

Plan de Continuité des Activités de l’Inserm

Version 1.1

FSD

Dernière mise à jour :

26 janvier 2018

DOCUMENTS ASSOCIES

Intitulés	Références
Procédure de fonctionnement de la cellule de crise stratégique	Annexe 1
Procédure type de fonctionnement de la cellule de crise opérationnelle DR/ADS	Annexe 2
Fiches action gestion de crise	Annexe 3
Fiches réflexes Gestion de crise	Annexe 4
Fiches réflexes PCA	Annexe 5
Guide de communication de crise	Annexe 6
Plan de continuité informatique	Annexe 7

REVISIONS ET VALIDATIONS DU DOCUMENT PAR LA DIRECTION INSERM

Rôle	Nom	Responsabilités	Date
	H. BRAHMI	Ressources humaines	28/03/2018
	F. CHAMBLIN	Finances	04/04/2018
	M. CONAN	Agence comptable	04/04/2018
	C. SCHILTZ	Prévention des risques	03/05/2018
	C. GIRY	Directrice générale déléguée	

DIFFUSION DU DOCUMENT PAR LE FSD

Fonctions - Entités	Destinataires	Date de diffusion

SUIVI DU DOCUMENT

Version	Type d'Action / date	Type de mise à jour	Propriétaire
1.0		Création du document	JC SARRON (FSD)

TABLE DES MATIERES

Table des matières

1. CONTEXTE ET OBJECTIFS DU PCA.....	5
1.1. OBJET DU PCA.....	5
1.2. PÉRIMETRE COUVERT PAR LE PCA.....	6
1.3. ARCHITECTURE ET CONTENU DU PCA.....	7
1.4. DÉFINITIONS.....	8
2. SCENARII DE RISQUES ET IMPACTS SUR LES ACTIVITES DE L'INSERM	11
2.1 LES SCENARII DE RISQUES COUVERTS PAR LE PCA.....	11
2.1.1 <i>L'arrêt des systèmes d'information et de communication.....</i>	<i>11</i>
2.1.2 <i>L'indisponibilité des bâtiments et des locaux.....</i>	<i>11</i>
2.1.3 <i>L'indisponibilité de personnels.....</i>	<i>12</i>
2.2 LES AUTRES SCENARII DE RISQUES IDENTIFIES.....	12
2.2.1 <i>L'invasion des locaux.....</i>	<i>13</i>
2.2.2 <i>Le conflit social.....</i>	<i>13</i>
2.2.3 <i>La destruction de documents originaux et officiels.....</i>	<i>13</i>
2.2.4 <i>Le risque image.....</i>	<i>14</i>
2.3 LES IMPACTS.....	14
2.3.1 <i>Consécutifs a un arrêt des systemes d'information et de communication.....</i>	<i>14</i>
2.3.2 <i>Consécutifs a une indisponibilité des bâtiments et des locaux (destruction).....</i>	<i>15</i>
2.3.3 <i>Consécutifs a une indisponibilité de personnels.....</i>	<i>16</i>
3. DISPOSITIF DE GESTION DE CRISE.....	17
3.1 LES OBJECTIFS DU DISPOSITIF DE GESTION DE CRISE	17
3.2 RAPPELS SUR LES PRINCIPES DE PILOTAGE D'UNE SITUATION DE CRISE.....	17
3.3 ORGANISATION DU DISPOSITIF DE GESTION DE CRISE	17
3.3.1 <i>Dispositif de gestion de crise de l'Inserm.....</i>	<i>17</i>
3.3.2 <i>Cellule de crise stratégique de l'Inserm.....</i>	<i>18</i>
3.3.3 <i>Cellules de crise opérationnelles.....</i>	<i>19</i>
3.3.4 <i>Cellules locales de gestion de l'urgence.....</i>	<i>19</i>
3.4 COMPOSITION, RÔLES, MISSIONS ET FONCTIONNEMENT DES CELLULES DE CRISE..	20
3.5 DÉCLENCHEMENT DE LA GESTION DE CRISE	20
3.5.1 <i>Veille opérationnelle.....</i>	<i>20</i>
3.5.2 <i>Alerte et signalement d'un événement.....</i>	<i>21</i>
3.5.3 <i>Évaluation et activation de la cellule de crise.....</i>	<i>22</i>
3.5.4 <i>Gestion de la situation de crise.....</i>	<i>22</i>
3.5.5 <i>Retour d'expérience.....</i>	<i>23</i>
3.6 COMMUNICATION DE CRISE	24
3.6.1 <i>Principes directeurs de la communication de crise à l'Inserm.....</i>	<i>24</i>
3.6.2 <i>L'appui de la Direction de l'Information Scientifique et de la Communication aux Délégations Régionales.....</i>	<i>25</i>
3.6.3 <i>Missions du pôle communication de crise.....</i>	<i>25</i>
3.6.4 <i>Organisation du pôle communication de crise.....</i>	<i>26</i>
3.6.5 <i>Évaluation du potentiel d'attractivité médiatique et questions récurrentes des médias.....</i>	<i>26</i>
3.6.6 <i>Pratique de la communication de crise.....</i>	<i>26</i>
4. PLAN DE CONTINUTE DES ACTIVITES.....	27
4.1 SECOURS DES ACTIVITES VITALES	27
4.2 SECOURS DES BATIMENTS ET DES LOCAUX.....	28

4.3	SECOURS DES INFRASTRUCTURES, RÉSEAUX ET SYSTÈMES D'INFORMATION (attente PCI DSI)	29
5.	OBJECTIFS DE REDEMARRAGE ET STRATEGIE DE CONTINUITE	30
5.1	LES BESOINS DE CONTINUITÉ ET LES OBJECTIFS DE REDÉMARRAGE	30
5.1.1	<i>Les activités entrant dans le cadre de la gestion de l'urgence (h+8).....</i>	<i>30</i>
5.1.2	<i>Les activités à reprendre dans un délai maximal de 24 à 72 h.....</i>	<i>31</i>
5.1.3	<i>Les activités à reprendre dans un délai maximal de 1 à 2 semaines.....</i>	<i>32</i>
5.1.4	<i>Les activités à reprendre sous un mois.....</i>	<i>33</i>
5.2	PLAN GÉNÉRAL DE REDÉMARRAGE ET DE RETOUR À LA NORMALE	34
5.3	LES BESOINS EN RESSOURCES CRITIQUES	35
5.3.1	<i>Synthèse des besoins en positions (hors gouvernance).....</i>	<i>35</i>
5.3.2	<i>Détail des besoins en positions et autres ressources.....</i>	<i>38</i>
5.3.3	<i>Fournisseurs critiques.....</i>	<i>38</i>
5.3.4	<i>Données critiques.....</i>	<i>38</i>
6.	STRATEGIE DE CONTINUITE DES ACTIVITES : PRINCIPES RETENUS.....	40
6.1	Siège.....	40
6.2	Délégation régionale.....	41
7.	MAINTIEN EN CONDITION OPERATIONNELLE.....	42
7.1	PRÉAMBULE	42
1.5.	MCO : ORGANISATION GÉNÉRALE	42
7.2	RÔLES ET MISSIONS	43
7.2.1	<i>Responsable PCA Inserm (RPCA).....</i>	<i>43</i>
7.2.2	<i>Correspondants PCA et référents.....</i>	<i>43</i>
7.2.3	<i>Coordonnées.....</i>	<i>43</i>
8.	CONTINUITÉ DES FOURNISSEURS CRITIQUES.....	44
9.	ACTIONS RECURRENTES A MENER DANS LE CADRE DE LA MCO DU PCA DE L'INSERM.....	45



1. CONTEXTE ET OBJECTIFS DU PCA

1.1. OBJET DU PCA

Le Plan de Continuité des Activités de l'Inserm répond à la nécessité de s'organiser face à un événement grave susceptible de provoquer un arrêt, total ou partiel, brutal ou non, des activités des délégations régionales ou de celles du siège localisées sur les sites suivants :

- Siège, 101 Rue de Tolbiac, 75013 Paris
- Biopark, Biopark. 13 rue Watt, 75013 Paris
- Héron Building, 66 avenue du Maine 75014 Paris
- Datacenter de Villejuif
- Datacentre de Montpellier (Cines)

Il a pour principal objectif d'assister les équipes de l'Inserm à se préparer à affronter un **scénario de risque majeur** et ainsi garantir la **sauvegarde des personnes** et des **actifs** du Groupe.

Le PCA apporte des réponses à trois enjeux stratégiques et opérationnels :

1. Préparer les équipes du siège de l'Inserm à **gérer une situation de crise** en anticipant les scénarios de risques possibles et les actions à mener pour en réduire la durée et l'intensité,
2. Identifier et déployer les **dispositifs de résilience** pour permettre un redémarrage et un retour à la normale le plus rapide possible des activités situées dans le périmètre du PCA,
3. S'aligner sur les pratiques de **bonne gouvernance des risques** déployées au sein des institutions étatiques, sous l'égide du Secrétariat Général à la Défense et à la Sécurité Nationale.

Le document expose et évalue les situations d'urgence potentielles. Il définit des règles d'organisation, de fonctionnement ainsi que des bonnes pratiques pour faire face à une situation de crise et de blocage des activités du siège de l'Inserm.

Remarque :

Le PCA n'est pas un Plan de Maîtrise des Risques définissant des dispositifs de prévention et de protection à mettre en oeuvre. Il présente et décrit les modalités d'actions à engager pour des situations où ces mesures ont échoué.



1.2. PÉRIMETRE COUVERT PAR LE PCA

Le Plan de Continuité des Activités couvre les activités de pilotage et de support exercées au Siège et dans les Délégations Régionales ainsi que les activités scientifiques de l'Inserm en dehors de celles des unités de recherche :

- **Fonctions et activités relatives à la gouvernance de l'Institution (Exécutif) :**
 - Présidence
 - Direction Générale

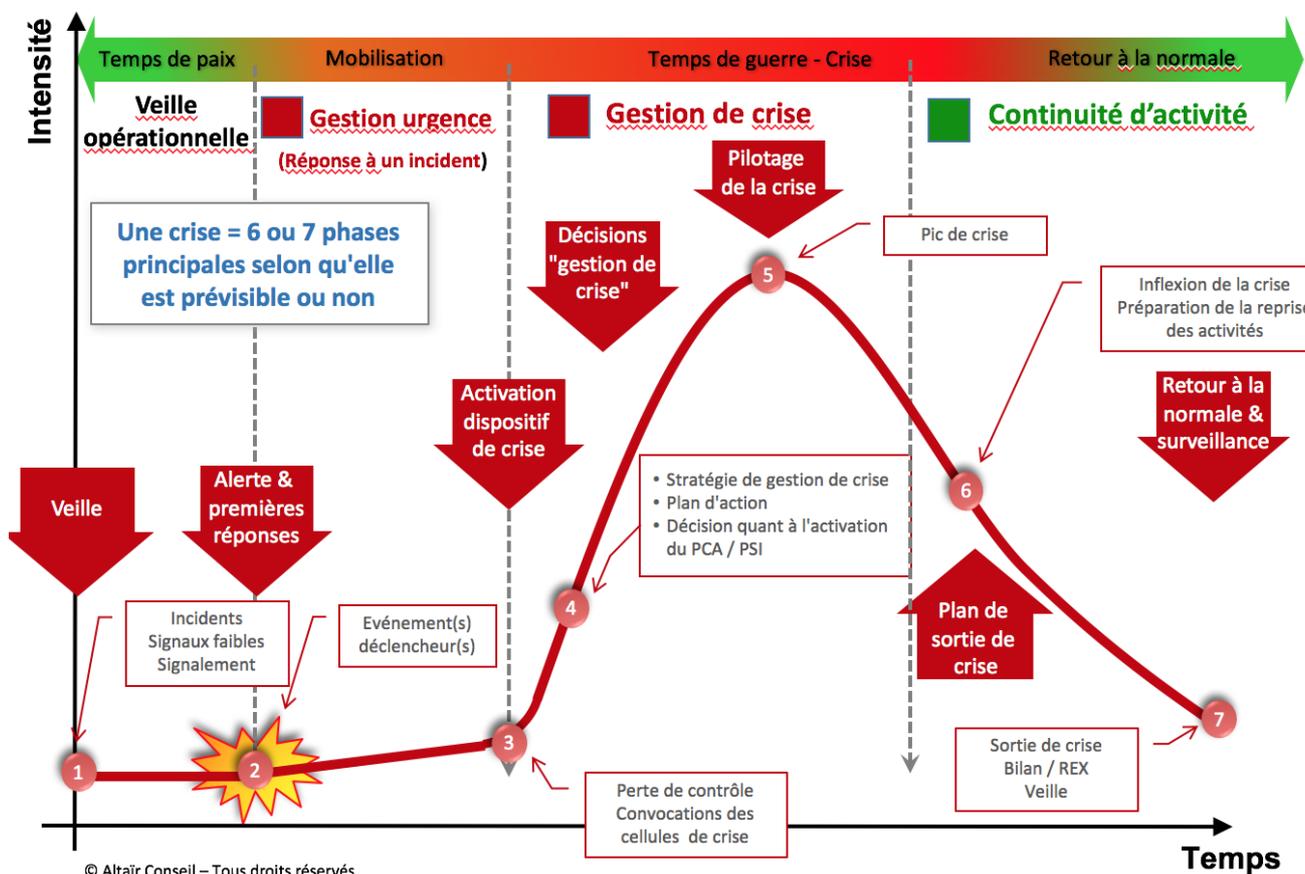
- **Fonctions et activités métiers de l'Inserm :**
 - Administration de la recherche dans les laboratoires
 - Expertise dans les domaines de la biologie, de la médecine, de la chirurgie, des biotechnologies et de la santé publique auprès de l'État

- **Fonctions et activités de support :**
 - Juridique
 - Communication
 - Ressources Humaines
 - Finance
 - Achats
 - Comptabilité
 - Systèmes d'Information
 - Services généraux du siège
 - Sécurité des personnes
 - Valorisation des projets

Le PCA de l'Inserm ne décrit pas le PCA spécifique à chaque unité de recherche et ne couvre pas les instituts spécialisés : AVIESAN, INCa, etc.

