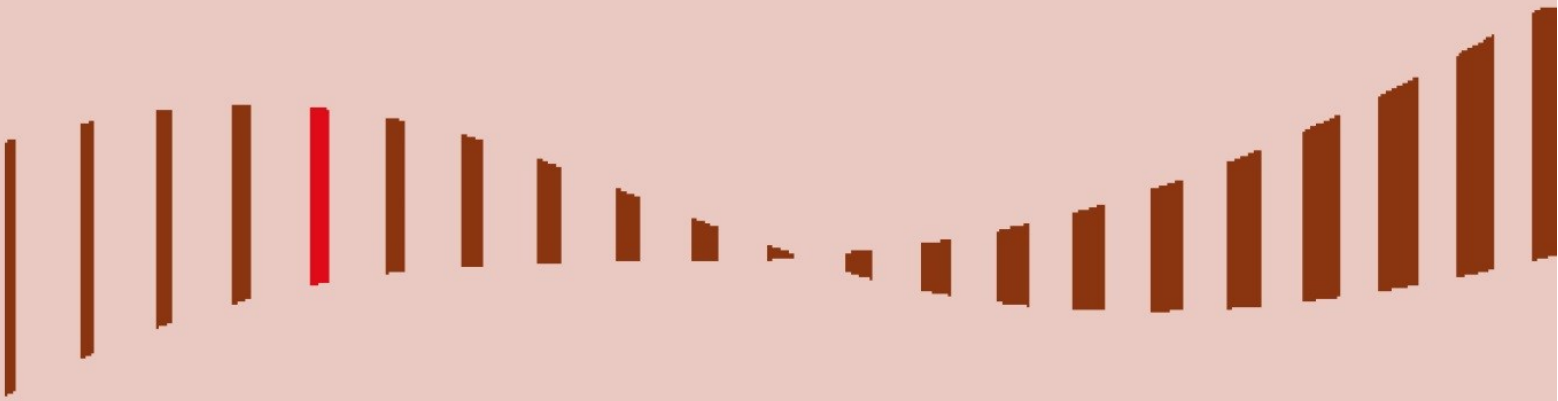
Guide pratique
Plan de Continuité Informatique
Principes de base

Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) - Janvier 2016 - V1.0



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES,
DE LA SANTÉ
ET DES DROITS DES FEMMES

asipsanté
AGENCE DES SYSTÈMES
D'INFORMATION
PARTAGÉS DE SANTÉ

Sommaire

1 Introduction

1.1 Objet du document

Le présent document propose une démarche consistant à créer un Plan de Continuité Informatique (PCI) pour prendre en compte, au niveau des infrastructures informatiques du Systèmes d'Information (SI), le Plan de Continuité d'Activité (PCA) d'une structure du domaine sanitaire ou médicosocial[1].

L'objectif est de permettre la mise en place des mesures qui garantissent, en situation d'incident, une continuité de fonctionnement du SI suffisante pour répondre aux exigences de continuité des activités métier.

Ce document fait partie des guides pratiques spécifiques de la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S).

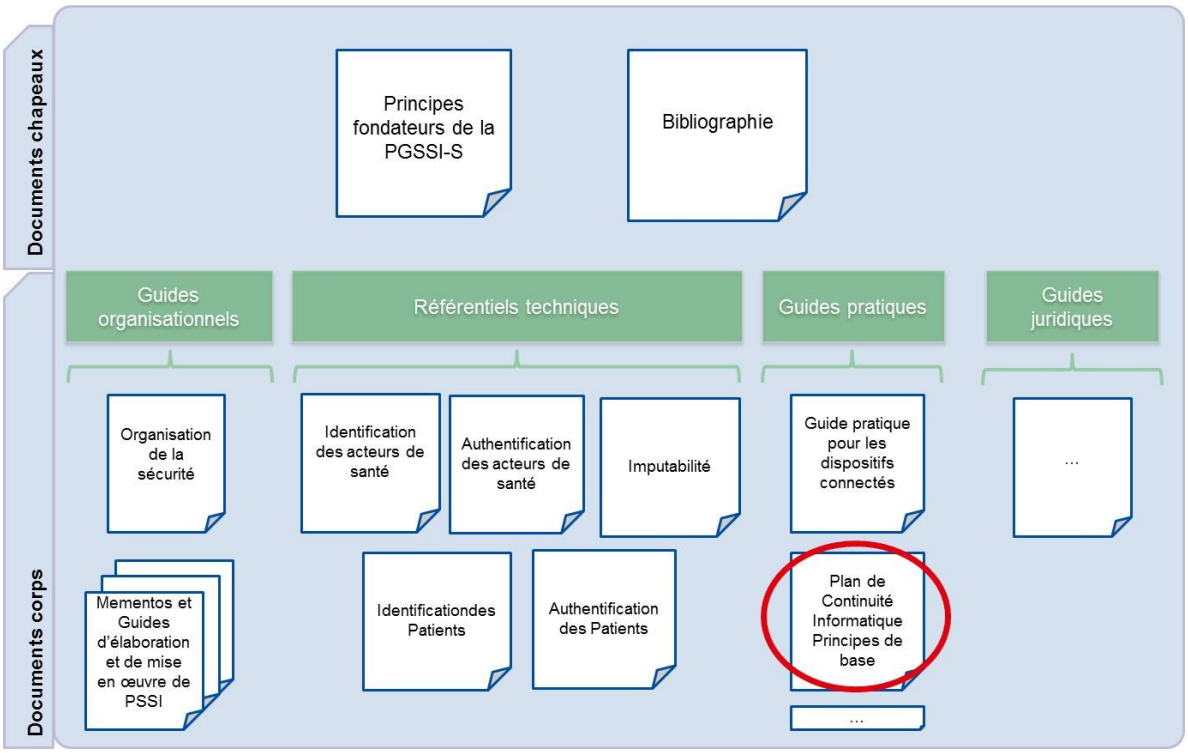


Figure 1 : Organisation des documents dans le Corpus documentaire de la PGSSI-S

Ce document s'adresse :

- aux responsables de structure ;
- aux personnes agissant sous leur responsabilité, en particulier celles impliquées dans :
  - la gestion de la continuité d'activité de la structure,
  - la direction et l'exploitation du SI,
  - la mise en œuvre de la sécurité des SI,
  - les prestations d'exploitation et de maintenance des moyens de sauvegarde.

[1] Par convention, le terme structure est utilisé dans le document pour désigner une structure d'exercice collectif du domaine de la santé quel que soit son type (ex. hôpital, clinique, centre de santé, maison de santé, EHPAD…) prenant en charge des patients. Ce guide ne s'adresse pas directement aux structures d'exercice individuel de type cabinet libéral, mais ces structures peuvent néanmoins s'en inspirer pour traiter la continuité de fonctionnement de leur SI.

1.2 Champ d'application du guide pratique

Dans le cadre de ce guide pratique, tous les contextes de SI au sens des « Principes fondateurs de la PGSSI-S » sont concernés quelles que soient les finalités du SI (production de soins, recherche clinique, …), le mode d'exercice et les étapes du cycle de vie de la donnée (conservation, échange/partage, …).

L'ensemble des composants qui constituent l'infrastructure informatique du SI entre dans le périmètre du guide, y compris les dispositifs connectés (ex : équipements biomédicaux connectés au réseau), connexions avec des partenaires, etc.

Le cartouche ci-après présente de manière synthétique le périmètre d'application du document.

Santé						**Médicosocial**
Production des soins	Fonctions supports à la production de soins	Coordination des soins	Veille sanitaire	Etudes et recherche	Dépistage et prévention	
✓	✓	✓	✓	✓	✓	✓
Commentaire						

Pour l'ensemble de ces périmètres, le présent guide décrit une approche applicable à l'intégration du SI de la structure dans son plan de continuité d'activité.

Limites du champ d'application du guide :

Ce guide s'attache uniquement aux services informatiques supports que fournit le SI aux processus métiers de la structure. Il ne prend pas en compte les éventuelles dispositions organisationnelles qui peuvent être mises en place pour assurer la continuité des activités métier en dehors des aspects SI. La continuité des activités métier est étudiée dans le cadre du plan de continuité d'activité (PCA) de la structure, et le PCI s'appuie sur ces résultats pour identifier les parties du SI nécessaires aux activités critiques.

En outre, il est important de souligner que la thématique PCI est liée à plusieurs autres sujets qui ne sont pas traités dans ce guide :

- plan de continuité d'activité (PCA) global de la structure : les concepts liés au PCA sont considérés comme connus du lecteur ; certains sont cependant rappelés au fil du guide ;
- analyse des risques liés au SI de la structure : le guide considère que la structure a établi le catalogue de ses principaux risques liés au SI, que ce soit dans le cadre de la mise en application du guide PSSI [Réf. n°6], à l'occasion d'une analyse de risques portant sur le SI de la structure, ou encore dans le cadre de la gestion des risques globale et non spécifique au SI mise en œuvre au sein de la structure. A défaut d'une telle analyse, le lecteur peut se reporter au guide PSSI [Réf. n°6], et notamment à son annexe 3 ;
- sauvegarde des données et externalisation des sauvegardes : ce point est évoqué dans ce guide, mais il est traité dans le guide pratique [Réf. n°5] du corpus documentaire PGSSI-S ;
- gestion des évènements survenant au sein du SI et gestion des incidents du SI : ces sujets feront l'objet d'un guide spécifique ;
- gestion de crise : ce point est évoqué dans le présent guide, mais il n'y est pas détaillé, les structures disposant généralement déjà d'une organisation pour la gestion des crises.

1.3 Enjeux relatifs à la continuité de fonctionnement des systèmes d'information de santé

Les systèmes d'informations de santé fournissent des services supports sur lesquels s'appuient de façon croissante les métiers des secteurs sanitaire et médicosocial :

- informatisation du dossier patient qui permet de faciliter l'accès partagé et contrôlé aux informations ;
- équipements médicaux connectés au reste du SI ;
- gestion administrative des patients.

Plus les professionnels intègrent les apports de ces dispositifs à leurs pratiques quotidiennes, plus l'indisponibilité de ces dispositifs peut induire des perturbations des activités, allant du simple désagrément jusqu'à la perte de chance pour le patient.

Afin de réduire les impacts négatifs de l'indisponibilité de tout ou partie du SI, des mesures doivent être prévues, mises en place et vérifiées. Ces mesures, de nature organisationnelle comme technique, peuvent intervenir :

- en prévention, pour répondre aux exigences formalisées dans la Politique de Sécurité des Système d'Information (PSSI) de la structure afin d'éviter la survenance d'un incident ;
- en palliatif, pour assurer un fonctionnement du SI à l'aide de moyens temporaires permettant d'assurer la continuité des processus essentiels ;
- en secours, pour restaurer un fonctionnement complet du SI à l'aide de moyens de remplacement, jusqu'à ce que le SI puisse être rétabli dans son environnement « habituel »[2].

