SÉGUR DU NUMÉRIQUE EN SANTÉ en Normandie

Accompagnement Cybersécurité

mars 2025

https://www.esegur-normandie/

SOMMAIRE

Rappels

Micros coupés pendant le temps des interventions

Temps de questions / réponses à la fin

Questions à poser en levant la main (chat bloqué)

Session enregistrée

Usage réservé aux participants, demander l'autorisation aux intervenants avant modification ou diffusion

Vos Contacts en région

Omar CHIBANE

Coordonnateur Collectif SI Normandie &
Référent régional Cyber ESMS

Olivier COUTANT

Coordinateur du Centre Régional
de Ressources Cybersécurité

Ouverture du Comité Régional

Fabian RICHARD

Responsable e-Santé & Transformation Numérique
Référent régional Cyberdéfense du système de santé
Direction de l'Attractivité des Métiers et de la Transformation Numérique du système de santé

ants

Gestion des incidents Cyber

RETEX, La Ligue Havraise
Julien LEGRAS, DSI

LIGUE HAVRAISE

JOUEUR

4 - Debriefing
- Bonne participation/communication
- Bonne gestion du stress
- Bonne répartition des tâches dans la confiance
- Quelques conseils vis-à-vis de la communication

3 – Fin de crise
- Retour du Calme
- Gestion de la cafetière

2 – Gestion de la crise
- Le DSI donne les instructions
- Le DSI submergé par les questions. Mauvaise préparation
  => Le travaille avance péniblement
- Les joueurs cherchent quel rôle jouer. Emergence d'idées (bonnes et mauvaises)
- Les joueurs se lancent et prennent rapidement leur autonomie.
  => Libération du DSI
- Gestion des imprévus (médias)

1 – Début du jeu
- Quand commence officiellement la crise ?
- Joueurs en attente
- Seul le DSI et la CDP sollicité par les *utilisateurs.*

0 – Participants :
- DG – DAF – DRH – CDP - Resp Communication

ants

Gestion des incidents Cyber

RETEX, La Ligue Havraise

Joueur

ASSO 2

Observateur

4 - Debriefing
- Bonne participation/communication
- Bonne gestion du stress
- Bonne répartition des tâches dans la confiance
- Quelques conseils vis-à-vis de la communication

3 – Fin de crise
- Les DRH/DAF s'interrogent sur leur présence
- Gestion de la cafetière

2 – Gestion de la crise
- La DG organise
- Le technicien submergé (pour des questions secondaires)
  => Durant une vraie crise, il n'aurait pas été autour de la table.
  => Qui pour faire le lien ?
- DRH/DAF observateurs
- Fonctionnement très vertical
- Gestion d'un VERITABLE imprévus

1 – Début du jeu
- Quand commence officiellement la crise ?
- Joueurs en attente
- La DG est très présente. C'est elle qui déclare le début de la crise
- Le technicien un peu en retrait

0 – Participants :
- DG – DAF – DRH – CDP - Resp Communication – Dir Etablissement

ants

Gestion des incidents Cyber

RETEX, La Ligue Havraise

Crise Réelle acteur

CRISE ACTUELLE

ACTEUR ☹

4 - Debriefing
- Relance au fur et à mesure
- Changement de tous les MDP (durcissement)
- Mise en place d'une liste blanche web
- 2FA pour télétravail et prestataires

3 – Fin de crise (J+4)
- Réinstallation de la ferme RDS
- Ouverture de comptes tests des environnements utilisateurs

2 – Remise en place de l'infrastructure (J+3)
- Nettoyage de l'AD
- Validation des sauvegardes
- Remise en place des serveurs BDD (perte de 4H)
- Remise en place des serveurs Fichier (perte de 3jrs)
- Remise en place AD (perte 1 mois)

1 – Début de la crise (J+2)
- (Alerte durant le week-end non traitées)
- Alerte générale : coupure réseau
- DSI informe les prestataires qui se mobilisent
- Les autres directions prennent en charge leur périmètre sans gêner le DSI
- Analyse de l'attaqeue

0 – Participants :
- DSI, Info-gérreur, Hébergeur – CERT… et les autres directions

ants

Plan de continuité et reprise d'activité

RETEX, Collectif SI PACA
Nadège VANNESTE, DSIO

Plan de Continuité et de Reprise d'Activité en ESMS

Nadège VANNESTE (Association 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 CAPSIS Conseil

Aidera.Var
Accompagner l'Autisme

- Projet stratégique AIDERA Var 2021/2025 : 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

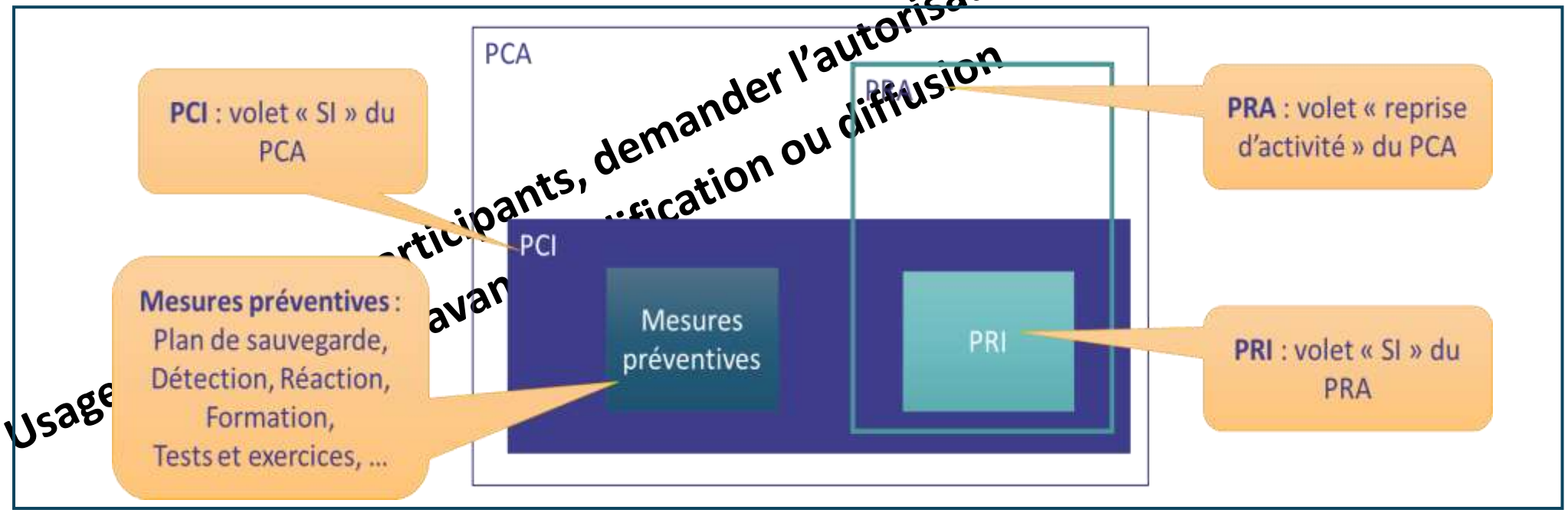
Action inscrite dans le projet associatif 2024-2028

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 acteurs 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

Articulation PLAN Bleu – PCRA

Plan bleu

Objectif : maintien des accompagnements dans des conditions particulières

Le pan bleu décrit les mesures préventives et conduite à tenir selon le risque identifié pouvant impacté léactivité (coupure d'eau, intempéries, cyber attaque par exemple)

Plan de Continuité et de Reprise d'Activité

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

Aussi, 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. Ces plans sont complémentaires, peuvent etre déclenchés simultanément ou indépendamment l'un de l'autre.

Illustration : en cas de cyberattaque, on peut avoir dans le plan bleu les mesures préventives (actions de sensibilisation) et la conduite à tenir (isolation réseau du poste , appel à la DSI,…) et le PCRA définit le fonctionnement en mode dégradé pour les activité essentielles en cas d'indisponibilité du SI

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

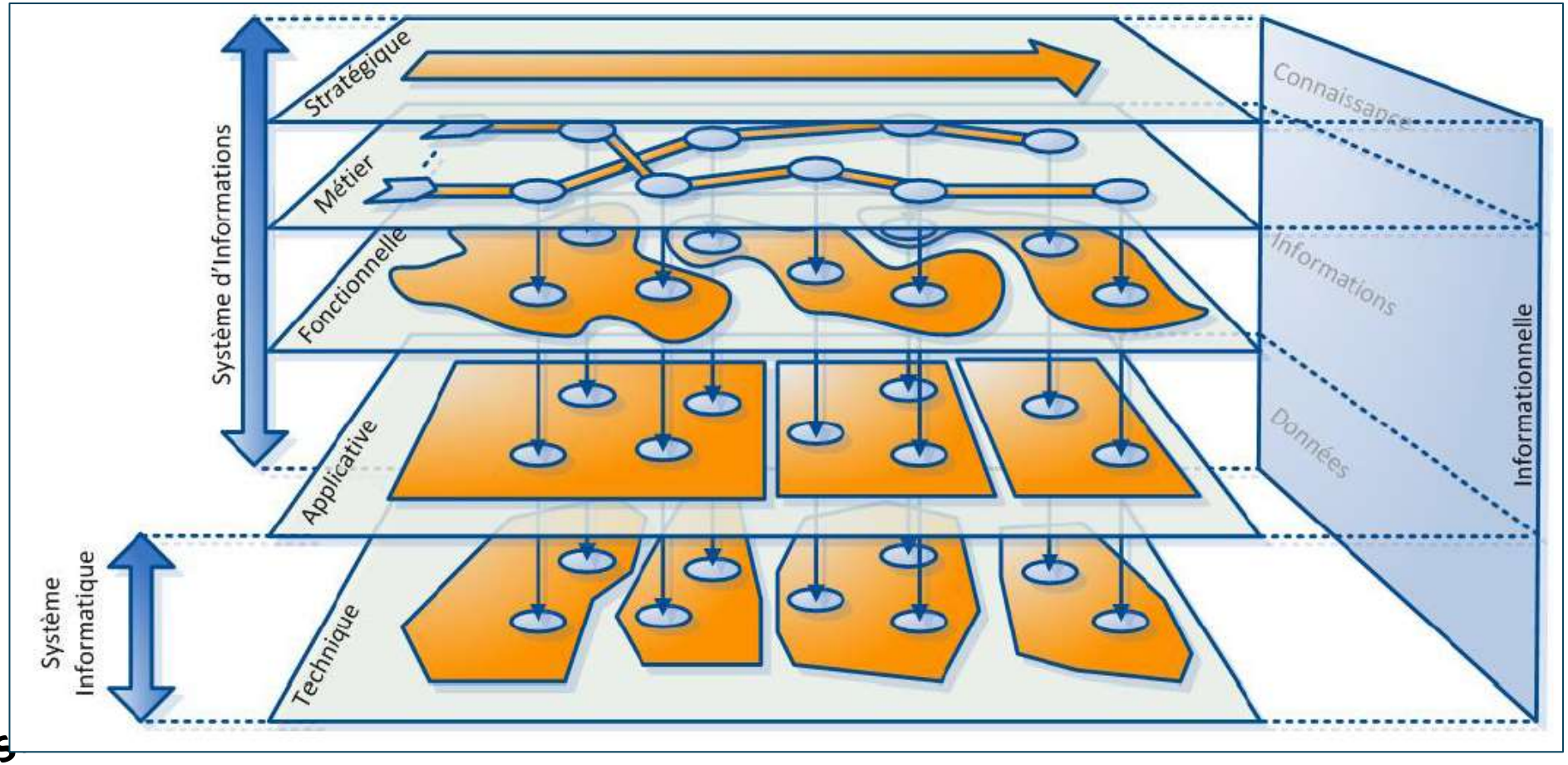
demander l'autorisation aux intervenants

ation ou diffusion

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

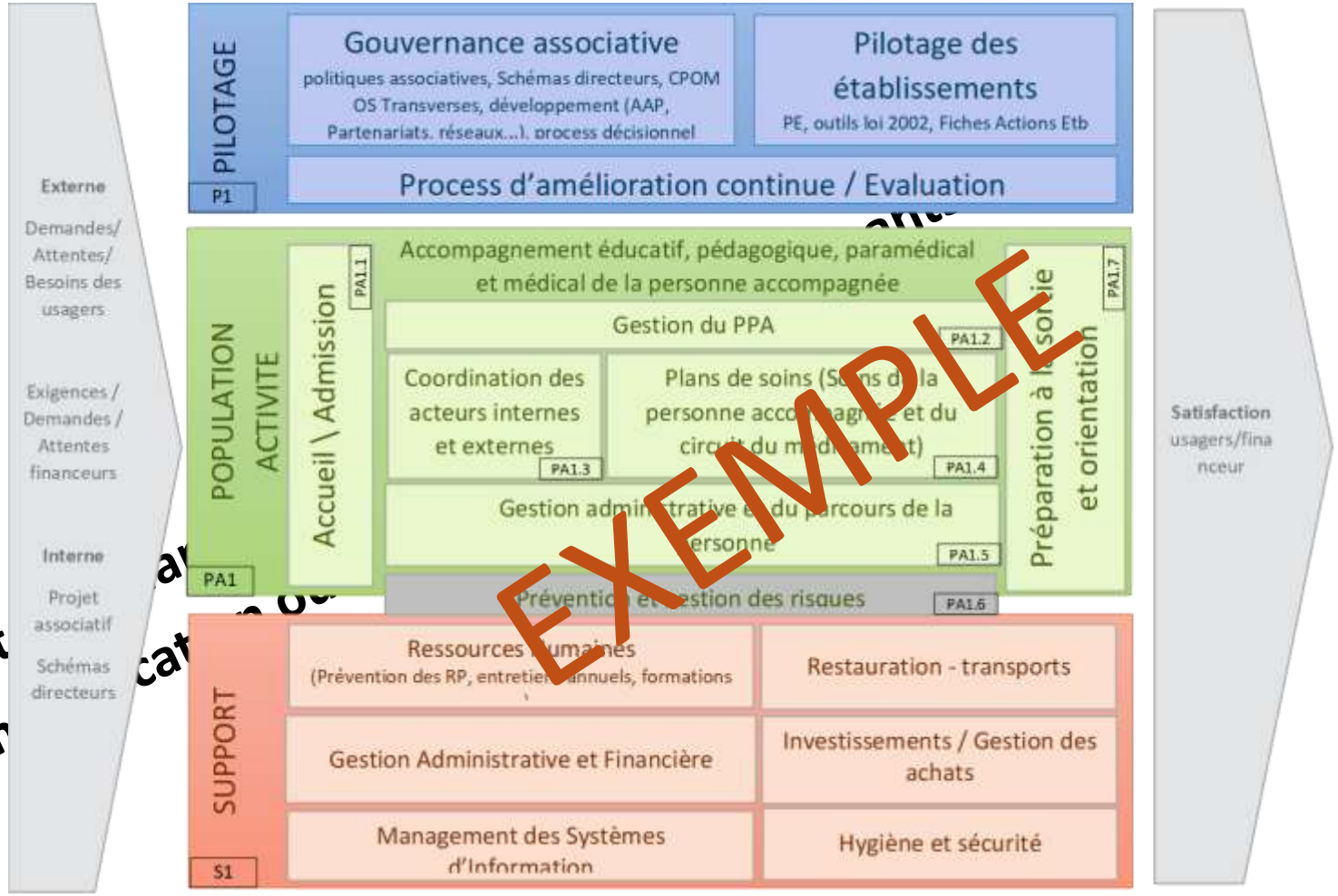
Process métiers



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 avant nécessité des mesures adaptées ou niveau 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

Accueil \ Admission

- Accueil de la personne
- Information et recueil des consentements
- Suivi des orientations et des notifications

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**

Gestion du PPA

- Recueil &Evaluation multidimensionnelle des besoins et attentes de la personne accompagnée
- Gestion du projet personnalisé

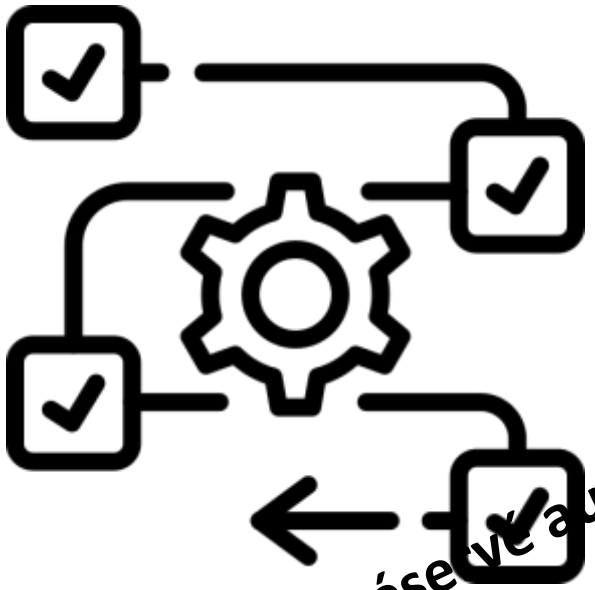
Sous processus	Personne Accompagnée	Social & organisation	Financier	Responsabilité / juridique	Réputation / image	DMIA	Total
Recueil &Evaluation multidimensionnelle des besoins et attentes de la personne accompagnée	2	2	1	2	2	1	**10**
Gestion du projet personnalisé	2	2	1	2	2	1	**10**

EXEMPLE

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
PA1	Plans de soins	Gestion du dossier médical	3	1	1	1	1	3	10
PA1	Plans de soins	Gestion des stocks de médicaments	2	2	1	2	1	2	10
S1	Ressources Humaines	Gestion de la formation	1	3	1	2	2	1	10
S1	Ressources Humaines	Gestion de la sortie	0	1	2	3	2	2	10
S1	Ressources Humaines	Gestion des accessibilités	0	2	2	2	2	2	10
S1	Gestion Administrative et Financière	Gestion des EPRD, ERRD	1	2	2	2	2	1	10

Les process essentiels



Exploitation des biens immobiliers

Traitement des situation de santé urgente

Dispensation, préparation, administration médicamenteuse

Gestion des acteurs internes et externes

Administration des soins

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 libéral/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	Directeur ESMS – Direction du	Directeur ESMS – cadre	Intervenants	Prestataires – fournisseurs de service (eau,	

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

Usage re

Application informatique

Selon outil BIA de l'Agence du Numérique en Santé

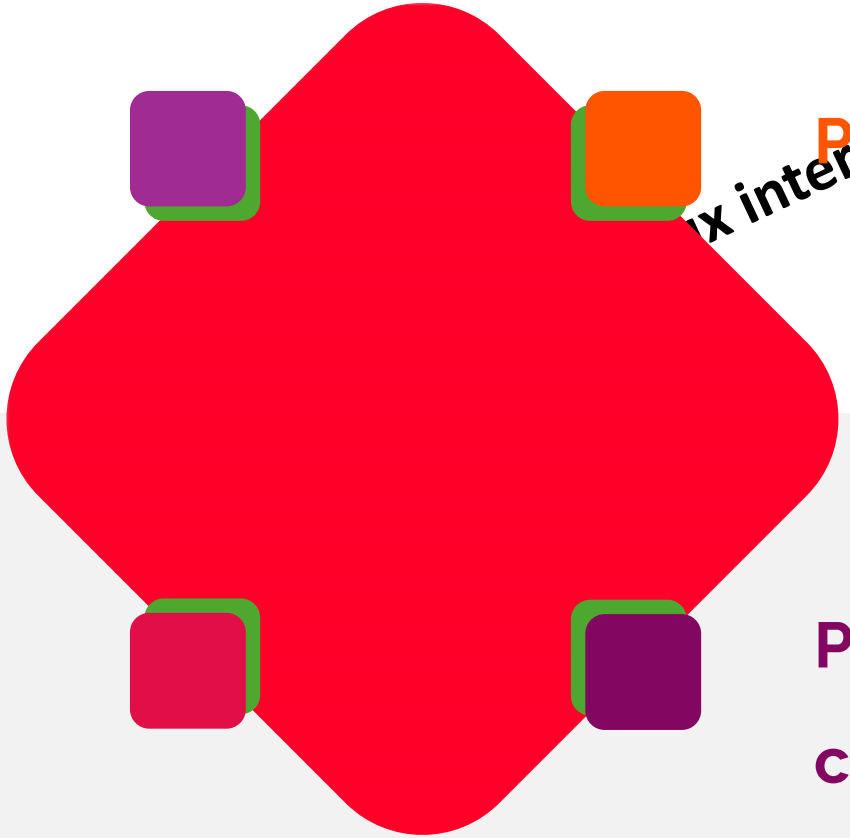
Applications informatiques										
Objectif :	Lister les applications informatiques utilisées dans le service d'activités et les associer aux activités. Ce travail d'inventaire permettra de plus facilement renseigner l'onglet lié à l'indisponibilité des systèmes d'informations.									
Nom de l'application 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-APP-biennale)**	**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

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

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

ants

La Cybersécurité en Normandie

Le Centre Régional de Ressources en Cybersécurité

Centre Régional de Ressources en Cybersécurité (CRRC)

Appui et accompagnement

Sécur'NeS est le Centre de Ressources Régional en Cybersécurité (CRRC) à destination des acteurs du sanitaire, médico-social et social.

Sécur'NeS est opéré par le GRADeS Normand'e-Santé et financé par l'ARS Normandie. Cette plateforme vise à accompagner les établissements au programme CaRE ainsi qu'à renforcer la sécurité des systèmes d'information en mettant à disposition des ressources et des outils en cybersécurité.

Et puis spécifiquement de :

- La **sensibilisation** au risque cyber ;
- **Accompagnement** aux respects de la réglementation ;
- **L'entraînement et l'organisation** aux incidents de cybersécurité (exercices de crise) ;
- L'accompagnement dans les programmes nationaux dédiés.

Centre Régional de Ressources en Cybersécurité (CRRC)

Appui et accompagnement

Un parcours Cyber ESMS en 5 étapes

Le **CRRC** propose un parcours structuré en **5 étapes** pour aider les **Établissements Sociaux et Médicaux Sociaux (ESMS)** à renforcer leur cybersécurité.

Auto-Diagnostic Cyber

Première évaluation pour identifier les points forts et les vulnérabilités

Convention

Engagement des parties prenantes et définition du cadre d'accompagnement

Diagnostic de maturité (3 niveaux)

Analyse approfondie pour situer l'établissement sur une échelle de maturité

Plan d'action personnalisé

Élaboration de mesures adaptées aux besoins spécifiques de l'établissement

Suivi

Accompagnement dans la mise en œuvre des actions et ajustements selon l'évolution des risques.

Centre Régional de Ressources en Cybersécurité (CRRC)

Appui et accompagnement

Usage réservé aux intervenants

ACCÈS LIBRE*

- Auto-diagnostic
- Sensibilisation (phishing, escap'game, …)
- Corpus documentaires
- Prestataires de réponse à incident (PRIS)

PARCOURS CYBER

- Diagnostic
- Mise en place d'un plan d'action
- Suivi continue.

MATURITÉ DÉPENDANT

- Audit annuaire
- Audit exposition internet
- Premier exercice de crises
- Plan de continuité et reprise d'activité (PCRA)

* Compris par défaut dans le parcours cyber ESMS

ants

La Cybersécurité en Normandie

Dispositifs d’alerte

Réaction en cas d'incident cyber

Service d'appui à la gestion des cybermenaces 24h/24 et 7j/7

Réaction en cas d'incident cyber

Service d'appui à la gestion des cybermenaces 24h/24 et 7j/7

En premier lieu sur un incident => CERT-Santé : https://www.cyberveille-sante.gouv.fr/

Notifier une violation de données personnelles

La notification doit être transmise à la **CNIL dans les meilleurs délais (72h)** à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Les moyens disponibles

CARE

- Entrée des ESMS dans Domaine 2 (PCRA)

Portail ANS

- Kits Exercices cyber
- Kits PCRA
- Documentation

CERT-Santé

- Réponse à incident
- Documentation
- Audits
- Alerting

ARS

- Veille et alerte
- Relai informationnel
- Appui à la crise
- Conseil et accompagnement

Centre Régional de Ressources Cybersécurité (CRRC)

- Plateforme régionale de sensibilisation
- Escape Game
- Jeu de gestion de crise
- Base documentaire
- Accompagnement aux exercices cyber (en développement)
- Appui au diagnostic cyber (en développement)
- Parcours de cybersécurité (en développement)

Partenaires régionaux

ants

La Cybersécurité en Normandie

Questions, échanges et propositions des participants

Questions, échanges et propositions des participants

Usage réservé aux partici
ava
demander l'autori
diffusion
n aux intervenants

ants

La Cybersécurité en Normandie

Clôture et prochaines étapes

Clôture du comité régional

Olivier ANGOT

Directeur
GRADeS Normand’e-Sante

Merci de votre attention

contact@securnes.fr

www.securnes.fr