1.3. ARCHITECTURE ET CONTENU DU PCA

Le Plan de Continuité des Activités de l'Inserm couvre les phases de gestion de crise et de continuité des activités présentées dans le schéma ci-dessous :

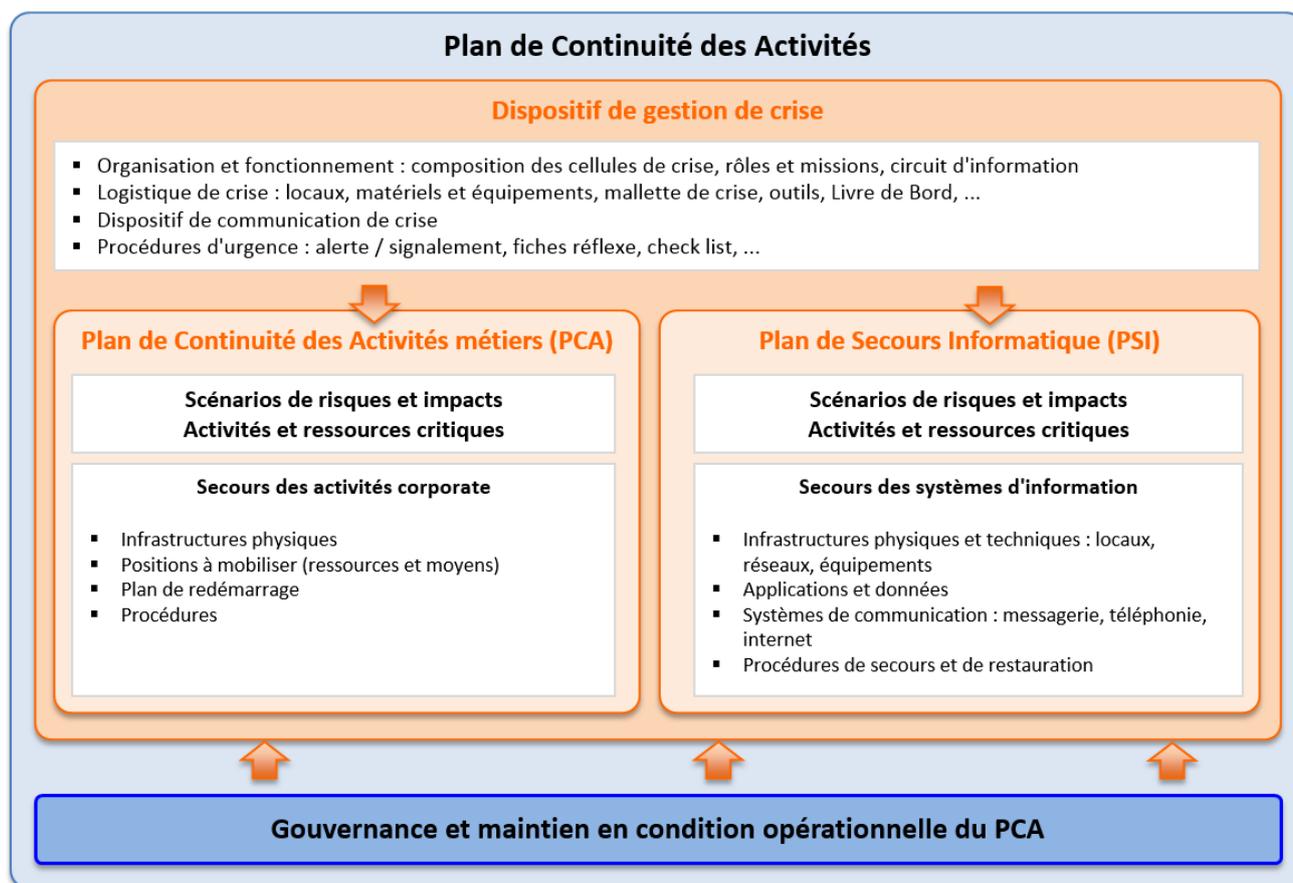


Le PCA est articulé autour de trois dispositifs complémentaires :

1. Un **dispositif de gestion de crise** permettant d'organiser le pilotage et les actions contribuant à réduire la durée et l'intensité d'une situation de crise (le dispositif de crise est repéré en haut de page par un carré **rouge**)
2. Un **plan de continuité** constitué d'un Plan de Continuité des Opérations et d'un Plan de Continuité Informatique pour organiser les opérations de redémarrage et de retour à la normale des activités. Le Plan de Continuité Informatique élaboré, validé et maintenu par la Direction des Systèmes d'Information est annexé au PCA (le plan de continuité est identifié en haut de page par un carré **vert**)
3. Un **dispositif de gouvernance et de maintien en condition opérationnelle** confié à un **Responsable PCA Inserm (FSD)** et des **Correspondants PCA métiers** (le dispositif de gouvernance et de maintien en condition opérationnelle est matérialisé en haut de page par un carré **bleu**)



L'architecture et le contenu du PCA sont synthétisés dans le schéma ci-dessous :



1.4. DÉFINITIONS

ACTIVITE VITALE	<ul style="list-style-type: none"> ▪ Activité qui, en cas d'interruption, doit être rétablie au plus vite (24 à 48 h maxi) pour éviter des pertes élevées ou d'autres impacts préjudiciables à la survie de l'institution
CELLULE DE CRISE	<ul style="list-style-type: none"> ▪ La cellule de crise est la structure de commandement unique en charge du pilotage, de la gestion de la crise et de la communication de crise, ▪ La cellule de crise est placée sous la responsabilité d'un pilote désigné par anticipation ou à l'occasion de l'entrée en situation de crise, ▪ La cellule définit une stratégie de résolution et prend les décisions nécessaires à une sortie rapide de la situation de crise, en particulier l'activation des plans de secours,



	<ul style="list-style-type: none">▪ A cet effet et en période de crise, la cellule de crise communique ses instructions à des cellules opérationnelles, mais aussi des équipes d'intervention, constituées et activées au sein de chaque métier impacté par la résolution de la crise.
CELLULE DE CRISE STRATÉGIQUE	<ul style="list-style-type: none">▪ C'est la plus haute structure décisionnelle de l'Inserm en matière de gestion de crise,▪ Son périmètre de responsabilité s'étend à l'ensemble des activités et des ressources de l'Inserm. Selon la nature et l'ampleur de la crise mais aussi les besoins de la situation, elle peut prescrire aux cellules de crise opérationnelles toute action qu'elle juge indispensable,▪ Outre les décisions relatives à la gestion de la crise et de la continuité d'activité, la cellule de crise stratégique assure également une fonction de support aux cellules de crise opérationnelles ouvertes dans les Délégations Régionales ou à l'Administration du Siège au travers d'une mobilisation des ressources et des moyens nécessaires à la sortie de la situation de crise.
CELLULE DE CRISE OPÉRATIONNELLE	<ul style="list-style-type: none">▪ Elle reprend l'essentiel des missions, des rôles et des objectifs de la cellule de crise stratégique de l'Inserm mais dans une dimension plus opérationnelle et limitée à son périmètre de responsabilité (gestion de la relation avec les équipes locales d'intervention, les partenaires locaux et les autorités locales)▪ La cellule de crise opérationnelle assure également l'alerte, le signalement et le reporting auprès de la cellule de crise stratégique de l'Inserm. Selon la situation rencontrée et les besoins, elle met en œuvre les consignes et les instructions qui peuvent lui être communiquées par cette dernière.
CRISE	<ul style="list-style-type: none">▪ Situation consécutive à un événement grave qui engendre une situation de rupture, de dérèglement et de déstabilisation dans le fonctionnement d'une organisation. Elle peut être le résultat d'un incident brutal et imprévisible (incendie, explosion, ...) ou d'un ensemble d'actes faiblement perceptibles mais répétés. Elle se caractérise par :<ol style="list-style-type: none">1. une intensité très élevée2. une charge émotionnelle forte3. des conséquences élevées : présence éventuelle de victimes, dégâts, arrêt des activités, perte d'image potentielle, ...4. Une absence temporaire de contrôle5. Une attractivité médiatique potentielle6. Une menace pour la pérennité de l'organisation, voire de l'institution7. L'implication de moyens exceptionnels pour la résoudre



INCIDENT	<ul style="list-style-type: none">▪ Evènement, anticipé ou non, qui perturbe le cours normal des activités de l'organisation, et porteur de conséquences potentiellement élevées pour la continuité des activités.▪ Non maîtrisé, un incident peut entraîner une situation de crise.
PLAN DE CONTINUITÉ DES ACTIVITES (PCA)	<ul style="list-style-type: none">▪ Le Plan de Continuité des Activités permet à toute organisation de pouvoir fonctionner, même en situation dégradée, en cas de survenance d'un sinistre majeur occasionnant un arrêt total ou partiel de ses activités.▪ Le PCA est un dispositif stratégique de planification et de réaction à un sinistre grave. Il expose l'ensemble des dispositifs (ressources, moyens, procédures) nécessaires au redémarrage et au retour à la normale des activités. Il est composé d'un volet métiers (Plan de Continuité des Opérations) et d'un volet technologique (Plan de Continuité Informatique). Le PCO décrit également les infrastructures de repli nécessaires à l'hébergement des activités (bâtiments, locaux, moyens matériels).▪ Il est déclenché par la cellule de crise et mis en œuvre par des équipes opérationnelles,▪ Pour être opérationnel, le PCA doit être anticipé (planification, formation, information), formalisé et régulièrement mis à jour et testé par un responsable désigné à cet effet (Maintien en condition opérationnelle).
PLAN DE CONTINUITÉ DES OPÉRATIONS (PCO)	<ul style="list-style-type: none">▪ Ensemble des ressources, moyens et procédures nécessaires au redémarrage et au retour à la normale des process et activités métier de l'Inserm
PLAN DE CONTINUITÉ INFORMATIQUE (PCI)	<ul style="list-style-type: none">▪ Le PCI traite des ressources, moyens et procédures nécessaires au redémarrage et au retour à la normale des systèmes d'information et de communication. Il décrit les dispositifs de secours informatique (appelés également solution de back up) nécessaires au redémarrage et au retour à la normale des activités informatiques : infrastructures techniques (bâtiments et locaux d'hébergement des équipements), matériels, réseaux, applications, données, compétences techniques, fournisseurs et prestataires de services, procédures de reprise des environnements, etc.
RÉSILIENCE	<ul style="list-style-type: none">▪ Capacité d'une organisation à résister à un incident, un accident, une crise dans des environnements hostiles, puis à revenir à une situation de fonctionnement normal.
STRATÉGIE DE CONTINUITÉ	<ul style="list-style-type: none">▪ Choix que fait l'Inserm des activités à privilégier au regard de leur continuité et des orientations sur l'organisation, les moyens et les responsabilités à déployer pour en assurer le redémarrage puis le retour à la normale.



2. SCENARII DE RISQUES ET IMPACTS SUR LES ACTIVITES DE L'INSERM

2.1 LES SCENARII DE RISQUES COUVERTS PAR LE PCA

2.1.1 L'arrêt des systèmes d'information et de communication

Le risque se traduit par une indisponibilité durable (2) des services informatiques et des moyens de communication délivrés quelle qu'en soit l'origine :

- Panne d'origine interne des ressources matérielles, applicatives, réseaux ou énergétiques,
- Panne d'origine externe des infrastructures publiques de communication,
- Destruction des infrastructures techniques consécutive ou non à un sinistre (incendie, explosion, inondation, catastrophe naturelle, ...),
- Acte de malveillance ou cybercriminel à l'encontre des équipements, des applications et des données (origine interne ou externe),
- Défaillance d'un prestataire de services ou d'un fournisseur critique : logiciels (lister) constructeur, opérateurs d'infrastructures critiques (énergie, télécommunication),
- Inaccessibilité des locaux techniques (mouvement social, phénomène climatique, indisponibilité des moyens de transport du fait d'une grève des transports, d'une pénurie de carburant, etc.)

Remarques :

- (1) Ne sont pas considérées comme arrêt critique des systèmes d'information et de communication toutes les interruptions temporaires allant de quelques minutes à quelques heures et qu'il convient de traiter dans le cadre d'anomalies ou d'incidents de production. Il revient aux services informatiques d'évaluer la nature d'un incident et son évolution potentielle vers une situation de crise nécessitant l'activation des dispositifs de gestion de crise et, si nécessaire, des plans de secours informatiques.
- (2) On entend par indisponibilité durable un arrêt informatique dépassant la **durée d'interruption maximale acceptable** (DIMA) pour les activités vitales de l'Inserm

2.1.2 L'indisponibilité des bâtiments et des locaux

Cette situation peut être la conséquence d'une destruction, partielle ou totale, des locaux ayant pour impact un arrêt total ou partiel des activités sur un site d'une délégation régionale ou un des sites du siège de l'Inserm :

- Siège, 101 Rue de Tolbiac, 75013 Paris
- Biopark, Biopark. 13 rue Watt, 75013 Paris
- Héron Building, 66 avenue du Maine 75014 Paris
- Datacenter de Villejuif
- Datacentre de Montpellier



Deux principaux événements sont associés à cette situation de risque :

- **L'incendie** : incident électrique, etc.
- **Le phénomène naturel** : inondation / crue centennale, pluies torrentielles, tempête, mouvements de terrain, etc.

Elle peut également être la conséquence d'une décision administrative prise par les autorités (préfet, commission de sécurité, ...) en cas de non-conformité du bâtiment avec des réglementations en vigueur en matière de sécurité des infrastructures (prévention / protection contre les incendies, systèmes d'aération ou d'évacuation de l'air, règles spécifiques IGH pour le site Paris Tolbiac) ou de santé des salariés (amiante, légionnelle, présence de polluants dans l'air, etc).