Outre les enjeux parfois critiques liés à leur disponibilité, les SI des secteurs sanitaire et médicosocial sont soumis à de fortes contraintes de sécurité, détaillées dans la PSSI de la structure (voir également guide PSSI [Réf. n°6]) :

- nécessité d'exactitude[3] des informations stockées et traitées ;
- exigence de confidentialité[4] de certaines de ces informations, notamment lorsqu'il s'agit de données de santé à caractère personnel ;
- besoin de traçabilité et d'imputabilité[5] des accès à ces informations, qu'il s'agisse de modification ou de simple consultation.

Or, ces contraintes doivent être prises en compte non seulement dans le fonctionnement normal du SI, mais également en situation d'incident où les mesures prévues par le Plan de Continuité Informatique sont mises en œuvre. Ces exigences, quand elles s'ajoutent à une

[2] Ce guide distingue la notions de « mesure palliative » de celle de « mesure de secours » pour souligner les spécificités de certaines étapes dans la réponse aux incidents qui affectent la continuité. Dans d'autres contextes ou documents, ces deux types de mesures sont rassemblés sous la même dénomination de « mesures de secours ».

[3] Egalement appelé « intégrité » en sécurité des systèmes d'information : le fait que les données ou les processus de traitement ne puissent être modifiés que par les personnels habilités à le faire et qu'à défaut tout changement illégitime puisse être détecté.

[4] Confidentialité : le fait que les données ne soient accessibles qu'aux utilisateurs habilités à les consulter.

[5] Traçabilité et imputabilité : le fait d'être capable de savoir quelles actions ont été réalisées vis-à-vis de ces informations, quand et par quel utilisateur.

situation de crise, peuvent nécessiter des compromis dont les impacts doivent impérativement être compris et maîtrisés.

Les SI de santé présentent des spécificités qui imposent des exigences particulières, voire qui interdisent l'usage de certaines solutions de continuité d'activité qui seraient acceptables dans d'autres secteurs.

Exemples :

- Dans le contexte des établissements de santé, l'activité est fortement liée aux personnes, et en cas d'incident, un patient ne peut pas être instantanément transféré sur un site de repli ni voir sa prise en charge brutalement interrompue puis reprise plus tard (comme pourrait l'être, par exemple, la fabrication d'un produit finalement assurée par une autre usine de l'entreprise pour répondre à une commande dans les délais).
- L'interruption d'une fonction du SI (équipements biomédicaux en particulier) peut, a priori, induire une perte de chance d'un patient, voire engager son pronostic vital. La dimension temporelle d'une interruption de service prend alors une criticité bien autre que des simples impacts financiers ou matériels.

2 Fondements du guide

Ce guide propose des éléments de démarche destinés à faciliter l'élaboration du volet « Systèmes d'Information » du Plan de Continuité d'Activité dans les secteurs sanitaire et médico-social. Ce volet du PCA constitue à proprement parler le « Plan de Continuité Informatique ».

Il complète, pour les secteurs sanitaire et médicosocial, les bonnes pratiques et standards établis par les documents de référence suivants :

- le « Guide pour réaliser un plan de continuité d'activité » publié par le SGDSN [Réf. n°2] ;
- Programme Hôpital Numérique : Fiche pratique 3 - plan type d'un Plan de reprise d'Activité du SI et bonnes pratiques [Réf. n°8], et Fiche pratique 5 : bonnes pratiques d'élaboration des procédures de fonctionnement en mode dégradé / de retour à la normale du système d'information [Réf. n°9] ;
- la norme ISO/CEI 27031 - « Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité » [Réf. n°10] ;
- la norme ISO/CEI 22301 – « Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences » [Réf. n°1] ;
- la norme ISO/CEI 27002 - « Code de bonnes pratiques pour la gestion de la sécurité de l'information » [Réf. n°7] ;

La démarche proposée ici est une démarche simplifiée. Pour mettre en œuvre une méthode plus approfondie, plus formelle et plus systématique, le lecteur se reportera aux pratiques de gestion de la continuité d'activité en vigueur au sein de sa structure ou aux documents mentionnés ci-dessus et présentés au chapitre 6 « Pour aller plus loin… ».

3 Introduction au PCI

Le Plan de Continuité Informatique (PCI) étant « au service » du Plan de Continuité d'Activité (PCA) de la structure, il est utile de rappeler quelques notions générales sur la continuité d'activité.

3.1 PCI et PCA

La norme ISO 22301:2012(F) définit la continuité d'activité comme la « *capacité de l'organisation à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définis après un incident perturbateur.* »

Une partie des activités de la structure s'appuie sur le SI pour sa bonne réalisation. Le dispositif de continuité de fonctionnement du SI est constitué de l'ensemble des mesures visant à répondre à divers scénarios de crises (incidents ou événements perturbant gravement le fonctionnement normal du SI, y compris situations extrêmes) afin de garantir :

- le maintien des fonctions assurées par ce SI dont dépendent des activités essentielles ou importantes de l'organisation. Ce maintien peut se faire temporairement selon un mode dégradé ;
- la reprise planifiée de ces fonctions.

Le PCI doit permettre à la structure, pour ce qui relève du SI, de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (éviter le risque de perte de chance des patients, image, survie de la structure...) et de tenir ses objectifs. [Réf. n°2]

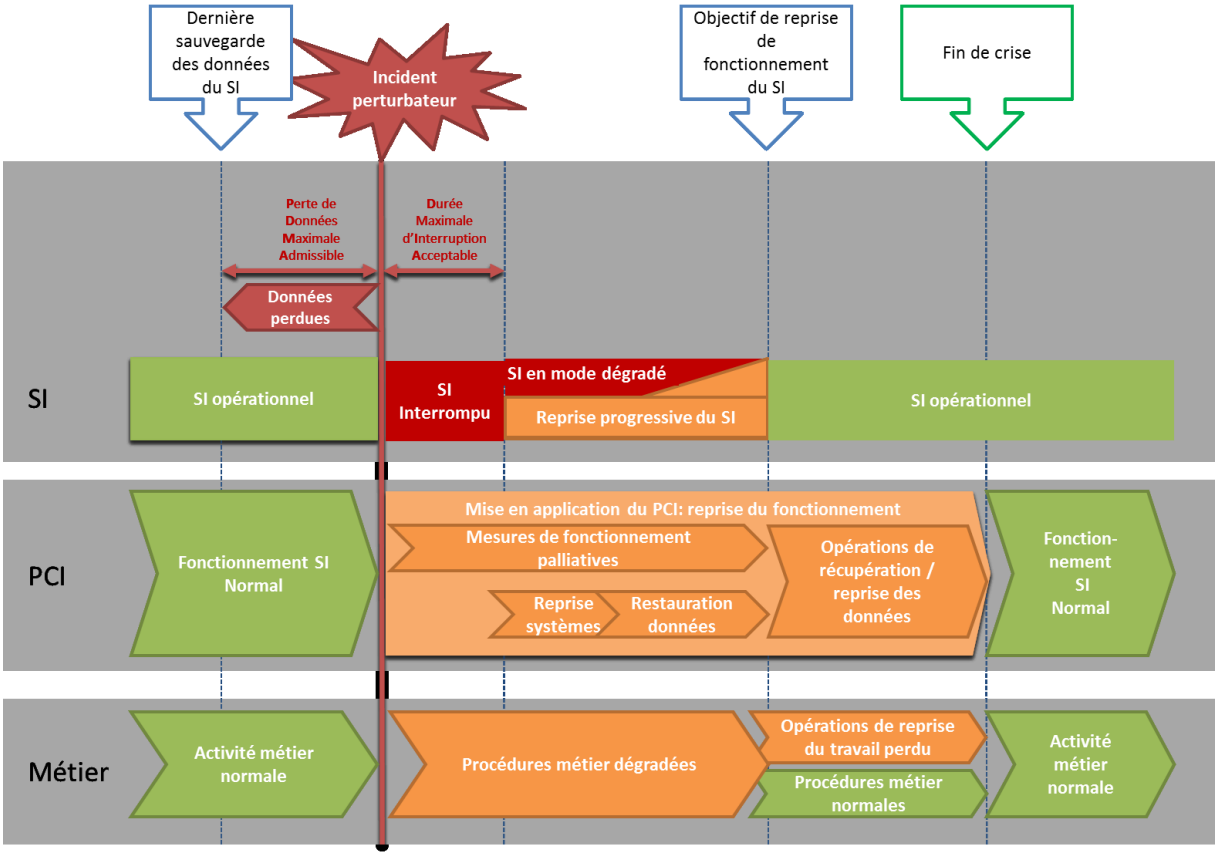
En fin de compte, l'objet des mesures de continuité de fonctionnement du SI est de participer à la continuité de l'activité de la structure elle-même. Ce sont les objectifs de continuité des activités métier qui conditionnent les attentes de continuité de fonctionnement vis-à-vis du SI.

Ces différentes mesures, organisationnelles et techniques, sont formalisées dans le Plan de Continuité Informatique (PCI).

Le PCI doit être considéré comme étant l'une des parties du PCA global de la structure.

3.2 Traitement d'un incident qui impacte la continuité de fonctionnement du SI

Le schéma ci-dessous présente, de manière macroscopique, les différentes phases du traitement d'un incident qui impacte la continuité de fonctionnement du SI.



Traitement d'un incident qui impacte la continuité de fonctionnement du SI

Ce schéma fait apparaître plusieurs points clé, présentés chronologiquement ci-dessous :

- l'**incident perturbateur**[6], qui provoque l'interruption du SI, par rapport auquel on identifie :
    - les pertes de données créées avant l'incident et après la **dernière sauvegarde des données**. La durée maximale avant un incident pendant laquelle les acteurs métiers acceptent de perdre des données est spécifiée, pour chaque type de données, par la **Perte de Données Maximale Admise** (**PDMA**, notion également liée à celle « d'**intégrité** des données » utilisée dans le cadre de la Politique de Sécurité du SI – voir [Réf. n°6] et exemple en Annexe 5),
    - la **Durée Maximale d'Interruption Admise** (**DMIA)** après survenance de l'incident. La DMIA est fixée pour chaque service fourni par le SI. Cette notion est également liée à celle de « **disponibilité** des services » décrite dans le cadre de la Politique de Sécurité du SI – voir [Réf. n°6]. Elle est définie en fonction des contraintes métiers des utilisateurs de ce service et de la possibilité de s'appuyer ou non sur des solutions alternatives temporaires en l'absence du service ;
- après le délai de réaction nécessaire à la détection de l'incident et à la mobilisation des acteurs, puis après le délai de décision nécessaire à la sélection des actions à mener dans le cadre de la gestion de crise, la cellule de gestion de crise déclenche la **mise en application du volet** « **Reprise du fonctionnement du SI »** du PCI :
    - la **reprise progressive du SI** se fait en mettant en œuvre une **reprise des systèmes** suivie d'une **restauration des données**, ou encore des **mesures de fonctionnement palliatives** ou de secours. Cette reprise donne la priorité aux systèmes les plus critiques,
    - pendant cette période, le **SI** fonctionne probablement **en mode dégradé**, mode dans lequel il ne fournit que partiellement les services attendus. Des **procédures métier dégradées** adaptées à cette réduction du niveau de service fourni par le SI peuvent alors être nécessaires ;
- le SI doit redevenir complètement opérationnel dans le délai fixé par **l'Objectif de reprise de fonctionnement du SI**. Les activités métier peuvent de nouveau s'appuyer sur les procédures fonctionnelles normales.
    - Les **opérations de récupération / reprise des données** doivent être menées. Elles portent sur les données éventuellement produites dans le cadre des procédures dégradées et de l'utilisation de moyens palliatifs d'une part, et sur la reconstitution ou la ressaisie des données perdues suite à l'incident d'autre part. Ces activités visant à réintégrer ces données dans le SI opérationnel sont menées aussi bien au niveau technique du SI qu'au niveau fonctionnel métier ;
- la **fin de crise** peut être décrétée quand il est validé que l'ensemble des systèmes et des données sont restaurés dans un état normal.

