Journée cybersécurité en santé

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

28 novembre 2024 - Aix-en-Provence

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

01

Introduction

Stéphanie Boschetti (ARS PACA)
Christophe Mattler (DNS)

9h - 9h30

Café d'accueil

Plénière

9h30 - 9h45 — **Introduction de la journée**
Stéphanie Boschetti (ARS PACA) et **Christophe Mattler** (DNS)

9h45 - 10h10 — **Actualités CAPSI**
Équipe CAPSI

10h10 - 10h55 — **Table ronde - Actualités de la cybersécurité et de la conformité numérique : les nouvelles réglementations qui vont concerner vos établissements**
Guillaume Desgens Pasanau (Magistrat et professeur en Droit du numérique - CNAM PARIS) / **Laure Duhesme** (Coordinatrice sectorielle santé - ANSSI) / **Océane Phan Tan Luu** (Avocate - Cabinet GAROE) / **Estelle Nicaud** (Responsable de missions - ANS)

11h15 - 11h40 — **Comment organiser la continuité d'activité en ESMS : retours d'expériences**
Nadège Vanneste (Directrice des systèmes d'information et de l'organisation - IRSAM) / **Marie-Aude Mathieu** (Directrice - AIDEREVAR)

11h40 - 11h45 — **Remise du prix « Énigme mystère »**
Équipe CAPSI

11h45 - 12h30 — **Table ronde - Réagir et se relever d'une cyberattaque : conseils et témoignages**
Olivier Ruet-Cros (Expert cybersécurité - CERT Santé) / **Wandrille Krafft** (Directeur du CSIRT - LEXFO) / **Christophe Frank** (Responsable des systèmes d'information - CH Cannes Simone Veil) / **Xavier Stoppini** (RSSI du GHT des Alpes Maritimes)

12h30 — **Conclusion**

Cocktail déjeunatoire

12h30 - 14h

Ateliers ludiques

14h - 16h30

Atelier : Gestion de crise numérique et recommandations de pratiques
Laure Duhesme - Célia Nowak (ANSSI)

Atelier : Réponse technique aux incidents de sécurité numérique
Olivier Ruet-Cros (CERT Santé) **et Wandrille KRAFFT** (Lexfo)

Atelier : Sensibiliser à la cybersécurité de manière ludique
Équipe CAPSI - Nathan Laze (Conscio Technologies)

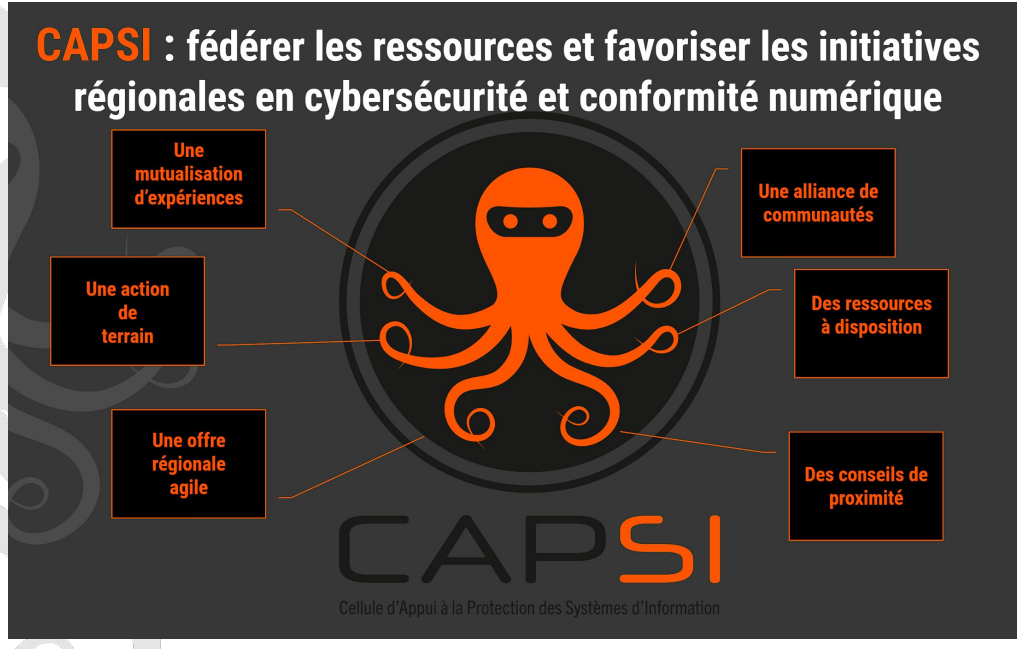
Atelier : Vis ma vie de pirate
CSIRT Urgence Cyber Région Sud

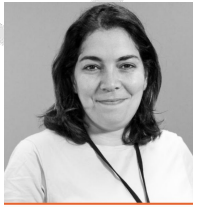
02

Actualités CAPSI

Équipe CAPSI

CAPSI : un élan et une dynamique collective au service de la sécurité numérique des établissements PACA





CAPSI : le Centre Régional de Ressources en Cybersécurité de la région PACA

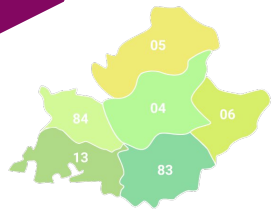
Secteur hospitalier

Médico-social

Exercice libéral

Coordi-nation

Communautés PACA



CAPSI

- Pilotage et gouvernance
- Animation régionale
- Incidents et crises
- Outils et solutions
- Conseils de proximité
- Conformité
- Sensibilisation

CENTRE HOSPITALIER AVIGNON

HÔPITAUX PUBLICS DE VAUCLUSE
Groupement Hospitalier de Territoire

Clean Room de GHT

Plan de reprise d'activité informatique mobile & modulaire

ch-avignon.fr

Les 5 objectifs (1/3)

*Une solution basée sur **cinq axes forts** et qui se veut pragmatique :*

Réactivité:

*Un stockage de la Clean Room **au plus proche** des établissements de santé*
Permettant une livraison et installation en quelques heures

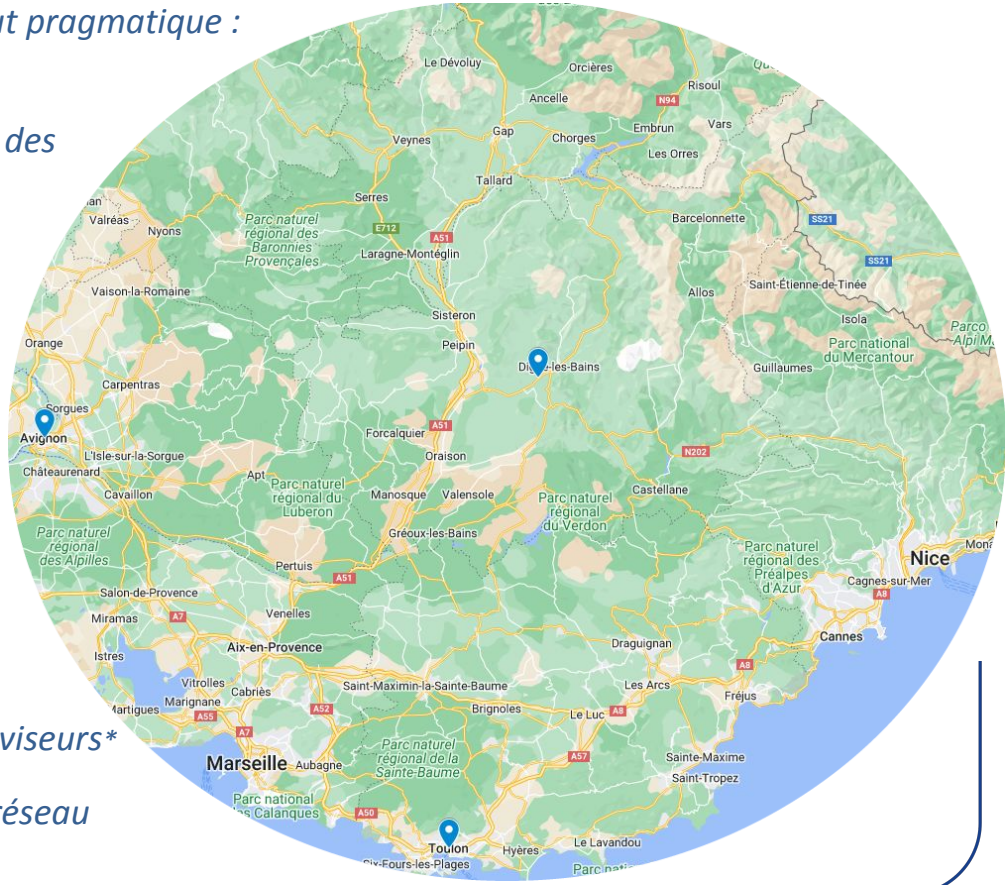
***Optimisation des équipements** en atelier :*
Baie préconfigurée, précâblée, palettisée et sur roulettes (Plug and Play)
Notre objectif :
*Permettre un redémarrage progressif des applications critiques en **24 à 48 heures****