2.1.3 L'indisponibilité de personnels

Deux scénarii de risques sont identifiés :

L'indisponibilité en nombre de salariés se traduisant par un effectif insuffisant pour garantir le fonctionnement normal des activités. Cette situation peut être consécutive aux événements suivants :

- Pandémie ou épidémie,
- Intoxication alimentaire, notamment pour les sites disposant de restauration collective,
- Indisponibilité des moyens de transport du fait d'un conflit social (SNCF, RATP, mouvements sociaux, ...) ou d'une pénurie de carburant généralisée,
- Attentat produisant des victimes parmi les personnels.

L'indisponibilité de personnes clés impactant directement soit le fonctionnement de process métiers clés à court terme (processus décisionnels, experts métiers), soit un ou plusieurs axes stratégiques de développement à moyen / long terme l'Inserm (dirigeants):

- Disparition / indisponibilité brutale d'un ou plusieurs dirigeants (Direction Générale / Comité de Direction)
- Disparition / indisponibilité brutale d'experts métiers : Pôles de référence, Direction des Systèmes d'Information, ...

2.2 LES AUTRES SCENARII DE RISQUES IDENTIFIES

Même si leur probabilité d'occurrence reste faible et qu'ils ne devraient pas générer un arrêt durable des activités, ces risques sont générateurs de **situations de crise** et porteurs de **perturbations** dont les événements et le contexte dans lequel ils s'inscrivent peuvent engendrer des difficultés plus ou moins fortes dans l'accomplissement des missions du Siège de l'Inserm.

Pour cette raison, et selon la nature et gravité de la situation de crise qui peut en résulter, le dispositif de **gestion de crise** sera activé selon un mode opératoire et des priorités d'action qui seront décidés par la Cellule de Crise Stratégique de l'Inserm au moment des faits.



2.2.1 L'invasion des locaux

Le risque a potentiellement pour origine les situations suivantes :

- Manifestations diverses d'associations en adhérence avec des thématiques d'actualité entrant dans le champ de compétence de l'Inserm (exemple : expérimentation animale, vaccination, etc.)
- Manifestation sur la voie publique
- Intrusion volontaire d'un forcené ou d'un groupuscule (Violence accueil + pénétration dans les locaux)
- De manière générale, toute intrusion ou forme de violence potentielle résultant de manifestations sur la voie publique (Sites parisiens : Tolbiac, Biopark, Héron Building)

Spécificités du dispositif de maîtrise des risques en place sur le site de Paris Tolbiac :

- Respect des réglementations IGH (Immeuble de Grande Hauteur)
- Accueil sécurisé : contrôle des flux de personnes (badges d'accès pour les salariés, accès visiteurs spécifiques, accueil physique), etc.
- Procédures de Sécurité : Présence 24/7 d'un Service de Sécurité Incendie et d'Assistance à Personne et existence d'un Plan d'urgence

2.2.2 Le conflit social

Mouvement social débouchant sur un arrêt de travail d'agents opérant sur des activités sensibles (informatique, centre de référence, etc.).

2.2.3 La destruction de documents originaux et officiels

Nombreux documents officiels et contractuels sont numérisés, les pratiques de stockage varient cependant selon les procédures en vigueur dans les départements. Seuls les originaux des documents contractuels et officiels sont à produire en cas de procédure judiciaire (condition de recevabilité). Cela concerne :

- Les actes de propriété et plus généralement tous les actes notariés
- Les marchés publics et contrats fournisseurs
- Les contrats de travail
- Les contrats avec des partenaires
- Les conventions
- Les documents sociaux : PV d'Assemblée Générale, de Conseils de Surveillance et d'Administration, de Direction Générale, etc.
- ...

2.2.4 Le risque image

Le risque image est la conséquence des scénarios de risques identifiés résultants d'un sinistre ou d'une crise pouvant intervenir sur l'ensemble des activités de l'Inserm en raison des situations suivantes :

- La médiatisation de l'événement du fait de son caractère spectaculaire, exceptionnel ou du fait de son adhérence à des sujets d'actualité (ex. présence d'un terroriste parmi les personnels, exercice d'activités interdites, etc.)
- L'impact humain élevé du fait de la présence de victimes (décès, blessés, personnes choquées psychologiquement),
- L'altération brutale, forte et durable des services délivrés aux unités de recherche, se traduisant notamment par une insatisfaction croissante et un mécontentement très élevé,
- La maîtrise perfectible ou insuffisante de la communication de crise,
- La mise en cause ou l'engagement de la responsabilité pénale de l'Inserm (personne morale, dirigeants)
- L'attaque à la réputation consécutive à une ou plusieurs campagnes de dénigrement dans les médias, sur internet et sur les réseaux sociaux (agents mécontents, groupes de pression, organismes concurrents, puissances étrangères, etc.)

2.3 LES IMPACTS

2.3.1 Consécutifs a un arrêt des systemes d'information et de communication

L'arrêt total ou partiel des activités métiers et support

- L'arrêt des traitements associés aux flux financiers
- L'arrêt des activités de contrôle et de gestion des encaissements (quittancement / facturation des prestations en fin de mois. Financement de partenaires : flux évalué à fin 2017 à 300 M€/mois)
- L'arrêt des activités de gestion de la trésorerie
- L'impossibilité de verser les salaires (milieu de mois)
- L'impossibilité de procéder au règlement des fournisseurs, notamment les plus exposés aux aléas financiers (300000 factures / an).

La proximité entre la date de survenance d'un risque et le traitement d'un ou plusieurs flux financiers (échéance de paiement ou d'encaissement) constitue un facteur aggravant.

L'arrêt des activités d'expertise auprès des Pouvoirs Publics

- La difficulté à répondre à une urgence de santé publique nationale.
- L'impossibilité de tenir le Gouvernement et les pouvoirs publics informés des connaissances acquises (expertise stratégique, plan nationaux, référence en santé public) et de contribuer ainsi à la veille scientifique et à l'élaboration de la politique nationale de la recherche et de la santé.



L'arrêt potentiel des échanges d'information (via les moyens de communication : téléphonie IP, messagerie Internet, services Intranet) :

- la difficulté d'établir des communications (téléphonie fixe, mails) : collaborateurs Inserm d'autres sites, interlocuteurs externes (autorités de tutelle, administrations, partenaires, prestataires, etc.) ; et donc de répondre à des demandes urgentes de l'État,
- En période de gestion de crise : la difficulté, voire l'impossibilité, à contacter des membres de la cellule de crise, à mobiliser des ressources internes, à communiquer des instructions urgentes à des collaborateurs localisés sur des sites distants.

2.3.2 Consécutifs a une indisponibilité des bâtiments et des locaux (destruction)

La présence de victimes (morts, blessés) parmi les agents et les tiers,

L'arrêt des activités métiers et support du site, avec éventuellement pour conséquence l'arrêt des systèmes d'information et de communication dans l'hypothèse d'un sinistre à Biopark, à Villejuif ou à Montpellier

La perte d'actifs :

- La destruction d'infrastructures (bâtiments, locaux) et de matériels,
- Potentiellement, la perte de données sensibles non dématérialisées : marchés publics, états des lieux, contrats, actes officiels (registres, actes de propriété, ...), ...

Les impacts financiers¹

- La perte éventuelle de flux financiers liés à l'exploitation (encaissement – cf. arrêt informatique)
- Des coûts directs : engagements de dépenses dans le cadre de la gestion de la crise pour la sécurisation des biens et des personnes, l'assistance et les secours, des prestations diverses (expertises, huissiers, avocats) et coûts de redémarrage des activités (relocalisation temporaire : location de locaux),
- Des investissements pour le retour à la normale : relocalisation et réaménagement d'un bâtiment et de locaux définitifs.
- Des coûts indirects en relation avec l'événement : procédures judiciaires en cas de mise en cause de responsabilités, charges de travail des salariés mobilisés, etc.



2.3.3 Consécutifs a une indisponibilite de personnels

Dégradation de la qualité des services délivrés (performance)

- Retards de traitements (demandes urgentes, échéances réglementaires),
- Débordement d'activités pour les personnels mobilisés (inadéquation "volume d'activité par rapport aux ressources disponibles"),
- Génération d'erreurs plus ou moins détectables.

Dégradation des pratiques managériales et des processus décisionnels

- Altération du processus décisionnel : rupture de la chaîne de commandement, décision opérationnelle ou stratégique inopportune ou retardée, tensions avec les autorités de tutelle,
- Risque image.



3. DISPOSITIF DE GESTION DE CRISE

3.1 LES OBJECTIFS DU DISPOSITIF DE GESTION DE CRISE

Le dispositif de gestion de crise a pour finalité de réduire la durée, l'intensité et l'ampleur d'une situation de crise. Les objectifs sont doubles :

<ul style="list-style-type: none">▪ Gérer la situation d'urgence et les risques de propagation de la crise	<ul style="list-style-type: none">○ Secourir et sécuriser les biens et les personnes○ Protéger le patrimoine et l'image de l'Inserm
<ul style="list-style-type: none">▪ En cas d'arrêt des activités, planifier le redémarrage des activités jusqu'à leur retour à la normale	<ul style="list-style-type: none">○ Activer et adapter les solutions de secours prévues○ Mobiliser les ressources et les moyens matériels nécessaires au redémarrage des activités

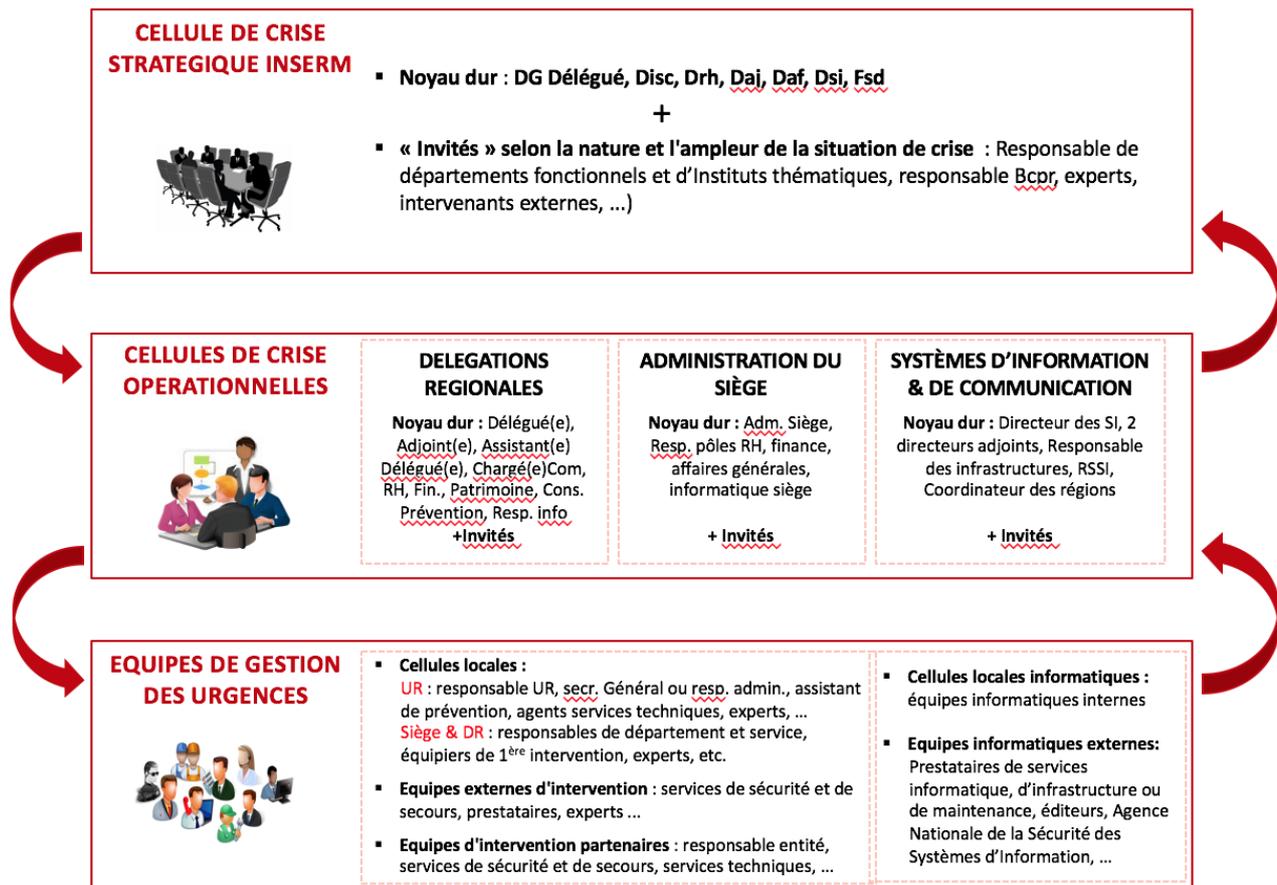
3.2 RAPPELS SUR LES PRINCIPES DE PILOTAGE D'UNE SITUATION DE CRISE

La [Fiche Réflexe FR-GC1](#) – Pilotage d'une situation de crise présente une liste des actions à mener par le pilote et les membres de la cellule de crise dans le cadre des opérations de pilotage de la crise. Les principales étapes de la gestion de crise sont également décrites dans les procédures de fonctionnement des cellules de crise.

3.3 ORGANISATION DU DISPOSITIF DE GESTION DE CRISE

3.3.1 Dispositif de gestion de crise de l'Inserm

L'organisation du dispositif de gestion de crise est articulée autour de trois niveaux d'intervention tels que représentés dans le schéma figurant en page suivante.



3.3.2 Cellule de crise stratégique de l'Inserm

La cellule de crise opère sur l'ensemble des compétences et du périmètre de responsabilité de l'Inserm. Elle est l'élément coordonnateur du dispositif général de crise, qui comprend notamment les cellules opérationnelles de crise des Délégations Régionales, de l'Administration du Siège et du Département des Systèmes d'Information. Elle se réunit sur demande de la présidence ou de la direction générale de l'Inserm selon l'évaluation faite de l'ampleur, des impacts et des enjeux d'une situation de crise avérée ou supposée. Sa mission principale est de préserver les intérêts et les actifs de l'institution en fixant des orientations ou en décidant des actions à mener pour, d'une part, réduire l'intensité et la durée d'une situation de crise, d'autre part, pour assurer la continuité des activités. Pour y parvenir, la cellule de crise mobilise les ressources et les compétences jugées nécessaires à l'atteinte des objectifs fixés.