[6] Incident : « situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise » (source ISO 22300)

3.3 Définitions liées à la continuité de fonctionnement informatique

Différents termes utilisés dans le domaine de la continuité de fonctionnement informatique sont présentés ci-dessous.

Incident :

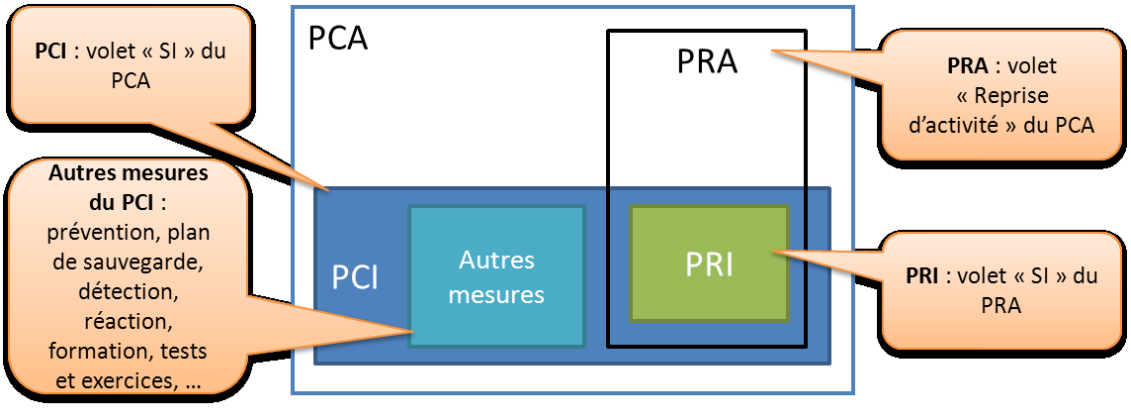
« Situation qui peut être, ou conduire à, une perturbation, une perte, une urgence ou une crise » (source ISO 22300)

Plan de Reprise d'Activité (PRA) :

Ensemble des mesures prévues pour rétablir l'activité de la structure après qu'elle ait été interrompue suite à un incident. Le PRA fait partie du PCA.

Plan de Reprise Informatique (PRI), également « Plan de Reprise d'Activité du SI (PRA du SI) » :

Ensemble des mesures prévues pour rétablir l'activité du SI après qu'elle ait été interrompue suite à un incident. C'est le volet du PRA consacré au SI.



Positionnements relatifs du PRI, PRA, PCI et PCA

Le PRI constitue une partie du PCI. La suite de ce guide traite du PCI dans sa globalité sans dissocier les mesures particulières de reprises (PRI).

Reprise du SI :

La reprise d'un SI totalement ou partiellement interrompu correspond au rétablissement de ses fonctions à l'aide de **mesures palliatives** et des **mesures de secours**. La reprise est généralement réalisée de manière progressive, en favorisant les fonctions du SI nécessaires aux activités les plus critiques de la structure, tel que prévu par le PCA et le PRA.

Le rétablissement de ces fonctions prioritaires du point de vue métier requiert souvent que soit préalablement rétabli un ensemble minimal de fonctions d'infrastructure nécessaires au SI lui-même : alimentation électrique, réseau informatique et services associés, service d'authentification des utilisateurs, …

Mode dégradé :

Un composant ou un service fourni par le SI, ou le SI dans son ensemble, est dit fonctionner en mode dégradé :

- quand il ne rend pas l'ensemble des fonctions qu'il est censé fournir ;
- quand il fournit certaines fonctions avec des performances inférieures aux attentes (temps de réponse, capacité de stockage, nombre d'utilisateurs connectés simultanément, débit des liaisons de communications…).

Pendant la phase de reprise du SI, celui-ci est fortement susceptible de fonctionner en mode dégradé, sur tout ou partie de son périmètre, puisque les moyens de secours ne peuvent généralement pas être tous mis en œuvre instantanément, et que les moyens palliatifs, activés plus rapidement, ont fréquemment des capacités limitées comparativement aux moyens nominaux.

Objectif Minimum de Continuité d'Activité (OMCA) :

L'Objectif Minimum de Continuité d'Activité définit le niveau d'activité au-dessous duquel des conséquences considérées inacceptables sont susceptibles de survenir, qu'elles soient immédiates (ex : perte de chance de patients) ou ultérieures (ex : impossibilité d'absorber le retard accumulé quand l'activité reviendra à une situation normale, entorse aux obligations légales de la structure, etc.).

L'objectif peut être formulé en termes de volume, de tâches réalisées, d'exigences de délai, de qualité, etc. Il en découle des exigences relatives au « service minimum » que doit fournir le SI dès lors que la durée maximale d'interruption acceptable (DMIA) est atteinte.

Disponibilité (du SI) :

« Disponibilité des données ou des traitements : le fait que les données (annuaire des fournisseurs, dossier patient, inventaire de pharmacie…) ou les traitements (application, web service, composant logiciel…) soient accessibles au moment prévu pour leurs usages autorisés. » [Réf. n°6].

La disponibilité est généralement utilisée pour qualifier les moyens (le SI en l'occurrence) qui contribuent à la réalisation d'activités. La continuité se distingue de la disponibilité par le fait qu'elle a pour objet l'activité alors que la disponibilité a pour objet le moyen au service de l'activité.

Note :

- Le terme de « système (à) haute disponibilité » est parfois rencontré. Il désigne des systèmes qui mettent en œuvre des solutions techniques, souvent par duplication (ou « redondance ») de leurs composants, afin de prévenir une interruption des services qu'ils fournissent.

  Ces solutions ne permettent pas nécessairement de couvrir tous les scénarios d'incident envisagés et il reste nécessaire de prévoir des solutions palliatives ou des solutions de secours dans le cadre d'un PCI.

- La définition de « disponibilité » établie par le standard ISO 27000, à savoir « Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées », peut s'appliquer aussi bien aux activités qu'aux moyens qui soutiennent ces activités. Il n'en reste pas moins que l'usage est de parler de « continuité des activités » plutôt que de « disponibilité des activités », et de parler de « disponibilité » d'un dispositif technique, d'où le distinguo fait dans ce guide entre ces deux termes.

Sauvegarde :

Opération qui consiste à dupliquer et à conserver de manière sécurisée des systèmes informatiques et/ou des données contenues dans un système informatique (ex. données métier, paramétrage et réglage du système…) afin d'assurer leur disponibilité et leur réutilisabilité même en cas d'incident ou d'erreur de manipulation portant atteinte à leur intégrité. Le terme anglais « backup » est aussi largement usité dans le milieu informatique pour désigner une sauvegarde. [Réf n°5]

Les principes généraux de sauvegarde des données sont définis dans un **Plan de sauvegarde**. Ce plan comprend l'ensemble des procédures liées à la sauvegarde et à la restauration pour un périmètre identifié sur lequel elles doivent être appliquées. [Réf n°5]

3.4 Organisation nécessaire

Pour que les incidents puissent être traités efficacement, la structure doit organiser la surveillance des évènements qui interviennent au sein du SI, leur analyse et leur qualification éventuelle en incident.

Les différentes étapes de traitement d'un incident qui impacte la continuité du SI doivent être pilotées par une structure dédiée avec, quand nécessaire, une mobilisation de la **cellule de crise** qui est l'organe central et indispensable de la gestion de la crise.

L'organisation de continuité de fonctionnement du SI s'appuie en premier lieu sur les circuits existants au sein de la structure en termes de continuité d'activité globale et de gestion de crise. Ces circuits rassemblent la direction et les responsables métiers, administratifs et techniques du bon niveau pour prendre les décisions en situation de crise.

4 Comment élaborer le PCI de votre SI ?

4.1 Synthèse de la démarche

La démarche proposée ici est une démarche simplifiée qui permet, dans la lignée du Guide PSSI [Réf. n°6], une première approche de l'élaboration d'un PCI pour le SI de votre structure. Elle est complémentaire aux Fiches pratiques proposées sur ce thème dans le cadre du Programme Hôpital Numérique ([Réf. n°8] et [Réf. n°9]).

Prise en compte de l'existant

Votre structure dispose peut-être déjà d'un **Plan de Continuité d'Activité**, d'un Plan de Gestion de Crise ou d'un corpus documentaire équivalent. Le plan de continuité d'activité identifie les activités métiers les plus sensibles à prendre en compte en situation de crise, afin que les missions essentielles de la structure puissent être poursuivies ou transférées à d'autres structures dans les meilleures conditions possibles.

Cet ensemble de documents permet de guider la définition des mesures permettant au SI d'être rétabli au niveau de service nécessaire aux activités critiques, dans les délais exigés par ces activités.

Dans le cas où votre structure ne dispose pas de ces informations, il sera nécessaire de les collecter auprès des responsables métiers de la structure, sous l'arbitrage de la direction.

Elaboration du PCI initial

Après une phase de cadrage avec la direction, l'élaboration du PCI de votre structure se déroule en six étapes :

1. identifier l'organisation à mettre en place pour l'élaboration et la mise en œuvre du PCI ;
2. identifier les scénarios d'incidents à prendre en compte ;
3. recueillir le besoin métier de rétablissement des services fournis par le SI ;
4. identifier les moyens[7] du SI concernés par chaque scénario d'incident et les mesures de prévention déjà en place ;
5. élaborer les mesures préventives, les mesures palliatives et les mesures de secours ;
6. préparer les moyens nécessaires et tester les solutions.

[7] Les « moyens du SI » désignent ici les différents dispositifs informatiques (postes de travail, serveurs, équipements réseau, liaisons Internet et liaisons partenaires,…), les dispositifs connectés (équipements biomédicaux connectés au réseau), les locaux techniques informatiques et les dispositifs associés (alimentation électrique, climatisation de salle informatique, …) ainsi que les personnels en charge du fonctionnement du SI et les documentations nécessaires à leurs activités.