- *Hors sauvegardes sur bandes*

Compatibilité :

*Système compatible avec l'ensemble les hyperviseurs**
**Adaptations mineures nécessaires pour Nutanix*
Elle supporte un large panel de connectiques réseau

- *Cuivre 1Gb/s & 10 Gb/s*
- *Fibre 1Gb/s & 10 Gb/s*



Les 5 objectifs (2/3)

Extensibilité :

*La Clean Room peut être **facilement étendue**, augmentant ainsi ses capacités et ses performances à coûts réduits et **sans interruption** de service*
*A pleine capacité, Elle peut offrir un volume maximal d'**un pétaoctet** en conservant une latence **en dessous de la milliseconde.***

*Un maximum de **dix hôtes de virtualisation** additionnels peut également être connecté à la Clean Room sans configuration supplémentaire (si ce n'est l'ajout de l'hôte lui-même).*

Adaptabilité :

Les technologies retenues sont simples, robustes et accessibles aux équipes informatiques modestes et généralistes.

*En complément de la Clean Room, notre proposition intègre également des périphériques spécialement **adaptés aux métiers.***

NIS 2 READY

Les 5 objectifs (3/3)

Sécurité & Résilience :

*Une **solution complètement isolée** du reste du SIH via des pares-feux, des commutateurs réseaux et un bastion d'administration dédié.*

Les liaisons extérieures sont assurées via 5G (Internet).

Les liaisons internes sont également assurées via 5G, mais encapsulées dans des tunnels sécurisés.

*La Clean Room intègre également sa propre solution de **sauvegardes immuables** (protégées des modifications malveillantes) permettant de mettre à l'abri les données fraîchement restaurées sur une période de 15 jours glissants à raison d'une sauvegarde par jour.*

Composition de la Clean Room :

Deux hyperviseurs prêts à l'emploi & une Baie de stockage

Un Serveur de sauvegarde

Cluster de Firewalls

Trois switchs de distribution

Deux routeurs 5G

Un onduleur

Accueillent le SIH de l'établissement en difficulté et permettent une remise en production dans les meilleurs délais

Contribue à mettre en sécurité les données de la Clean Room via une sauvegarde immuable

Isole la Clean Room du reste du système d'information
Assure et sécurise le trafic interne et externe

Assurent la connexion des stations d'administration, des équipements réseau, et des postes client à réinstaller

Permettent le rétablissement des connexions distantes WAN & SSL vers les postes clients

Prémunit la Clean Room d'éventuels aléas électriques

Contenu de la Clean Room :

VCenter / Vm d'administration

Facilite la gestion des machines virtuelles
Est souvent nécessaire à la restauration des sauvegardes

Bastion Guacamole

Solution de bastion libre robuste et reconnue
Sécurise et enregistre les accès à l'administration de la Clean Room

Solution de clonage de systèmes d'exploitation

Solution libre permettant de pallier l'indisponibilité ou l'absence du logiciel de déploiement de systèmes d'exploitation de l'établissement

Sauvegarde intégrée

Assure la sauvegarde immuable du socle technique de la Clean Room mais également des données de l'établissement.

Périphériques :

*Ordinateurs fixes et imprimantes permettant une **reprise d'activité rapide** au niveau des différents points d'admission patients, dans les salles de soins, l'éventuel laboratoire, mais également en salles de crise*

*Des ordinateurs portables répondant aux **besoins de mobilité** (Chariots de soins, encadrement, direction)*

*Lecteurs bi-fentes destinés à la **lecture des cartes** VITALE (CDRI) et CPX*

*Des points d'accès 5G permettant une **connexion à internet** directe mais également une **connexion à la Clean Room** et ses applications via un tunnel sécurisé*

Prochaines étapes :

Définition des prérequis nécessaires à la mise en œuvre d'une Clean Room:

- *Cartographie applicative (inventaire, criticité, priorité de redémarrage, RPO*, RTO*)*
- *Sanctuarisation:*
  - *Du coffre-fort de mots de passe,*
  - *Des sauvegardes (y compris son catalogue)*
  - *De la base documentaire requise (PRA/Plan blanc numérique, cartographie réseau, contacts, etc.)*

Tests en conditions réelles:

- ~~*Maquetter une Clean Room opérationnelle*~~
- *POC au sein d'un établissement du GHT de Vaucluse*
- *POC dans un autre établissement d'un autre GHT en lien avec un exercice de crise Cyber*

*RTO: Durée maximale d'interruption admissible
*RPO: Perte maximale de données admissible

Préparation de la Clean Room V2

Proactivité : Ajout d'une solution de monitoring Open Source

Flexibilité : Amélioration du service KVM

Extensibilité / compatibilité: Ajout de switch fibre

CENTRE HOSPITALIER AVIGNON

HÔPITAUX PUBLICS DE VAUCLUSE
Groupement Hospitalier de Territoire

Merci de votre attention

ch-avignon.fr

03

Table ronde

Actualités de la cybersécurité et de la conformité numérique : les nouvelles réglementations qui vont concerner vos établissements

Guillaume Desgens Pasanau (Magistrat et professeur en Droit du numérique - CNAM PARIS)
Laure Duhesme (Coordinatrice sectorielle santé - ANSSI)
Océane Phan Tan Luu (Avocate - Cabinet GAROE)
Estelle Nicaud (Responsable de missions - ANS)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

PANORAMA RÉGLEMENTAIRE ET FOCUS SUR NIS 2

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

PANORAMA DES RÉGLEMENTATIONS CYBER À VENIR

Actualités réglementaires relatives à la SSI

Quel texte ?	Qu'est-ce qui est visé ?	Où en est-on ?
NIS 2	**Cybersécurité des entités critiques** 18 secteurs d'activité concernés dont l'administration publique	Directives en cours de transposition
REC	**Résilience des entités les plus critiques** ~ OIV, en s'appuyant sur NIS 2 pour le volet SSI	
CRA	**Sécurité des logiciels et des produits** comportant des éléments numériques	Règlement en attente de publication
LPM 2024-2030	**Alerte des victimes d'incidents ou vulnérabilités,** neutralisation de menaces, connaissance des MOA	En vigueur depuis le 1er juin 2024 (31 décembre pour certaines dispositions)

NIS : network and information systems security REC : résilience des entités critiques CRA : cyber resilience act LPM : loi de programmation militaire OIV : Opérateur d'Importance Vitale

FOCUS SUR NIS 2

NIS 2 : de la cybersécurité des opérateurs critiques vers la cybersécurité de masse

- Fin 2020, décision de la Commission européenne **d'étendre le périmètre** et les ambitions de la directive :
  → Des milliers d'entités se retrouveront concernées par la directive NIS 2 à l'échelle nationale

- Nécessité de préciser le **périmètre**, les **exigences de sécurité** et les mécanismes de **régulation :**
  → NIS 2 est plus **prescriptive** que NIS 1

- **Nécessité** d'une évolution soutenue par la France :
  → **Prise de conscience** massive
  → Intégration des premiers éléments de base de la cybersécurité
  → Proportionnalité des exigences face aux enjeux des entités et des secteurs concernés, à leur capacité

Evolutions et obligations de NIS 2

- Principales évolutions avec NIS 2 :
  - **Extension du périmètre des entités et des SI régulés** (> 10 000 entités concernées vs 300 sous NIS 1)
  - **Mécanisme de proportionnalité** distinguant deux catégories d'entités (essentielles ou importantes)
    en fonction de la criticité de leur activité et de leur taille
  - **Capacités renforcées de supervision, de contrôle et de sanction** (comparable au RGPD)
- Obligations :
  - **Se notifier à l'ANSSI et communiquer des informations à jour** (point de contact, etc.)
  - **Déclarer à l'ANSSI les incidents majeurs**
  - **Mettre en place des mesures de gestion des risques cyber** (référentiel de règles en construction)

LES ENTITÉS ESSENTIELLES ET IMPORTANTES

NIS 2 intègre deux typologies d'entités différentes :

- Les entités essentielles (**EE**)
- Les entités importantes (**EI**)

NIS 2 intègre la proportionnalité entre **EE** et **EI** dans :

- Les mesures de sécurité
  - Possibilité d'avoir des niveaux d'exigences différents entre les **EE** et les **EI**, notamment pour prendre en considération les moyens et enjeux d'une grande entreprise versus d'une PME.
- La régulation
  - Pour les **EE** : régulation dite « ex-ante » (contrôle à discrétion de l'autorité nationale compétente)
  - Pour les **EI** : régulation dite « ex-post » (contrôle en cas de connaissance d'une non-conformité)
- Les sanctions
  - Seront d'une ampleur comparable à celles du RGPD
  - De manière simplifiée, sanctions pouvant aller jusqu'à 2% du CA mondial pour les **EE** et 1,4% pour les **EI**

Critères d'inclusion dans le périmètre soumis à NIS 2

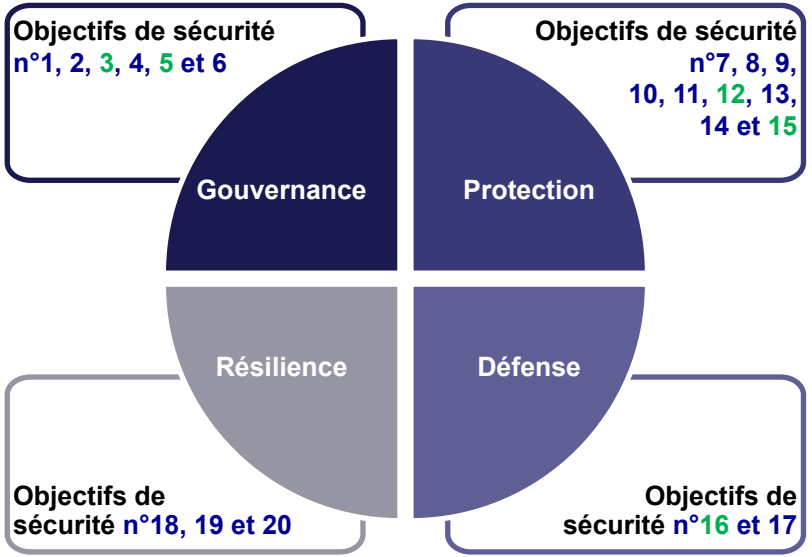
Représentation <u>simplifiée</u> selon la taille de l'entité et la criticité du secteur d'activité

Taille de l'entité	Nombre d'employés	Chiffre d'affaires (en M€)	Bilan annuel (en M€)	Secteurs hautement critiques (annexe I de la directive)	Autres secteurs critiques (annexe II de la directive)
Intermédiaire et grande	x ≥ 250	y ≥ 50	z ≥ 43	**ENTITES ESSENTIELLES**	**ENTITES IMPORTANTES**
Moyenne	250 > x ≥ 50	50 > y ≥ 10	43 > z ≥ 10	**ENTITES IMPORTANTES**	**ENTITES IMPORTANTES**
Micro et petite	x < 50	y < 10	z < 10	**NON CONCERNÉES**	**NON CONCERNÉES**

NB : certaines entités ne répondant pas à ces critères mais jugées critiques pourront faire l'objet d'une désignation unitaire

Structuration du référentiel de règles NIS 2

- La cible fixée vise à maîtriser et à réduire les risques en lien avec la cybercriminalité, tout en prenant en compte le mécanisme de proportionnalité
- Les objectifs de sécurité, définis pour répondre à la cible, s'inscrivent dans le modèle :
  - **Gouvernance**
  - **Protection**
  - **Défense**
  - **Résilience**
- Ces objectifs répondent aux obligations des articles 20 et 21 de la directive



Les objectifs en **vert** sont applicables exclusivement aux **entités essentielles**

La transposition en droit national

Objectif :

a. **Transcription des obligations et options européennes** en exigences nationales en droit français au travers de textes législatif et réglementaires.

b. Articulation et simplification du cadre réglementaire :
   - REC / LPM 2013 / DORA

Quelques informations :

c. **Processus législatif en cours** : l**e projet de loi a été présenté en Conseil des Ministres** le 15 octobre 2024

d. En parallèle du processus législatif et du processus réglementaire **existe un processus de consultation qui les alimente**, démarré en 2023 et qui se poursuit.

IA Act : règlement européen sur l'Intelligence Artificielle et son utilisation

Principales caractéristiques et portée du règlement européen sur l'IA (AI Act)

- Entrée en vigueur le 1er Août 2024, pleinement applicable dans 24 mois. Attention les interdictions seront applicable dans 6 mois (au 31 décembre 2024)
- Interdépendance avec :
  - Le Règlement Général sur la Protection des Données (RGPD), qui garantit la sécurité et la confidentialité des données sensibles
  - Les Règlements 2017/745 et 2017/746), qui établissent des exigences pour l'efficacité et la sécurité des dispositifs médicaux.
- Définition de l'IA : « un « système d'intelligence artificielle » est un logiciel développé à l'aide d'une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que du contenu, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels ils interagissent ».
- L'annexe I énumère (a) les approches d'apprentissage automatique, (b) les approches logiques et fondées sur la connaissance et (c) les approches statistiques. Cela signifie que le règlement s'applique aussi bien aux techniques qui apprennent automatiquement à partir de données sans programmation explicite (apprentissage automatique) qu'à celles qui impliquent une programmation humaine (approches logiques, fondées sur la connaissance et statistiques).
- Ne s'applique pas à certains domaines « *Il est donc nécessaire d'exclure de son champ d'application les systèmes et modèles d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques. En outre, il est nécessaire de veiller à ce que le présent règlement n'affecte pas autrement les activités de recherche et de développement scientifiques sur les systèmes ou modèles d'IA avant leur mise sur le marché ou leur mise en service* » **Préambule 25 et article 2**

Cas concrets

Catégorie	Description	Exemples	Implications opérationnelles
Pas un dispositif médical ou dispositif à faible risque	Systèmes qui : - Ne relèvent pas de la définition des dispositifs médicaux de l'UE. - Sont classés comme dispositifs médicaux de classe I, sans usage direct pour le diagnostic, les décisions thérapeutiques, la surveillance physiologique ou contraceptive. - Non soumis à une évaluation tierce de conformité.	▪ **Applications de fitness ou nutrition** fournissant des conseils personnalisés pour un mode de vie sain (non considérées comme dispositifs médicaux, ligne 19 du préambule MDR). ▪ **IA pour les rendez-vous médicaux** identifiant les patients susceptibles de manquer un CT scan. ▪ **Système d'information hospitalier** optimisant la facturation.	❑ Surveillance minimale : aucun audit externe requis. ❑ Encouragement à l'adoption de codes de conduite pour garantir transparence et sécurité. ❑ Pertinent pour les hôpitaux cherchant à automatiser les tâches administratives ou à réduire les coûts de gestion.
Dispositifs/logiciels médicaux à haut risque	Systèmes utilisés directement pour : - Le diagnostic des patients. - Les décisions thérapeutiques. - La surveillance de processus physiologiques. - Les finalités contraceptives. Classés comme dispositifs de classe IIa ou plus (Règle 11 du MDR).	• **Application évaluant des lésions cutanées pour fournir des estimations de risque** et des conseils médicaux (diagnostic, classe IIa). • **IA surveillant les effets secondaires des traitements** et recommandant des ajustements (monitoring thérapeutique, classe IIa).	❑ **Nécessité d'une évaluation tierce de conformité avant mise sur le marché**. (CNIL) ❑ Documentation technique et systèmes de gestion des risques obligatoires. ❑ Exigences robustes sur la transparence et la supervision humaine pour garantir la sécurité.
Dispositifs/logiciels médicaux à risque inacceptable	Systèmes interdits car : - Exploitent les vulnérabilités de certains groupes (âge, handicap). - Utilisent des techniques subliminales pour influencer le comportement. - Provoquent un préjudice physique ou psychologique. - Incluent des risques éthiques majeurs.	• **Scoring social basé sur l'IA par des autorités publiques** (implications sociales au-delà du domaine de la santé). • **Systèmes biométriques en temps réel dans les espaces publics** (interdits pour la surveillance, mais autorisés pour le contrôle d'accès dans les hôpitaux).	❑ Risques éthiques majeurs à éviter absolument. ❑ Formation et sensibilisation des équipes hospitalières sur l'utilisation acceptable des données et de l'IA. ❑ Besoin d'alignement avec le RGPD et les législations sur les droits fondamentaux pour prévenir les abus.

Impact opérationnel 1/2

Obligations immédiates (d'ici décembre 2024) :

Les RSSI doivent se préparer à respecter les interdictions qui seront applicables dès la fin de l'année 2024, avec des actions concrètes pour garantir la conformité.

Actions pratiques :

- **Identifier les systèmes interdits dans votre environnement :**
  Passez en revue les systèmes d'IA utilisés dans l'établissement (logiciels de triage, biométrie, systèmes de décision).
  👉 Les systèmes d'identification biométrique en temps réel pour surveiller des espaces publics à des fins non médicales peuvent être interdits. A faire *: Créez un registre des systèmes d'IA actuellement en usage.*

- **Cartographier les données sensibles utilisées par les systèmes d'IA :**
  Identifier où et comment les données de santé sensibles sont traitées pour détecter d'éventuelles incompatibilités avec les exigences du RGPD et l'impact des deux Règlements sur les dispositifs médicaux.

- **Former les équipes à la nouvelle réglementation :**
  Mettez en place des sessions de sensibilisation sur les principes clés de l'IA Act (risques, transparence, explicabilité).
  👉 Collaborer avec les DPO (Data Protection Officers) pour intégrer les exigences RGPD dans la formation des équipes et travailler sur la conformité réglementaires avec les différentes législations

Impact opérationnel 2/2

Obligations à moyen terme (d'ici août 2026)

Les obligations de conformité complète imposent une transformation des pratiques et des processus internes, notamment pour les systèmes d'IA à haut risque.

Actions pratiques :

- **Évaluer et documenter les systèmes d'IA à haut risque :**
  Vérifiez si vos outils répondent à la définition de dispositifs médicaux (diagnostic, surveillance thérapeutique).
  👉 Prendre en compte les sujets de recherches et les outils qui ne sont pas encore sur le marché pour anticiper les mises en œuvre. Anticipez les audits pour les systèmes classés à haut risque. Préparez des rapports montrant les processus de validation, de tests et de robustesse des algorithmes.
- **Mettre en place une supervision humaine :**
  Développez des protocoles permettant aux utilisateurs humains de comprendre et d'intervenir sur les décisions des systèmes d'IA.
  👉 Prévoir des revues manuelles des diagnostics produits par l'IA dans les processus cliniques.
- **Adapter les chartes informatiques et les politiques internes :**
  Ajoutez des clauses spécifiques dans les chartes informatiques sur l'utilisation responsable de l'IA.
  👉 Incluez des engagements sur l'équité des algorithmes et l'explicabilité des décisions automatisées, ajouter des clauses spécifiques à l'IA. Formation des étudiants, des praticiens et de l'ensemble des parties prenantes.

👉 Mettez en place des politiques de gestion des incidents spécifiquement dédiées aux systèmes d'IA (erreurs algorithmiques, biais identifiés).

👉 Profitez des initiatives européennes permettant de tester les systèmes d'IA en environnement contrôlé avant leur déploiement.

Merci

04

Comment organiser la continuité d'activité en ESMS : retours d'expériences

Nadège Vanneste (Directrice des systèmes d'information et de l'organisation - IRSAM)

Marie-Aude Mathieu (Directrice - AIDEREVAR)

Plan de Continuité et de Reprise d’Activité en ESMS

Plan de Continuité et de Reprise d'Activité en ESMS

Marie Aude MATHIEU (AIDERAVAR)
Nadège VANNESTE (Association IRSAM)

Aidera.Var
Accompagner l'Autisme

IRSAM

PCRA - Contexte

- Guide méthodologique élaboré par CAPSI à tester
- Expérimentation du kit PCRA proposé par l'Agence du numérique en santé dans le cadre du programme CARE

L'association IRSAM et AIDERAVAR sont accompagnées par CASSIs Conseil

Aidera.Var
Accompagner l'Autisme

- Projet stratégique AIDERA Var 2021/2026 : place du numérique (mise en place du DUI, changement de logiciel paie compta, …)
- Développement de l'association (multi site et dispositifs) – besoin de structurer

IRSAM

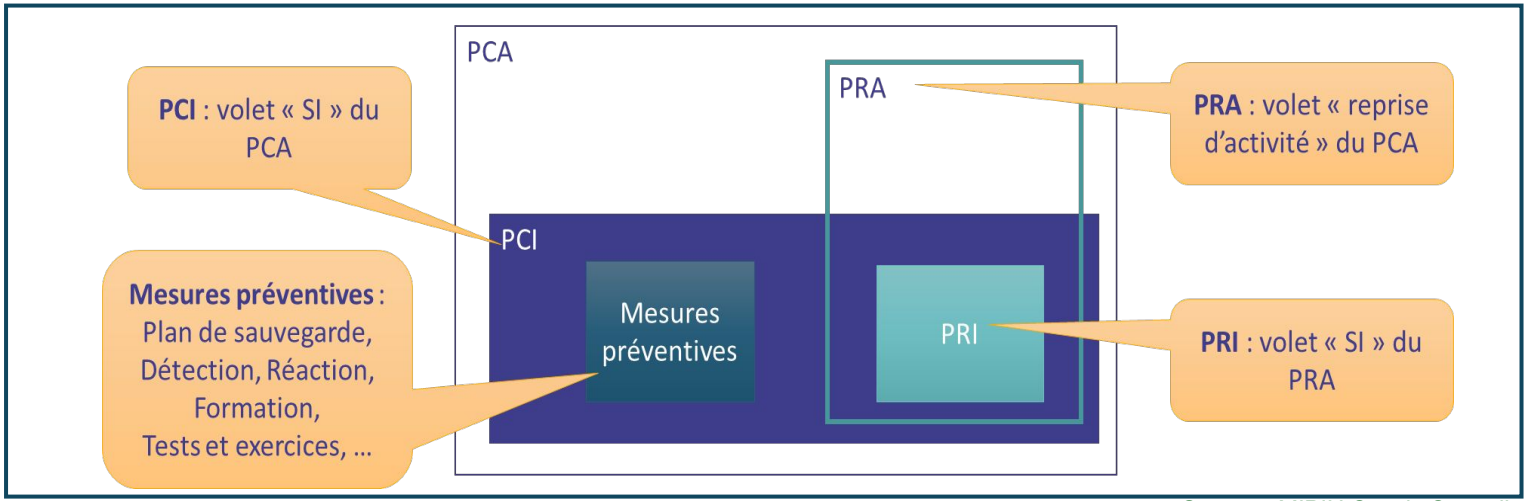
Action inscrite dans le projet associatif 2024-2028

Préconisation suite à l'exercice de crise cyber réalisé en octobre 2023

PCRA - Définitions

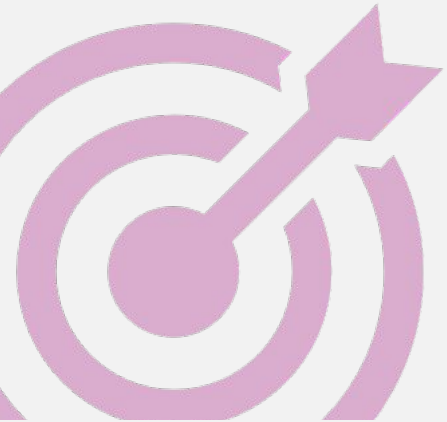
Plan de continuité d'activité

Ensemble des mesures **techniques** et **organisationnelles** visant à assurer le maintien des activités de l'organisme face à des menaces. Avec une capacité de réponse efficace garantissant la sécurité ainsi que la confiance des usagers, les valeurs et la qualité de l'accompagnement de l'organisme.



Source : MIPIH Cassis Conseil

Les 6 objectifs du PCRA



1

Prioriser

Assurer la continuité d'accompagnement des usagers et des processus métier critiques en cas d'un événement perturbateur

2

Anticiper

Éviter une situation risquée en identifiant les besoins de continuité d'activité

3

Rechercher

Disposer de solutions de continuité et de reprise d'activité qui prennent en compte les singularités de l'OG

4

Procéder

Comprendre la mise en œuvre des solutions de continuité et de reprise d'activité à travers les procédures opérationnelles

5

Éprouver

S'assurer de la faisabilité et de l'opérationnalité par des tests ou des exercices

6

Formaliser

Formaliser le pilotage stratégique du PCRA par la rédaction du PCRA cadre

Source: ANS

PLAN Bleu – Plan Blanc – PCRA

	Champ d'application	Objectif principal	Type de crise	Exemple d'actions
Plan Blanc	Etablissements sanitaires	Gestion de crise sanitaire ou afflux massif de patients	Catastrophe, crise sanitaire	Rappel de personnel, augmentation des capacités de traitement
Plan Bleu	Etablissements sociaux et médico sociaux	Protection des personnes vulnérables (personnes âgées, handicapées…)	Canicule, pandémie, catastrophe naturelle	Réorganisation des soins, protection des résidents
PCRA	Tout type d'organisme	Maintenir la continuité des activités essentielles	Catastrophe, cyberattaque	Priorisation des ressources, mode dégradé, reprise d'activité

Plan bleu: maintien des accompagnements dans des conditions particulières

PCRA: sécurisation des activités essentielles (« continuité d'activité ») – définition de modes dégradés et des actions de reprise d'activité

Ces 2 plans visent à repousser le seuil de rupture capacitaire, maintenir la production et la réalisation des services d'activités essentiels à l'accompagnement des usagers

PROJET PCRA - Méthodologie

Présentation projet à la direction
Définition du COPIL

↓

Cadrage de l'activité

Périmètre / Objectif / Planning / Livrable

↓

Attente de continuité
(identification des processus essentiels)

Cartographie des processus existant et métier
Identification et priorisation des processus essentiels
Identification des interlocuteurs des processus essentiels

↓

Constitution d'un plan de continuité d'activité direction

Rappel de processus essentiels
Liste des parties prenantes / moyen de communication
Plan de communication (interne/externe)
RACI (Rôles et responsabilité) / actions réglementaires

↓

Constitution d'un plan de continuité d'activité opérationnel
(par processus essentiel)

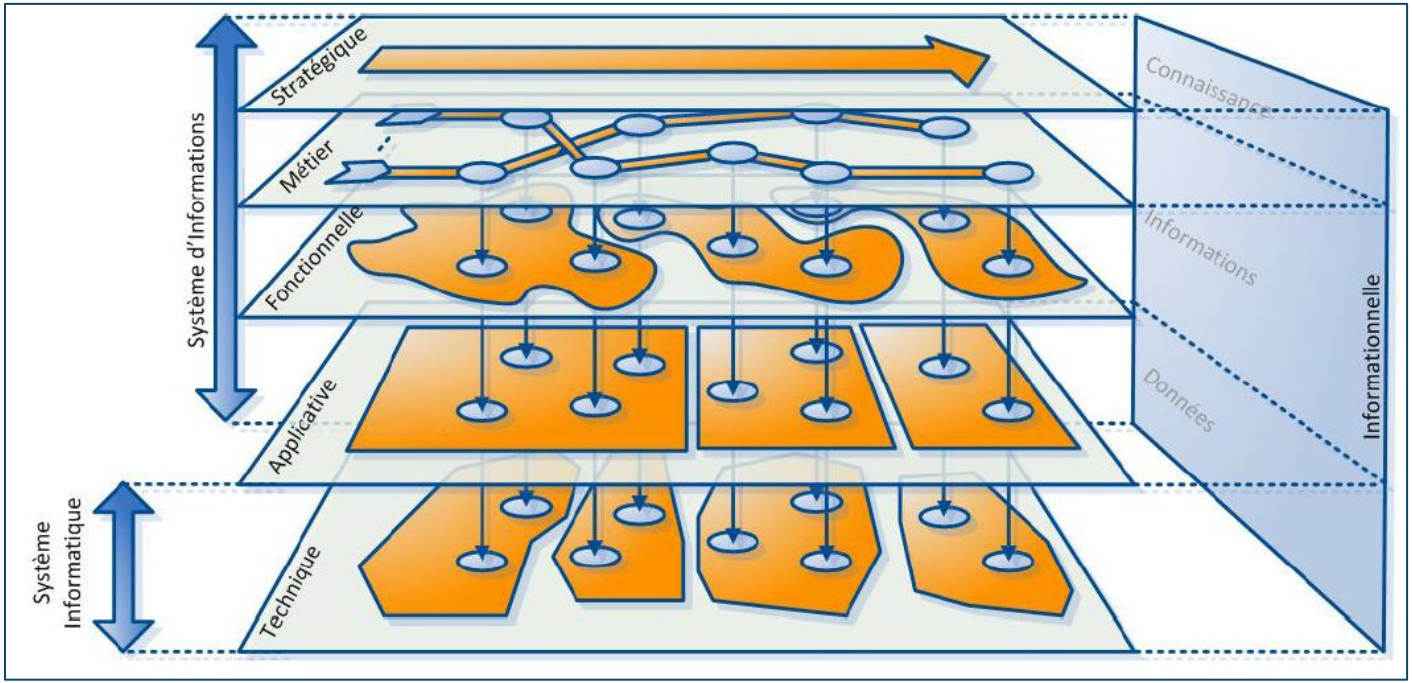
Lien entre Processus-Activités-Applications
Définition du fonctionnement en mode dégradé
Rédaction d'une fiche de synthèse

→

Identification des vulnérabilités du SI par analyse de risque (EBIOS RM simplifié)

Définition des valeurs métiers et des biens supports
Définition des évènements redoutés, des impacts et de la gravité
Définition et évaluation du couple SR/OV (sources de risque et Objectifs visés)
Identification des parties prenantes et de leurs niveaux de menaces
Elaboration des scénarios stratégiques
Détermination des scénarios stratégiques
Analyses et traitement des risques

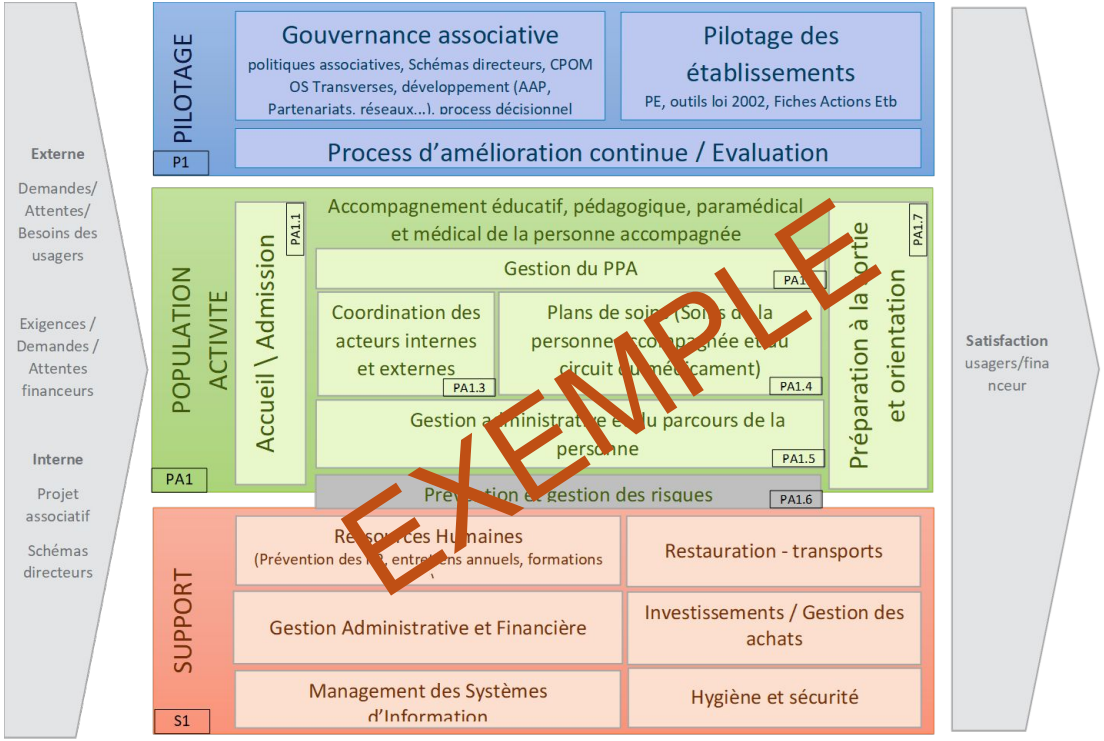
Process métiers



Source : ANAP

Service – Processus

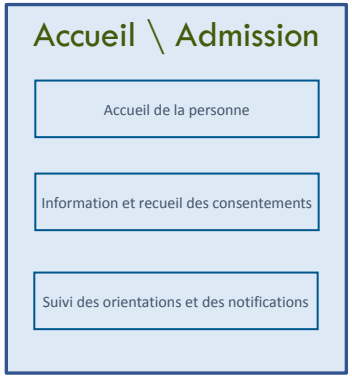
Travail sur les attentes et mesures de continuité par **processus métiers**



Critères d'évaluation

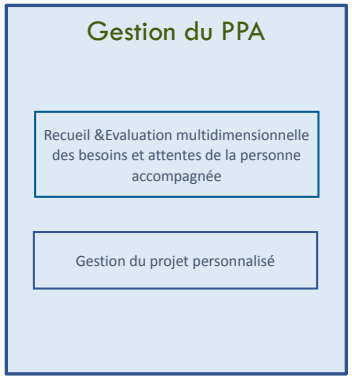
Valeur	Personne accompagnée	Social & organisation	Financier	Responsabilité / juridique	Réputation / image	DMIA
1 – Mineure	Gêne / inconfort pour un usager **Pas d'impact**	- Gêne ponctuelle dans la prise en charge d'usagers, ou l'activité - Démotivation des acteurs / perte de temps	Perte financière sans impact significatif pour le responsable du traitement	Absence de plainte ou plaintes sans suite	Evènement peu ou pas médiatisé, sans effet ou effet négligeable sur l'image de l'organisme.	1 mois
2 – Significative	Défaut d'accompagnement : Absence/report de soins et/ou soins inadéquats pour un usager entraînant une atteinte physique et/ou psychologique **Impact réversible sur les personnes ou les biens, sans intervention nécessaire**	- Surcharge de travail et/ou désorganisation modérée mais temporaires dans la prise en charge des usagers Conflit social - Interruption ou ralentissement temporaire de certaines activités	Perte financière avec des impacts modérés pour le responsable du traitement	Contentieux	Dégradation passagère d'image ou de confiance dans l'acteur de santé ou le service offert	2 semaines
3 – Majeur	Défaut d'accompagnement : Absence/report de soins et/ou soins inadéquats pour un usager entraînant pouvant engendrer une mise en danger de l'usager ou de son entourage. **Impact réversible ayant nécessité des mesures adaptées ou niveau 4 potentiel**	- Désorganisation importante et durable de l'activité entraînant une perte significative d'activité et/ou une replanification des soins ou un recours à des organismes tiers. - Conflit social paralysant la structure	Perte financière avec des impacts importants pour le responsable du traitement	- Atteinte à la vie privée d'un usager - Condamnation pénale et/ou financière.	- Perte d'image ou de confiance dans l'acteur de santé ou le service offert - Mise en cause de la stratégie de l'organisme détenteur du système ou d'un organisme tiers	3 jours
4 – Catastrophique	Mise en danger d'une population / Menace du pronostic vital - Atteinte irréversible ou décès d'un ou plusieurs usager(s). **Impact irréversible ou impact vital pour les personnes, les biens ou pour les sytèmes**	- Arrêt prolongé d'une part importante ou de toute l'activité. - Arrêt du projet Fermeture de la structure	Perte financière mettant en cause la pérennité du responsable du traitement	- Condamnation pénale et/ou financière - Atteinte à la vie privée d'une population Risques judiciaires	- Rejet définitif de l'acteur de santé ou du service offert - Mise en cause de l'existence de l'organisme détenteur du système ou d'un organisme tiers	3 heures

EVALUATION DES PROCESSUS



Sous processus	Personne Accompagnée	Social & organisation	Financier	Responsabilité / juridique	Réputation / image	DMIA	Total
Accueil de la personne	2	1	1	2	2	2	**10**
Information et recueil des consentements	**2**	**1**	**2**	**3**	2	2	**12**
Suivi des orientations et des notifications	**1**	**1**	**1**	**2**	1	1	**7**

EXEMPLE

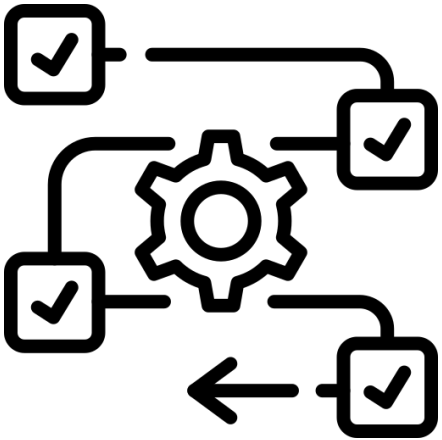


Sous processus	Personne Accompagnée	Social & organisation	Financier	Responsabilité / juridique	Réputation / image	DMIA	Total
Recueil &Evaluation multidimensionnelle des besoins et attentes de la personne accompagnée	2	2	1	2	2	1	**10**
Gestion du projet personnalisé	2	2	1	2	2	1	**10**

Processus évalués

Fonction	Processus	Sous processus	Patient	Social & organisation	Financier	Responsabilité / juridique	Réputation / image	DMIA	Total
S1	Hébergement - Restauration - transports	Gestion des biens immobiliers	3	3	3	3	2	4	18
PA1	Coordination des acteurs internes et externes	Gestion des « urgences »	3	3	1	3	2	4	16
PA1	Coordination des acteurs internes et externes	Gestion des acteurs internes / externes	3	3	1	2	2	4	15
PA1	Plans de soins	Délivrance / Préparation / Administration médicamenteuse	3	3	1	3	1	4	15
PA1	Plans de soins	Administration des soins	3	2	1	3	1	4	14
S1	Hébergement - Restauration - transports	Gestion hôtelière	3	2	2	1	2	4	14
S1	Hébergement - Restauration - transports	Distribution de la restauration	3	2	2	1	2	4	14
S1	Hébergement - Restauration - transports	Gestion des transports	3	2	1	2	2	4	14
PA1	Coordination des acteurs internes et externes	Coordination et planification des activités	3	3	1	1	2	3	13
S1	Gestion Administrative et Financière	Suivi des marchés et des achats	2	2	2	2	2	3	13
S1	Hébergement - Restauration - transports	Gestion de la lingerie	3	2	1	2	2	3	13
PA1	Accueil \ Admission	Information et recueil des consentements	2	1	2	3	2	2	12
PA1	Plans de soins	Gestion des prescriptions	3	2	1	2	1	3	12
PA1	Gestion administrative et du parcours de la personne	Gestion des présences absences des personnes accompagnées	3	3	1	1	1	3	12
S1	Ressources Humaines	Gestion des temps et activités	2	3	1	2	2	2	12
S1	Gestion Administrative et Financière	Comptabilité	1	2	3	2	2	2	12
S1	Gestion Administrative et Financière	Gestion des budgets	1	2	3	2	2	2	12
S1	Ressources Humaines	Gestion de la paie	0	3	1	2	3	2	11
S1	Gestion Administrative et Financière	Gestion facturation et recouvrement	2	2	2	2	2	1	11
PA1	Accueil \ Admission	Accueil de la personne	2	1	1	2	2	2	10
PA1	Gestion du PPA	Recueil &Evaluation multidimensionnelle des besoins et attentes de la personne accompagnée	2	2	1	2	2	1	10
PA1	Gestion du PPA	Gestion du projet personnalisé	2	2	1	2	2	1	10

Les processus essentiels



IRSAM

Exploitation des biens immobiliers

Traitement des situation de santé urgente

Dispensation, préparation, administration médicamenteuse

Gestion des acteurs internes et externes

Administration des soins

Aidera.Var
Accompagner l'Autisme

Gestion des biens immobiliers

Gestion des Urgences sanitaires//Astreinte

Délivrance/préparation/ médicamenteuse

Gestion des acteurs internes/externe (planning salariés, intérimaires,…)

Gestion des transports, restauration, hôtellerie

Description des processus essentiels

		Description	Référent	Qui l'applique	Pour qui	Parties prenantes	Interlocuteurs
Exploitation des biens immobiliers (gestion hôtelière)	17	Gestion de l'hébergement – utilisation des locaux	Directeurs ESMS	Chefs de service - coordinateurs	Intervenants et personnes accompagnées		
Gestion des « urgences » Astreinte - gestion trouble comportement – appel au sanitaire (urgence)	16	Appel de l'astreinte pour valider l'application d'un protocole ou un départ aux urgences médical avec appel du SAMU en amont.	Cadre d'astreinte (Dir ESMS, Dir pôle et CDS)	Tout intervenant	Personnes accompagnées	Médecin, cadre de santé	
Délivrance / Préparation / Administration médicamenteuse	15	Délivrance des médicaments par les pharmacies Préparation par la pharmacie ou les IDE Administration médicamenteuse par les IDE Aide à la prise des médicaments par le personnel soignant ou éducatif	Médecin ou cadre de santé	IDE/IDE liberal/Aide Soignant	Intervenants et personnes accompagnées	Pharmarcie DUI VIVALITY Ogyris	
Gestion des acteurs internes / externes	15	Gestion du planning des salariés et des remplacements pour assurer l'accompagnement	Cadre d'astreinte – chef de service	chef de service coordonateur	Intervenants et personnes accompagnées	Octime Partenaire travail interimaire Partenaires libéraux DUI Vivality Ogirys	
Entretien Maintenance des biens immobiliers	15	Entretien et maintenance des bâtiments qui accueillent les résidents.	Directeur ESMS – Direction du patrimoine	Directeur ESMS – cadre logistique	Intervenants	Prestataires – fournisseurs de service (eau, energie,…)	

Identification des vulnérabilités du SI par analyse de risque (EBIOS RM Simplifiée)

IRSAM

Hiérachisation des processus de la structure en fonction des besoins de cybersécurité exprimés

Num	Processus	Disponibilité	Intégrité	Confidentialité	Tracabilité	Score	Besoin de sécurité numérique
1.4	Plans de soins et circuit du médicament	5	4	4	4	17	ESSENTIEL
2.2	Gestion des SI	4	4	4	4	16	ESSENTIEL
1.8	Gestion des situations de santé urgentes	5	3	3	4	15	ESSENTIEL
2.1	Ressources humaines	3	3	3	4	13	IMPORTANT
2.4	Gestion des achats	2	3	4	4	13	IMPORTANT
2.5	Gestion financière	3	3	3	4	13	IMPORTANT
1.2	Gestion du PPA (projet personnel d'accompagnement)	1	3	4	4	12	IMPORTANT
2.3	Hébergement, Restauration et transport	5	3	1	3	12	IMPORTANT
1.6	Prévention et gestion des risques	1	3	3	4	11	MODERE
1.3	Coordination des acteurs internes et externes	3	2	4	2	11	MODERE
1.5	Gestion administrative et du parcours de la personne	2	3	2	4	11	MODERE
1.1	Accueil et Admissions	2	2	2	2	8	STANDARD
3.2	Pilotage des établissements	2	2	2	2	8	STANDARD
3.3	Amélioration continue et évaluation	2	2	2	2	8	STANDARD
1.7	Préparation à la sortie de la personne ou ré-orientation	1	2	2	2	7	STANDARD
3.1	Gouvernance associative	1	2	2	2	7	STANDARD

Activités, Impacts , DMIA (RTO) et priorisation

Selon outil BIA de l'Agence du Numérique en Santé

Activités du service d'activités

Objectif :	Faire l'inventaire des activités principales qui font le quotidien du processus métier. Puis, au regard du seuil de criticité défini pour chaque typologie d'impact, évaluer si l'arrêt de cette activité est critique selon les temporalités. Cela est le point de départ qui permet de définir le périmètre à traiter dans le PCA.

Bilan de l'Impact sur L'activité (BIA)

Activités	4 h	24 heures	3 jours	2 semaines	1 mois	Personnel	Usager	Opérationnel	Juridique	Médiatique	Financier	DMIA	Période critique ?	Activité prioritaire
Réparation externe urgente (d'eau, électricité, chauffage, réseaux informatique)	Non critique	Critique	Critique	Critique	Critique	X	X	X			X	8h		VRAI
Entretient externe courant (réseaux informatique, internet, énergie)	Non critique	Non critique	Non critique	Non critique	Critique			X	X			1 mois		FAUX
Entretient interne locaux (maintenance du quotidien)	Non critique	Non critique	Non critique	Critique	Critique	X	X	X				2 semaines		FAUX
Visite de sécurtié (incendie-annuelle, ERP-triennale)	Non critique	Non critique	Non critique	Non critique	Critique			X	X			1 mois		FAUX
Controle des accès	Non critique	Critique	Critique	Critique	Critique	X	X	X	X			8h	Week-end	VRAI
Affectation des locaux	Non critique	Non critique	Non critique	Critique	Critique	X	X	X				5 jours		VRAI
Etat des lieux entrant/sortant	Non critique	Non critique	Non critique	Non critique	Non critique		X							FAUX
Plannification annuelle des travaux rénovation	Non critique	Non critique	Non critique	Non critique	Non critique	X	X	X		X	X	3 mois		FAUX
Gestion des risques	Non critique	Non critique	Non critique	Non critique	Critique	Oui	X	Oui		X		1 mois		Non

EXEMPLE

Ressources nécessaires

Selon outil BIA de l'Agence du Numérique en Santé

Ressources nécessaires	
Objectif :	Identifier les ressources matérielles nécessaires pour assurer les activités critiques dans une situation dégradée. Il s'agit absolument des besoins minimums. L'objectif est de pouvoir anticiper certains besoins, par exemple en achetant ou réservant du matériel pour des situations de crise.

Activités	Objectif de redémarrage	Besoins en matériel				
		Ordinateurs	Imprimantes	Téléphonie	Administratif	Autres
Réparation externe urgente (d'eau, électricité, chauffage, réseaux	8h			Pour appel fournisseur	Contrat fournisseur	Coordonnées fournisseurs
Entretient externe courant (réseaux informatique, internet, énergie)	1 mois				Contrat fournisseur	Registre de sécurité
Entretient interne locaux (maintenance du quotidien)	2 semaines	utilisation de messagerie interne (Slack)		utilisation de messagerie interne (Slack)		Outillage
Visite de sécurtié (incendie-annuelle, ERP-triennale)	1 mois	Accès aux documents	Edition de document		Salle de réunion	Registre de sécurité
Controle des accès	8h	Utiliation du logiciel				
Affectation des locaux	5 jours	Document partagé		Pour faire les demandes		
Etat des lieux entrant/sortant	0	Modèle de fiche	Impression du modèle et scan du CR			Fiche papier
Plannification annuelle des travaux rénovation	3 mois	Excel		Pour appel fournisseur	Contrat fournisseur	Coordonnées fournisseurs
Gestion des risques	1 mois	Ageval				

EXEMPLE

Application informatique

Selon outil BIA de l'Agence du Numérique en Santé

Applications informatiques										
Objectif :	Lister les applications informatiques utilisées dans le service d'activités et les associer aux activités. Ce travail d'inventaire permettra de plus facilement renseigner l'onglet lié à l'indisponibilité des systèmes d'informations.									
Nom de l'application informatique	**DMIA de l'application informatique**	**Réparation externe urgente (d'eau, électricité, chauffage, réseaux**	**Entretient externe courant (réseaux informatique, internet,**	**Entretient interne locaux (maintenance du quotidien)**	**Visite de sécurité (incendie annuelle, ERP périodique)**	**Controle des accès**	**Affectation des locaux**	**Etat des lieux entrant/sortant**	**Plannification annuelle des travaux**	**Gestion des risques**
Slack	**2 semaines**	X								
Excel	**1 an**		Pour la gestion des contrat							
Slack	**2 semaines**			X						
Word-Excel	**2 semaines**				X					
A vérifier	**2 jours**					X				
Excel	**5 jours**						X			
Excel	**3 mois**								X	
EGVAL	**1 mois**									X

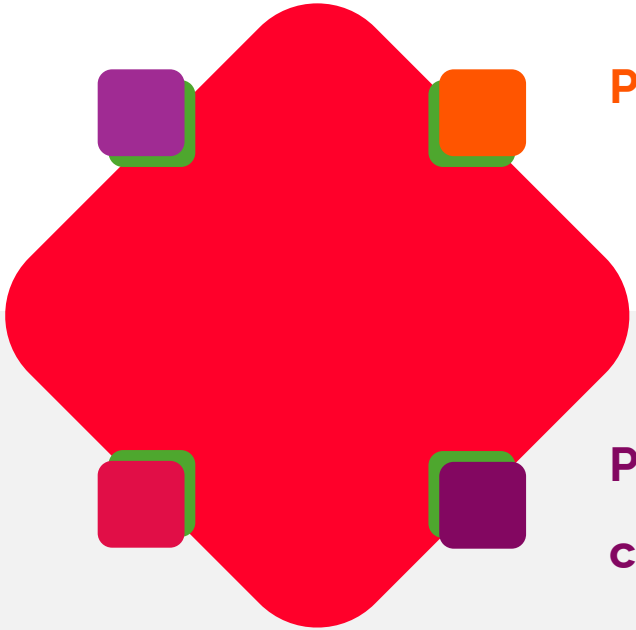
EXEMPLE

Outil BIA – Mesures de continuité d'activité

4 types de scénarios

Perte des bâtiments

Perte des SI



Perte des fournisseurs

Perte des compétences

Solutions de continuité à **4h, 24h, 3 jours, 2 semaines et un mois**

Mesures de continuité d'activité

Application	Activité	Solution de continuité				
		à 3 heures	à 24 heures	à 3 jours	à 2 semaines	à 1 mois
DUI Vivality Plan de soin Ou DUI OGIRYS Plan de soin	Commande médicaments Préparation des piluliers (si nécessaire) Préparation du chariot de soins Distribution aux personnes Enregistrement/traçage de la prise de médicaments dans le plan de soins Intervention, si nécessaire, de l'IDE - tracer la non prise de médicaments dans le plan de soins Commande exceptionnelle de médicament	Transmission de l'ordonnance papier à la pharmacie par transport par un personnel de l'établissement (cadre de santé, IDE ou direction) Utilisation du DLU 'papier' pour : • Préparer les piluliers • Préparer les chariots de soins • Distribuer les médicaments Traçabilité des administrations à partir du traitement/ordonnances dans le DLU 'papier' Traçabilité de la non prise de médicament dans le plan de soins papier et/ou dans la fiche de transmission NOTA - Edition du DLU systématique à chaque mise à jour du plan de soins (nouvelle ou changement de prescription) et classement dans une pochette par personne accompagnée.				
MSS - Medimail	Commande médicaments Commande exceptionnelle de médicament	Attendre		Transmission de l'ordonnance papier à la pharmacie par transport par un personnel de l'établissement (cadre de santé, IDE ou direction)		
Excel - planning présence/absence	Commande médicaments Commande exceptionnelle de médicament	Planning imprimé et affiché en A3 à l'infirmerie ou la pharmacie		Mise en place d'un PC autonome avec solution bureautique. Refaire le fichier Excel à la main à partir de l'impression papier	Maintenir le fichier Excel en local	
Serveur de fichier établissement	Commande médicaments Commande exceptionnelle de médicament	Planning imprimé et affiché en A3 à l'infirmerie ou la pharmacie		Mise en place d'un PC autonome avec solution bureautique. Refaire le fichier Excel à la main à partir de l'impression papier	Maintenir le fichier Excel en local	

Solution de reprise d'activité

Application	PDMA (RTO)	Actions de reprise à réaliser	Documents associés
DUI - Plan de soin	24h	Procédure de collecte des administrations pour enregistrement/saisie manuelle lors du retour à la normale. - Modification et nouvelle prescription - Traçabilité des administrations : Pas de ressaisie dans l'outil informatique. Mettre un commentaire dans le dossier usage "panne informatique, voir la version papier".	
MSS - Medimail	-	Rien de particulier Procédure medimail de 'contrôle'/'renvoi' sur les dernières heures avant interruption	
Excel - planning présence/absence		Remettre le fichier "local" sur le serveur établissement. Réintégrer les présence/absence (prévisionnel et réalisé) dans Vavaliy	
Serveur de fichier établissement		Remettre le fichier "local" sur le serveur établissement. Réintégrer les présence/absence (prévisionnel et réalisé) dans Vavaliy	

Mise en application

Principes retenus

Une gouvernance « associative »

- Un seul plan cadre
- Un document par processus essentiel.

Mise en œuvre opérationnelle

Réaliser les actions identifiées (mesures, actualisation de procédures, création d'outils / modèles de documents…)

Déclinaison au niveau établissement et services

- ⇨ Applicabilité par établissement
- ⇨ En annexe de chaque procédure, spécification des éléments propres à chaque établissement et service

IRSAM

Aidera.Var
Accompagner l'Autisme

Points de vigilance

Approche par processus

Peut être chronophage si on ne dispose pas d'une cartographie
Alternative: Approche par les risques

Embarquer les parties prenants – Donner du sens

Penser le management de la continuité d'activité

Actualisation régulière nécessaire

Aidera.Var
Accompagner l'Autisme

IRSAM

Merci

05

Remise du prix « Énigme mystère »

Équipe CAPSI

Les vainqueurs sont…

Maleaume PAYRARD

et

Pascal SABATIER

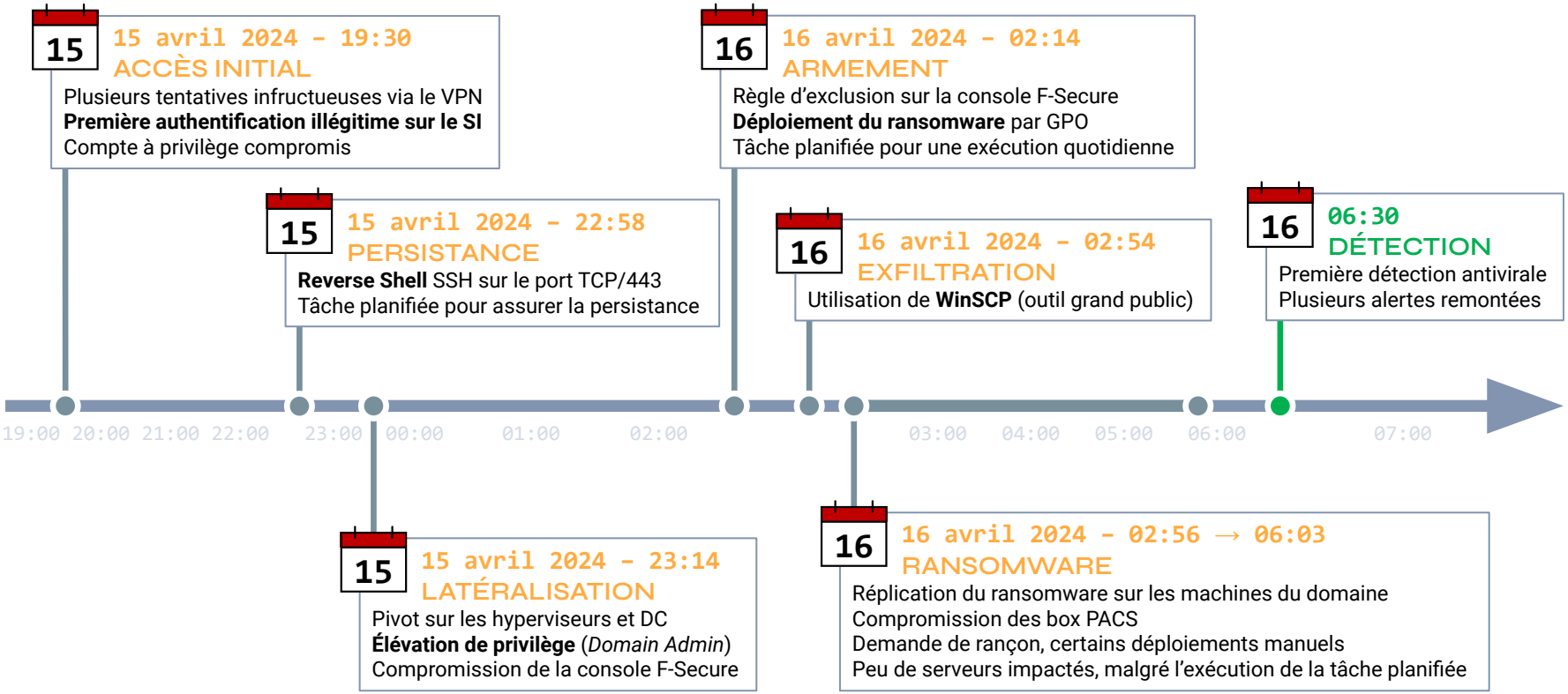
06

Table ronde

Réagir et se relever d'une cyberattaque : conseils et témoignages

Olivier Ruet-Cros (Expert cybersécurité - CERT Santé)
Wandrille Krafft (Directeur du CSIRT - LEXFO)
Christophe Frank (Responsable des systèmes d'information - CH Cannes Simone Veil)
Xavier Stoppini (RSSI du GHT des Alpes Maritimes)

Chronologie détaillée de la compromission



TLP:AMBER

07

Conclusion

Équipe CAPSI

Cocktail déjeunatoire

Rendez-vous à 14h pour les ateliers ludiques

Salle Jeanne	Salle Maryline	Salles Paradis et Marceau	Salle Fanny
ATELIER	ATELIER	ATELIER	ATELIER
Gestion de crise numérique et recommandations de pratiques	Réponse technique aux incidents de sécurité numérique	Sensibiliser à la cybersécurité de manière ludique + stand Conscio	Vis ma vie de pirate

Merci