La cellule de crise est placée sous la responsabilité du directeur général délégué ou d'un pilote désigné par lui. Le président de l'Inserm en est membre de droit. Elle est composée d'un noyau dur (directeur général délégué, directeur des ressources humaines, directeur de l'information et de la communication scientifique, directeur des affaires financières, directeur des affaires juridiques, directeur des systèmes d'information, fonctionnaire de sécurité et de défense, ou de leurs suppléants) et de personnes non prévues dans la composition de la cellule, mobilisées en fonction de la nature et de la gravité de la crise : responsables d'instituts thématiques, responsables d'autres départements ou de services, bureau central de la prévention et de la coordination des risques, experts internes / externes, ...



3.3.3 Cellules de crise opérationnelles

Organisées au sein des délégations régionales, de l'administration du siège ou du département des systèmes d'information, les cellules opérationnelles mettent en œuvre les mesures nécessaires à une sortie rapide d'une situation de crise et à la préservation des actifs de l'Inserm.

Elles assurent la supervision des cellules locales de gestion de l'urgence situées au plus près du terrain et auxquelles elles communiquent des instructions. A ce titre, passée la phase de première urgence, elles assurent l'animation, la coordination et le management des actions de sortie de crise, de redémarrage et de retour à la normale des activités.

Lorsque la cellule de crise stratégique est activée, la cellule de crise opérationnelle concernée assure un reporting auprès de celle-ci (alerte / signalement, évolution de la situation, actions engagées, ...) et un rôle d'appui par des propositions ou une prise en charge des actions de sortie de crise.

La cellule de crise opérationnelle de l'Administration du Siège assure le pilotage sur le plan organisationnel et opérationnel, des décisions et des actions permettant de préserver le capital humain, scientifique et immobilier du Siège (sites parisiens) et de résoudre le plus rapidement possible une situation de crise sur site.

La cellule de crise de chaque Délégation Régionale assure le relais en région de la cellule de crise stratégique pour des crises de haute intensité. Elle assure le pilotage sur le plan organisationnel et opérationnel, des décisions nationales et des actions permettant de préserver le capital humain, scientifique et immobilier et de résoudre le plus rapidement la situation de crise. Pour les autres crises en région, elle intervient avec pouvoir décisionnel et opérationnel.

La cellule de crise informatique est en charge de gérer et de traiter les situations de crise affectant les systèmes d'information et de communication. Elle est vouée à assurer la continuité des moyens en termes de systèmes d'information bureautiques et métiers.

3.3.4 Cellules locales de gestion de l'urgence

Elles sont activées localement (Unité de Recherche, site déporté de l'Inserm, supervision des systèmes d'information) dès survenance d'une urgence et ont pour responsabilité première d'assurer la mise en sécurité des personnels et des actifs matériels et immatériels de l'Inserm. Passée cette première phase d'urgence, elles appliquent les instructions qui leur sont transmises par les services de sécurité et de secours ainsi que par la cellule de crise opérationnelle référente.

Le responsable de chaque cellule locale de gestion de l'urgence assure une transmission régulière à la cellule de crise opérationnelle référente des informations clés sur l'évolution de la situation : actions engagées, progression des événements, résultats des mesures engagées, identification des risques, transmission à la cellule de crise des besoins en ressources et moyens supplémentaires.



Les cellules de gestion de l'urgence en UR sont constituées autour d'un **noyau dur** le plus souvent composé des profils suivants :

- Responsable de l'Unité de Recherche
- Secrétaire général ou Responsable administratif
- Assistant de prévention
- Responsable ou agent(s) des services techniques
- Expert

Durant la phase de première urgence et dans l'attente de l'arrivée des secours, elles mobilisent également les équipiers de première intervention pour encadrer l'évacuation des locaux, secourir les victimes et mettre en sécurité les installations :

- Guide-file
- Serre-file
- Coordinateur d'évacuation
- Sauveteurs Secouristes au Travail
- Equipiers d'intervention technique
- ...

3.4 COMPOSITION, RÔLES, MISSIONS ET FONCTIONNEMENT DES CELLULES DE CRISE

Trois procédures de fonctionnement des cellules de crise sont annexées au présent plan de continuité des activités : la première pour la [cellule de crise stratégique](#), la seconde pour la [cellule de crise opérationnelle de l'Administration du Siège](#) et la troisième pour la [cellule de crise opérationnelle d'une Délégation Régionale](#). Elles décrivent la composition, l'organisation et le fonctionnement de la cellule de crise stratégique et des cellules de crise opérationnelles.

Elles recensent l'ensemble des actions à réaliser dans le cadre de la gestion d'une crise selon son phasage : avant ouverture de la cellule de crise, en début de crise, en cours de crise, en fin de crise.

Ces référentiels incluent également un annuaire de crise.

A ces procédures, sont également associées des fiches action et des fiches réflexes annexées au présent document.

3.5 DÉCLENCHEMENT DE LA GESTION DE CRISE

Le déclenchement de la gestion de crise résulte d'une évaluation faite après exploitation de renseignements issus de la veille opérationnelle ou bien d'une alerte.

3.5.1 Veille opérationnelle

La veille est un processus permettant à l'Inserm d'identifier, de remonter et d'analyser des informations à caractère anticipatif relatives à une situation à risque ou à un incident (signaux faibles ou précurseurs).



Tout agent, avec l'accord de sa hiérarchie, est appelé à signaler et transmettre tout événement (aléa, incident, ...) de basse intensité potentiellement porteur d'une situation de crise.

Pour cela, la [Fiche action FR-GC1](#) (Rapport d'incident / Veille opérationnelle) doit être renseignée et communiquée par mail à l'interlocuteur spécifiquement mentionné sur la fiche (Fonctionnaire de Sécurité et de Défense, référent ou correspondant PCA, avec copie à la Direction émettrice). Les destinataires en région des rapports d'incident les retransmettent au Fonctionnaire de Sécurité et de Défense (FSD).

Le FSD prend connaissance du rapport d'incident et après consultation éventuelle du responsable du Bureau de Coordination et de Prévention des Risques, décide, avec ou sans le concours de la Direction Générale, des suites à donner : enquête et investigations complémentaires, communication pour action à un département de l'Inserm, information du pilote de la cellule de crise, etc.

Le FSD et la Direction Générale pourront également faire le choix de mettre en place une veille renforcée afin:

- d'approfondir l'incident, les questions identifiées, les causes et conséquences possibles,
- de mobiliser un état-major restreint susceptible de décider des suites à donner,
- d'activer un dispositif ad hoc de renseignement, de traitement, d'exploitation et de diffusion des informations,
- de s'assurer que les dispositifs de gestion et de communication de crise sont opérationnels si l'on a besoin de les activer et de les mobiliser
- de procéder à une pré-alerte de la cellule de crise, de cellules opérationnelles, de responsables de domaines (métiers/support) et d'experts,
- de procéder aux opérations d'anticipation : diagnostic, actions à mener, préparation d'éléments relatifs à la communication interne et/ou externe, détection des signaux impliquant le déclenchement et le basculement dans une situation de crise, détection des risques possibles de sur-accident.

Selon une fréquence à déterminer (trimestre ou semestre), le FSD communiquera à la Direction Générale une synthèse des rapports d'incidents collectés (pilotage).

3.5.2 Alerte et signalement d'un événement

Tout agent, partenaire ou prestataire, avec l'accord de sa hiérarchie, est appelé à signaler et transmettre tout événement (aléa, incident, ...) de moyenne et haute intensité potentiellement porteur d'une situation de crise :

- **En heures ouvrables (HO) : par appel téléphonique du Secrétariat de Direction** qui relaie cette information aux membres de la cellule de crise stratégique par envoi d'un sms (pré alerte sur événement non caractérisé, premier bilan, décision de réunion de la cellule de crise) et/ou envoi d'un mail à l'adresse crise@inserm.fr qui retransfère le mail vers le secrétariat de direction et le FSD.
- **En heures non ouvrables (HNO) : par appel téléphonique de la plateforme téléphonique d'un prestataire** de l'Inserm qui relaie cette information aux membres de la cellule de crise stratégique par envoi d'un sms avec accusé de réception suivi le cas échéant d'une relance téléphonique.



3.5.3 Évaluation et activation de la cellule de crise

Afin de permettre au pilote ou à son suppléant de fonder une décision sur l'opportunité d'activer ou non la cellule de crise, 3 fiches actions sont à mises à disposition pour aider à collecter des informations fiables sur l'évènement ([Fiche-action FR-GC2 Rapport de situation](#)), et d'autre part pour fournir une aide à la décision dans la perspective d'activer la cellule de crise à partir de critères relatifs à la **gravité** et à la **complexité** de la situation ([Fiche-action FR-GC3 Matrice d'évaluation d'une situation de crise](#)).

Le **premier rapport de situation** (FR-GC2) est renseigné dans les plus brefs délais par le secrétariat de direction ou la plateforme téléphonique du prestataire, puis transmis au Fonctionnaire de Sécurité de Défense, Responsable du Plan de Continuité des Activités (RPCA), son suppléant ou tout autre collaborateur désigné à cet effet par le pilote de la cellule de crise (Personnel encadrant témoin ou partie prenante de l'évènement, administrateur du siège, directeur des systèmes d'information en cas d'arrêt des S.I., etc.). Il est complété à partir des informations collectées auprès de l'émetteur de l'alerte. Le FSD complète ce document à partir des données complémentaires obtenues du terrain au travers de différentes sources internes et externes d'information (rapport des autorités de secours, prestataires). Il est ensuite transmis au pilote de la cellule de crise.

Le document est complété et mis à jour au fur et à mesure de l'évolution de la situation. Les rapports de situation sont tracés et archivés par le secrétariat de la cellule de crise.

Pour les aléas entrant dans le périmètre de la DSI la [Fiche-action FA-GC4 Assistance à l'évaluation d'une situation informatique](#) précise les évènements donnant lieu à une activation systématique de la cellule de crise informatique ainsi qu'un outil de cotation des incidents identifiés ou avérés permettant de décider de l'ouverture de la cellule de crise.

Cette cotation prend en compte plusieurs critères d'analyse (Type d'incident, étendue, impacts métiers & clients internes) et une échelle de valeur allant de 1 à 3.

Ces données doivent aussi être mises en perspectives de la criticité des applications figurant dans la fiche.

3.5.4 Gestion de la situation de crise

Les **procédures de fonctionnement des cellules de crise** (cf. annexes 1 à 3), explicitent la composition, le rôle et les missions de la cellule de crise stratégique et des cellules de crise opérationnelles.

De manière plus détaillée, la [Fiche réflexe FR-GC1 Pilotage d'une situation de crise](#) et la [Fiche réflexe FR-GC4 Check-list communication de crise](#) et le [guide de communication de crise](#) fournissent au responsable de la cellule de crise un fil directeur pour la gestion et la communication de crise.

Le livre de bord, présenté dans la [Fiche action FA-GC6](#), doit être ouvert dès l'activation de la cellule de crise. Il sera complété tout au long de la gestion de crise. Il peut être manuscrit ou dématérialisé pour en faciliter le

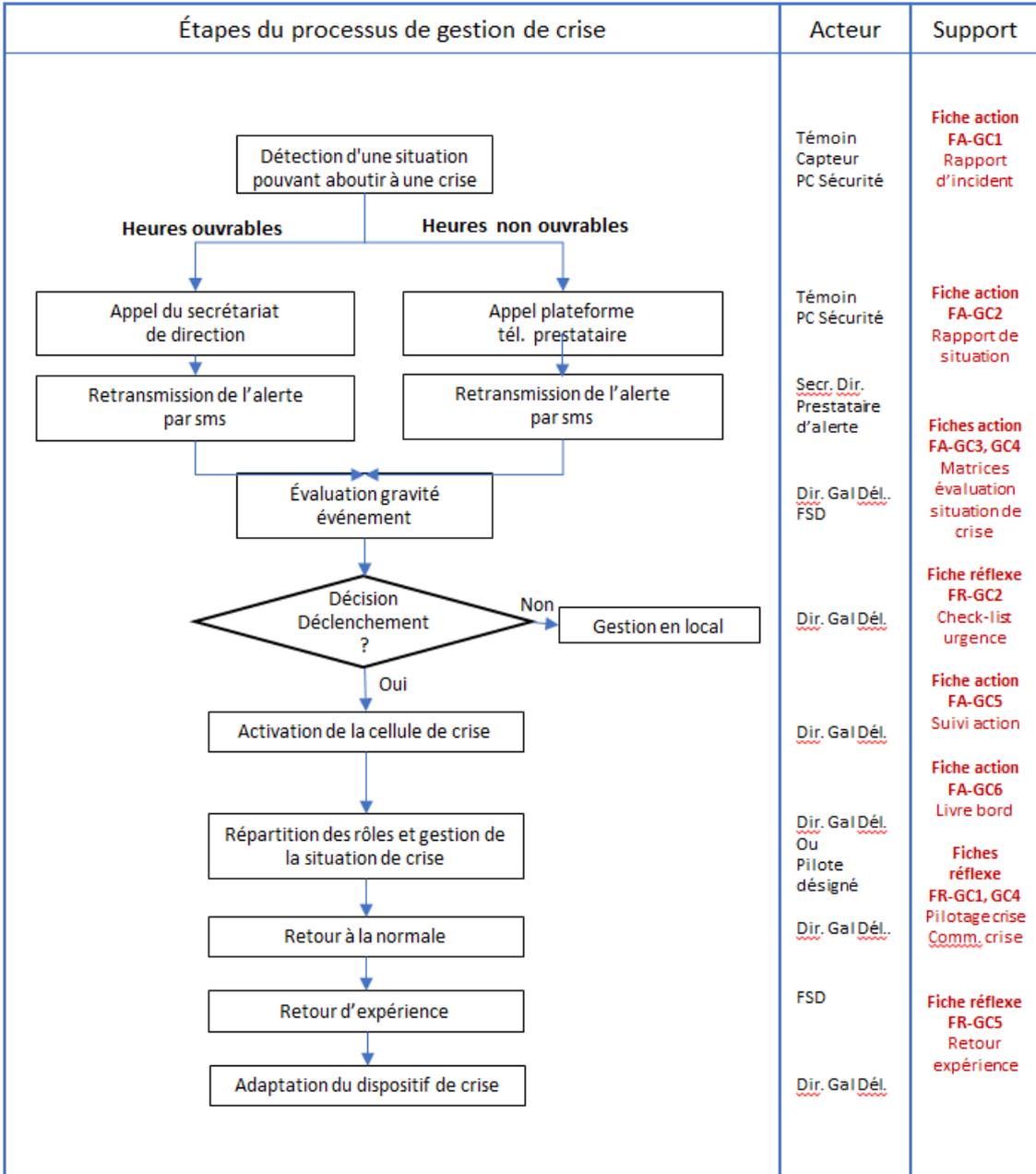


partage entre plusieurs cellules de crise. La [Fiche action FA-GC7 filtrage des appels téléphoniques](#) est utilisée pour suivre les appels téléphoniques et messages à destination de la cellule de crise.