4.2 Organisation

La mise en place d'une fonction de responsable PCI est nécessaire, afin de centraliser :

- la **coordination** de **l'élaboration** du PCI en collaboration avec le responsable PCA de la structure, le responsable du SI et le RSSI ;
- le pilotage des **tests** des mesures prévues au PCI, qu'il s'agisse de tests internes au SI, ou de tests dans le cadre d'exercices de mise en œuvre du PCA global de la structure ;
- le **reporting** de la maîtrise de la continuité de fonctionnement du SI à la direction et au RSSI de la structure ;
- la coordination du **maintien à jour** du PCI ;

La fonction de responsable PCI n'est pas exclusive d'autres fonctions, et peut par exemple être remplie par la personne en charge de la fonction de RSSI.

Il est également nécessaire, si ce n'est pas déjà fait dans le cadre du PCA, d'identifier en amont les personnes en mesure de dresser le diagnostic le plus pertinent de l'état du SI en situation d'incident, afin que cette étape puisse être réalisée dans les meilleurs délais.

Il est recommandé que les mêmes outils soient utilisés pour la gestion du PCA global de la structure et pour la gestion du PCI, qui constitue un des volets du PCA.

4.3 Identifier les scénarios d'incident à prendre en compte

Cette étape consiste à identifier les scénarios d'incident à prendre en compte dans le plan de continuité informatique afin de pouvoir préparer les mesures qui assureront la continuité de fonctionnement du SI dans ces situations.

Ces scénarios doivent recouvrir différents types d'incidents qui, en impactant le SI de manière directe ou indirecte, empêchent ou gênent de manière inacceptable les activités critiques de la structure.

Si la structure a déjà établi son PCA, sur la base d'une analyse globale de risques de la structure, il convient de se baser sur les scénarios retenus dans ce cadre. Il peut néanmoins être nécessaire de préciser certains cas de figures spécifiques s'ils n'ont pas été déjà identifiés, notamment les situations où seul le SI est, dans un premier temps, directement touché par l'incident (voir ci-dessous). Les situations où le SI est directement affecté par un incident doivent a priori avoir été identifiées par l'analyse des risques liés aux SI, dans le cadre de l'élaboration et de la maintenance de la Politique de Sécurité du SI de la structure (se reporter au Guide PSSI [Réf. n°6] si nécessaire).

Pour une première approche, il est recommandé de ne pas multiplier les scénarios[8], et de se limiter à ceux qui présentent des spécificités suffisamment fortes pour se distinguer les uns des autres dans la façon dont ils devront être pris en compte. Les scénarios retenus pourront être affinés ultérieurement si le besoin s'en fait sentir.

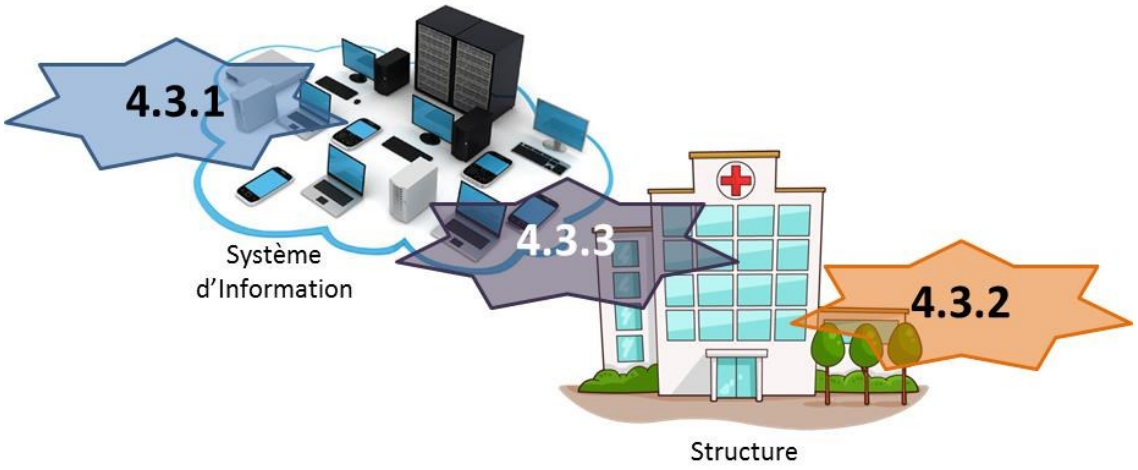
> ✍ Il peut être judicieux de traiter les scénarios d'incidents par ordre de criticité décroissant, la criticité d'un scénario étant généralement identifiée dans le PCA. Cette démarche permet de construire et de mettre en application le PCI de manière progressive, en s'attachant en priorité aux situations qui présentent le plus grand risque pour la structure.

Il est probable qu'un incident réel ne corresponde jamais exactement à l'un des scénarios prévus, et même dans le cas contraire il y aura le plus souvent des circonstances ou des faits particuliers qui n'auront pas été pris en compte *a priori*. Ce n'est pas problématique dans la mesure où :

- d'une part, les « briques » de solutions construites dans le cadre des scénarios étudiés peuvent généralement être réutilisées avec les ajustements nécessaires ;
- d'autre part la capacité d'adaptation acquise avec l'étude des différents scénarios et avec les exercices de mise en œuvre du PCI seul ou du PCA permettent d'améliorer la prise en compte de différentes variantes des scénarios généraux prévus.

Il est présenté dans le schéma et le tableau suivant trois scénarios génériques d'incident, qui peuvent servir de base dans l'élaboration du PCI selon les scénarios pris en compte par le PCA de la structure. Les numéros associés correspondent aux numéros des sections dans lesquelles ces scénarios sont explicités.

[8] Ni chercher à détailler, au-delà de quelques exemples illustratifs, les différentes combinaisons d'évènements ou de causes susceptibles d'aboutir à la situation considérée.



Incident...	n'affectant pas directement la structure…	affectant directement la structure…
et n'affectant pas directement le SI	*Pas d'incident*	4.3.2 Incident affectant la structure
et affectant directement le SI	4.3.1 Incident affectant le SI	4.3.3 Incident affectant la structure et le SI

Un quatrième scénario, qui ne correspond pas à un incident mais dont la prise en compte dans le PCI est utile, est également proposé en section 4.3.4.

4.3.1 Incident affectant le SI

Dans ce type de scénario d'incident, le SI subit un incident avec pour conséquence de ne plus être en mesure de fournir tous les services attendus aux activités de la structure.

Le SI peut être affecté de façon totale ou partielle. L'incident peut être de différentes natures, comme l'illustrent les exemples ci-après :

Nature de l'incident	Exemples
physique ou environnemental	• **incendie** de la salle informatique complète ou d'un seul local technique d'étage ; • **inondation** de la salle informatique ; • impact de **foudre** à proximité entrainant la destruction de certains composants d'équipements.
technique	• panne de **climatisation** de la salle informatique entrainant la surchauffe des équipements et leur arrêt ; • coupure de l'**alimentation électrique** pendant une durée dépassant la capacité des onduleurs ; • dysfonctionnement de l'onduleur provoquant une **surtension électrique** et la destruction de l'ensemble des alimentations des équipements, voir la destruction des équipements eux-mêmes.
logique	• **virus** informatique pas encore pris en compte par les antivirus qui se propage à l'ensemble des postes de travail et serveurs utilisant le même système d'exploitation et qui sature ainsi le réseau interne ou bloque les équipements eux-mêmes ; • **piratage** d'un service en ligne proposé par la structure, aboutissant au verrouillage par les pirates (par chiffrement notamment) de données de santé à caractère personnel (dossiers patient…) et à un chantage où une « rançon » est exigée par les pirates en échange de la clé permettant de restaurer l'accès aux données verrouillées ; • **erreur** de manipulation par le personnel informatique au cours d'une mise à jour système qui bloque de nombreux serveurs informatiques.
perte des communications	• rupture de la **liaison Internet** ou du raccordement de bâtiments annexes au SI à la suite de travaux mal maîtrisés (internes ou externes à la structure).
humaine	• intoxication alimentaire de l'ensemble de l'équipe informatique qui avait organisé un dîner commun le soir précédant, interdisant la réalisation de certaines opérations d'exploitation indispensables au bon fonctionnement du SI.

Ce type de scénario est spécifique dans la mesure où l'environnement de réalisation des activités métier n'est pas directement perturbé par l'incident, et où ces activités sont malgré tout gênées par la défaillance partielle ou totale du SI.

4.3.2 Incident affectant la structure

Dans ce type de scénario d'incident, le SI est pleinement opérationnel. En revanche, l'incident impacte directement certaines activités métier.

La particularité de ce scénario est qu'il va falloir « accompagner » les mesures prévues par le PCA afin de fournir un accès exceptionnel au SI dans l'éventuel environnement de repli des activités métier concernées par l'incident.

> Exemple : situation dans laquelle, quelle qu'en soit la raison (incendie, inondation, panne électrique durable), une partie du bâtiment doit être évacuée sans que les locaux hébergeant le SI ne soient concernés. Si le PCA prévoit, par exemple, que les soins et le suivi des patients puissent être réalisés à l'aide des applications habituelles du SI dans des locaux de repli, le PCI doit alors intégrer des solutions permettant d'assurer la connexion dans ces locaux au SI et la protection des composants sensibles du SI qui seront déployés dans ce cadre.

4.3.3 Incident affectant la structure et le SI

Dans ce type d'incident, la structure est affectée dans sa globalité, aussi bien au niveau des activités métier qu'au niveau du SI.

Le SI doit alors est restauré conjointement aux activités métier, tel que le prévoit le PCA de la structure dans ce type de situation.

> Exemple : Un incendie ravage l'essentiel des locaux de la structure. Le PCA prévoit que les patients évacués soient répartis dans différentes autres structures voisines. Dès lors, le PCI doit intégrer les solutions et les procédures pour que les dossiers patients soient rendus disponibles à ces structures (quel que soit le mode d'accès : accès en ligne fourni par un site d'hébergement externe DMP ou autre, édition papier depuis un site de repli, …), tout en respectant autant que possible les exigences de sécurité relatives au contrôle d'accès à ces informations.
>
> Autres exemples : pandémie, accident industriel rendant dangereuse toute la zone de la structure…

4.3.4 Interruption partielle et planifiée du SI

Une interruption partielle et planifiée du SI ne constitue pas un incident, mais elle correspond en revanche à un scénario qui se réalise fréquemment, par exemple lors de l'arrêt d'un système à des fins de maintenance.

Quand les exigences de continuité d'activité de la structure le requièrent, et notamment quand l'activité doit être maintenue 24h/24 ou si l'interruption dépasse les plages horaires non ouvrées, la démarche de préparation de l'interruption est similaire à celle suivie dans le cas de scénarios d'incident. Il convient alors de décliner un sous-scénario pour chaque système ou ensemble de systèmes susceptible de devoir être interrompu dans ce cadre.

