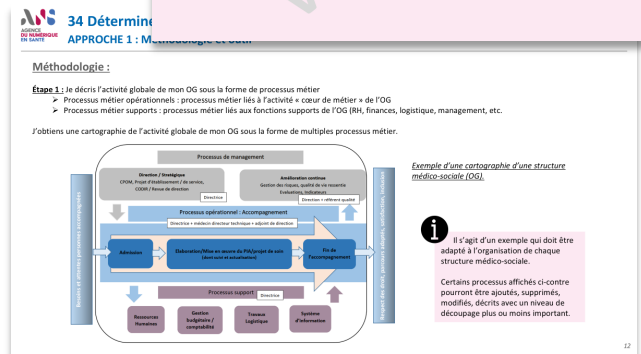
- 1 Identifier les référents métier de chaque processus métier intégré au PCRA, à interroger pour la réalisation du Bilan d'Impact sur l'Activité BIA
- 2 Définir les indicateurs de criticité utiles à la réalisation du BIA :
 - Déterminer le seuil de criticité pour chacun des impacts
 - Déterminer l'échelle temporelle de criticité de l'arrêt de l'activité
- 3 Réaliser les entretiens des référents métiers identifiés : description des activités du processus métier et identification des solutions de continuité et de reprise d'activité
- 4 Saisir les informations des onglets 1 à 5 de l'outil BIA
- 5 A partir de l'onglet « 6 - Fiche processus métier », éditer les fiches processus métier



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

Bilan d'impact sur l'activité													
Activités du processus métier													
Objectif : Faire l'inventaire des activités principales qui font le quotidien du processus métier. Puis, au regard du seuil de criticité défini pour chaque type d'impact, évaluer à l'aide de cette activité est critique selon les temporalités. C'est en ce point de départ que l'on commence à travailler sur le PCRA.													
Activités	Echelle de mesure de criticité de l'arrêt de l'activité					Impact			Processus		Outils		Description / Commentaires
	1 heure	17 heures	Jour	Semaine	Mois	Processus métier	Processus métier	Processus métier	Processus métier	Processus métier	Processus métier	Processus métier	Processus métier
Activité 1	Non critique	Non critique	Critique	Critique	Critique	+	+	+	+	+	+	+	Tout le service
Activité 2	Non critique	Non critique	Non critique	Non critique	Non critique	+	+	+	+	+	+	+	Le dernier mois de l'année
Activité 3	Critique	Critique	Critique	Critique	Critique	+	+	+	+	+	+	+	Tout le jour, en fin de journée
Activité 4													
Activité 5													
Activité 6													
Activité 7													
Activité 8													
Activité 9													
Activité 10													



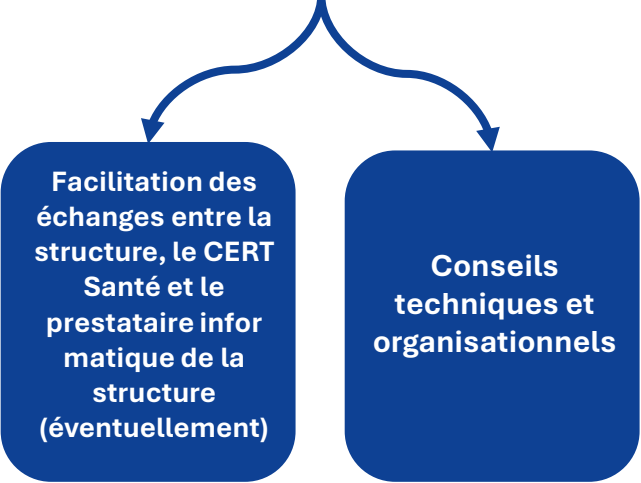


Pour aller plus loin : Que faire en cas d'incident cyber ?

(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.



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

Déclaration sans délai




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

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

Si violation données personnelles suspectée ou avérée



Démarches de notification à la CNIL

Si origine malveillante



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



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.

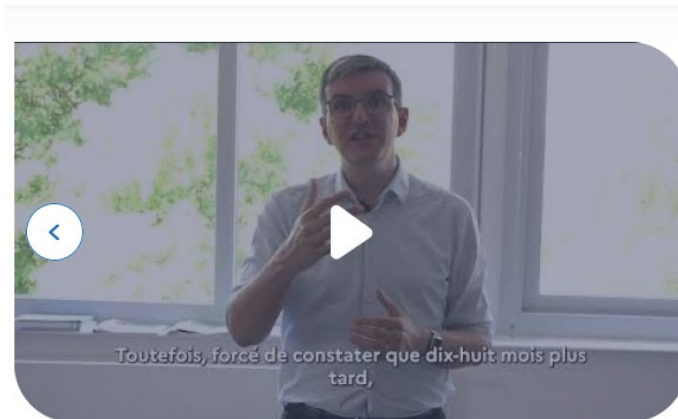
Faux-phishing partagé à l'été 2024

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.



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