3.5.5 Retour d'expérience

La [Fiche réflexe FR-GC5 Retour d'expérience](#) et la [Fiche action FA-GC8 Fiche événement](#) aident à conduire le retour d'expérience nécessaire à la capitalisation des enseignements et à l'amélioration continue du dispositif de crise.

Le schéma ci-dessous décrit les différentes étapes du processus de gestion de crise :





3.6 COMMUNICATION DE CRISE

3.6.1 Principes directeurs de la communication de crise à l'Inserm

La communication est une dimension essentielle dans la résolution des situations de crise. En pareille circonstance, la gestion de l'information est souvent aussi importante que la gestion de la crise elle-même. Il n'est pas rare qu'un défaut de communication ou qu'une mauvaise communication entraîne une aggravation de la situation.

La communication de crise répond à un double objectif :

- Préserver l'image et la notoriété de l'Inserm,
- Restaurer ou maintenir la confiance de tous les acteurs en situation : tutelles partenaires, fournisseurs et prestataires, journalistes et médias, public, agents, ...

Si un événement indésirable grave constitue toujours une situation sensible, il n'est pas appelé à devenir systématiquement une crise médiatique. L'organisation mise en place par l'Inserm s'inscrit dans une démarche préventive de la crise médiatique : apprécier avec discernement le risque de crise potentielle induit par chaque événement indésirable grave, en intégrant la gestion des médias comme élément de pilotage stratégique, ceci dès l'amont de l'alerte. Il est souvent possible de prévenir ou de limiter la survenue d'une crise consécutive à un événement indésirable grave en procédant de façon diligente.

C'est la raison pour laquelle la réflexion sur la stratégie de communication doit être lancée dans les premiers instants en cas de crise potentielle ou avérée. Elle doit être validée par la cellule de crise stratégique sur avis de la Direction de l'Information Scientifique et de la Communication ou par la Direction de l'Information Scientifique et de la Communication lorsque seule une cellule opérationnelle est activée. La [Fiche réflexe FR-GC4](#) fournit une check-list des actions de communication de crise. Le [guide de communication de crise](#) éclaire l'organisation et le contenu des actions de communication de crise à développer.

Si le besoin de communiquer apparaît dans le cadre d'une crise en région, la Direction de l'Information Scientifique et de la Communication se rapproche de la cellule de crise opérationnelle de la Délégation Régionale concernée. Elle définit, en lien avec son délégué régional ou son suppléant, le niveau de cette communication : niveau national ou niveau local. Elle informe la direction générale et le délégué régional concerné du déroulement et de l'effet de la gestion de la communication.

La gestion de la communication locale est privilégiée dans un premier temps. L'expérience montre en effet souvent que l'intervention du Siège induit ou accentue la perception de crise par les médias.

- La direction générale doit être informée de la situation suffisamment en amont. Elle doit également être informée du contenu de l'information susceptible d'être diffusée.
- Le délégué régional a la responsabilité de la coordination de la communication interne ou externe locale, en liaison avec la Direction de l'Information Scientifique et de la Communication qui valide les messages.



Un porte-parole peut être désigné par le pilote de la cellule de crise pour assurer la communication auprès de la presse pendant tout ou partie de la durée de la crise. Seuls le président, le directeur général délégué, le directeur de l'Information Scientifique et de la Communication et les autres porte-paroles expressément désignés sont habilités à communiquer par oral ou par écrit avec les médias.

Aucune réponse ne doit être donnée directement et «à chaud» aux demandes des médias, mais :

- il faut faire préciser la nature de la demande, la nature du support et le nom du correspondant,
- il doit être indiqué qu'il sera répondu dans les délais les plus brefs et si possible dans
- l'heure.

3.6.2 L'appui de la Direction de l'Information Scientifique et de la Communication aux Délégations Régionales

Une hot-line est activée en situation de crise par la DISC.

Cette assistance se traduit par :

- une aide pour l'évaluation de l'opportunité de communiquer au regard de la situation,
- un conseil sur les relais médias
- une aide à la formulation des messages en fonction des types de presse,
- un conseil sur le dispositif à mettre en place et sur sa graduation :
 - communiqués de presse,
 - entretiens et/ou interviews individuels,
 - encadrement et autorisations de reportages,
 - conférences et/ou points de presse.
- une veille médias. (monitoring) sur le traitement rédactionnel, audiovisuel ou Internet de la situation.

3.6.3 Missions du pôle communication de crise

Le pôle communication de crise est directement relié à la cellule de crise stratégique.

Sa mission est d'assurer la gestion des médias pendant la crise, à savoir :

- l'élaboration des messages,
- l'interface avec les porte-parole,
- les relations avec la presse,
- l'organisation des rencontres, interviews et reportages,
- la veille médias.



3.6.4 Organisation du pôle communication de crise

Le pôle communication de crise est structuré autour de 5 activités principales :

- Pilotage du pôle,
- Relations presse,
- Pilotage des sites web et des réseaux sociaux (y compris mission de veille médias),
- Communication interne,
- Veille et restauration de l'image de marque.

Le pôle est susceptible de mobiliser d'autres compétences au sein du Département de l'Information scientifique et de la Communication.

3.6.5 Évaluation du potentiel d'attractivité médiatique et questions récurrentes des médias

Cf : [Fiche-réflexe FR-GC4](#)

3.6.6 Pratique de la communication de crise

Cf : [Guide de communication de crise](#)



4. PLAN DE CONTINUITE DES ACTIVITES

Le plan de continuité des activités de l'Inserm vise à organiser le secours des activités vitales, le secours des bâtiments et des locaux et le secours des infrastructures, réseaux et systèmes d'information.

4.1 SECOURS DES ACTIVITES VITALES

Pour pallier une indisponibilité temporaire du système d'information, des bâtiments et locaux ou des personnels, des **procédures de fonctionnement dégradé** des activités vitales à reprendre sous 48 ou 72 h sont décrites dans les Fiches Réflexes PCA, présentées en annexe 5 :

- [Fiche-réflexe PCA1](#) Siège : besoins en positions
- [Fiche-réflexe PCA1.1](#) DR : besoins en positions
- [Fiche-réflexe PCA2](#) Siège : secours des activités paie
- [Fiche-réflexe PCA2.1](#) DR : secours des activités paie
- [Fiche-réflexe PCA3](#) Siège : secours des activités finance
- [Fiche-réflexe PCA3.1](#) DR : secours des activités finance
- [Fiche-réflexe PCA4](#) Siège : secours des paiements
- [Fiche-réflexe PCA5](#) Achats en état d'urgence

Ces fiches décrivent pour chaque activité vitale les solutions de secours identifiées ainsi que les plans, procédures ou modes opératoires auxquelles elles renvoient.

Dans le cadre des évolutions à venir du PCA, ces procédures pourront être enrichies (nouvelles activités vitales) et complétées pour tenir compte des modifications introduites dans l'exploitation des process (organisation, circuits de traitement et d'information, moyens alloués, changement de modes opératoires, etc.).

Au titre des actions de maintien en condition opérationnelle du PCA, les correspondants PCA des métiers sont les propriétaires des procédures de redémarrage pour leur périmètre métier. Ils seront sollicités si une mise à jour s'avérait nécessaire.



4.2 SECOURS DES BATIMENTS ET DES LOCAUX

Délocalisation

L'indisponibilité des locaux pourra amener la cellule de crise à décider la délocalisation d'une partie des personnels sur une ou plusieurs positions de repli. A titre d'exemple, le tableau suivant illustre les solutions de secours envisagées et les ressources indispensables nécessaires à la reprise d'activité d'une entité Inserm parisienne. Le détail des positions et des postes de travail est disponible dans les Fiches-reflexe PCA1 et PCA1.1. pour l'ensemble des sites.

Sites sinistrés	Sites de secours	Solutions à déployer
Tolbiac	Biopark	<ul style="list-style-type: none"> • Réquisition de bureaux (X positions) • Salles de réunion (600 m2 disponibles) • Site de repli possible pour la cellule de crise stratégique Inserm
	Héron Building	<ul style="list-style-type: none"> • Salles de réunion (~ X positions) • Site de repli possible pour la cellule de crise stratégique Inserm, la cellule de crise ADS ou d'autres activités
	Utilisation des capacités d'hébergement des Délégations Régionales parisiennes	<ul style="list-style-type: none"> ▪ Paris 5 : X positions ▪ Paris 6 : X positions ▪ Paris 7 : X positions ▪ Paris 11 : X positions ▪ Paris 12 : X positions
Biopark	Tolbiac	<ul style="list-style-type: none"> • Réquisition de bureaux (X positions) • Salles de réunion (~ X positions)
	Utilisation des capacités d'hébergement des Délégations Régionales parisiennes	<ul style="list-style-type: none"> ▪ Paris 5 : X positions ▪ Paris 6 : X positions ▪ Paris 7 : X positions ▪ Paris 11 : X positions ▪ Paris 12 : X positions
DR parisienne	Tolbiac - Biopark	<ul style="list-style-type: none"> • Réquisition de bureaux (X positions) • Salles de réunion (~ X positions)
	Utilisation des capacités d'hébergement des Délégations Régionales parisiennes	<ul style="list-style-type: none"> ▪ Paris 5 : X positions ▪ Paris 6 : X positions ▪ Paris 7 : X positions ▪ Paris 11 : X positions • Paris 12 : X positions

Télétravail

Sur décision de la cellule de crise, des personnels pourront être amenés, à titre exceptionnel et pour cause de force majeure, à travailler depuis leur domicile. Selon la nature et l'ampleur du sinistre, la cellule de crise procédera à la désignation des personnes habilitées à travailler en télétravail. Pour leur permettre d'accéder à l'environnement informatique de production, les salariés disposeront d'un accès VPN sur leur poste de travail.



4.3 SECOURS DES INFRASTRUCTURES, RÉSEAUX ET SYSTÈMES D'INFORMATION (attente PCI DSI)

Le Plan de Continuité Informatique (PCI) de l'Inserm expose l'organisation, les moyens et les procédures mis en œuvre par la Direction des Systèmes d'Information pour garantir à l'Inserm la reprise de son système informatique en cas de sinistre.

Celui-ci s'appuie sur la contractualisation d'une prestation de secours avec le Cines qui fournit à l'Inserm les infrastructures nécessaires au redémarrage des services informatiques délivrés en cas d'indisponibilité du Datacenter de Villejuif.

Les principaux dispositifs prévus par le PCI :

- Prestation de back up sur le Datacenter dU Cines, à Montpellier
 - Mise à disposition de matériels (serveurs, postes de travail, réseaux, espace de stockage) et fourniture de prestations de services (support & assistance technique, local sécurisé) ?
 - Délai de prévenance de X h ?
 - Exercice annuel ?
- Sauvegarde quotidienne des données d'exploitation (restauration des données à J - 1),
- Secours de la messagerie et de la téléphonie sous 72h (?)
- Matériels de secours disponibles (spares) :
 - X postes de travail (besoin de 50 postes ou portables sous un délai de 72heures + 50 postes de travail ou portables sous un délai maximum de 2 semaines)
 - Plusieurs serveurs
- Solution technique de télétravail opérationnelle : capacité à supporter plus de 100 utilisateurs en simultané à tester
- Procédures formalisées de restauration des environnements de production :
 - Secours des réseaux (LAN & Wan)
 - Secours des locaux et des équipements (data center x 2)
 - Secours des environnements de production (données et applications)
 - Procédures de restauration éventuelles
- Engagements de service contractuels et PCA des fournisseurs critiques ? : à lister
 - Infogérance des postes de travail : Pro Servia
 - Infogérance des infrastructures nationales (Datacenter de Villejuif et Cines) : Open
 - Tierce maintenance applicative : Atos
 - Gestionnaire de réseau : Renater



- Télécommunications : SFR
 - Gestionnaire des locaux du Datacenter de Villejuif : DR Paris 11
 - Prestataire de Facility Management des locaux Biopark : ?
 - Maintenance du Datacenter (alarme incendie) : ?
 - Maintenance des équipements de communication : Nextiraone
 - ...
- Plan de test et d'exercice du PCI

5. OBJECTIFS DE REDEMARRAGE ET STRATEGIE DE CONTINUITE

5.1 LES BESOINS DE CONTINUITÉ ET LES OBJECTIFS DE REDÉMARRAGE

5.1.1 Les activités entrant dans le cadre de la gestion de l'urgence (h+8)

Activités	SIÈGE	ADS	DR
Pilotage de la crise (redémarrage de la chaîne de commandement)			
▪ Activation / animation des cellules de crise (stratégique, opérationnelles)	X	X	X
▪ Mobilisation des moyens et des ressources nécessaires	X	X	X
▪ Gestion de la communication de crise (stratégie, relations presse, Internet et réseaux sociaux, veille média et e-réputation, communication interne)	X	X	X
▪ Décision d'activation des plans de secours (redémarrage aude activités)	X	X	X
Informatique (cas des situations de crise informatique)			
▪ Pilotage de la cellule de crise informatique (mobilisation des ressources et des compétences, communication)	X	X	X
▪ Mobilisation des ressources et des compétences en vue de la remise en état des infrastructures, serveurs, réseaux et moyens de communication (téléphonie fixe & mobile, messagerie, intranet) : évaluation des impacts, analyse / investigation des systèmes en arrêt, intervention / réparation	X		X
▪ Prise de décision quant à la mise en œuvre des solutions de secours informatique (Plan de continuité informatique, télétravail)	X		
▪ Supervision des infrastructures de production	X		
▪ Moyens de communication : téléphonie IP, messagerie, intranet	X		
Affaires générales (cas des situations d'indisponibilité des locaux)			
▪ Logistique de la cellule de crise		X	X
▪ Remise en état des environnements de travail		X	X
▪ Préparation du redéploiement d'équipes sur un autre site		X	X
▪ Gestion des accès (badges, sécurité)		X	X
Ressources humaines (cas des situations de crise exposant les personnels à des risques professionnels)			
▪ Expertise en santé et sécurité au travail (prévention et coordination des risques)		X	X
Sécurité et Défense			
▪ Coordination des mesures de sûreté et interface avec les autorités compétentes (Hauts Fonctionnaires de Défense et de Sécurité, SGDSN, services du Ministère de l'Intérieur ou des Armées, etc.)	X		X
▪ Expertise stratégique de sécurité nationale (OIV)	X		



5.1.2 Les activités à reprendre dans un délai maximal de 24 à 72 h

Activités	SIÈGE	ADS	DR
Finance			
▪ Gestion de trésorerie : consultation et pilotage de la trésorerie			X
▪ Traitement des demandes urgentes d'achat dans le cadre de la gestion d'une situation de crise (accord d'engagement de dépense, émission d'un bon de commande)	X		X
▪ Réalisation d'opérations sur les comptes (décaissements urgents : salaires, fournisseurs)	X		X
Agence comptable			
▪ Visa dépenses et télétransmissions à la DGFIP	X		
Ressources humaines			
▪ Traitement de la paie et versement des salaires	X		
▪ Relations sociales en lien avec la situation de crise	X		X
Informatique			
▪ Redémarrage des services sur site principal ou secondaire après activation du plan de secours informatique :	X	X	X
▪ Finance / Gestion de trésorerie : SaFIR	X		X
▪ RH / Paie : Sirène	X		X
▪ Gestion des tickets d'incident	X		X
▪ Maintenance en conditions opérationnelles des infrastructures		X	X
▪ Infogérance des postes de travail (prestation externalisée)		X	X
▪ Architecture et méthodes		X	X
Information scientifique et communication			
▪ Relations presse	X		X
▪ Communication web et médias sociaux	X		X
▪ Communication interne	X		
Affaires générales (Administration du Siège)			
▪ Accueil téléphonique		X	X
▪ Accueil physique : orientation dans les locaux de repli		X	X
▪ Gestion du courrier		X	X
▪ Gestion de crise : préparation du relogement des équipes sur les sites de secours : préparation des locaux, création des badges d'accès, travaux résiduels d'aménagement		X	X



5.1.3 Les activités à reprendre dans un délai maximal de 1 à 2 semaines

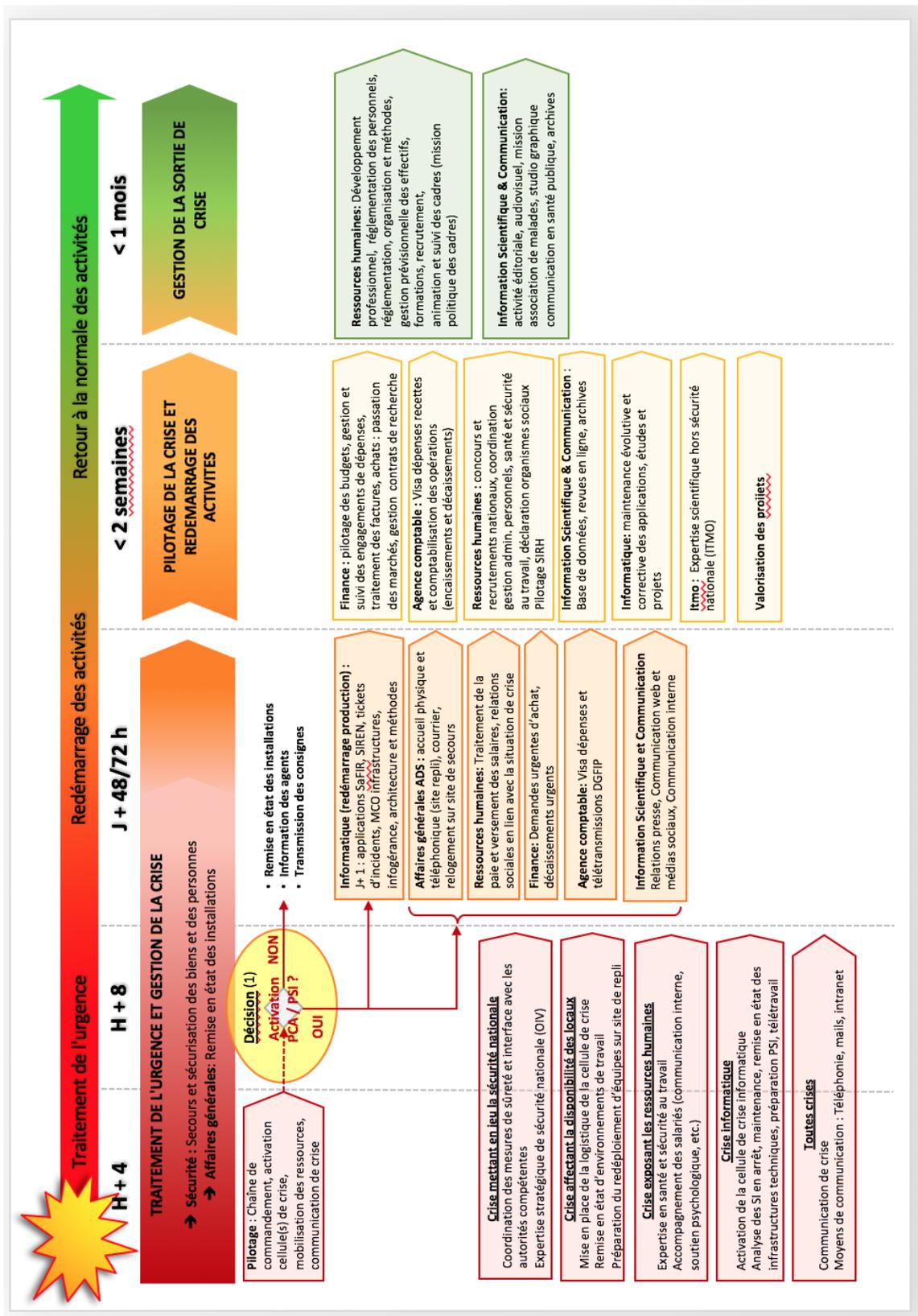
Activités	SIÈGE	ADS	DR
Finance			
▪ Gestion budgétaire : pilotage des budgets, gestion et suivi des engagements de dépenses	X		X
▪ Traitement des factures (gestion du circuit d'enregistrement, liquidation, traitement / gestion des échéanciers de paiement)	X		X
▪ Achats : passation des marchés	X		X
▪ Cellule Tiers	X		X
▪ Gestion des contrats de recherche	X		X
Agence comptable			
▪ Visa dépenses recettes et comptabilisation des opérations (encaissements et décaissements)	X		
Ressources humaines			
▪ Développement professionnel : concours et recrutements nationaux	X		
▪ Coordination de la gestion administrative des personnels	X		X
▪ Santé et sécurité au travail (hors gestion de crise)	X		X
▪ Déclaration aux organismes sociaux			
▪ Pilotage du système d'information de gestion des ressources humaines	X		X
Informatique			
▪ Vie applicative : maintenance évolutive et corrective des applications	X		
▪ Etudes et projets	X		
Information scientifique et communication			
▪ Base de données, revues en ligne, archives	X		
Expertise scientifique hors sécurité nationale			
▪ ITMO	X		



5.1.4 Les activités à reprendre sous un mois

Activités	SIÈGE	ADS	DR
Ressources Humaines			
▪ Développement professionnel : Réglementation des personnels, organisation et méthodes	X		X
▪ Réglementation, organisation et méthodes	X		
▪ Gestion prévisionnelle des effectifs : études et enquêtes, bilan social, suivi d'exécution de la masse salariale	X		X
▪ Formations scientifiques et soutien à la recherche	X		X
▪ Formations (administration du siège)		X	
▪ Recrutement (administration du siège)		X	
▪ Animation et suivi des cadres (mission politique des cadres)	X		
Information scientifique et technique			
▪ Activité éditoriale	X		
▪ Audiovisuel	X		
▪ Mission association de malades	X		
▪ Studio graphique	X		
▪ Communication en santé publique	X		
▪ Archives	X		

5.2 PLAN GÉNÉRAL DE REDÉMARRAGE ET DE RETOUR À LA NORMALE



- **Décision** : Au regard des impacts de l'événement sur la continuité des activités (indisponibilité > 72h des infrastructures, des ressources ou des services informatiques), la cellule de crise doit prendre la **décision d'activation du PCA** (repli sur les sites de secours, déploiement du PCI, mobilisation des équipes) dans un **délai maximum de 8h** suivant le début de la crise afin de permettre aux équipes de procéder à un redémarrage des activités vitales dans un délai de 48/72h maximum.



5.3 LES BESOINS EN RESSOURCES CRITIQUES

5.3.1 Synthèse des besoins en positions (hors gouvernance)

On entend par position un poste de travail utilisateur complet (local de travail + agent + bureau équipé + outils informatiques). Les activités des instituts thématiques ne sont pas pris en compte dans les décomptes suivants.

Les données suivantes comptabilisent les ressources humaines, les postes de travail et les surfaces de bureau (hors locaux techniques, halls, couloirs et dégagements, salles de pause, etc.) nécessaires en cas d'indisponibilité du site Tolbiac ou Biopark aux différentes échéances de reprise d'activité :

Sous 8 heures maximum :

Activités	Salle	Bureaux
Siège Tolbiac sinistré : 19 positions, 2 salles de crise, 3 bureaux		
▪ Cellule de crise stratégique	Salle 12 positions de 40 m ²	2 bureaux de 15 m ²
▪ Cellule de crise ADS	Salle 7 positions de 25 m ²	1 bureau de 15 m ²
Biopark sinistré : 10 positions, 2 bureaux		
▪ Cellule de crise informatique	Salle 10 positions de 30 m ²	2 bureaux de 12 m ²

Sous 72 heures maximum :

Activités	Positions	Bureaux
Siège Tolbiac sinistré : 24 positions, 11 bureaux ou espace +175 m²		
▪ Finance	2	1 bureau ou espace 15 m ²
▪ Agence comptable	2	1 bureau ou espace 15 m ²
▪ Ressources humaines	4	2 bureaux ou espace 20 m ²
▪ Adm. Siège RH	2	1 bureau 10 m ²
▪ Adm. Siège Aff. Gales	5	3 espaces : 5, 20 et 25 m ²
▪ Adm. Siège Informat.	5	2 bureaux + espace 20 m ²
▪ Adm. Siège Finance	-	-
▪ Information et com.	4	2 bureaux ou espace 20 m ²
Biopark sinistré : 12 positions, 4 bureaux ou espace 60 m²		
▪ DSI	12	4 bureaux ou espace 60 m ²

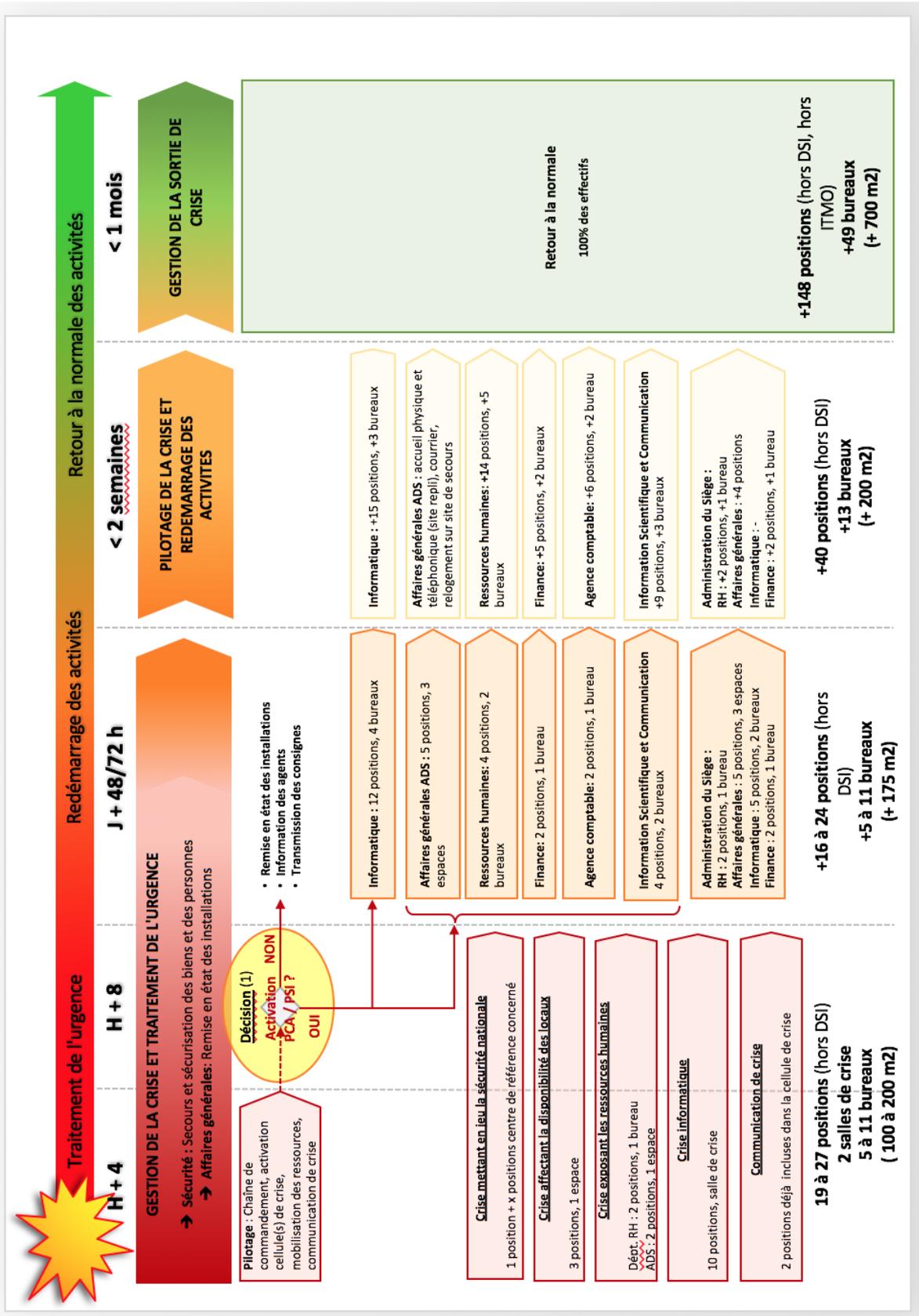


Sous 1 à 2 semaines maximum :