> Exemple : La maintenance des serveurs hébergeant le DPI nécessite un arrêt d'une heure de ceux-ci. Le PCI doit alors prévoir une procédure permettant de maintenir l'accès aux informations essentielles contenues dans les dossiers patients pendant la période de maintenance ainsi que l'intégration dans le DPI des données produites pendant la période de maintenance.

4.4 Recueillir le besoin métier de rétablissement des services

Cette étape consiste à spécifier, pour chaque activité critique de la structure :

- la Durée Maximale d'Interruption Acceptable (DMIA, voir chap. 3.2) ;
- l'Objectif Minimum de Continuité d'Activité (OMCA, voir chap. 3.3) en mode dégradé ;
- la durée acceptable de fonctionnement en mode dégradé (voir chap. 3.3) ;
- la Perte de Données Maximale Admise (PDMA, voir chap. 3.2), afin notamment de fixer les modalités de sauvegarde des données concernées en fonctionnement normal du SI ;
- les éventuelles contraintes spécifiques à prendre en compte, en particulier celles liées aux contraintes de sécurité pesant sur les données utilisées (ex : exigences légales de confidentialité des informations médicales à caractère personnel, exigences règlementaires de traçabilité des prescriptions médicamenteuses…).

Ce sont les responsables des activités qui sont en mesure de fournir l'essentiel de ces informations au responsable du PCI, si elles ne sont pas déjà identifiées dans le PCA de la structure.

> ✍ Un exemple de tableau de collecte de ces informations, librement adaptable, est proposé en annexe 1.
>
> ✍ Lors du recueil, auprès des acteurs métier, du besoin métier de rétablissement des services du SI, il est important d'expliciter aux interlocuteurs le contexte pour lequel ces informations seront utilisées, à savoir des situations d'incident rares. Des exemples d'incidents, comme ceux exposés aux chapitres 4.3.1 à 4.3.3, sont alors très utiles pour illustrer ces situations et bien les différencier d'indisponibilités ou de « pannes » ponctuelles et très temporaires d'applications ou de composants du SI. En effet, ces acteurs peuvent comprendre que les possibilités de rétablissement des services diffèrent beaucoup entre, par exemple, le cas d'un équipement réseau d'étage qui tombe en panne, facilement remplaçable, et celui de la destruction de la salle informatique suite à un incendie de la partie du bâtiment qui l'héberge. C'est bien pour le second cas que le besoin de rétablissement des services doit être exprimé dans le cadre du PCI (et de manière générale, en fonction des scénarios d'incident envisagés par le PCA).

- Si la structure a déjà mené une analyse de risques du SI spécifique pour tout ou partie de ses activités, les besoins métiers pour ces activités en termes de rétablissement des services en cas d'incident sont probablement disponibles en tant qu'« éléments d'entrée » de cette analyse de risques.
- La méthode d'élaboration de Politique de Sécurité du SI proposée par le Guide PSSI [Réf. n°6] est une méthode simplifiée qui s'appuie sur une analyse de risques générique pour les structures des secteurs sanitaire et médicosocial. De ce fait, elle ne prévoit pas de phase de recueil des besoins de sécurité (dont les besoins de continuité) sauf à ce que des risques particuliers soient pressentis. Aussi, en cas d'utilisation de cette méthode pour élaborer la PSSI de la structure, l'élaboration du PCI nécessitera un recueil spécifique des besoins de continuité du SI.
- Dans tous les cas, que ce soit par une analyse spécifique des risques ou par l'application du Guide PSSI, la question des risques liés au SI et des enjeux associés doit avoir été traitée et une Politique de Sécurité du SI doit avoir été élaborée.

4.5 Identifier les moyens du SI concernés et les mesures existantes

Moyens du SI concernés

Cette étape consiste à identifier, pour chaque processus critique de la structure, **les moyens[9] du SI** nécessaires, en situation d'incident, au respect de l'Objectif Minimum de Continuité d'Activité (OMCA) en mode dégradé et ceux nécessaires au mode secours.

Pour ce faire, deux démarches sont possibles :

- si la structure a établi une cartographie de ses processus, le travail consiste à identifier les moyens du SI directement mis en œuvre dans chaque processus critique (une application informatique par exemple), puis les moyens indirectement mis en œuvre (par exemple, le réseau informatique utilisé par cette application).
- si la cartographie des processus n'est pas disponible, le travail consiste, à partir des moyens qui constituent le SI, à vérifier pour chacun d'eux s'il participe de façon directe ou indirecte à l'accomplissement de processus critiques (et lesquels). L'inventaire des moyens du SI éventuellement établi au cours de la mise en application de l'étape 2 de la démarche proposée par le guide PSSI [Réf. n°6] peut servir de base à ce travail.

Il est important, dans cette phase d'identification, de n'omettre aucun type de moyens du SI, et notamment :

- les dispositifs connectés :

  Exemple : équipements biomédicaux connectés au réseau ;

- les moyens « télécoms » :

  Exemple : liaison Internet, connexions partenaires, téléphonie, etc. ;

- les moyens externalisés :

  Exemple : hébergement de serveurs dans un Datacenter, recours à des applications distantes dans le cadre d'un contrat de service, sauvegardes externalisées chez un hébergeur de données, intervention régulière de personnel externe pour l'exploitation ou la maintenance du SI…).

Mesures existantes

Même si elles n'offrent qu'une couverture partielle, les mesures de continuité existantes pour les moyens concernés doivent être identifiées au cours de cette étape, afin de les prendre en compte dans l'étape d'élaboration de solutions. En effet, **des mesures de continuité pertinentes sont peut-être déjà en place**, bien que pas encore formalisées dans le PCI.

La **PSSI** de la structure est susceptible de préciser différentes dispositions de sécurité du SI qui contribuent aux mesures de prévention. Il est nécessaire de prendre ces mesures en compte dans le PCI et de renvoyer à la documentation qui les détaille.

Pour ce qui concerne les **moyens externalisés**, les mesures mises en œuvre par les fournisseurs se traduisent par des engagements de continuité fixés contractuellement, et par une organisation de circuits d'information et de coordination activables en situation de crise. Ces dispositions existantes doivent être répertoriées dans le PCI.

[9] Voir définition en bas de page du chapitre 4.1

✍ Il est important de souligner que des mesures de résilience ou de disponibilité ne constituent souvent que des mesures de prévention qui ne permettent pas de se prémunir contre tous les scénarios qui doivent être pris en compte. Les situations dans lesquelles les solutions existantes ou nouvelles sont efficaces, et celles où elles ne le sont pas, doivent être à chaque fois clarifiées.

Exemples :

- Une alimentation redondante ou des disques redondants ne préservent pas la continuité de fonctionnement en cas d'incendie dans les locaux informatiques.
- L'utilisation d'un onduleur (mesure) connecté à une ressource critique (moyen) répond en tant que mesure palliative temporaire à un scénario de rupture d'alimentation électrique, dans l'attente de la mise en œuvre d'une solution de secours (démarrage du groupe électrogène par exemple) ou du rétablissement de l'alimentation électrique normale (sous réserve que ce rétablissement puisse intervenir avant l'épuisement des batteries de l'onduleur).

4.6 Élaborer les mesures de prévention, les mesures palliatives et les mesures de secours

4.6.1 Définitions

Les mesures qui contribuent à la continuité de fonctionnement du SI, et qui doivent être décrites dans le PCI, sont de trois types :

- **Mesures de prévention** : ces mesures permettent de **réduire la probabilité d'occurrence d'un incident** susceptible d'interrompre les services fournis aux métiers par le SI ;
- **Mesures palliatives** : ces mesures permettent de rétablir rapidement, à l'aide de moyens alternatifs, certains services que doit fournir le SI, quitte à les fournir dans un **mode dégradé** (cf. chap. 3.2) qui réponde néanmoins à l'exigence d'activité minimale de la structure (« OMCA » cf. chap. 3.3) ;
- **Mesures de secours** : ces mesures couvrent l'ensemble des procédures et moyens mobilisés afin de **reconstituer un SI opérationnel et stable**, capable de rendre les services attendus dans un mode non dégradé : sites de repli, location de matériel, transport du personnel informatique vers le site de repli, …

> Qu'il s'agisse des aspects de prévention, palliatifs ou de secours, les **moyens externalisés** du SI doivent systématiquement être pris en compte dans le cadre du PCI.
>
> Le PCI doit préciser les engagements contractuels qui ont été négociés avec les fournisseurs de ces moyens externalisés, et si nécessaire les compléter par d'autres moyens, afin d'assurer l'adéquation du dispositif global avec le besoin de continuité de la structure.

4.6.2 Mesures de prévention

Des mesures de prévention sont généralement déjà intégrées aux SI existants. Il s'agit de mesures permettant de réduire la probabilité de survenance d'un incident.

Type de mesure	Exemples
techniques	• mesures de sécurité contre les malveillances (verrouillage des locaux techniques, antivirus…) ou contre les incidents physiques (prévention et détection des incendie, des fuites d'eau dans les locaux informatiques…) ; • double adduction réseau, onduleur, générateur électrique… ; • systèmes de disques durs en miroir ou en RAID 5, salle complète en redondance, « load balancing ».
logiques	• maintenance préventive du matériel et des logiciels (dont les mises à jour de sécurité).
humaines	• formation du personnel qui exploite le SI afin d'éviter les erreurs de manipulation.

Le PCI doit identifier et prendre en compte ces différentes mesures de préventions existantes (cf. chap. 4.5).

4.6.3 Mesures palliatives

Les solutions palliatives permettent au SI de continuer à fournir certains services, le cas échéant en **mode dégradé**, quand tout ou partie SI de production normal ne fonctionne plus.

Elles doivent être simples à mettre en œuvre, car elles sont mobilisées dans des situations d'urgence, avec des moyens humains peut-être limités. Elles sont généralement destinées à être opérationnelles rapidement.

Exemples :

- Une mesure palliative à la perte de la connexion Internet de la structure pourrait être, pour un fonctionnement en mode dégradé, l'utilisation temporaire de « clés web »[10]pour les postes de travail dont les utilisateurs ont un besoin impératif d'échange avec l'extérieur, sous réserve des mesures de sécurité adéquate ;
- Si des échanges numériques ne sont pas incontournables, des échanges par Fax peuvent également constituer une solution palliative, quitte à devoir procéder ultérieurement à une ressaisie des données dans les systèmes informatiques. Il est important de noter que la solution palliative par clés web requiert l'acquisition de ces clés web et le paiement des abonnements de téléphone mobile associés, qui doivent être anticipés pour être prêts en cas de survenance de l'incident ;
- Dans une grosse structure, la mesure palliative en cas de coupure d'alimentation électrique, consistant en l'activation automatique des onduleurs électriques peut être accompagnée d'une procédure visant à arrêter tous les équipements non critiques du SI afin de prolonger la durée de fonctionnement sur batterie des équipements et application les plus critiques.
- Le système de gestion du Dossier Patient Informatisé (DPI) peut, pour répondre aux exigences du PCA, conserver une copie des dossiers patients rattachés à chaque service de la structure sur les postes de travail du service, afin qu'en cas d'inaccessibilité prolongée de l'application centrale (dysfonctionnement applicatif, panne serveur, coupure réseau…) un mode palliatif et dégradé de consultation locale puisse être activé dans le cadre d'une procédure bien définie.
- Le logiciel de saisie des prescriptions et de suivi de leur réalisation, lié au DPI, peut, pour répondre aux exigences du PCA, diffuser régulièrement (par exemple toutes les heures) sur un poste de travail de chaque service une version imprimable (fichier « pdf » par exemple) du plan de soins et l'état de réalisation des prescriptions pour chaque patient du service. En cas d'indisponibilité du logiciel, les états peuvent être imprimés pour assurer la continuité de l'application du plan de soins et la saisie manuelle, sur ces fiches, des prescriptions affectées. La procédure doit prévoir, en cas de mise en application de cette mesure palliative, qu'un point soit réalisé au sein du service afin, si nécessaire, de mettre à jour les fiches papiers avec les réalisations de prescription réalisées depuis l'heure à laquelle elles ont été établies par le logiciel.

