GRIVES

ieSS Innovation e-Santé Sud

CAPSI

PASQUAL PACA CORSE Sécurité Qualité ieSS

ars Agence Régionale de Santé Provence-Alpes Côte d'Azur

RREVA

Médit PACA - Corse

# LES JOURNÉES VIGILANCES ESMS – 2024

## AIX EN PROVENCE

27 Juin 2024

# CYBERVIGILANCE

Cybervigilance, incidents de sécurité, anticiper et se préparer
avec le **Plan de Continuité et de Reprise d'Activité**
retours d'expérience

# Projet
# PCRA AIDERA Var

- 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

**CONTEXTE**

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

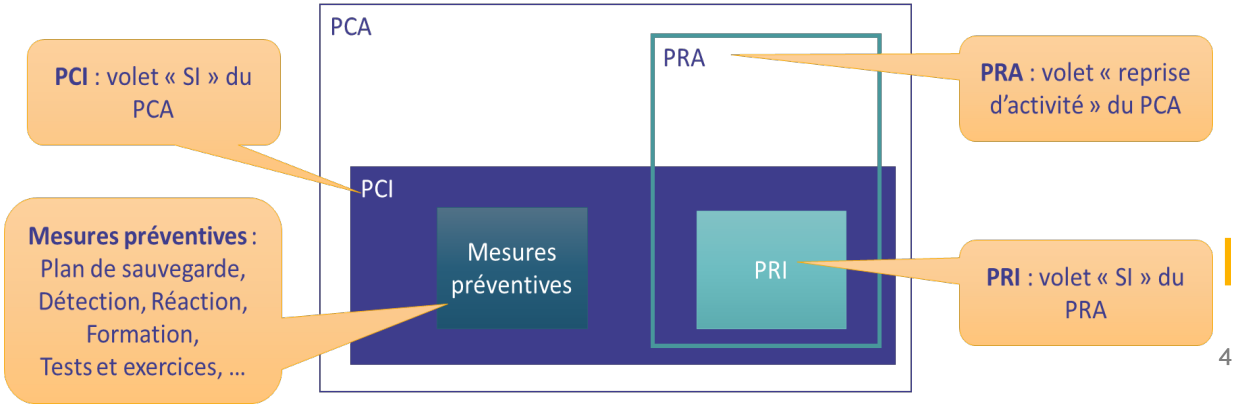
L'association IRSAM et AIDERAVAR sont accompagnées par CASSIs Conseil

IRSAM

Aidera.Var
Accompagner l'Autisme

# 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.



# 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

Liste des parties prenantes / moyen de communication
Plan de communication (interne/externe)
RACI (Rôles et responsabilité) / actions règlementaires

↓

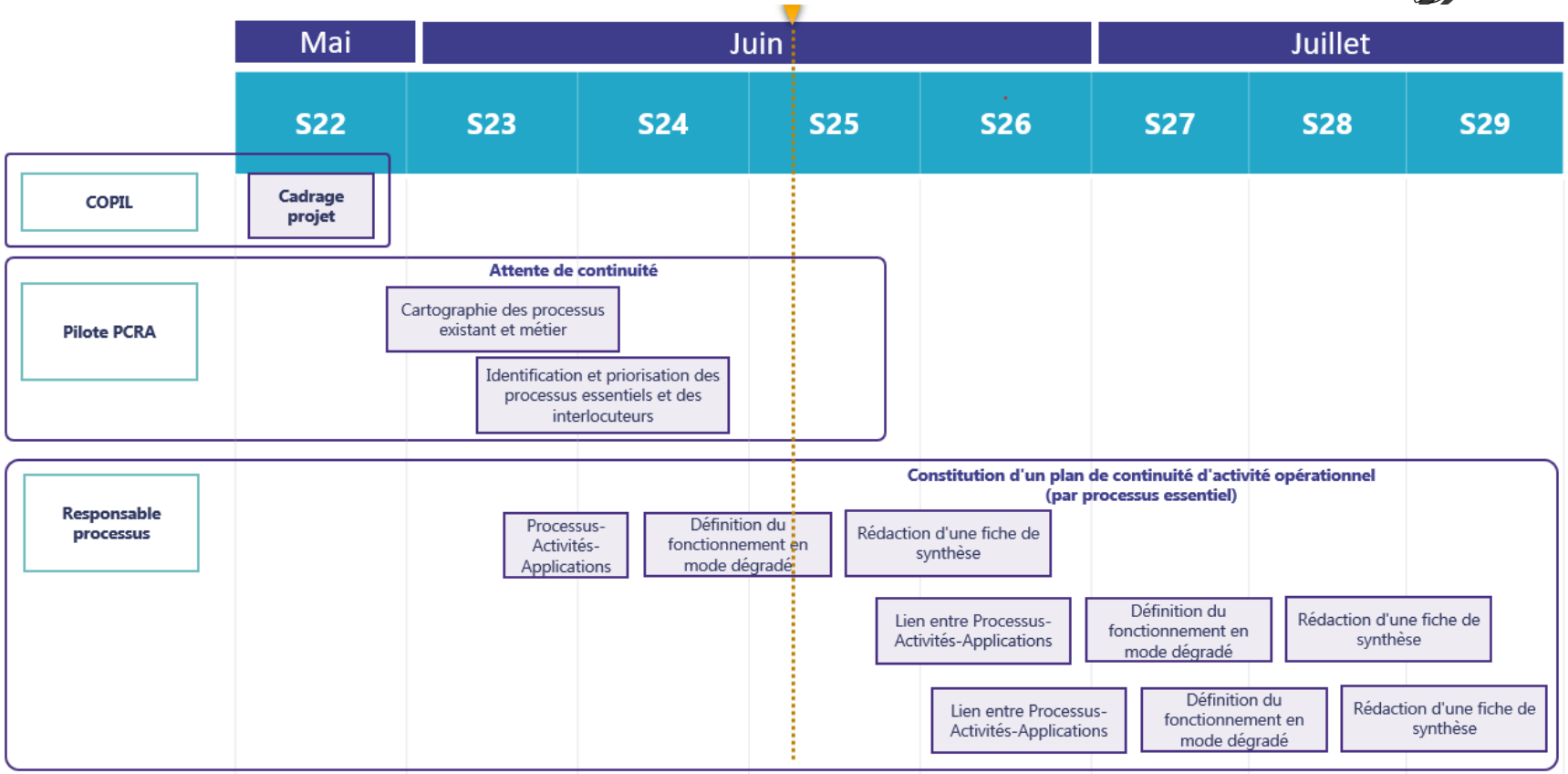
Constitution d'un plan de continuité d'activité opérationnel (par processus essentiel)

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

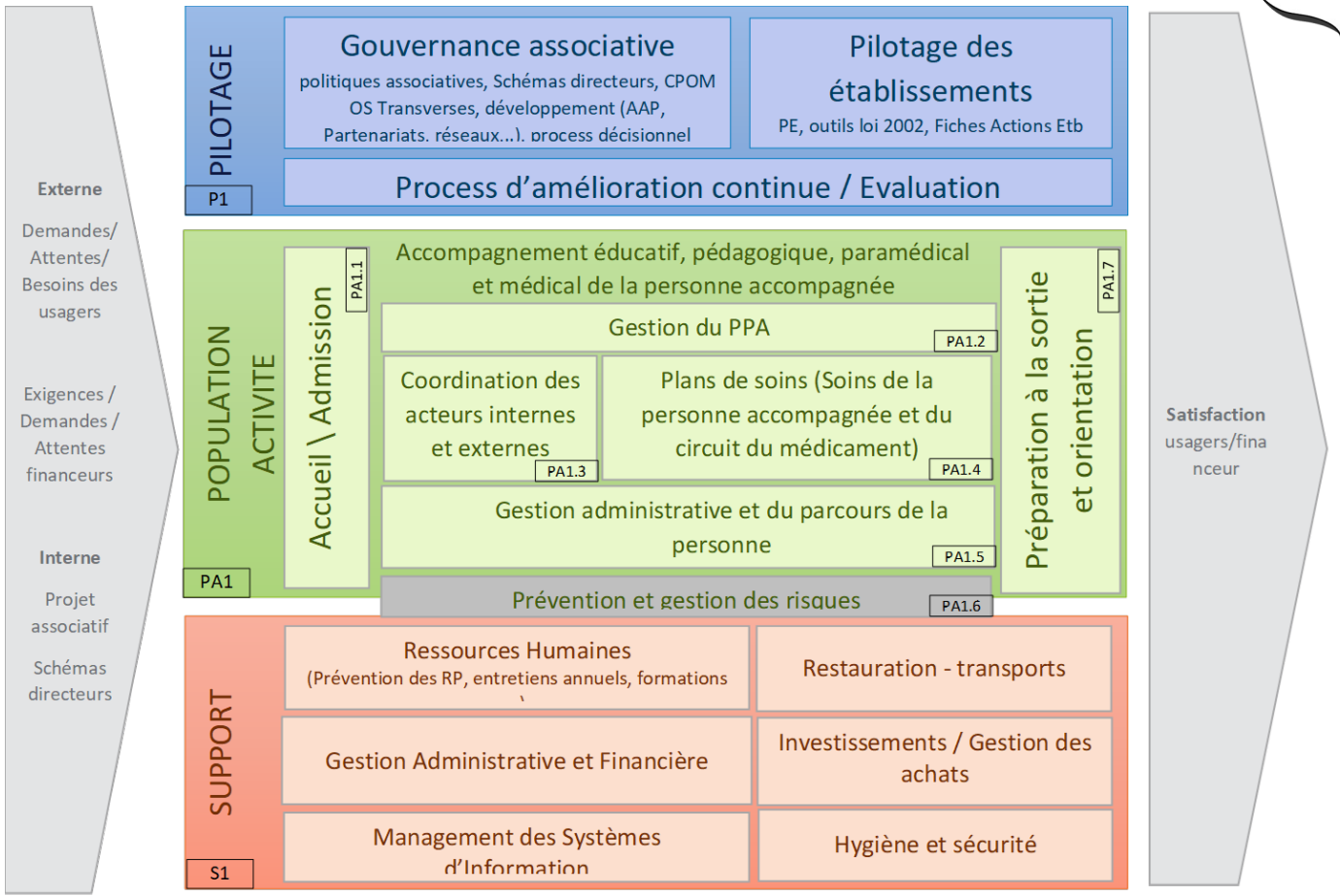
Identification des vulnérabilités du SI par analyse de risque (EBIOS RM simplifié)

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

# Planning prévisionnel



# Cartographie des processus



# Critères d'évaluation

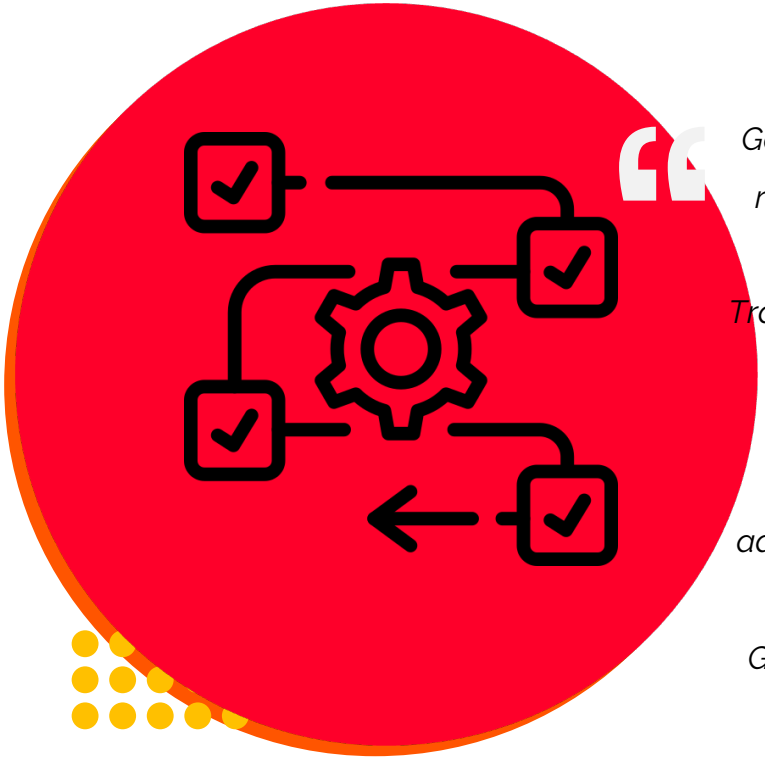
| Valeur | Personne accompagné | Social & organisation | Financier | Responsabilité / juridique | Réputation / image | DMIA |
|---|---|---|---|---|---|---|
| **1 – Mineure** | Gêne / inconfort pour un usager<br>**Pas d'impact** | - Gêne ponctuelle dans la prise en charge d'usagers, ou l'activité<br>- 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 :<br>Absence/report de soins et/ou soins inadéquats pour un usager entraînant une atteinte physique et/ou psychologique<br>**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<br>Conflit social<br>- 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 :<br>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.<br>**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.<br>- Conflit social paralysant la structure | Perte financière avec des impacts importants pour le responsable du traitement | - Atteinte à la vie privée d'un usager<br>- Condamnation pénale et/ou financière. | - Perte d'image ou de confiance dans l'acteur de santé ou le service offert<br>- Mise en cause de la stratégie de l'organisme détenteur du système ou d'un organisme tiers | 3 jours |
| **4 – Catactrophique** | Mise en danger d'une population / Menace du pronostic vital<br>- Atteinte irréversible ou décès d'un ou plusieurs usager(s).<br>**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.<br>- Arrêt du projet<br>Fermeture de la structure | Perte financière mettant en cause la pérennité du responsable du traitement | - Condamnation pénale et/ou financière<br>- Atteinte à la vie privée d'une population<br>Risques judiciaires | - Rejet définitif de l'acteur de santé ou du service offert<br>- Mise en cause de l'existence de l'organisme détenteur du système ou d'un organisme tiers | 3 heures |

# Priorisation des processus

| Processus | Valeur | Patient | Social & organisation | Financier | Responsabilité / juridique | Réputation / image | DMIA |
|---|---|---|---|---|---|---|---|
| Gestion des prescriptions (soins et médicaments) | 12 | 3 | 2 | 1 | 2 | 1 | 3 |
| Gestion des présences absences des personnes accompagnées | 12 | 3 | 3 | 1 | 1 | 1 | 3 |
| Comptabilité | 12 | 1 | 2 | 3 | 2 | 2 | 2 |
| Gestion des budgets | 12 | 1 | 2 | 3 | 2 | 2 | 2 |
| Coordination et planification des activités | 13 | 3 | 3 | 1 | 1 | 2 | 3 |
| Gestion des rendez-vous / plannings | 13 | 3 | 3 | 1 | 2 | 2 | 4 |
| Suivi des marchés et des achats | 13 | 2 | 2 | 2 | 2 | 2 | 3 |
| Gestion de la lingerie | 13 | 3 | 2 | 1 | 2 | 2 | 3 |
| Administration des soins | 14 | 3 | 2 | 1 | 3 | 1 | 4 |
| Gestion hôtelière | 14 | 3 | 2 | 2 | 1 | 2 | 4 |
| Distribution de la restauration | 14 | 3 | 2 | 2 | 1 | 2 | 4 |
| Gestion des transports | 14 | 3 | 2 | 1 | 2 | 2 | 4 |
| Gestion des acteurs internes / externes (planning salarié, intérimaire, libéraux) | 16 | 3 | 3 | 2 | 2 | 2 | 4 |
| Délivrance / Préparation / Administration médicamenteuse | 15 | 3 | 3 | 1 | 3 | 1 | 4 |
| Gestion des « urgences » Astreinte - gestion trouble comportement – appel au sanitaire (urgence) | 16 | 3 | 3 | 1 | 3 | 2 | 4 |
| Gestion des biens immobiliers | 18 | 3 | 3 | 3 | 3 | 2 | 4 |

52

# Les process essentiels



## IRSAM

*Gestion de l'hébergement, de la restauration et des transports*

*Traitement des situation de santé urgente*

*Dispensation, préparation, administration médicamenteuse*

*Gestion des acteurs internes et externes*

*Gestion de la paie*

## AIDERA Var

*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*

# 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 |

# 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.<br>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 | | | | |

# Application informatique

*Selon outil BIA de l'Agence du Numérique en Santé*

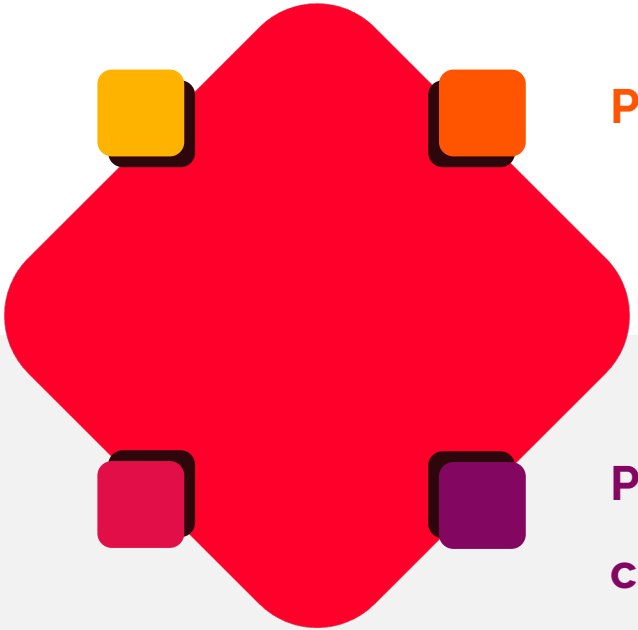
| Applications informatiques | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Objectif :** | Lister les applications informatiques utilisées dans le service d'activités et les associer aux activités.<br>Ce travail d'inventaire permettra de plus facilement renseigner l'onglet lié 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 sécurtié (incendie-annuelle, ERP-triennale)** | **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 |

# Définition du fonctionnement en mode dégradé

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**

# Prochaines actions

Poursuivre les travaux par processus

Adaptation au niveau des etablissements et services

Construire le plan de 'gouvernance' associé avec les directeurs, chefs de services et l'ensemble des parties prenantes

**Expérimentation**

A articuler avec les exercices de gestion de crise cyber

MERCI

# MERCI


GRIVES
ieSS
Innovation e-Santé Sud
CAPSI
PASQUAL
PACA CORSE Sécurité Qualité
ieSS
ars
Agence Régionale de Santé
Provence-Alpes
Côte d'Azur
RREVA
Médit
PACA - Corse