Activités	Positions	Bureaux
Siège Tolbiac sinistré : +40 positions, + 13 bureaux ou espaces +180 m2		
▪ Finance	+5	+2 bur. ou + espace 25 m2
▪ Agence comptable	+6	+2 bur. ou + espace 30 m2
▪ Ressources humaines	+14	+5 bur. ou + espace 70 m2
▪ Adm. Siège RH	+2	+1 bur. ou + espace 10 m2
▪ Adm. Siège Aff. Gales	+4	3 espaces : 5, 20 et 25 m2
▪ Adm. Siège Informat.	-	2 bureaux + espace 20 m2
▪ Adm. Siège Finance	-	-
▪ Information et com.	+9	+3 bur. ou + espace 45 m2
Biopark sinistré : +15 positions, + 3 bureaux ou + espaces 45 m2		
▪ DSI	+15	+3 bur. ou + espace 45 m2

Sous 1 mois maximum :

Activités	Positions	Bureaux
Siège Tolbiac sinistré : +40 positions, + 13 bureaux ou espaces +180 m2		
▪ Finance	+41	+14 bur. ou + esp. 200 m2
▪ Agence comptable	+8	+3 bur. ou + espace 40 m2
▪ Ressources humaines	+61	+20 bur. ou + esp. 300 m2
▪ Adm. Siège RH	+4	+1 bureau ou espace 20 m2
▪ Adm. Siège Aff. Gales	-	-
▪ Adm. Siège Informat.	-	-
▪ Adm. Siège Finance	-	-
▪ Information et com.	+34	+11 bur.ou + esp. 150 m2
Biopark sinistré : +15positions, + 3 bureaux ou + espaces 45 m2		
▪ DSI	-	-
▪ Instituts thématiques	-	-





5.3.2 Détail des besoins en positions et autres ressources

- Cf [Fiche réflexe FR-PCA1 Siège besoins en positions](#)

5.3.3 Fournisseurs critiques

La liste des fournisseurs critiques doit être établie et documentée par les correspondants PCA dans les procédures [Fonctionnement de la cellule de crise stratégique](#), [Fonctionnement de la cellule de crise opérationnelle DR](#) et [Fonctionnement de la cellule de crise ADS](#).

5.3.4 Données critiques

Ce chapitre dresse par fonction une liste de données vitales ou sensibles dont la disponibilité est indispensable pour gérer une situation de crise et procéder aux opérations de redémarrage des activités. Lorsqu'elles sont dématérialisées (cas le plus fréquent), ces données sont sauvegardées et peuvent être restaurées dans le cadre du PSI selon un délai qui ne doit pas excéder 72 h. Lorsqu'elles sont dématérialisées où qu'elles doivent être disponibles dans un délai inférieur à 72h, leurs propriétaires devront anticiper leur indisponibilité éventuelle en procédant à une sauvegarde stockée dans un lieu sécurisé.

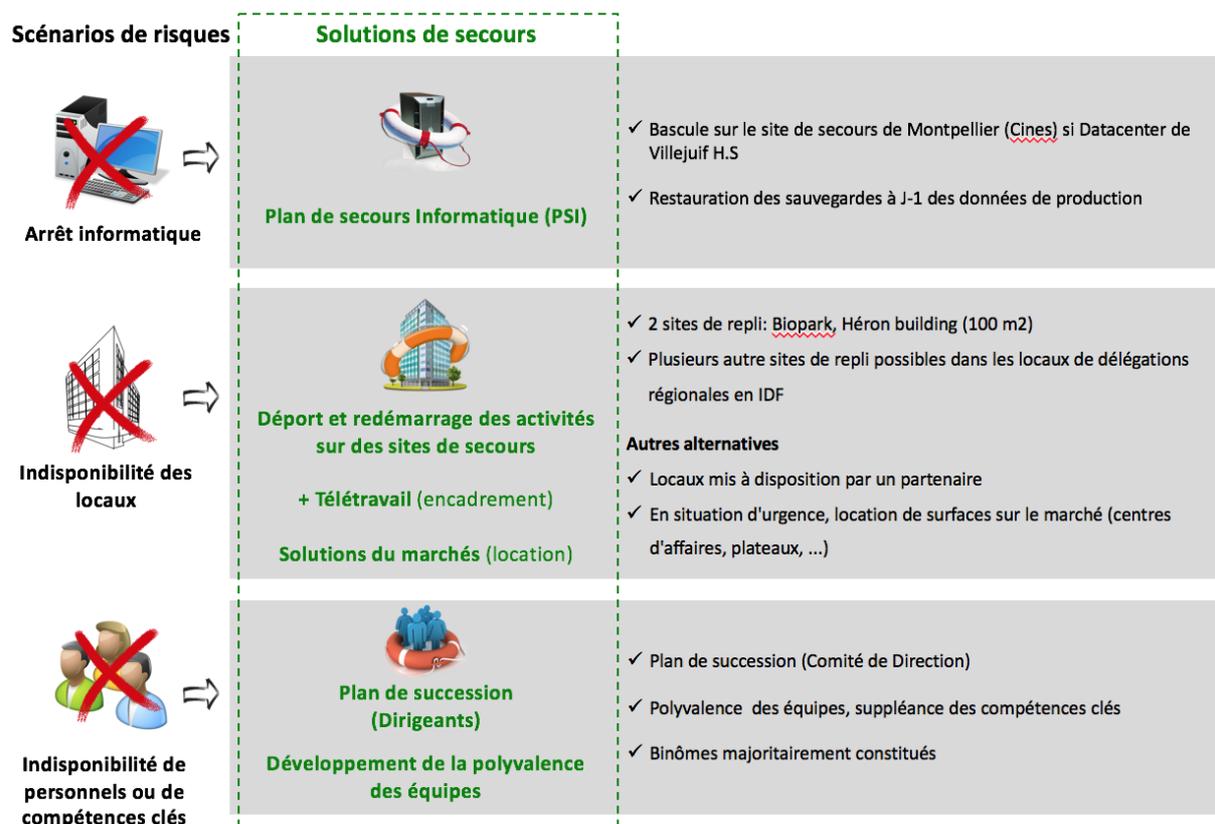
FONCTIONS	DONNEES CRITIQUES	OBJECTIFS (Gestion de crise / continuité)
Ressources Humaines	<p>Contrats de travail et avenants</p> <p>Annuaire de tous les salariés avec les coordonnées d'une personne à contacter (Avec l'accord du salarié et en conformité avec les obligations CNIL)</p> <p>Procédure de connexion à la plateforme DGFIP + sauvegarde des habilitations, des identifiants et des codes d'accès</p> <p>Délégations et échéancier de signature</p> <p>Chéquiers de secours</p>	<ul style="list-style-type: none"> ▪ Etre en mesure de produire le document contractuel (cas de litige avec un agent) ▪ Avoir connaissance des informations nécessaires au calcul de la rémunération et au versement des salaires (fonctionnement dégradé) ▪ Gestion administrative des salariés, versement des salaires ▪ Disposer d'une liste des salariés présents sur chaque site pour en situation de crise : <ul style="list-style-type: none"> ○ Etre en mesure de recenser les salariés présents ○ Contacter le salarié ou une personne désignée par lui ▪ Gestion de trésorerie : Gérer et contrôler les flux financiers ▪ Procéder à des opérations d'encaissements et de décaissements ▪ Identifier les collaborateurs ayant la délégation de signature avec leur montant d'engagement ▪ Identifier les échéances de paiement ▪ Etre en mesure de procéder à des paiements d'urgence en situation de crise
Finance		
Achats	<p>Annuaire des fournisseurs critiques</p> <p>Documents signés des marchés publics</p>	<ul style="list-style-type: none"> ▪ Disposer d'une liste des fournisseurs critiques de l'Inserm précisant les coordonnées et les points de contacts ▪ Etre en mesure de produire le document contractuel en cas de litige ou de contestation avec un fournisseur ▪ Prendre connaissance des conditions contractuelles en cas d'arrêt informatique
Moyens Généraux	<p>Annuaire des fournisseurs et prestataires critiques (+ liste de substitution) précisant les coordonnées des prestataires ou artisans pouvant intervenir en situation d'urgence (maintenance, nettoyage, gardiennage,...)</p> <p>Dossier de site à jour</p> <p>Baux, états des lieux, conventions d'hébergement</p>	<ul style="list-style-type: none"> ▪ Etre en mesure de missionner en urgence un prestataire pour remettre en état des infrastructures, des installations ou des équipements critiques ▪ Transmettre aux services de secours et d'urgence, dès le début de leur intervention, les informations topographiques, techniques et organisationnelles indispensables de chaque site (plans de masse et de situation, localisation des équipements techniques, ...) ▪ Etre en mesure de produire le document contractuel en cas de litige ou de contestation avec un bailleur
Informatique	<p>Procédures critiques de production des systèmes : documentation technique et utilisateurs, procédure de paramétrage, de redémarrage des systèmes de production, etc.</p> <p>Documentation contractuelle des fournisseurs et prestataires critiques : contrats et annexes contractuelles (engagements de services), PSI, annuaire</p> <p>Procédure de télétravail</p>	<ul style="list-style-type: none"> ▪ Procéder au redémarrage des différents environnements informatiques : réseaux, systèmes, applicatifs, données, postes de travail utilisateur, ... • Informer et solliciter en urgence l'intervention des fournisseurs • En cas de défaillance du fournisseur : <ul style="list-style-type: none"> ○ Prendre connaissance de la procédure et des conditions de redémarrage et de retour à la normale ○ Identifier les modalités de gestion de la relation en situation de crise ▪ Permettre aux collaborateurs devant travailler depuis leur domicile d'accéder à l'environnement de travail informatique
Juridique	<p>Actes officiels (titres de propriété, conventions, servitudes, procès verbaux, délibérations, registres des Conseils, dossiers Assurances...)</p>	<ul style="list-style-type: none"> ▪ Etre en mesure de produire les documents officiels et originaux



6. STRATEGIE DE CONTINUTE DES ACTIVITES : PRINCIPES RETENUS

6.1 Siège

Le redémarrage des activités prend appui sur les solutions de secours suivantes :



Arrêt du système d'information et de communication > 24 heures : activation du Plan de Continuité Informatique et du back up basé sur le Datacenter de Montpellier.

Indisponibilité de bâtiments et de locaux : redéploiement des activités et repli des effectifs nécessaires au redémarrage sur les sites disponibles (Tolbiac, Biopark, Héron Building ou Délégations Régionales parisiennes) et activation du télétravail

Indisponibilité de personnels :

- **Dirigeants** : activation du plan de succession (Direction Générale et Comité de Direction)
- **Experts** : suppléance organisée (binômes)
- **Personnels** : mise en œuvre de la polyvalence au sein des équipes.



6.2 Délégation régionale

Le redémarrage des activités d'une Délégation Régionale prend appui sur les solutions de secours selon le même principe que 6.1. Les modalités de ré déploiement sont adaptées en fonction des caractéristiques et de l'environnement de chaque région.





7. MAINTIEN EN CONDITION OPERATIONNELLE

7.1 PRÉAMBULE

Le **maintien en condition opérationnelle du PCA (MCO)** et des dispositifs de gestion et de communication de crise ne saurait dépendre seulement de son référentiel et de la documentation qui s'y rattache.

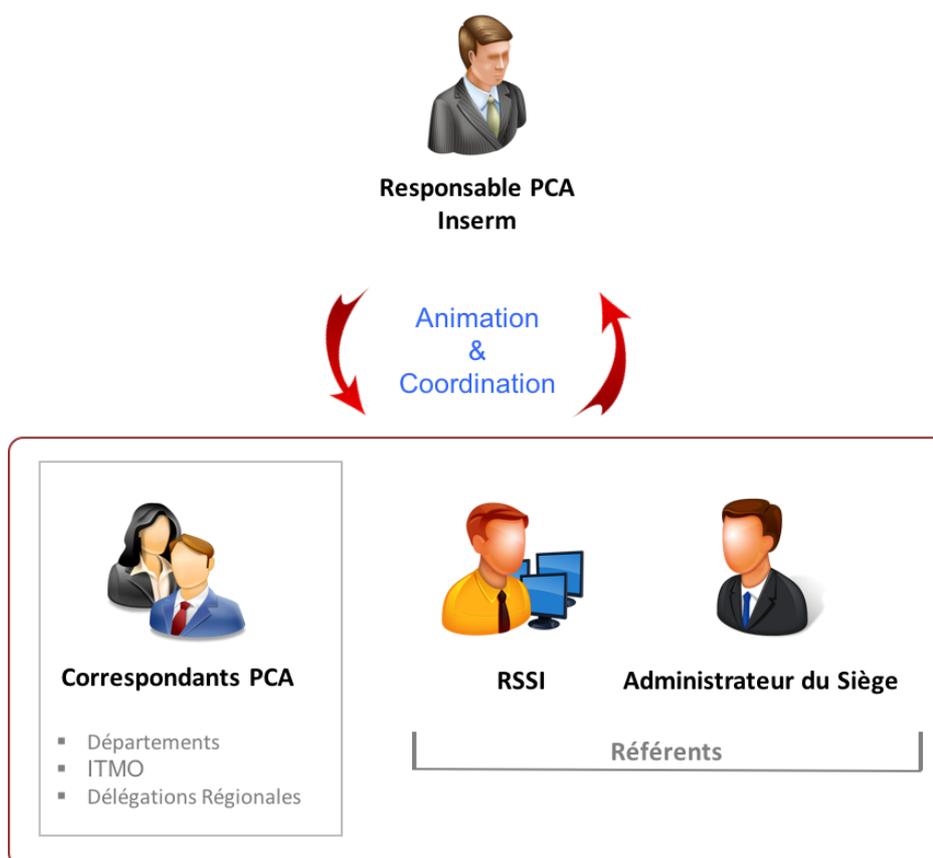
L'efficacité des solutions prévues dépend avant tout de la **préparation des hommes** et de l'**opérationnalité** des mesures et moyens mis en œuvre ou prévus.

Trois actions concourent à cet objectif :

La MCO du plan de continuité, en particulier la mise à jour des informations et des dispositifs prévus,
La formation des principaux acteurs en situation (membres des cellules de crise),
La réalisation régulière d'exercices et de simulations (sur table ou en grandeur réelle), ...

Remarque : les programmes d'actions relatifs à la formation et aux exercices de crise ne sont pas présentés dans le plan de continuité des activités

1.5. MCO : ORGANISATION GÉNÉRALE





7.2 RÔLES ET MISSIONS

7.2.1 Responsable PCA Inserm (RPCA)

Le Responsable PCA (FSD) est en charge du **pilotage du PCA**, de son **animation** de sa **maintenance** au sein de l'Inserm. En situation de crise, le RPCA est également le Coordinateur en charge de la logistique et du bon fonctionnement de la cellule de crise. Il est également contributeur à la résolution de la situation de crise, notamment au travers des actions de coordination des travaux de redémarrage et de gestion de la crise entre la Cellule de Crise Stratégique et les cellules opérationnelles métiers ou les cellules de crise régionales.

Ses principales missions sont les suivantes :

1. La définition et la proposition à la Direction Générale d'une **politique de continuité** adaptée aux enjeux de l'Inserm,
2. **L'animation et la coordination des plans d'action** en relation avec les correspondants PCA métiers, le RSSI et l'Administration du Siège : conception / déploiement des solutions de continuité, sensibilisation, information et formation des parties prenantes, maintenance des dispositifs, etc.
3. Le **maintien en condition opérationnelle** du PCA et des dispositifs de gestion et de communication de crise déployés au sein de l'Inserm :
 - Contrôle de la conformité des dispositifs internes et externes en place,
 - Tests régulier des dispositifs et organisation d'exercices de crise,
 - Mise à jour régulières du référentiel PCA, de la documentation associée et des moyens matériels mis en place.

7.2.2 Correspondants PCA et référents

Le Correspondant PCA est l'interlocuteur désigné pour toutes les questions relatives à la continuité des processus et des activités métiers de son périmètre fonctionnel. En coordination avec le RPCA Inserm, il assure l'évolution et la maintenance des solutions de continuité et de fonctionnement dégradé.

Ses missions recouvrent :

- L'évaluation des impacts et des besoins d'évolution de tout ou partie des dispositifs de continuité au regard des modifications observées ou à venir de son périmètre d'activité, en particulier des procédures métiers nécessaire au redémarrage des activités
- Le contrôle et l'auditabilité des PCA et des objectifs de redémarrage des fournisseurs et prestataires critiques
- La participation aux plans d'action relatifs au déploiement et à la maintenance du PCA en coordination avec le RPCA Inserm.

7.2.3 Coordonnées

Les coordonnées du responsable, des correspondants et des référents PCA sont mentionnées dans les procédures de fonctionnement des cellules de crise stratégique et opérationnelles.



8. CONTINUITÉ DES FOURNISSEURS CRITIQUES

Le redémarrage et le retour à la normale des activités de l'Inserm sont conditionnés à la permanence des services délivrés par les fournisseurs classifiés "critiques" au regard de la continuité des activités de l'Institution (informations détaillées dans les procédures de fonctionnement des cellules de crise). Cela passe par l'existence de dispositifs de gestion de crise et de continuité des activités parmi les fournisseurs et prestataires identifiés comme critiques. Les PCA doivent être opérationnels c'est à dire testés, auditables et conformes aux objectifs et conditions de redémarrage des activités de l'Inserm.

Pour cela, les actions suivantes sont à réaliser dans le cadre du maintien en condition opérationnelle :

Vérifier dans les contrats de prestations existants la présence de clauses relatives aux dispositifs PCA mis en place par le prestataire :

- La définition des engagements de service en matière de redémarrage des prestations délivrées en cas d'interruption des activités chez le prestataire (SLA). En cas d'inexécution, la portée juridique des responsabilités ainsi que les couvertures d'assurance seront évaluées à cette occasion,
- La communication à l'Inserm du PCA mis en place et précisant notamment :
 - Les scénarios de crise retenus, le niveau d'exposition du prestataire et les impacts sous-tendus pour l'Inserm (conséquences),
 - Les dispositifs de prévention et de protection déployés (Plan de Maîtrise des Risques),
 - Les dispositifs de continuité et de fonctionnement dégradé prévus,
 - Les dispositifs de gestion de crise avec identification des circuits d'information, des interfaces et des points de contact en cas de sinistre,
 - Les indicateurs clés de performance (KPI) permettant d'apprécier et de suivre le niveau de qualité et de continuité du service délivré.
 - Les actions récurrentes à réaliser pour s'assurer de l'opérationnalité et de l'auditabilité de ces dispositifs.

A défaut, et plus largement pour tout nouveau contrat de service, demander aux Directions métiers de l'Insermet/ou aux acheteurs, d'intégrer ces clauses spécifiques en matière de continuité des activités.

Procéder régulièrement (au mois une fois tous les 12 à 18 mois) à un contrôle des dispositifs prévus par le fournisseur :

- Audit du PCA du prestataire (questionnaire d'auto-évaluation, visite de site(s),
- Revue du contrat de services et des dispositifs PCA du prestataire pour intégrer les éventuelles évolutions
- Participation à des tests, des exercices ou des simulations



9. ACTIONS RECURRENTES A MENER DANS LE CADRE DE LA MCO DU PCA DE L'INSERM

En coordination avec les Correspondants et Référénts PCA, le RPCA de l'Inserm prend les mesures nécessaires à l'opérationnalité du PCA conformément à la politique de continuité de l'Inserm et aux orientations ou décisions instruites par le Président et le Directeur Général.

Dans cette perspective, le RPCA rend compte annuellement des actions entreprises et à mener.

Travaux annuels à mener dans le cadre de la MCO

Thèmes	Actions	Responsable(s)
Procédure d'alerte et de signalement	<ul style="list-style-type: none"> ▪ Contrôler et actualiser les procédures d'urgence de chaque site : organisation, circuits d'information, conduites à tenir, coordonnées des secours, ▪ Dresser un retour d'expérience et intégrer les éventuelles modifications consécutives à des exercices incendie ou d'évacuation réalisés depuis la dernière revue du PCA ou si des incidents notables se sont déroulés. 	RPCA + Administrateur du Siège
Cellules de crise	<ul style="list-style-type: none"> ▪ Contrôler et mettre à jour l'annuaire de crise ainsi que la composition des cellules de crise pour prendre en compte les évolutions de la gouvernance de l'Inserm (FR8-Annuaire de crise) + actualisation éventuelle des sites de repli des cellules de crise, ▪ Formation / Exercices : construire et planifier le programme de formation et d'exercice de crises, ▪ Dans l'hypothèse de l'existence d'une salle de crise dédiée, procéder à un contrôle du fonctionnement des équipements et des matériels 	RPCA Inserm + Administrateur du Siège
Revue annuelle du PCA	<ul style="list-style-type: none"> ▪ Selon les besoins, procéder à une actualisation du périmètre du PCA, des scénarios de risques et de leurs impacts sur la continuité des activités de l'Inserm, ▪ Vérifier la conformité des stratégies de continuités déployées ▪ Faire procéder par les correspondants PCA de chaque métier (ou filiales) à un contrôle et une actualisation thématiques suivantes : <ul style="list-style-type: none"> ○ Activités critiques ○ Objectifs de redémarrage ○ Ressources critiques : nombre de positions nécessaires, compétences clés, moyens informatiques ○ Solutions de contournement ou de fonctionnement dégradée des activités vitales (en cas d'arrêt informatique) ○ Procédures / modes opératoires métiers à joindre au PCA ○ Annuaire et PCA des fournisseurs critiques 	RPCA + Correspondants PCA métiers / DR



Thèmes	Actions	Responsable(s)
Revue annuelle du PSI	<ul style="list-style-type: none">▪ Faire procéder par la DSI à un contrôle et une actualisation des PSI :<ul style="list-style-type: none">▪ Périmètre couvert / non couvert, scénarios de risques identifiés, impacts▪ Solutions de secours déployées▪ Inventaire et actualisation éventuelle des procédures techniques de redémarrage jointes aux PSI▪ Actualisation des dispositifs de gestion des crises informatiques : membres et coordonnées des cellules de crise informatiques, procédure d'alerte et de signalement des incidents techniques, annuaire et PCA des fournisseurs et prestataires critiques,▪ Tests / exercices de continuité :<ul style="list-style-type: none">○ Dresser un bilan et un REX des tests / exercices menés○ Annexer au PSI le planning et les conditions de réalisation du programme à venir	RPCA + DSI + RSSI
Bâtiments et locaux de secours	<ul style="list-style-type: none">▪ Procéder à une actualisation des sites de secours (redémarrage des activités)<ul style="list-style-type: none">○ Coordonnées, accès, positions disponibles, ...○ Nouveaux sites○ Besoins en aménagement et en équipements	RPCA + Administrateur du Siège
Communication de crise	<ul style="list-style-type: none">▪ Procéder à une revue et une actualisation éventuelle du guide et des procédures de communication de crise + annuaire : journalistes, relations publiques▪ Etablir et planifier le programme de média-training	RPCA + DISC

ANNEXE 1

Procédure de fonctionnement de la cellule de crise stratégique

DIFFUSION RESTREINTE

- [Procédure de fonctionnement de la cellule de crise stratégique](#)

ANNEXE 2

Procédure de fonctionnement de la cellule de crise opérationnelle

DR et Administration du Siège

DIFFUSION RESTREINTE

- [Procédure de fonctionnement de la cellule de crise ADS](#)
- [Procédure de fonctionnement de la cellule de crise DR BORDEAUX](#)
- [Procédure de fonctionnement de la cellule de crise DR LILLE](#)
- Procédure de fonctionnement de la cellule de crise DR LYON
- Procédure de fonctionnement de la cellule de crise DR NANTES
- Procédure de fonctionnement de la cellule de crise DR MARSEILLE
- Procédure de fonctionnement de la cellule de crise DR MONTPELLIER
- Procédure de fonctionnement de la cellule de crise DR TOULOUSE
- Procédure de fonctionnement de la cellule de crise DR STRASBOURG

- [Procédure de fonctionnement de la cellule de crise DR PARIS 5](#)
- Procédure de fonctionnement de la cellule de crise DR PARIS 6
- Procédure de fonctionnement de la cellule de crise DR PARIS 7
- [Procédure de fonctionnement de la cellule de crise DR PARIS 11](#)

ANNEXE 3

FICHES ACTION

(Documentation utilisable en situation de crise)

- [Fiche-action GC1](#) [Rapport d'incident / veille opérationnelle](#)
- [Fiche-action GC2](#) [Rapport de situation](#)
- [Fiche-action GC3](#) [Matrice d'évaluation d'une situation de crise](#)
- [Fiche-action GC4](#) [Matrice d'évaluation d'une situation de crise informatique](#)
- [Fiche-action GC4.1](#) [Tableau des applicatifs critiques](#)
- [Fiche-action GC5](#) [Suivi des actions de première réponse à un événement grave](#)
- [Fiche-action GC6](#) [Livre de bord](#)
- [Fiche-action GC7](#) [Suivi des appels téléphoniques](#)
- [Fiche-action GC8](#) [Retour d'expérience : fiche événement](#)

ANNEXE 4

FICHES REFLEXES GESTION DE CRISE

- [Fiche-réflexe GC1 Pilotage de la situation de crise](#)
- [Fiche-réflexe GC2 Check-list traitement de l'urgence et secours](#)
- [Fiche-réflexe GC3 Matériels et équipements de gestion de crise](#)
- [Fiche-réflexe GC4 Check-list communication de crise](#)
- [Fiche-réflexe GC5 Retour d'expérience](#)

ANNEXE 5

FICHES REFLEXES PCA

DIFFUSION RESTREINTE

- [Fiche-réflexe PCA1](#) Siège : besoins en positions
- [Fiche-réflexe PCA1.1](#) DR : besoins en positions
- [Fiche-réflexe PCA2](#) Siège : secours des activités paie
- [Fiche-réflexe PCA2.A](#) DR : secours des activités paie
- [Fiche-réflexe PCA3](#) Siège : secours des activités finance
- [Fiche-réflexe PCA3.1](#) DR : secours des activités finance
- [Fiche-réflexe PCA4](#) Siège : secours des paiements
- [Fiche-réflexe PCA5](#) Achats en état d'urgence

ANNEXE 6

PLAN DE CONTINUITÉ INFORMATIQUE DE L'INSERM

DIFFUSION RESTREINTE