Les solutions palliatives ne remplacent en aucun cas les solutions de secours, mais les complètent en proposant un moyen temporaire de répondre rapidement à un besoin métier.

[10] Dispositif permettant l'accès à Internet via le réseau téléphonique mobile notamment (2G, 3G, 4G…)

Le choix de leur mise en place implique donc un coût complémentaire aux systèmes de secours classiques qui doit être mis en balance avec le gain effectif.

Le principal critère qui préside à l'adoption ou non d'une solution palliative, outre les facteurs mentionnés plus haut, est le délai de rétablissement d'un service minimal acceptable à l'aide de la solution de secours envisagée. Si le délai prévisible est trop long, une solution palliative doit, si possible, être intégrée au PCI.

Accessoirement, une solution palliative peut être mise en œuvre pour réduire ultérieurement le coût d'absorption du retard accumulé pendant la durée de mise en place de la solution de secours. Le personnel qui ne dispose plus de son outil de travail normal peut alors être affecté au traitement –probablement moins efficace– d'une partie du travail qui s'accumule.

En synthèse, une solution palliative permet de rétablir le service :

- avec un niveau parfois dégradé mais qui permet de satisfaire l'objectif minimum de continuité d'activité (OMCA – voir chap. 3.3) ;
- et dans un délai qui permet de répondre à l'exigence de durée maximale d'interruption acceptable (DMIA – voir chap. 3.2), là où cette durée est trop courte pour qu'une solution de secours puisse être mise en place dès le départ.

4.6.4 Mesures de secours

La démarche d'élaboration de solutions de secours dans le cadre du PCI est la même que celle suivie de manière générale pour le PCA de la structure. Elle doit notamment prendre en compte :

- le personnel en charge du SI, qu'il soit interne ou qu'il s'agisse de prestataires de services, et les diverses problématiques associées (transport, restauration, contrat, notamment si le site d'hébergement du SI de secours est différent du site habituel) ;
- les locaux d'hébergement du SI et leur environnement (sécurité physique, électricité, climatisation,…) ;
- les moyens de communication nécessaires au raccordement des équipements terminaux et aux échanges avec l'extérieur de la structure ;
- les moyens matériels et logiciels ;
- les contraintes de sécurité issues de la PSSI.

La priorité de mise en œuvre des différentes solutions de secours est établie en fonction des exigences métiers, de la dépendance entre les différents composants du SI et des contraintes propres à chaque solution.

4.6.5 Impact des solutions prévues sur le reste des activités

Dans la phase d'élaboration des solutions, il est important de vérifier si leur mise en œuvre aura un impact sur des activités autres que celles directement concernées par l'interruption du SI.

Exemples :

- La mise en œuvre d'une solution palliative peut induire des tâches manuelles supplémentaires de la part du personnel, lequel personnel ne pourra pas, ou moins, se consacrer à d'autres activités auxquelles il contribue normalement. L'impact sur ces autres activités doit être qualifié, faire l'objet d'un accord avec les responsables des activités concernées, et être acté dans le PCA ;
- Une solution palliative d'imagerie médicale pourrait utiliser un format d'image moins compressé, donc plus volumineux, et entrainer ainsi un

« ralentissement du réseau » perceptible pour de nombreux utilisateurs. Il convient alors de vérifier si ce ralentissement reste acceptable pour la durée d'utilisation prévue de la solution palliative.

4.6.6 Réversibilité et réintégration des données

Toute solution de secours doit être réversible, puisqu'elle est par définition temporaire et que les fonctions remplies doivent pouvoir être « rebasculées » à terme vers le SI normal avec les données associées.

En outre, il est impératif de prévoir :

- une fois la reprise informatique effectuée : la réintégration, dans le système de production de secours, des données produites par les solutions palliatives ;
- puis, une fois le retour à la situation normale effectué (i.e. quand on a quitté le système de production de secours pour revenir au système de production normal) : la réintégration, dans le système de production nominal, des données produites dans l'environnement de secours ;
- un renforcement de la communication au sein des services afin de garantir la bonne transmission des informations entre les équipes sur les mesures palliatives activées et à prendre en compte pour la suite de l'activité.

Ces opérations doivent être décidées et spécifiées en amont, et faire partie de la procédure référencée au PCI sur laquelle les différents acteurs concernés se sont accordés.

De plus, il convient notamment de s'assurer dans le cadre d'un PCI :

- que les opérations d'indexation des données seront valides au final, s'il y a une exigence de numéros de séquence uniques, croissants et consécutifs ;
- que des traitements annexes ne seront pas réalisés plusieurs fois sur les mêmes données à l'occasion de leur réintégration si une telle situation était problématique,…

Exemple : Dans le cas de la mise en œuvre de la mesure palliative présentée dans l'exemple au chapitre 4.6.3 pour le logiciel de saisie des prescriptions et de suivi de leur réalisation, il convient, lors du retour à un fonctionnement normal, d'assurer l'intégration des informations portées manuellement sur les fiches de suivi du plan de soin dans le logiciel afin que le DPI soit à jour. Plusieurs options sont possibles, parmi lesquelles :

- la ressaisie dans le logiciel par chaque personnel de santé pour les prescriptions qu'il a lui-même affectées ;
- la ressaisie dans le logiciel, par une personne spécifiquement habilitées et disposant des compétences nécessaires, des prescriptions affectées par des personnels de santés tiers, dans des conditions qui garantissent :
    - l'imputabilité de la saisie de ces informations,
    - l'identification du personnel ayant réalisé l'affectation des prescriptions, a priori différent de celui ayant effectué la ressaisie,
    - et la conservation des éléments justificatifs correspondants, comme par exemple une version numérisée de la fiche papier renseignée manuellement dans le cadre des mesures palliatives,
    - l'ensemble pouvant, si les exigences médico-légales le requièrent, faire l'objet d'une validation explicite et authentifiée de la part du personnel ayant réalisé l'affectation des prescriptions.

Si, pour une raison ou une autre, les informations ne peuvent être réintégrées dans le logiciel, il est indispensable qu'apparaisse clairement dans le DPI la période pour laquelle les informations de suivi de prescription sont conservées par un moyen alternatif (exemple version scannée de la fiche), afin que toute consultation du dossier permettre de retrouver facilement ces informations, plutôt que de faire apparaître un « vide » ambigu dans le suivi des prescriptions.

4.6.7 Sélection des solutions

Les éventuels risques ou points de vigilance associés à chaque solution doivent être clairement identifiés, qu'il s'agisse de différences dans les services fournis par rapport à la situation normale ou de difficultés liées au retour au mode normal.

Les coûts des solutions palliatives et de secours, et des différentes options éventuelles, doivent être présentés à la direction pour validation, en distinguant :

- les coûts permanents ;

  Exemple : un contrat avec un prestataire permettant l'accès à des locaux de repli sous réserve qu'il soit disponible, ou au contraire la location permanente et donc garantie d'un local de repli.

- les coûts en cas d'activation.

  Exemples :

  - tarif de location effectif en cas d'utilisation de la première option présentée dans l'exemple ci-dessus pour le local de repli ;
  - personnel devant être mobilisé en renfort afin de réaliser les opérations de ressaisie éventuellement nécessaires (voir chapitre précèdent)

Les coûts liés à la formation et au maintien de compétence du personnel informatique comme des utilisateurs pour la maîtrise des solutions palliatives, si elles sont très différentes des solutions nominales, doivent également être pris en compte au moment du choix des solutions.

4.6.8 Documentation

Le PCI doit faire l'objet d'une documentation précise et maintenue à jour, qui formalise l'ensemble des éléments décrits dans ce guide.

La fiche pratique « Programme Hôpital Numérique - Fiche pratique 3 : plan type d'un Plan de reprise d'Activité du SI et bonnes pratiques » [Réf. n°8] propose un plan pour cette documentation.

Dans la pratique :

- les mesures préventives sont souvent identifiées dans la documentation spécifique à chaque partie du SI ou à ses moyens d'infrastructure (réseau, électricité, climatisation…), et référencées dans un document utilisé à la fois dans le cadre de la PSSI (pour la dimension « disponibilité ») et dans celui du PCI ;
- les solutions de secours, les modalités de leur mise en œuvre et les procédures associées sont souvent formalisées dans le **Plan de Secours** ;
- les solutions du SI qui constituent des **solutions palliatives**, fournissant un service **dégradé ou non**, peuvent faire l'objet d'un volet spécifique du Plan de Secours, ou être traitées dans un corpus de documents séparés.
- les objectifs et les modalités de sauvegarde des systèmes et des données sont formalisés dans le **Plan de Sauvegarde** (voir guide sauvegarde [Réf. n°5]).

Ces différents documents doivent être intégrés à la gestion documentaire globale du PCA de la structure. Les moyens utilisés pour cette gestion doivent garantir la disponibilité rapide de la documentation dans tous les cas d'incident pris en compte.

Quand il est identifié que les solutions prévues ne répondent pas totalement aux exigences de continuité, quelles qu'en soient les raisons, ces limites doivent être précisées dans le PCI, comme indiqué au chapitre 5.3.

4.7 Préparer les moyens nécessaires aux mesures de continuité et tester les solutions

La démarche de préparation des moyens nécessaires au PCI est similaire à celle qui serait suivie pour le PCA global d'une structure.

Concernant les mesures prévues, il s'agit de préparer de façon concrète les solutions élaborées.

Organisation générale :

- Prendre en compte les mesures de prévention existantes ou planifiées et vérifier leur adéquation aux besoins de continuité.
- Documenter les mesures prévues et les procédures opérationnelles associées.

  Il est nécessaire de veiller au maintien à jour de la documentation requise pour la mise en œuvre du PCI en situation de crise. Outre les nécessaires exemplaires papiers, on peut noter qu'il est aujourd'hui aisé de s'appuyer sur des solutions numériques sécurisées pour l'accès à cette documentation.
- Etablir les habilitations d'accès aux ressources du SI qui peuvent être nécessaires dans le cadre spécifique du PCI en plus des habilitations habituelles.

Moyens techniques :

- Acquérir le matériel supplémentaire nécessaire et assurer son stockage dans un local distant du site principal.

  Il est recommandé que les moyens techniques destinés aux solutions palliatives et au secours soient spécifiquement **suivis**, protégés et clairement **distingués** des autres, afin qu'ils restent disponibles à tout moment et qu'ils ne puissent être confondus avec des équipements inutilisés (risquant alors d'être réaffectés).

  Exemple : Cas classique, dans les petits établissements, des environnements de développement/intégration, ou des environnements de formation, qu'il est prévu dans le cadre du PCI de « promouvoir » en environnement de production en cas de panne du serveur principal de production (à condition qu'ils soient maintenu à jour au niveau matériel comme logiciel).
- Les solutions techniques élaborées (par exemple le poste d'accès à Internet via « clé web » évoqué plus haut) doivent être testées régulièrement, soit dans le cadre d'exercices, soit dans le cadre de tests spécifiques (voir chap. 5.1).

  Ces moyens, et la documentation à jour nécessaire à leur mise en œuvre, doivent être stockés de manière à être **accessibles** aux personnes en charge de la mise en œuvre du PCI en situation de crise. Ce stockage doit être cohérent avec les scénarios d'incidents pris en compte.

  Exemple : les moyens de secours informatique potentiellement mobilisés en cas d'incendie de la salle informatique ne doivent pas être stockés à proximité de cette salle, voire dans le même bâtiment.
- Acquérir et préparer le matériel et les services supplémentaires nécessaires à la gestion de l'incident.

  Exemples : téléphone mobile et abonnement associé au numéro d'appel dédié aux astreintes pour le SI, boîte de messagerie électronique chez un hébergeur externe afin de disposer d'un moyen pour les échanges de documents avec

les divers correspondants en situation de crise si la messagerie interne ne fonctionne plus (Attention, ce type de dispositif de messagerie doit être exclusivement réservé à la gestion de crise, et ne doit en aucun cas être utilisé pour des échanges liés à la production ni pour des données métiers ou des informations sensibles de la structure).

Autre exemple : comptes utilisateurs « génériques », s'ils sont autorisés par la PSSI de la structure, destiné à être utilisés à titre exceptionnel à fin d'exécution de certaines procédures du PCI (exemple : ressaisies d'informations pour le compte d'autres utilisateurs du SI, voir exemple au chapitre 4.6.6) et qui doivent être préparés en amont afin d'être disponibles en cas d'activation du PCI. Note : Ces comptes utilisateurs « génériques » ne sont en aucun cas des comptes partagés. Ils ne doivent être affectés simultanément qu'à un et un seul utilisateur, pour une durée limitée, et cette attribution doit être tracée dans un cadre formel afin de garantir l'imputabilité des actions réalisées à l'aide de ce compte. Les moyens d'authentification associés au compte doivent être réinitialisés à la fin d'affectation du compte à l'utilisateur.

Fournisseurs :

- Contractualiser avec les fournisseurs en prenant en compte les exigences de continuité de service et la gestion de crise.
- Demander aux fournisseurs de solutions logicielles et/ou de matériel biomédical qu'ils intègrent des fonctionnalités qui facilitent la définition et la mise en œuvre de PCI, ou qu'ils fassent évoluer leurs produits dans ce sens.
- Modifier les contrats des prestataires de services qui interviennent sur le SI et qui sont susceptibles d'être mobilisés en situation de crise.

Personnel :

- Modifier les contrats de travail du personnel susceptible d'être mobilisé en cas de crise en respectant la procédure interne requise.
- Prévoir un dispositif d'astreinte afin de garantir que le personnel nécessaire est toujours disponible, y compris en dehors des heures d'activité normale des équipes du SI, pour intervenir en cas d'alerte d'incident, procéder aux premiers diagnostics rapide et déclencher si nécessaire le processus d'escalade prévue par le PCI, le PCA ou le dispositif de gestion de crise.
- Former le personnel susceptible de mettre en œuvre ou d'utiliser les moyens prévus.

Il est important que les fonctions ou les compétences impérativement requises en cas d'activation du PCI soient identifiées. Les personnes correspondantes doivent être formées en nombre suffisant, et le planning de présence ou de disponibilité doit être géré en conséquence (à l'image de ce qui se pratique pour le reste du PCA).

Concernant l'organisation des astreintes dans le cadre du PCI, la « mutualisation » du personnel d'astreinte entre structures géographiquement proches peut être une option intéressante. Elle requiert néanmoins que le personnel concerné soit autorisé à accéder aux locaux du SI, voire au SI lui-même, des structures « partenaires » et acquiert un minimum de connaissances de ces SI afin de pouvoir assurer efficacement ses tâches de premier diagnostic et de remontée d'alerte en cas d'incident.

5 Faire vivre le PCI

Pour que le PCI reste efficace dans la durée, certaines actions doivent être menées de manière récurrente :

- s'entraîner et vérifier régulièrement l'efficacité du PCI ;
- maintenir à jour le PCI :
    - dans le cadre d'une revue interne,
    - dans le cadre de tout nouveau projet concernant le SI.

5.1 S'entraîner et vérifier régulièrement l'efficacité du PCI

Le PCI est un sujet éminemment opérationnel et, comme le PCA dont il dépend, il n'a d'utilité que s'il peut être mis en application de manière efficace.

Pour cela, il est indispensable de procéder à des exercices de mise en œuvre qui permettent :

- de vérifier la **validité et la complétude des procédures et des solutions** prévues ;
- d'**entrainer le personnel concerné**, informaticien ou non, aux procédures prévues et à leurs conséquences éventuelles en termes de modification temporaire des processus métiers ;
- de vérifier la **disponibilité des compétences nécessaires** en s'assurant que les personnes qui détiennent les compétences requises sont toujours présentes ou en possibilité d'intervenir en cas de besoin.

Ces exercices peuvent être :

- des **exercices internes au SI**, étape souhaitable en préalable à tout autre type d'exercice ;
- des **exercices intégrés aux exercices PCA** de la structure, qui constituent le type d'exercice cible et permettent de vérifier :
    - l'efficacité et l'adéquation aux besoins métiers des solutions et de leur mise en œuvre,
    - la coordination entre SI et métier en situation de crise.

Il existe différents types d'exercices possibles et utiles, dont certains ne requièrent que des moyens très restreints :

- **Exercice « sur table »** : il s'agit de réunir les différents protagonistes pour « jouer le scénario », sans impacter les systèmes de production ni réellement mettre en œuvre les mesures de réaction prévues. Les acteurs peuvent ainsi s'entraîner à l'organisation prévue, aux procédures, à la connaissance des mesures, à l'enchaînement des actions, et à la communication entre les différentes personnes impliquées.
- **Exercice en environnement de test** : il s'agit de simuler la mise en œuvre effective des mesures prévues dans le cadre d'un scénario d'incident donné, mais dans un

environnement de test supposé similaire à l'environnement de production. Les acteurs peuvent s'exercer concrètement aux mesures organisationnelles et techniques, mais sans impact direct sur la production.

- **Exercice en environnement de production** : véritable test en situation presque réelle (puisque l'incident n'est que simulé), ce type d'exercice est indispensable une fois que les deux premiers types de test donnent satisfaction. Il permet en effet de confronter le PCI à l'organisation et aux conditions d'environnement réelles de la structure.

  La production pouvant être perturbée par ce type d'exercice, il est essentiel que les directions métiers soient associées à sa préparation et qu'elles donnent leur accord en toute connaissance des impacts potentiels du test.

Il est recommandé de mener ces trois types d'exercices dans l'ordre indiqué ci-dessus, qui est l'ordre croissant de complexité, de sensibilité et de coût de l'exercice. Dans les deux premiers types de test, des utilisateurs métiers du SI peuvent être associés dès lors que la maîtrise « technique » de l'exercice a été validée.

A l'issue de chaque exercice, une séance de bilan et de retour d'expérience permet d'identifier, d'une part les points faibles à traiter, et d'autre part les points forts à maintenir ou à développer. Cette démarche permet de tirer parti des résultats du test pour améliorer le système et de s'inscrire ainsi dans une logique d'amélioration continue.

> ✍ *Il est intéressant de souligner que les opérations d'arrêt de systèmes pour maintenance peuvent constituer une opportunité de mise en œuvre effective du PCI, mais dans un cadre planifié.*

> ✍ *Le retour d'expérience à la suite d'incidents réels est également une source précieuse d'enseignement et d'amélioration du PCI. C'est l'occasion de dresser un bilan concerté de l'efficacité des mesures qui ont été activées et des améliorations éventuelles à apporter au PCI.*
>
> *Ce retour d'expérience à la suite d'incidents réels constitue également une opportunité de communication et de sensibilisation sur les mesures mises en œuvre ou sur les améliorations à apporter à ces mesures, notamment du fait d'une plus grande sensibilité des directions et des acteurs métiers qui ont vécu les conséquences de l'incident.*

5.2 Maintenir à jour le PCI

L'architecture et les fonctions du SI évoluent, les activités métiers évoluent, les exigences du PCA et de la PSSI évoluent. Le PCI doit évoluer en conséquence.

> Exemple : dans le cadre du déploiement d'une nouvelle application, l'ajout de nouveaux serveurs sur une alimentation protégée par un onduleur ne doit pas surcharger l'onduleur, ni réduire sa durée de fonctionnement sur batterie à un niveau inacceptable pour les serveurs préexistants.

Deux processus permettent de s'assurer du maintien à jour du PCI :

- la **revue** interne au service informatique, qui doit avoir lieu au moins une fois par an et dont les modalités peuvent être définies dans le cadre du PCA. Cette revue permet de s'assurer :
  - que les nouveaux éléments sont pris en compte dans le plan de sauvegarde, dans les tests techniques et dans les exercices ;
  - que les moyens nécessaires au déroulement du PCI sont disponibles et adéquats : personnel en compétences et en nombre suffisants, systèmes de secours, taille des locaux de repli…,
  - que les documentations et procédures sont maintenues à jour ;
- l'intégration de la problématique **PCI pour chaque nouveau projet** impliquant l'évolution du SI afin de veiller à la prise en compte des nouveaux composants du SI dans le PCI, tant au niveau organisationnel que technique. Cette intégration du sujet PCI dans les projets permet de s'assurer :
  - de la mesure de l'impact des projets d'évolution du SI sur le PCI,
  - du développement, si nécessaire, de nouvelles mesures de continuité qui seront ajoutées au PCI afin de prendre en compte les moyens ajoutés au SI ou modifiés par le projet,
  - de l'adaptation des tests techniques, exercices, plans de sauvegarde, etc. au PCI ainsi modifié.

5.3 Identifier les limites du PCI

Il est possible que le PCI ne réponde pas totalement aux exigences qui découlent du PCA :

- soit que certaines activités identifiées par le PCA n'ont pas encore été prises en compte dans le PCI ;
- soit que les coûts ou les contraintes pour une réponse pleinement satisfaisante ne peuvent être assumés par la structure ;
- soit que toutes les mesures prévues par le PCI ne sont pas encore déployées du fait de l'étalement dans les temps des travaux nécessaires ;
- soit que les mesures mises en place ne s'avèrent pas totalement efficaces à l'occasion des tests techniques ou d'exercices, et qu'aucune solution améliorée ne peut être mise en œuvre dans les délais souhaités.

Dans ces différents cas, il est essentiel que les limites effectives du PCI soient explicitées et prises en compte par le PCA pour que les métiers puissent prévoir les mesures organisationnelles et fonctionnelles qui limiteront les impacts de l'absence de la continuité informatique attendue en situation de crise.

Cette analyse des limites du PCI par rapport au PCA doit être soumise à l'approbation des directions métier de la structure.

Elle doit faire l'objet d'une revue et d'une mise à jour en cohérence avec les événements sur ce sujet (déploiement des mesures de continuité, conclusion d'exercices de continuité informatique…) et avec la mise à jour régulière du PCI.

6 Pour aller plus loin…

Au-delà des principes et éléments exposés dans ce guide, vous souhaiterez peut-être disposer d'une méthode plus détaillée afin d'élaborer le PCI du SI de votre structure dans un cadre plus formalisé.

A cette fin, deux documents en particulier peuvent vous être utiles :

- à un premier niveau, opérationnel et pratique, le « Guide pour réaliser un plan de continuité d'activité » publié par le (SGDSN) [Réf. n°2] propose une démarche exhaustive, détaillée dans des fiches pratiques très complètes ;
- à un second niveau, beaucoup plus formel, la norme ISO 22301 « Sécurité sociétale - Systèmes de management de la continuité d'activité - Exigences » [Réf. n°1] définit la démarche et l'organisation nécessaire à la gestion maîtrisée et à l'amélioration continue de la continuité d'activité.

Il convient de noter que ces deux documents traitent de la gestion de la continuité d'activité au sens large, et ne sont pas focalisés sur les aspects Système d'Information. Les éléments qu'ils proposent restent néanmoins valides pour les SI, et peuvent également être utilisés pour le plan de continuité d'activité global de la structure (celui qui traite de la continuité des activités métiers menées au sein de la structure).

Annexe 1 : Exemple de tableau de collecte des informations pour le PCI

Le tableau ci-dessous est fourni à titre d'exemple de support de recueil des informations de synthèse nécessaires à l'élaboration du PCI.

Les trois lignes pré-remplies constituent des exemples d'activités et d'informations nécessaires à la définition d'un PCI pour ces activités.

Activités	Tâches critiques	DMIA	Durée max. en mode dégradé	OMCA	PDMA	Contraintes
Admission d'un patient sous contrainte (psychiatrie)	Edition de certificats médico-légaux en temps réel. Obligation de saisie typographique légale	4 heures (délai admissible avant envoi du certificat en préfecture et ARS)	24 heures si traitement de texte disponible sur monoposte	Produire les documents médico-légaux en temps réel	N/A (certificat envoyé dès édition)	Disponibilité sous 4 heures d'un poste de travail équipé d'un traitement de texte. Rétablissement en 24 heures de la fonction d'édition de certificats médico-légaux
Prescription de médicaments	Prescription fournie en temps réel à la pharmacie pour dispenciation	4 heures (délai admissibles pour récupération des données à postériori)	24 heures si procédure papier manuscrite	Prescriptions tracées par écrit à 100%	N/A (prescription envoyée en temps réel et rattrapage des données ultérieurement)	Rétablissement en 24 heures de la fonction de diffusion des prescriptions à la pharmacie.
Validation des prises de traitement au moment de la distribution	Vérification qu'il n'y a pas eu d'oubli de prise ou de redondance de prise (ex. somnifère donné deux fois)	4 heures, soit l'espace entre deux prises de traitement (i.e.1 prise en mode dégradé acceptable)	24 heures si procédure papier manuscrite	Validation tracées à 100%	Aucune (les traces de validation doivent être disponibles)	La procédure dégradée papier contourne l'interdiction de recopie manuelle des ordonnances qui vise à éviter les erreurs de saisie. Elle ne doit pas perdurer au-delà de 24 heures. Rétablissement de la fonction validation en 24 heures.

Rappel :

- DMIA : Durée Maximale d'Interruption Acceptable (voir chap. 3.2) ;
- Durée maximale supportable de fonctionnement en mode dégradé (voir chap. 3.3) ;
- OMCA : Objectif Minimum de Continuité d'Activité (voir chap. 3.3) en mode dégradé ;
- PDMA : Perte de Données Maximale Admise (voir chap. 3.2), afin notamment de fixer les modalités de sauvegarde des données concernées en fonctionnement normal du SI.

Annexe 2 : Glossaire

Sigle / Acronyme	Signification
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
BCP	« Business Continuity Plan » (Plan de continuité métier) : équivalent anglais de PCA
DMIA	Durée Maximale d'Interruption Acceptable
DRP	« Disaster Recovery Plan » (Plan de récupération après sinistre) : équivalent anglais de PRA
GT	Groupe de Travail
OMCA	Objectif Minimum de Continuité d'Activité
PCA	Plan de Continuité d'Activité
PCI	Plan de Continuité Informatique
PDMA	Perte Maximale de Données Admise
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
PRA	Plan de Reprise d'Activité
PRI	Plan de Reprise Informatique
PS	Professionnel de Santé
PSSI	Politique de Sécurité des Systèmes d'Information
RPO	« Recovery Point Objective » (Objectif de point de restauration) : équivalent anglais de PDMA
RSSI	Responsable de la Sécurité des Systèmes d'Information
RTO	« Recovery Time Objective » (Objectif de délai de rétablissement) : équivalent anglais de DMIA
SGDSN	Secrétariat Général de la Défense et de la Sécurité Nationale
SI	Système d'information
SIS	Système d'Information de Santé
SSI	Sécurité des Systèmes d'Information

Annexe 3 : Documents de référence

Référence n°1 : Norme ISO 22301 – « Sécurité sociétale - Systèmes de management de la continuité d'activité – Exigences »

Référence n°2 : Guide pour réaliser un plan de continuité d'activité (SGDSN)[11]

Référence n°3 : Guide d'hygiène informatique – Chapitre XI (ANSSI)[12]

Référence n°4 : Corpus documentaire de la PGSSI-S (référentiels et guides pratiques)[13]

Référence n°5 : Guide Pratique Règles de sauvegarde des Systèmes d'Information de Santé - PGSSI-S (voir Réf. n°4)

Référence n°6 : Guide d'élaboration et de mise en œuvre d'une PSSI pour les structures des secteurs sanitaire et médico-social : Structure sans approche SSI formalisée - PGSSI-S (voir Réf. n°4)

Référence n°7 : ISO/CEI 27002 - « Code de bonnes pratiques pour la gestion de la sécurité de l'information »

Référence n°8 : Programme Hôpital Numérique[14] - Fiche pratique 3 : plan type d'un Plan de reprise d'Activité du SI et bonnes pratiques

Référence n°9 : Programme Hôpital Numérique - Fiche pratique 5 : bonnes pratiques d'élaboration des procédures de fonctionnement en mode dégradé / de retour à la normale du système d'information

Référence n°10 : ISO/CEI 27031 - « Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité »

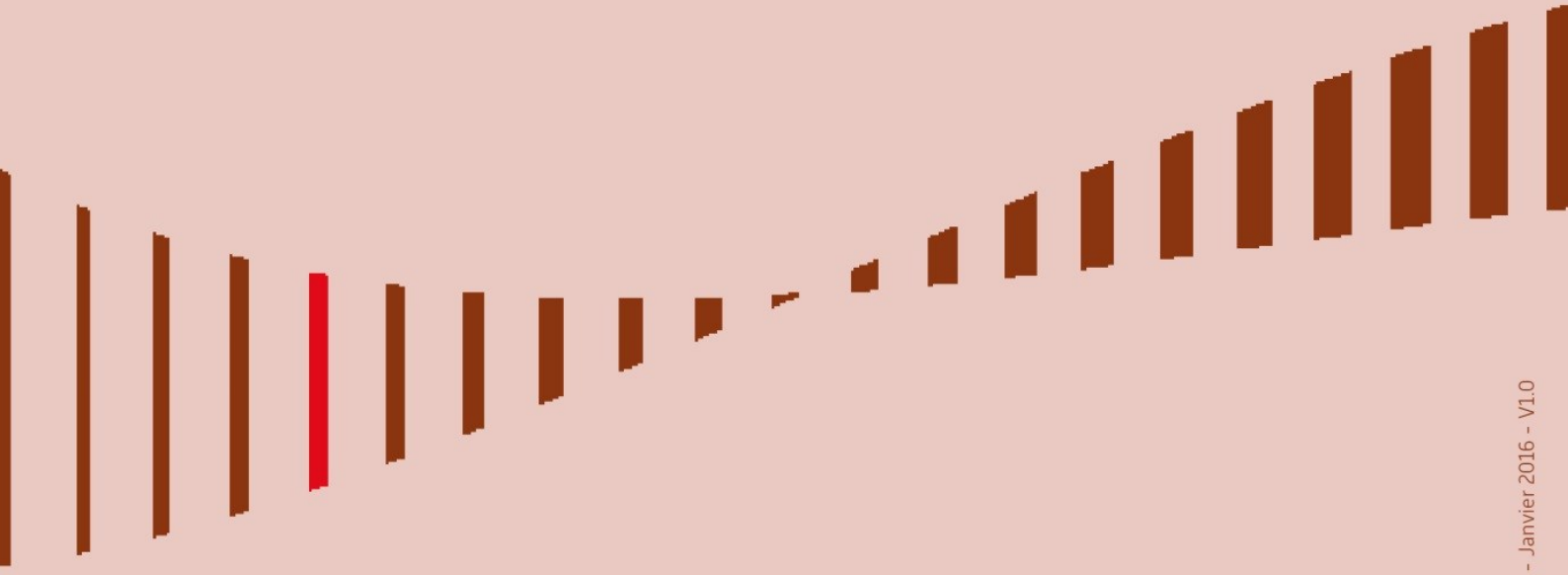
Référence n°11 : PSSI – MCAS : Politique de Sécurité des Systèmes d'Information pour les Ministère en Charge des Affaires Sociales http://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo

[11] http://www.sgdsn.gouv.fr/site_article128.html

[12] http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

[13] http://esante.gouv.fr/pgssi-s/espace-publication

[14] http://www.sante.gouv.fr/mise-en-oeuvre-du-programme-hopital-numerique-par-les-etablissements-de-sante.html



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DES AFFAIRES SOCIALES,
DE LA SANTÉ
ET DES DROITS DES FEMMES

asipsanté

Agence des systèmes d'information partagés de santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr