Dossier technique

Plan de Continuité d'Activité

Stratégie et solutions de secours du S.I.

Septembre 2003

COMMISSION TECHNIQUES DE SECURITE LOGIQUE

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, rue Pierre Semard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

TABLE DES MATIERES

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Robert	**BERGERON**	*CAP GEMINI ERNST & YOUNG*
Annie	**BUTEL**	*PRICEWATERHOUSECOOPERS*
Jean-Claude	**GANDOIS**	*LEGRAND*
Guy	**JOVER**	*CNAMTS*
Guy	**KHOUBERMAN**	*ACOSS CNIR SUD*
Siegfried	**NOEL**	*TELINDUS*

Nous tenons également à remercier la commission « Espace RSSI » et son président, **Pierre SINOQUET**, pour les échanges fructueux que nous avons eus sur le thème de la continuité d'activité.

1 INTRODUCTION

Ce document s'adresse avant tout aux responsables sécurité, directions informatiques, risk managers ou au contrôle interne. Elle concerne aussi tout acteur (Direction Générale, Direction Juridique, Direction des Ressources Humaines, Direction Administrative et Financière, ...) dès lors que sa fonction contribue entre autres à définir, implémenter, maintenir ou garantir la sécurité. Il a pour objectif d'apporter une aide au choix et à la mise en œuvre de moyens visant à assurer une disponibilité des systèmes d'information adaptée aux besoins de l'entreprise.

Le problème de la continuité du système d'information (SI) peut être abordé à diverses occasions, comme par exemple :

- dans le cadre d'un Plan de Continuité d'Activité (PCA). Ces projets stratégiques d'entreprise sont réalisés à la demande des Directions Générales. Ils ont pour but de garantir la survie de l'entreprise. Le secours de moyens informatiques ne constitue que l'un des aspects d'un PCA ;
- lors de l'élaboration d'un Plan de Secours Informatique (PSI). Le PSI concerne le secours des moyens informatiques. Il doit cependant susciter une implication forte de la Direction Générale. Le Plan de Secours Informatique vise à garantir le service minimum requis pour les systèmes d'information ;
- lors de la mise en place d'une nouvelle application, lors de changements importants concernant les architectures techniques ou lors de négociation de contrats de service. Il s'agit alors de répondre à un besoin ponctuel précis, tout en s'intégrant dans une stratégie globale (PCA, Plan de Secours Informatique), si elle existe.

Le document comporte trois parties principales :

- La prise en compte des besoins et la définition d'une stratégie de secours (chapitre 2). Ce chapitre fournit des éléments d'aide :
  - à l'analyse préalable des risques ;
  - au choix des dispositifs à mettre en œuvre (dispositifs permanents relevant de la qualité ou dispositifs de secours à déclencher uniquement en situation de sinistre).
- L'élaboration du Plan de Secours Informatique (chapitre 3). Ce chapitre décrit son organisation, ses composants essentiels et son intégration dans un plan plus global de continuité d'activité.
- La présentation des principaux dispositifs pouvant être retenus pour assurer la disponibilité d'un système d'information (chapitre 4).

Un glossaire est disponible à la fin de ce document.

2 STRATEGIE DE SECOURS

L'élaboration d'un Plan de Secours Informatique est une opération complexe par le nombre de situations à envisager (sinistre de locaux, panne de matériel, erreurs, malveillance, etc) et par le nombre et la difficulté des tâches à réaliser pour rétablir une situation acceptable pour l'entreprise. Cette opération est toujours longue à mettre en place et suppose une charge de travail importante des équipes concernées. Les exigences de continuité de service sont de plus en plus fortes et conduisent à des solutions coûteuses. Aussi convient-il de définir une stratégie de secours adaptée aux enjeux et aux contraintes de l'entreprise.

Ce chapitre présente les étapes classiques conduisant à la définition de la stratégie de secours.

On pourra se reporter utilement aux documents du CLUSIF consacrés aux méthodes et en particulier à MEHARI qui détaillent les définitions et les étapes d'étude des vulnérabilités et d'analyse des risques.

2.1 Définitions

Dans la suite du document, nous ferons référence à certaines notions d'analyse de risques, selon les méthodes MARION ou MEHARI :

L'impact : le niveau d'impact mesure les conséquences de la réalisation d'un risque sur l'entreprise. La définition des niveaux d'impact permet de préciser les situations non supportables par l'entreprise (pertes financières, atteinte à l'image, désorganisation, ...) et de disposer ainsi d'une référence commune pour l'évaluation des risques.

La potentialité : le niveau de potentialité permet d'appréhender d'une manière simplifiée la probabilité de réalisation d'un risque. On utilise habituellement 4 à 5 niveaux, ce qui est suffisant pour faire la part des choses entre le cas d'école et le risque qui a de fortes chances de se réaliser à court terme.

La gravité : combinaison de l'impact et de la potentialité. Le niveau de gravité d'un risque mesure son degré d'acceptabilité par la Direction Générale.

2.2 Démarche

2.2.1 Les phases de la démarche

La démarche pour la définition de la stratégie de secours peut être décomposée en 5 phases :

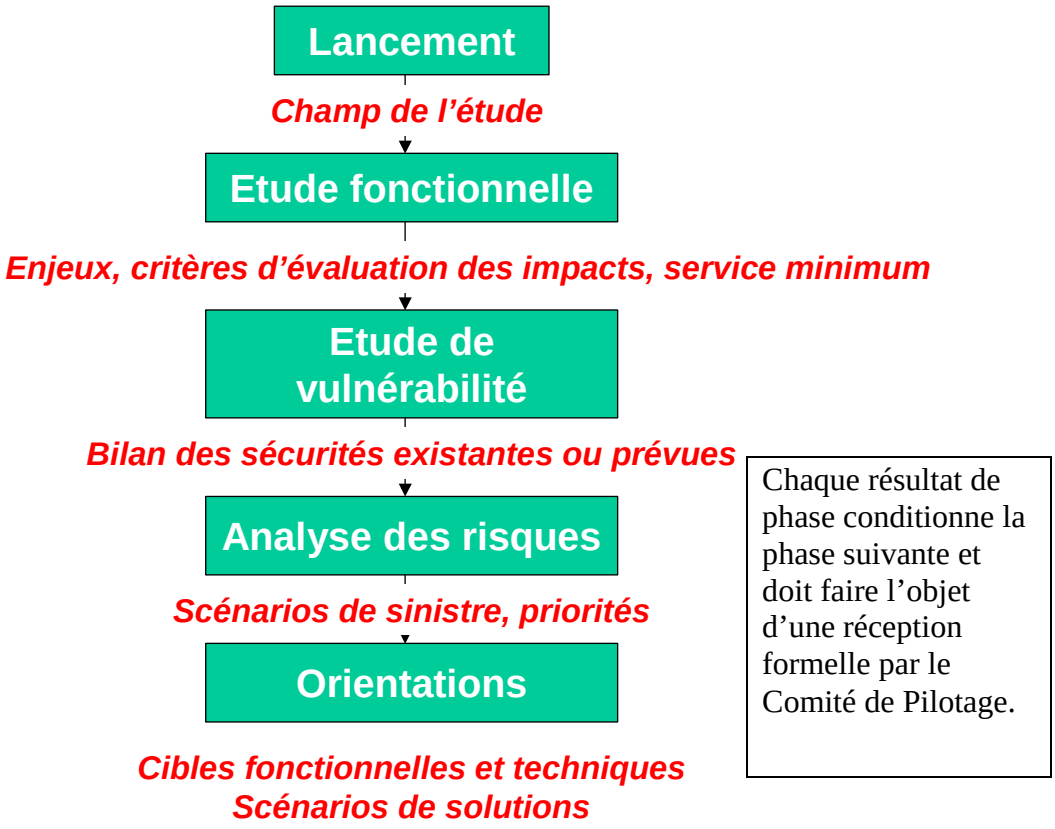

Figure 1 : Démarche de stratégie de secours

2.2.2 Phase de lancement

Avant de commencer une étude de Plan de Secours Informatique, il est essentiel d'en préciser le champ. Il convient en particulier de faire valider par la Direction de l'entreprise, via un comité de pilotage, les activités concernées et les types de risques à prendre en compte. Il peut s'agir de l'ensemble des activités ou au contraire d'un plan de secours limité à un domaine stratégique. Pour chaque activité concernée, on désignera un correspondant PSI de l'équipe projet.

La difficulté de ce type d'étude réside essentiellement dans la mise en oeuvre d'un PSI adapté à l'environnement. L'adoption d'une méthodologie personnalisée, facilitera l'appropriation par les responsables concernés.

Il y a lieu de faire préciser par la Direction les risques qu'elle souhaite couvrir. Selon les choix exprimés, les « objets à risque » concernés (matériels informatiques, matériels de téléphonie, fournitures externes, personnel, locaux, ...) et la nature des risques (faut-il par exemple traiter le risque social ?) seront précisés.

Selon les risques retenus et le périmètre souhaité, le plan de secours sera un Plan de Secours Informatique ou s'apparentera à un Plan de Continuité d'Activité.

Les fiches guides d'analyse de risque fournies en annexe de ce document listent par grandes familles les objets à risques pouvant être pris en compte dans un PSI ainsi que les principaux risques associés.

2.2.3 Phase d'étude fonctionnelle

La phase d'étude fonctionnelle a pour but de définir pour chaque activité les exigences de continuité. Il convient pour cela d'examiner les enjeux, d'identifier les activités essentielles et d'évaluer les conséquences d'interruption ou de dégradation de ces activités (arrêt temporaire ou définitif, perte de données, dégradation du service). La comparaison de ces différentes situations doit permettre d'étalonner les niveaux d'impacts (définition du caractère « non supportable » d'une situation) qui seront utilisés ultérieurement, dans la phase d'analyse des risques.

L'étude fonctionnelle doit également permettre de préciser les conditions minimales permettant d'assurer un niveau d'activité acceptable en toutes circonstances. Il faut pour cela :

- répertorier les éléments du système d'information indispensables à la poursuite de l'activité (applications, moyens de communication, informations) ;
- préciser par activité le service minimum acceptable :
  - les applications nécessaires ;
  - les ressources humaines ;
  - les locaux ;
  - les équipements (postes de travail, téléphones, imprimantes, réseau ...) ;
  - le délai de reprise d'activité ;
  - la durée du service minimum ;
  - le niveau de dégradation du service acceptable (temps de réponse, activités pouvant être manuelles...) ;
  - les conditions de retour à la normale ;
  - les fournitures externes indispensables.

Le recensement sera réalisé avec plus de profit en réunissant des groupes fonctionnels représentant chaque métier de l'entreprise. Dans ce cas il est nécessaire de procéder ensuite à des consolidations et de vérifier la cohérence globale des besoins exprimés (une tendance naturelle conduit souvent les responsables utilisateurs à considérer que leur activité est stratégique). Si nécessaire, un arbitrage sera réalisé par la Direction Générale. Lorsque les solutions à mettre en oeuvre auront été chiffrées, la notion de « service minimum acceptable » pourra être reconsidérée (processus itératif).

On déduira de cette phase la liste des applications constituant le noyau stratégique du PSI.

2.2.4 Phase d'étude de vulnérabilité

Comme dans toute étude de sécurité, il est nécessaire d'évaluer les dispositifs de sécurité actuels ou prévus. Si cette évaluation n'a pas déjà été réalisée dans le cadre d'une étude globale, il faut au minimum faire une revue des thèmes suivants :

- l'organisation de la sécurité ;
- la couverture assurance des risques informatiques ;
- la sécurité générale (environnement, accès physiques, sécurité incendie et dégâts des eaux, consignes de sécurité) ;
- les moyens de secours en place ou prévus (serveurs, réseau, terminaux, alimentation électrique, climatisation, fournitures, personnel, ..., selon le champ de l'étude). Il est important à ce stade de l'étude d'apprécier le degré de confiance qu'il est possible d'accorder à ces moyens de secours (les délais de mise en œuvre sont-ils garantis ?, ces moyens sont-ils documentés et testés ?) ;
- les moyens de protection des informations stockées :

    - supports informatiques : sauvegardes de recours, archives (accompagnés de procédures de restauration fiables) ;
    - supports papier (dossiers, archives, documentation, ...) ;
- les moyens mis en œuvre pour assurer la sécurité des échanges extérieurs (protection du réseau, ...) ;
- les contrats de maintenance des matériels et des logiciels (vérification du degré d'engagement des prestataires) ;
- les contrats fournisseurs pour les fournitures sensibles (garanties de rétablissement de service en cas d'interruption) ;
- les moyens d'administration et d'exploitation des systèmes (audit des vulnérabilités des systèmes et des applicatifs, suivi des alertes, ...).

L'examen de ces thèmes pourra conduire à des mesures préventives visant à réduire la potentialité des risques.

Pour la réalisation de cette étude, on pourra s'appuyer utilement sur les questionnaires d'audit des méthodes MARION ou MEHARI.

2.2.5 Phase d'analyse des risques

La phase d'analyse des risques a pour objet la classification des risques d'indisponibilité totale ou partielle du système d'information et la mise en évidence des priorités dans le traitement des risques. La réalisation d'un plan de secours ou d'un Plan de Continuité d'Activité est une opération lourde. La définition de priorités peut faciliter sa réalisation par tranches.

L'analyse des risques peut être décomposée en deux étapes :

- une étape technique d'étude des scénarios de sinistres ;
- une étape fonctionnelle d'étude d'impact.

L'étude technique consiste, en s'appuyant sur le constat de la phase précédente, à répertorier pour chaque objet à risque un ou plusieurs risques significatifs, puis, pour chaque risque retenu, à étudier et décrire les conséquences directes de sa réalisation sur le système d'information. A ce stade, on ne se préoccupe pas encore de l'impact du sinistre. L'objectif est de réaliser un bilan des conséquences directes en termes :

- de durée d'indisponibilité des moyens (applications, services, ...) ;
- de perte d'information (dernières mises à jour, flux, archives, ...) ;
- de potentialité du risque. Selon la méthode utilisée lors de la phase précédente, la potentialité sera soit directement attribuée, soit calculée.

L'étape fonctionnelle consiste à mesurer l'impact des risques potentiels à l'aide de critères définis lors de la phase de lancement. Cette évaluation doit être réalisée avec le concours de responsables fonctionnels afin de tenir compte des moyens de contournement existants éventuels.

Une mesure de gravité est alors déterminée en combinant impact et potentialité (cf. Méthodes MARION et MEHARI – Table d'aversion des risques). La hiérarchisation des risques est réalisée selon leur niveau de gravité décroissant. Elle permet de préciser les risques à prendre en compte dans le plan de secours ainsi que leur priorité de prise en compte.

<u>Remarque</u> : des fiches guides d'analyse des risques sont fournies en annexe de ce document. Elles proposent des risques types pour chaque famille d'objet à risque, avec pour chacun d'eux des exemples de conséquences à analyser et de parades à envisager (à ce stade de l'étude, on utilisera ces fiches pour vérifier l'existence éventuelle des parades).

2.2.6 Phase d'orientation : cible fonctionnelle et choix des solutions techniques de secours

La cible fonctionnelle se détermine par l'analyse de l'organigramme fonctionnel du système d'information et la classification des fonctions et sous fonctions selon les besoins en disponibilité estimés par les directions opérationnelles. Cette classification permettra de déterminer le noyau fonctionnel stratégique et minimum pour la survie de l'entreprise.

Sur la base de scénarios de sinistres, il faudra estimer la durée d'interruption de service associée à chaque fonction vitale, en tentant de les regrouper selon des critères de gravité (4 à 5 maximum) préalablement déterminés et pouvant aller d'une situation de « désastre » à un simple arrêt du service.

Tous les « objets » du système d'information (applications, matériels, équipements réseaux, fournitures, …) nécessaires au fonctionnement de ce noyau seront identifiés et regroupés en sous ensembles indissociables.

Au regard de ces éléments, il sera dès lors possible d'envisager et d'évaluer des scénarios de reprise et des moyens de secours appropriés pour ramener l'impact estimé à un niveau acceptable. On s'assurera aussi de conserver la cohérence d'ensemble des éléments constitutifs du secours du noyau stratégique. Le développement d'interfaces spécifiques ou la définition de procédures manuelles sont souvent nécessaires pour obtenir le niveau de service souhaité ou dégradé selon les contraintes et les moyens retenus.

Il faudra aussi établir un plan de circulation des informations et évaluer les besoins en surfaces de bureaux et postes de travail pour permettre aux utilisateurs « stratégiques » d'assurer le service minimum en situation de crise.

Enfin, pour repartir après sinistre, il faudra étudier les moyens pour restaurer et synchroniser les données associées à ce noyau fonctionnel.

La démarche décrite ci-dessus aboutit au cahier des charges du Plan de Secours Informatique.

3 LE PLAN DE SECOURS INFORMATIQUE

3.1 Introduction

Après élaboration du cahier des charges du plan de secours, une étude des solutions doit être menée tant sur les aspects techniques que sur les aspects organisationnels. A l'issue de cette étude, un dossier de choix de solutions sera soumis aux instances de décision afin de définir le contenu définitif du Plan de Secours Informatique (les différents types de solutions envisageables seront présentés dans le chapitre 4). A ce stade de l'étude, le chiffrage des solutions peut conduire à un ajustement des moyens demandés.

Un *plan de préparation* sera alors exécuté pour la mise en place des solutions retenues. Ce plan comporte les phases d'étude détaillée, de mise en place, de test et de formalisation des procédures opérationnelles. L'ensemble de ces solutions et de ces procédures constituent le *plan d'exécution* activé en cas de sinistre.

Le plan de préparation pourra avec profit faire l'objet d'un tableau de bord, désignant les responsables des actions, et en mesurant l'avancement.

L'objet de ce chapitre est de préciser les principaux thèmes à traiter au cours du plan de préparation. La documentation produite dans cette phase constituera le Plan de Secours Informatique.

3.2 Organisation

Les différentes tâches de pilotage et de mise en œuvre du secours doivent être affectées à des « acteurs ». Ces acteurs sont des entités opérationnelles prédéfinies composées de personnes en nombre suffisant, de manière à ce que, en cas de sinistre, la réalisation de la tâche soit garantie.

Les premiers intervenants sont chargés d'appliquer les consignes et de donner l'alerte, selon les procédures d'escalade définies.

En cas de sinistre, on distinguera ensuite :

- le comité de crise ;
- la cellule de coordination ;
- les équipes d'intervention ;
- les services utilisateurs.

On désignera également par « structure de crise » l'ensemble Comité de Crise-Cellule de Coordination.

3.2.1 Le Comité de Crise

Le comité de crise doit être composé au minimum des Directions suivantes : Direction Générale, Principales Directions utilisatrices, Direction des Services Généraux et des Ressources Humaines, Direction Informatique, Direction de la Communication, Responsable du Plan de Secours. Le comité de crise prend les principales décisions concernant le secours. Il juge en particulier de l'opportunité de déclencher tel ou tel volet du Plan de Secours Informatique, en fonction du contexte. Le Comité de Crise peut se faire assister de compétences spécifiques, internes ou externes, notamment pour la communication et les aspects juridiques.

Des moyens de communication avec le comité de crise doivent être prédéfinis et garantis en cas de sinistre (lieu de réunion, numéros de téléphone, de fax, ...).

3.2.2 La Cellule de Coordination

Le pilotage proprement dit des opérations de secours peut être confié à une cellule de coordination, qui déchargera le comité de crise de tâches de coordination.

La cellule de coordination sera idéalement composée d'un petit nombre de personnes : le Responsable du Plan de Secours Informatique (personne maîtrisant l'ensemble du Plan) et les personnes chargées de la coordination des opérations informatiques et de la logistique.

Certaines décisions peuvent être déléguées à cette cellule de coordination par le comité de crise, notamment l'anticipation du déclenchement de certains dispositifs (exemple : réservation du site de secours chez un prestataire).

3.2.3 Les équipes d'intervention

La réalisation des tâches de secours incombe aux équipes d'intervention définies selon les compétences requises, la disponibilité et le lieu d'intervention. On devra s'assurer que les contrats de travail sont compatibles avec un déplacement des équipes concernées sur un autre site.

Exemples :

- équipe logistique chargée du transport des matériels ;
- équipe d'intervention informatique, composée d'un spécialiste réseau et d'un agent de maintenance, chargée des opérations sur le site de secours ;
- équipe chargée de la communication de crise ;
- équipe d'intervention réseau chargée du paramétrage réseau sur le site de secours des utilisateurs ;
- etc.

Notons enfin que certains acteurs externes à l'entreprise doivent également être identifiés : prestataire de secours, fournisseurs d'énergie, opérateur téléphonie, fournisseur d'accès Internet, …

L'ensemble des intervenants internes et externes avec leurs coordonnées doit être répertoriés dans un « annuaire du plan de secours » tenu à jour.

3.2.4 Les services utilisateurs

Les services utilisateurs prennent en charge leur propre plan de reprise d'activité en fonction des moyens de secours mis à leur disposition. Parmi les tâches qui incombent aux responsables de ces services, on notera :

- les tâches d'attente du secours ;
- l'organisation du redémarrage (normal ou dégradé) ;
- la mise en place de procédures de contournement éventuelles ;
- l'organisation de travaux exceptionnels (exemple : rattrapages).

Il est important de s'assurer que des compétences humaines seront bien disponibles en toutes circonstances et connaissent les procédures techniques à suivre dans le contexte du système de secours. Si besoin, il est possible de s'appuyer sur des compétences des intervenants externes, qui ont déjà participé à des tests de continuité précédents.

3.3 Déclenchement

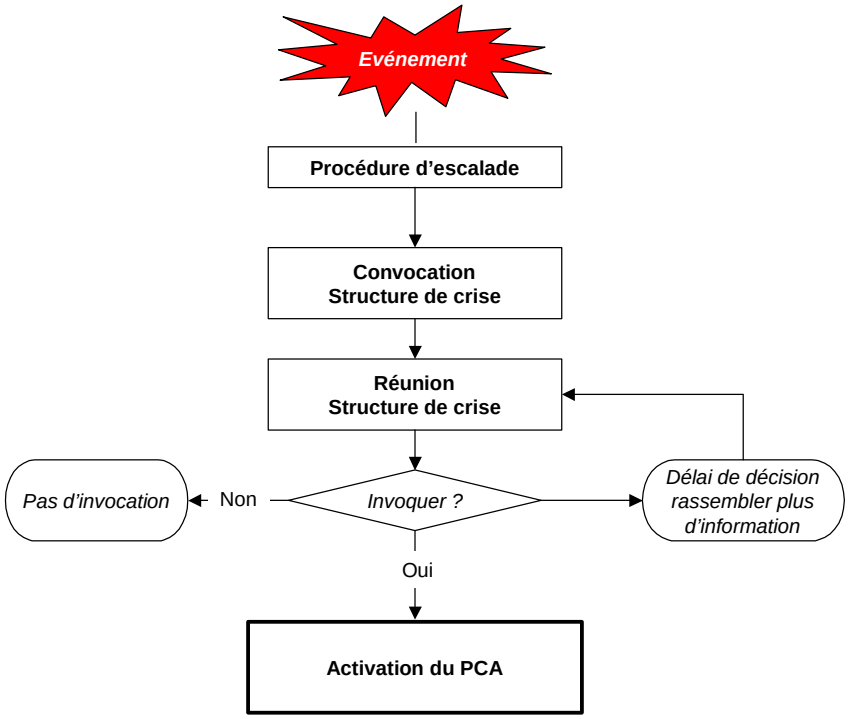

Figure 2 : Déclenchement

La structure de crise est composée du comité de crise et de la cellule de coordination.

Les procédures d'escalade sont essentielles. Lorsqu'un incident survient, la personne informée qui est souvent à un poste de sécurité de l'entreprise doit savoir qui contacter et comment contacter (notamment en cas d'indisponibilité des moyens habituels de communication). Cette personne doit à son tour, selon le type et la gravité de l'incident, connaître les personnes à contacter pour avoir des précisions ou bien mobiliser la structure de crise. Il est important de définir à l'avance qui est habilité à activer la structure de crise et surtout n'appeler que les personnes strictement désignées afin d'éviter un encombrement inutile des lignes.

3.4 Les dispositifs de secours

Un plan de secours est composé de dispositifs élémentaires (procédures techniques ou organisationnelles) dont l'activation dépendra de l'événement survenu et du contexte général. Le déclenchement de certains dispositifs ou leurs modalités d'exécution peuvent en effet dépendre de nombreux éléments (exemple : la communication de crise).

Les dispositifs d'un plan de secours peuvent être classés par types d'activité :

- la mobilisation des ressources nécessaires :
  - ressources humaines : mobilisation des équipes d'intervention ;
  - réservation des moyens de secours (réquisition de moyens, alerte d'un prestataire externe, ...) ;

    - récupération des sauvegardes ;
    - récupération de la documentation ;
- le secours des équipements informatiques :
    - restauration des environnements système ;
    - adaptations techniques (le matériel de secours n'est pas toujours identique au matériel d'origine) ;
    - restauration des applications ;
    - validation des restaurations ;
- le secours des réseaux :
    - mise en place des équipements de secours ;
    - basculement sur liaisons de secours ;
    - paramétrage des différents équipements ;
- le secours de la téléphonie :
    - reroutage des appels ;
    - mise en place d'équipements de secours ;
    - paramétrage ;
- la reprise des traitements :
    - adaptations logicielles ;
    - adaptation des procédures d'exploitation ;
    - récupération de flux et synchronisation des données ;
    - traitements exceptionnels ;
    - validations fonctionnelles ;
- la logistique :
    - transports ;
    - fournitures ;
    - gestion de crise du personnel (choix des personnels à mobiliser, rotation des équipes, prise en compte des situations individuelles , ...) ;
- le relogement :
    - organisation du relogement d'urgence ;
    - préparation des sites d'accueil ;
- la reprise des activités des services utilisateurs :
    - tâches utilisateurs avant mise en place des moyens de secours ;
    - organisation d'un service minimum ;
    - travaux exceptionnels (procédures de contournement, rattrapages, ...) ;
- la communication de crise :
    - interne (personnel, autres entités, ...) ;
    - externe (clients, partenaires, public, ...) ;
- les dispositifs de post-reprise :
    - dispositifs préalables et d'accompagnement (assurance, remise en état des locaux, sauvetage des matériels, ...) ;
    - dispositifs de retour à la normale (constituent un plan spécifique).

Pour être opérationnels, ces dispositifs de secours doivent être accompagnés de dispositifs permanents destinés à les maintenir à niveau (exemples : le plan de sauvegarde, les procédures de mise à jour et de formation des acteurs du PSI, ...).

3.5 Documentation

La documentation constitue un élément essentiel d'un plan de secours. Elle est en général assez volumineuse et très évolutive (nouvelles affectations de personnel, évolution de configurations, nouvelles applications, ...). Pour toutes ces raisons, il est conseillé de gérer la documentation à l'aide d'un outil spécialisé dans la gestion de plans de secours ou de plans de continuité d'activité. On veillera également à la confidentialité de ces documents, susceptibles de contenir des informations stratégiques de l'entreprise et nominatives.

La documentation d'un plan de secours peut être structurée en 4 niveaux, selon l'objectif visé : communiquer, mettre en œuvre, gérer, contrôler.

3.5.1 Les documents de communication sur le plan de secours

La communication interne sur le plan de secours ne doit pas être négligée. Elle doit permettre aux différents responsables d'avoir une bonne vue d'ensemble des solutions prévues et de leurs conditions générales de mise en œuvre. Cette documentation inclura notamment :

- un rappel des objectifs de continuité de service ;
- une description générale des différents dispositifs du plan de secours (secours des équipements informatiques, secours des télécommunications, solutions de relogement, communications de crise, ...) ;
- une description générale de la structure de crise ;
- les principes d'alerte de la structure de crise et de pilotage des opérations ;
- un rappel des risques résiduels.

3.5.2 Les documents de mise en œuvre du Plan de secours

Ces documents constituent le cœur du plan de secours. Ils sont destinés aux personnes ayant la responsabilité des différents dispositifs du plan et décrivent tous les éléments utiles à leur mise en œuvre : procédures, documentation technique, éléments de synchronisation, contrats, … La documentation technique devra, par son niveau de détail, permettre de réduire les erreurs humaines liées au stress.

Concrètement, cette documentation comportera au minimum :

- un annuaire du plan de secours, répertoriant tous les intervenants potentiels, internes ou externes, avec leurs coordonnées ;
- une description de la stratégie de secours retenue pour chaque risque identifié. Ce document est destiné à la structure de crise pour l'aider dans ses décisions. La stratégie de secours définit l'ensemble des dispositifs de secours à déclencher selon le contexte de l'incident (type d'événement, étendue des dégâts, ...) ;
- le planning des différentes phases de reprise ;
- les fiches de tâches à réaliser, structurées par acteur et / ou dispositif de secours ;
- la « feuille de route » de chaque acteur du plan, pour chaque cas répertorié ;
- l'ensemble des annexes utiles (documents de procédures, documentation technique, copies de contrats, schémas, ...).

Associée à un outil de pilotage, cette documentation permettra également à la structure de crise le suivi du déroulement des opérations.

Un exemplaire de cette documentation (papier et / ou outils de gestion du plan) sera conservé à l'extérieur de l'entreprise, dans un lieu sécurisé dont l'accessibilité doit être compatible avec les objectifs de redémarrage.

3.5.3 Les documents de gestion du plan de secours

Pour la gestion du plan de secours, il convient d'établir une documentation complémentaire destinée aux responsables du plan et des dispositifs associés. Cette documentation a pour but de faciliter les évolutions ultérieures. Elle peut être constituée de tableaux d'analyse des ressources et de leur utilisation, de listes de diffusion des documents. Elle inclut également l'historique des résultats de tests et les plans d'ajustement consécutifs.

3.5.4 Les documents de contrôle du plan de secours

- Tableaux de bord :
  - Planning de tests ;
  - Compte-rendu détaillé des tests ;
  - Indicateurs de qualité des dispositifs et du plan ;
  - Evaluation des risques résiduels.

3.6 Maintenance du plan

3.6.1 Organisation

Un responsable du plan de secours sera nommé. Il aura pour missions principales :

- effectuer, suivre et gérer les tests et les modifications qui en découlent
- engager et suivre le processus d'actualisation du plan de secours en fonction de l'évolution des risques (nouvelles menaces, nouveaux projets, nouvelles technologies, …) ;
- maintenir, sécuriser et diffuser la documentation du plan de secours.

Des circuits d'informations seront mis en place afin qu'il ait connaissance :

- des nouveaux risques ;
- des évolutions techniques et structurelles ;
- des nouveaux projets.

Un comité plan de secours composé des responsables des différents dispositifs et des responsables des moyens techniques (informatique, Services généraux) sera réuni régulièrement (au moins 2 fois par an). Ce comité animé par le responsable du plan, aura la charge d'évaluer les nouveaux risques et de proposer un plan d'actions qui traitera de :

- la mise en œuvre des moyens de sécurité ;
- l'actualisation de la documentation ;
- l'évolution éventuelle du contrat avec le prestataire ;
- les tests des nouveaux secours.

Le responsable du plan assurera la coordination de l'ensemble de ces actions.

3.6.2 Outils

Un plan de secours est à la fois complexe (il est composé de nombreux dispositifs destinés à faire face à toutes sortes de situations), et très évolutif (changements d'organisation, d'activités, d'enjeux, de personnes, d'architectures techniques, d'applications, ...). Sa gestion à l'aide d'un simple outil de traitement de texte est illusoire.

La maintenance d'un plan de secours est grandement facilitée par l'utilisation d'un outil spécialisé. On recherchera notamment dans cet outil les fonctionnalités suivantes :

- la gestion complète de la documentation de mise en œuvre de chaque dispositif constitutif du Plan ;
- la gestion des ressources nécessaires à la mise en œuvre des dispositifs ;
- la production du planning des opérations de reprise, selon la situation à traiter ;
- la gestion des tests (planification, suivi des résultats, mesure d'efficacité du plan, ...) ;
- la gestion des stratégies de secours, en fonction des types de sinistre et de leur gravité ;
- la production d'indicateurs de qualité et d'efficacité des différents dispositifs et du plan global ;
- les modes de diffusion de la documentation (listes de diffusion automatisées, intranet, ...) ;
- le contrôle de la mise à jour régulière de la documentation.

On préférera un outil s'appuyant sur une base de données et qui facilitera l'étude d'impact des évolutions (recherche des tâches qui incombaient à une personne mutée, identification des dispositifs impactés par un changement applicatif, recherche des scénarios de sinistre à revoir suite à un déménagement de service, ...).

3.7 Plan de test

Le Plan de Secours Informatique doit être validé par un plan de test permettant en premier lieu de réceptionner chacun des dispositifs de secours, leur synchronisation, et ensuite de contrôler par des tests réguliers, plus ou moins proches de situations réelles, le caractère opérationnel du plan de secours.

Trois catégories de tests sont à distinguer :

- les tests techniques unitaires : ces tests techniques sont destinés à valider un élément du secours (par exemple le secours d'un serveur) : validation de la configuration de secours, validation des procédures et des délais, validation du choix des intervenants, validation de la documentation ;
- les tests d'intégration : les tests d'intégration doivent permettre de valider la compatibilité des différents éléments de secours, la synchronisation des opérations techniques et la charge des différentes équipes ;
- les tests en vraie grandeur : ce dernier type reprend les caractéristiques des tests d'intégration avec comme objectif supplémentaire un test de réactivité des équipes et une vérification de bon fonctionnement par un travail effectif d'utilisateurs dans des conditions proche d'une situation de crise (moyens réduits, documentation absente ou réduite, ...). Les tests en vraie grandeur ne pourront être exécutés que si les tests décrits précédemment sont réussis. Ils peuvent constituer un risque pour l'activité qu'il convient d'évaluer préalablement. Ces tests pourront être « à blanc » (travail des utilisateurs en parallèle sur des copies jetables des applications de production), ou être réels et prévoir dans ce cas à la fin du test l'intégration du travail effectué dans les bases de production. Les tests en vraie grandeur permettent également de tester le pilotage des opérations (structure de crise et outils de pilotage). Les tests en vraie grandeur pourront être impromptus (au moins vis à vis des équipes d'intervention).

Dans le cadre du plan de test on s'assurera que chaque année les dispositifs les plus critiques du Plan de Secours Informatique font l'objet d'un ou plusieurs tests. Le nombre de tests d'intégration ou en vraie grandeur conseillé est de 1 à 2 par an. Les tests techniques unitaires seront réalisés périodiquement (1 fois par trimestre) et systématiquement après toute évolution de l'équipement à secourir ou après toute modification concernant le dispositif de secours.

Pour chaque test, on réalisera les opérations suivantes :

- la formalisation des objectifs visés ;
- la description du scénario de test : préparation, simulation, cas testés, modalités de tests utilisateurs, travail à blanc ou réel, modalités de validation, … ;
- la préparation du test : réservation des moyens techniques et humain, présentation et validation des tâches et du planning (sauf si test impromptu), remise de documentation, … ;
- la désignation d'un ou plusieurs observateurs chargés de suivre le déroulement des opérations et de noter les problèmes rencontrés ;
- la rédaction d'un compte-rendu de test et d'un bilan permettant de prononcer la validation de tout ou partie du plan de secours et proposant les actions correctives nécessaires.

4 LES SOLUTIONS DE SECOURS

4.1 Les solutions de secours informatiques

La solution globale est la résultante de plusieurs solutions adaptées en fonction des exigences de reprise demandées et des pertes de données acceptées par les utilisateurs. Chacune d'entre elles étant la combinaison d'un certain nombre d'attributs qui peuvent globalement être regroupés en 3 grandes classes :

a. le mode de gestion contractuelle des moyens de secours (comment les conditions de déclenchement et de mise à disposition sont-elles formalisées ? Comment sont gérées les priorités dans le cas de moyens mutualisés) ;
b. le type de moyens mis en œuvre (moyens fixes ou mobiles, locaux ou distants, …) ;
c. le niveau de préparation et de disponibilité des moyens (les moyens sont-ils « prêts à l'emploi », ou nécessitent-ils des préparations complémentaires ?) et les limites d'utilisation des moyens de secours (les moyens mis en œuvre ont-ils une limitation dans le temps, pour des raisons contractuelles, techniques, de performances, de montée en charge, … ?).

Par le terme « combinaison », on entend qu'il existe un nombre important de solutions résultant de l'association des différentes valeurs possibles pour ces attributs. Par exemple, dans une situation donnée, la solution optimale peut être :

Gestion = accord contractuel avec fournisseur externe pour des moyens mutualisés

Moyens = container mobile

Etat de Disponibilité = matériel opérationnel sans fichiers

Dans un autre cas de figure, c'est la solution suivante qui peut être la mieux adaptée :

Gestion = interne, avec des moyens dédiés

Moyens = installation fixe sur site interne distant

Etat de disponibilité = configuration « miroir »

Il est cependant important de noter que toutes les solutions dignes de confiance nécessitent des investissements (matériels et immatériels) et des dépenses permanentes en temps normal. C'est dangereux de croire que l'on pourra attendre le jour du sinistre pour définir précisément et mettre en place une solution de secours. De la même façon qu'il n'existe pas et n'existera jamais « d'assurance du lendemain », il est totalement illusoire de penser que l'on trouvera toujours, au pied levé, un fournisseur, ou une « relation » qui pourra « dépanner au moins quelques temps », et que cela ne dépend que du prix que l'on est alors prêt à payer.

Les scénarios de solutions élaborés dans la phase « Orientation » de la démarche d'élaboration d'un Plan de Secours Informatique (cf. §2.2.6.) sont constitués d'un ensemble de dispositifs destinés à assurer la continuité de la chaîne informatique nécessaire aux activités stratégiques, pour un ensemble défini de risques.

Dans un contexte d'informatique répartie, le scénario retenu sera le plus souvent constitué d'un ensemble de solutions techniques et / ou organisationnelles qui seront combinées selon la situation. Ces solutions élémentaires seront des solutions de secours propres à différents domaines tels que :

- le réseau local ;
- les accès réseau externes ;

- le cas particulier des accès Internet ;
- le secours de serveurs stratégiques devant assurer un service 24h / 24 ;
- le secours de serveurs pouvant supporter une indisponibilité de 24h ;
- le secours de la fonction téléphonie ;
- le secours d'un call-center ;
- le secours d'un plateau utilisateurs ;
- etc.

De très nombreuses solutions de secours sont possibles, s'étageant de la mise en place et de l'exploitation permanente d'installations complètement dupliquées, jusqu'à la conclusion plus ou moins formelle d'accords d'aide réciproque entre sociétés.

On s'assurera de la cohérence globale des choix réalisés pour chacun de ces sous-systèmes. Il est notamment nécessaire, avant validation du scénario retenu de solution, de faire une analyse des risques résiduels afin d'une part de vérifier que les risques qui devaient être traités le seront effectivement et que les solutions envisagées n'induisent pas de nouveaux risques inacceptables.

Les critères d'évaluation d'une solution de secours peuvent être classés en deux groupes.

A - Les critères permettant de vérifier qu'un scénario de solution répond aux besoins exprimés dans le cahier des charges du plan de secours :

- le délai de reprise : le délai total de reprise est la somme des délais de déclenchement, temps de mise en œuvre (approvisionnement, restauration, tests, ...), et temps de re-synchronisation des données. Ce facteur, ainsi que la durée maximale de disponibilité des installations de secours sont des paramètres essentiels pour calculer les pertes d'exploitation résiduelles éventuelles, donc l'efficacité de la solution. Une attention particulière devrait être portée aux délais de détection et de prise de décision, afin de les minimiser ;
- le degré de fraîcheur des données remises à disposition des utilisateurs ;
- le degré de couverture : la solution envisagée permet-elle de couvrir les risques retenus ? Quels sont les risques résiduels non traités ? La solution est-elle utilisable hors sinistre (déménagement, conversion, ...) ?

B - Les critères permettant d'évaluer les avantages et inconvénients des scénarios envisagés :

- la vraisemblance de la solution : une solution peut paraître viable et digne de confiance à un moment donné, mais la garantie de sa disponibilité et de son évolution dans le temps parallèlement à celle des besoins de l'entreprise n'est pas acquise. En outre certaines solutions doivent tenir compte de possibilités d'accumulation de risques – géographiques, sectoriels, … - et enfin, la réalisation de tests réalistes réguliers est un facteur déterminant et une preuve de vraisemblance (ou d'invraisemblance !) ;
- la souplesse de mise en place du Plan de Secours Informatique : il est souvent difficilement envisageable de traiter rapidement tous les risques inacceptables. Une solution souple permettra de construire le plan de secours de manière modulaire, par tranches, et permettra ainsi de s'adapter à différentes contraintes (budget, disponibilité des ressources internes, synchronisation avec d'autres projets de l'entreprise, acquisition du savoir-faire, degré de maturité du marché, ...) ;
- l'évolutivité de la solution : traduit sa capacité à prendre en compte les évolutions au sein de l'entreprise (architecture technique, organisation, enjeux, nouveaux risques, ...) ;

- les coûts : chaque type de solution entraîne un cortège de frais fixes, variables, récurrents :
  - les coûts de préparation (mise en place) de la solution ;
  - les abonnements et contrats divers ;
  - les coûts ultérieurs de maintenance et de réactualisation de la solution (tests, évolutions des configurations, charge d'exploitation supplémentaire, consommations...) ;
  - les coûts d'utilisation de la solution (une partie de ces coûts peut être prise en charge par une assurance).

Le développement ci-dessous va passer en revue les différentes typologies de solutions de secours pour chacun des attributs mentionnés au début, ainsi que leur adéquation aux critères qui viennent d'être définis.

4.1.1 Typologie et modes de gestion des moyens de secours

A – Typologie des solutions de secours

Trois grands types de solutions sont habituellement rencontrés, faisant appel soit à des moyens internes, soit à des moyens externes à l'entreprise :

Accords de réciprocité (entre sites d'une même entreprise ou entre entreprises différentes) :

Si ce type de solution est très attirant sur le plan financier (il s'agit souvent d'accords gracieux), il est dans la plupart des cas totalement illusoire sur le plan de la vraisemblance et de l'efficacité, notamment depuis la généralisation des traitements interactifs : difficultés de suivi et de synchronisation de l'évolution des parcs informatiques des « partenaires », invraisemblance du maintien permanent d'une surcapacité dans chacun des sites, sous-estimation des problèmes de conflits de priorités et d'intérêts risquant de naître au moment du sinistre, graves problèmes juridiques potentiels de validité des pouvoirs des signataires et de transfert et de limitation de responsabilités en cas de non-respect des engagements, quasi-impossibilité de faire des tests, oubli ou sous-estimation des problèmes de logistique dans l'espace et le temps (accueil utilisateurs, connectique, ...).

Pour les mêmes raisons, et du fait de l'absence de professionnalisme, les notions de durée de mise à disposition et de temps de mise en œuvre sont immatérielles, car pouvant tendre respectivement vers zéro et l'infini sous la pression de la réalité.

La capacité à couvrir d'autres cas que des sinistres est en général nulle, du fait de la probabilité d'effets de cascade.

Compte tenu de l'évolution de la complexité des architectures des systèmes d'information, ce type de solution n'est envisageable que dans des cas très particuliers et ne peut être que partielle.

Appel à des moyens de secours partagés (éventuellement spécialisés) :

Dans ce cas, plusieurs entités prévoient de pouvoir avoir recours à un même ensemble de moyens pouvant être dédiés à usage de secours. Les modalités de gestion possibles seront examinées au paragraphe suivant. En temps normal, ces moyens peuvent être affectés à d'autres tâches non prioritaires permettant de leur conférer une certaine rentabilité

(service bureau non répétitif, mise au point d'applications, banc d'essai ou de simulation, démonstrations, …).

La vraisemblance de la solution est acceptable si on est attentif à maîtriser le nombre d'entités partageant les structures, l'homogénéité des niveaux de prévention en place chez les partenaires, la non-accumulation de risques sectoriels, et la qualité des tests.

Le coût de ce type de solution varie suivant le degré de mutualisation des installations, et des possibilités de rentabilisation : comme cette dernière peut être aléatoire (puisque les installations ne peuvent abriter que des activités non prioritaires), le coût peut être déjà significatif (plusieurs pourcents du coût d'acquisition des moyens mis en œuvre).

La protection vis-à-vis de sinistres résultant d'erreurs ou de malveillances logiques peut même être envisagée si la structure de secours dispose d'étalons anti-virus ou est alimentée à partir de sauvegardes préparées selon des procédures THS (Très Haute Sécurité).

Elles ne sont cependant pas acceptables dans les cas où il est impératif que les moyens de secours ne soient pas mutualisables en cas de sinistre (puisque par définition, dans le cas de moyens partagés, le risque de « collision » de besoins n'est jamais nul). Elles ne doivent donc pas être retenues dans le cas d'entités soumises à des astreintes de service, où lorsque les risques résiduels ne peuvent pas être transférés aux assurances.

Limitation contractuelle : dans le cas de moyens partagés, le prestataire (surtout s'il est extérieur à l'entreprise) peut avoir défini une durée limite de mise à disposition, de façon à borner ses risques d'appels simultanés aux mêmes ressources.

Appel à des moyens dédiés (éventuellement spécialisés) :

Dans cette catégorie, on considère que chaque entité dispose d'un environnement qu'elle est la seule à pouvoir réquisitionner en cas de sinistre. Ceci n'exclut pas que les installations soient affectées à d'autres tâches non prioritaires en dehors des situations de crise.

Cette solution représente la version optimale en matière de vraisemblance, puisque l'on peut pré-définir avec certitude la disponibilité, les délais de mise en œuvre, et les niveaux de dégradation fonctionnels ; en outre, il est aisé de conduire des tests fréquents, et l'utilisation des infrastructures est possible pour résoudre des cas d'indisponibilité ne résultant pas de sinistres matériels.

Le seul inconvénient est en général le coût de création et d'entretien de telles infrastructures. Ce type de solution est en général réservé à des besoins de haute disponibilité, ou rendu nécessaire par la spécificité des équipements.

Limitation logistique : les moyens mis en œuvre, notamment au niveau des infrastructures de repli doivent être acceptables, y compris en cas d'utilisation prolongée du site de secours.

B – Modes de gestion des moyens de secours

On distingue généralement 4 méthodes de gestion des solutions de secours, selon leur degré de formalisation et d'externalisation :

Gestion formelle externe :

Dans ce cas, il est prévu d'obtenir les moyens de secours auprès d'une entité extérieure à l'entreprise, soit auprès d'une société spécialisée, soit auprès d'une autre entreprise garantissant de dégager et / ou mettre à disposition une capacité de traitement adéquate au moment d'un sinistre ; les relations entre demandeur(s) et fournisseur(s) sont régies par

des accords contractuels précis (en termes de services devant être fournis et de manquements aux engagements) et testés régulièrement (voir la fiche « Contrat »).

Il est possible dans ce cas de garantir raisonnablement un bon niveau de vraisemblance, et de bien cerner les paramètres de délais et durées.

La vraisemblance est notamment bien mise en valeur par la conduite régulière des tests contractuels. Il est à noter que les points délicats se trouvent au niveau :

- des clauses de limitations de responsabilités du fournisseur, si celui-ci est amené à faillir à sa mission du fait de conflits de priorités ou de problèmes techniques ;
- de la capacité du fournisseur à s'adapter rapidement aux évolutions technologiques ;
- du maintien de la sécurité du S.I., notamment dans le cas de moyens partagés.

Il est en outre possible, dans la plupart des solutions appartenant à cette catégorie, de couvrir des risques liés à des conflits sociaux.

Gestion formelle interne :

Ici, les solutions de secours sont internes à l'entreprise (vs. prestataire externe), et sont régies, comme ci-dessus, par des contrats de service précis et testées régulièrement.

Les avantages de ce type de solution résident dans la souplesse de l'adéquation aux besoins, d'utilisation et d'évolution.

Au niveau des coûts, il est difficile de préjuger de l'intérêt de cette solution par rapport à la précédente, dans la mesure où d'une part elle comporte certains éléments de réduction des coûts (conservation des investissements en interne, effets d'échelle sur des infrastructures existantes), mais qui peuvent être annulés par des éléments contraires (coût de la phase d'apprentissage, difficulté à maintenir le niveau d'opérabilité de la solution, nécessité de dédoubler les investissements en cas d'évolution matérielle divergente des sites, …).

La couverture de risques sociaux est en général plus difficile avec ce type de solutions et on doit souvent craindre une propagation des problèmes.

Gestion formelle mixte (type GIE) :

Ici, les solutions de secours sont partagées entre plusieurs entités ayant une communauté d'intérêt, dans un cadre légal et contractuel précisant parfaitement les conditions du partage des coûts et des moyens.

Les avantages fonctionnels de ce type de solution sont nombreux (coût global, adéquation de la solution, utilisation pour des tâches non prioritaires, …), mais la mise au point contractuelle est en général délicate (comportement en cas de conflits de priorité, gestion des besoins spécifiques et des cas d'évolutions divergentes des entités membres, risque d'accumulation de risques sectoriels, admission et retrait de membres, imputation et propriété des investissements, gestion de la phase transitoire de création, attribution des responsabilités d'animation du groupe et d'administration des moyens, …).

Pour maintenir la vraisemblance de la situation (notamment au niveau de la conduite des tests, de l'administration des moyens, et de la gestion des obsolescences), ces structures confient généralement la gestion des moyens de secours à des sociétés spécialisées dans ce domaine.

Gestion informelle (interne ou externe) :

Dans ce cadre, les solutions de secours (qu'elles soient internes à l'entreprise ou attendues d'une entité externe) sont supposées être disponibles en dehors de tout cadre contractuel sérieux : les hypothèses relatives aux délais de mise en œuvre, aux durées de mise à disposition, aux comptabilités matérielle et logicielle, aux limitations de responsabilité, ..., ne sont pas documentées et / ou contresignées par les différentes parties concernées.

Ce type de gestion peut induire des risques juridiques importants, des perturbations majeures sur le site d'accueil, de grandes difficultés de mise en œuvre et de test.

A l'heure des réseaux, de l'informatique répartie et du caractère de plus en plus stratégique des moyens informatiques et de communication, la gestion informelle doit être proscrite.

4.1.2 Type de moyens mis en œuvre

Un Plan de Secours Informatique doit permettre de traiter à la fois des incidents techniques et des sinistres majeurs. Le tableau suivant présente un ensemble de solutions à considérer, locales et externes, selon le niveau d'exigence de disponibilité du S.I.

Ces solutions sont développées dans la suite du chapitre.

	Haute Disponibilité	Moyenne Disponibilité	Faible disponibilité
Sous-systèmes	Reprise immédiate ou quasi-immédiate (quelques minutes). Perte de données très limitée.	Secours en quelques heures (moins de 12 heures). Perte de données limitée (quelques minutes à quelques heures).	Secours en 48 heures ou plus. Perte de données en général inférieure à 24 heures.
Serveurs stratégiques	Serveurs de secours dédiés, géographiquement distants, internes ou externes, en fonctionnement (applications et données). Architecture à haute disponibilité : solutions de type load balancing, cluster de serveurs, mirroring (applications et données).	Serveurs de secours dédiés, géographiquement distants, internes ou externes, interconnectés avec les serveurs à secourir. Système prêt à fonctionner, de type : mirroring distant où copie distante des mises à jours et mise à niveau périodique des bases de données de secours.	Moyens de secours géographiquement distants, internes ou externes et pouvant être mutualisés.
Réseau local	Redondance des équipements. Matériels et rocades de secours avec bascule automatique.	Matériels et rocades de secours.	Kit de câblage volant Existence de locaux de secours utilisateurs externes pré-câblés et pouvant être équipés rapidement (postes de travail, fournitures, ...).
Accès réseaux externes (voix, images et données)	Au moins deux arrivées externes séparées, si possible sur deux sites distincts et via des opérateurs différents. Basculement des communications sur le site de secours en cas de sinistre, avec un maximum d'automatismes. Maillage du réseau d'entreprise.	Nœud de secours externe avec basculement automatique ou manuel (paramétrage). Contrat prévoyant l'intervention de l'opérateur pour une remise en état des liaisons dans un délai déterminé. Matériels de secours.	Engagement d'intervention du fournisseur avec obligation de résultats. Transfert des appels par le fournisseur vers un site de secours.
Téléphonie (équipements)	Secours de l'autocommutateur, si possible dans un local éloigné et basculement automatique des communications.	Contrat prévoyant le transfert des appels par le fournisseur vers un site de secours prêt à prendre les appels (équipements téléphoniques et humains en place).	Autocommutateur de secours. Transfert des appels par le fournisseur vers un site de secours. Mise en place d'un message pré-enregistré.
Cas particulier des accès Internet (site web)	Double connexion à Internet sur chaque site (site principal et site de secours) avec des fournisseurs d'accès différents. Le basculement peut alors être automatique grâce à la mise à jour des DNS et / ou politique de « peering » entre les fournisseurs d'accès.	Connexion Internet sur le site de secours avec basculement manuel des connexions du site principal vers le site de secours par mise à jour des DNS notamment.	Connexion Internet sur le site de secours avec basculement manuel des connexions du site principal vers le site de secours par mise à jour des DNS notamment.

Avant même de définir les moyens informatiques à mettre en œuvre, il y a lieu d'examiner le type d'infrastructure dans ou à partir de laquelle ils doivent opérer. Quatre grandes familles peuvent être considérées :

Installations fixes :

Deux cas d'utilisation sont à envisager :

- soit un (ou plusieurs) site informatique distant intégré à la production et capable d'assurer à lui seul le secours à chaud des moyens informatiques ;
- soit un (ou plusieurs) site distant en attente d'utilisation en cas de sinistre.

Site informatique distant intégré à la production et capable d'assurer à lui seul le secours à chaud des moyens informatiques :

Cette solution correspond au besoin de haute disponibilité et aux contraintes de temps réel sans perte de données. Elle conduit au doublement d'équipements informatiques, mais elle allège considérablement les procédures de reprise d'activité en cas de sinistre. Son coût doit être apprécié dans sa globalité.

Le choix de l'architecture dépend des objectifs en termes de délais de reprise des activités et de fraîcheur des données.

Quelle que soit l'architecture, ces solutions supposent de disposer d'une copie des données sur les équipements de secours et de serveurs prêts à fonctionner, c'est à dire sous tension, et avec les applications.

Ce qui différenciera les différentes architectures possibles, c'est :

- la fréquence de mise à jour de la copie distante des données (cf. la réplication, § 4.4.2), qui peut être immédiate ou différée de plusieurs minutes ou plusieurs heures ;
- la participation ou non des équipements du second site à la production. Cette participation peut être réalisée soit par répartition de la charge d'une même application sur les deux sites, ce qui suppose un mirroring intégral des données entre les deux sites, soit par répartition des applications en production sur les deux sites, chaque application disposant d'une copie en attente sur l'autre site. Ce dernier cas est techniquement moins complexe que le précédent et supporte une réplication différée.

La complétude de la solution est étroitement liée aux capacités des systèmes d'exploitation, des systèmes de gestion de bases de données et des applicatifs.

Site distant en attente d'utilisation en cas de sinistre :

C'est la solution la plus traditionnelle ; dans le cas d'un déclenchement, un certain nombre des personnels de l'entité sinistrée (informaticiens et éventuellement utilisateurs) se déplace sur le site de secours pour y soumettre les transactions et effectuer les traitements. Ce type de solution possède à priori des moyens de télécommunications relativement limités, et exclut notamment la connexion à distance des terminaux habituels (les solutions basées sur des télécommunications sophistiquées sont examinées au paragraphe suivant).

Ces solutions entraînent des conséquences négatives importantes au niveau de l'organisation du travail des équipes d'exploitation (déplacements, éclatement possible des équipes, modification des flux d'entrées / sorties, éloignement des archives et documentations), et ne peuvent en général se concevoir raisonnablement que si le centre de secours est à peu de distance du site à protéger (ce qui entraîne une fragilité vis-à-vis de risques sectoriels).

Sites de secours utilisateurs :

Le plan de secours utilisateurs est à définir dans le cadre d'un Plan de Continuité d'Activité et n'entre pas de ce fait dans le champ de ce document consacré au Plan de Secours Informatique (PSI). Cependant, lors du choix du site de secours informatique, il convient de prendre en compte les possibilités d'accès à des sites susceptibles d'héberger des utilisateurs.

Dans le cas où l'étude du Plan de Secours Informatique s'inscrit dans un projet plus large, les choix réalisés pour l'hébergement des utilisateurs peuvent avoir un impact sur la répartition de certains matériels de secours, entre le site dédié au secours informatique et celui ou ceux prévus pour les utilisateurs (notamment pour des raisons de performances).

Moyens mobiles :

Dans ce type d'organisation, on prévoit de transporter et d'installer, après la notification du sinistre, l'infrastructure d'accueil informatique, soit auprès du site sinistré, soit à proximité d'un autre site de repli (que celui-ci ait été planifié ou non).

Les solutions consistent habituellement soit en des structures de type container modulaires, soit en des unités de type gonflables, équipées dans les deux cas (en standard ou en option) de matériels de conditionnement d'air et de courant, de dispositifs de sécurité, de moyens de pré-cablage, ... Elles peuvent être ou non livrées « peuplées » avec des moyens de traitement.

Les avantages de ce type de solution tiennent à leur souplesse d'adaptation en fonction des conditions réelles du sinistre, et à la limitation des perturbations au niveau des utilisateurs, des équipes informatiques (qui restent proches de leur point d'attache et des utilisateurs), et des circuits d'entrées / sorties des informations ; en outre, la re-connexion du réseau est relativement aisée, si on a bien pris soin de dédoubler préventivement les têtes de lignes.

Ces solutions ne sont évidemment viables que lorsque les situations géographiques et topologiques s'y prêtent (ce qui exclut en général le cœur des agglomérations).

Le délai de reprise initiale est évidemment handicapé par les délais d'acheminement et de montage des installations, et de la sensibilité aux impondérables liés aux transports.

Intégration de services :

L'ensemble des solutions ci-dessus peut être – ou non – assorti de la prestation de services (fournis par des équipes internes à l'entreprise, ou par des fournisseurs extérieurs).

On y trouve, entre autres, l'assistance à la mise au point du Plan de Reprise du site à protéger, l'assistance à la mise en place des aménagements d'infrastructure (matérielle ou logicielle), l'assistance aux tests, l'assistance au re-démarrage, le stockage de doubles de matériels ou de fournitures spécifiques au site protégé, le stockage de sauvegardes, la mise à disposition de personnels d'exploitation, la gestion des astreintes, la fourniture d'assurances complémentaires de frais supplémentaires et reconstitution de média, ...

4.1.3 Niveau de préparation et disponibilité des moyens

Pour des raisons d'équilibrage coût / performance des moyens de secours, on peut être amené à définir des solutions dont le niveau de préparation opérationnelle peut varier. Différents niveaux peuvent être envisagés :

Environnement « peuplé latent » :

Dans ces solutions (également appelées « salles rouges », même lorsqu'il s'agit de moyens mobiles), l'ensemble des équipements informatiques de secours est présent en permanence dans l'infrastructure de secours ; ils sont évidemment conservés en état de marche permanent, mais les données et programmes de l'entité potentiellement utilisatrice n'y sont pas chargés en résidant (cette absence peut même s'étendre au système d'exploitation).

Le degré de vraisemblance est élevé, à condition évidemment de conduire régulièrement des tests poussés.

Les coûts sont évidemment significatifs, et ils atteignent couramment plusieurs pour-cent du budget informatique même pour des installations partagées dans des conditions raisonnables de probabilités d'utilisation simultanée des moyens.

Le délai de reprise peut être de plusieurs dizaines d'heures, puisqu'il faut recharger tout ou partie du système d'exploitation, en adapter les paramètres, recharger les applications et données utilisateurs, re-constituer les informations perdues du fait du cycle de sauvegardes, re-synchroniser les applications, ...

Environnements « miroirs » partiels ou complets :

Ici, non seulement les matériels sont opérationnels en permanence, mais tout ou partie du système d'exploitation, des programmes, et des données de l'entité utilisatrice y résident en permanence.

Suivant les architectures système et les technologies employées, ceci peut ne pas être compatible avec des solutions partagées.

Même lorsqu'on parvient à les partager, ces solutions sont coûteuses, car elles impliquent des travaux d'infrastructure significatifs pour permettre l'alimentation permanente en données « fraîches » et le dédoublement des réseaux locaux et distants. Leur mise en place peut par contre permettre d'alléger (mais surtout pas de supprimer !) les procédures de sauvegarde, dans la mesure où les mêmes informations résident simultanément sur deux sites différents (on suppose évidemment que la configuration miroir est à une distance géographique raisonnable du site à protéger !).

Le degré de vraisemblance que l'on est en droit d'attendre est évidemment maximum, puisque les contraintes logistiques et les temps de basculement sont quasiment nuls. Les risques de dé-synchronisation des installations sont élevés, et le maintien permanent de la cohérence logique est un problème significatif.

Il faut noter une sensibilité particulière de ce type de solutions aux sinistres immatériels (erreurs et malveillances logiques, virus), toute intervention effectuée sur l'installation principale étant immédiatement activée sur l'installation miroir, sauf à installer des « filtres » complexes.

Une certaine gradation peut être considérée dans ces solutions :

- les « secours de première urgence », dits aussi « back-up d'astreinte » ;

  Il s'agit de moyens de secours de périmètre très limité, mais permettant la reprise quasi instantanée des applications les plus stratégiques, permettant une certaine « rémanence » des systèmes, pendant les quelques heures durant lesquelles s'effectue le rechargement de la solution de secours principale (dite « back up lourd).

Ils sont typiquement dédiés à des systèmes hautement transactionnels à cycle très rapide (GPAO à flux tendus, pilotage de caisses enregistreuses ou d'automates bancaires, EDI avec délais de relevé des boîtes à lettres, serveurs Web,…).

Ils sont en général construits sur une dérivation spécialisée du réseau, dont ils « écoutent » en permanence les transactions pour maintenir à niveau leurs fichiers, et certains peuvent démarrer automatiquement en l'absence de signaux reçus de l'installation qu'ils protègent. Evidemment, du fait de leur taille restreinte, leurs performances, ainsi que la pertinence des données qu'ils contiennent se dégradent très vite dès qu'ils passent en autonome, mais ceci doit être suffisant pour assurer un relais.

Du fait de l'architecture restreinte de cette solution, les coûts d'exploitation peuvent être limités, surtout si on parvient à partager les moyens. Par contre, les frais d'étude et de mise en place peuvent être élevés, puisqu'il faut analyser les caractéristiques de l'application « plastron » minimale.

- les moyens à « production répartie » ;

  Dans ce cas, les deux centres (secouru et de secours) se partagent en permanence la charge de travail ; tous les fichiers et accès réseau stratégiques sont dupliqués, et les mises à jour se font au fil de l'eau ; idéalement, les traitements sont effectués indifféremment (et alternativement) sur chacun des sites, depuis l'un quelconque d'entre eux.

  Ces solutions nécessitent bien sûr d'accepter une dégradation notable en cas de sinistre, mais le redémarrage peut être fiable et très rapide. Par contre, les sinistres immatériels (y compris les mouvements sociaux) restent très délicats à aborder.

  Les coûts sont importants, mais évidemment moins élevés que dans la solution ci-dessous.

- les environnements de « miroir intégral ».

  Dans ce cas extrême, toutes les activités stratégiques de l'environnement de production sont en permanence doublées dans l'environnement de secours, dont c'est la seule mission. Contrairement à la solution précédente, l'environnement de secours ne participe pas à la production quotidienne.

  Les temps de redémarrage sont évidemment très réduits, ainsi que le niveau de dégradation fonctionnelle.

  Les coûts de possession sont très élevés, pouvant aller jusqu'au doublement du budget d'exploitation.

4.2 Le secours de la téléphonie

4.2.1 Le raccordement au réseau

Le premier point de vulnérabilité concerne l'accès physique au réseau public. Il est en général unique ou secouru par un second câblage passant dans la même tranchée.

Différents niveaux de secours peuvent être considérés pour le secours de ce raccordement :

- un double raccordement à la boucle locale. Les deux raccordements sont physiquement distincts et éloignés. Ce type de solution peut être envisagé lorsque le site s'y prête (campus, bâtiment donnant sur plusieurs rues, ...) ;

- un double raccordement à la boucle locale, avec accès à deux centraux différents. Cette solution permet de se prémunir à la fois contre les risques de rupture du raccordement, de coupure de la boucle locale et d'indisponibilité du central téléphonique ;
- raccordement de secours physiquement distinct vers un second opérateur ;
- d'autres solutions de secours sur site peuvent être envisagées en fonction des conditions locales.

4.2.2 Les moyens téléphoniques de secours

Secteur particulièrement sensible en matière de sécurité, l'autocommutateur reste le lien indispensable à toute entreprise sur les aspects communications téléphoniques et parfois informatiques.

Selon la nature des risques à couvrir, et de délai d'interruption tolérable, plusieurs solutions de secours peuvent être envisagées :

- une redondance des équipements de l'autocommutateur et du câblage : autocommutateur maître et autocommutateur(s) satellite(s) avec duplication des annuaires, si possible dans des bâtiments différents ;
- un renvoi automatique des appels sur un site secondaire opérationnel dans un délai requis ;
- un contrat prévoyant la livraison d'équipements de secours mobiles de téléphonie dans des délais garantis qui devront être vérifiés ;
- des lignes directes, hors autocommutateur.

Remarque : dans le cas d'une téléphonie sous IP, on se reportera également aux solutions de secours du réseau informatique.

L'utilisation de GSM peut être envisagée, mais, dans le cas de catastrophes touchant une population importante, cette solution peut s'avérer totalement inopérante pour cause de saturation du réseau ou de détérioration d'antennes relais. Il est donc important de prévoir d'autres solutions de secours (autocommutateur dans un autre site, ligne doublée avec un centre opérateur, Internet, ou autres moyens de communication).

Il est clair qu'une flotte de lignes se négocie auprès des opérateurs, mais ne couvrira en aucun cas la totalité des besoins pour des raisons principalement budgétaires.

4.2.3 Le routage des liaisons téléphoniques (sur numéro unique)

Dans le cas où un équipement téléphonique de secours est disponible sur un site distant, se pose le problème du transfert des appels entrants vers ce nouveau site.

Il est possible dans ce cas de souscrire un contrat spécifique de transfert des appels du site sinistré vers le site de secours auprès de l'opérateur téléphonique.

Deux solutions sont à envisager :

- soit le reroutage de l'ensemble des numéros SDA (Sélection Directe à l'Arrivée) vers un numéro unique ;
- soit le reroutage à l'identique des numéros SDA du site sinistré vers le site de secours.

Dans le premier cas, il est nécessaire de prévoir un filtrage des appels entrants par un opérateur, ce qui peut poser des problèmes en cas de mixité entre des appels vocaux et des transmissions de fax ou des transmissions informatiques. Dans ce cas, il peut être envisagé un filtrage des trames Numéris avant l'autocommutateur, à condition que le numéro initialement appelé soit retransmis par l'opérateur.

Dans tous les cas, une étude de faisabilité technique doit être réalisée par l'opérateur en fonction de la localisation du site à secourir et du site de secours.

Remarque : une solution alternative peut consister à demander à l'opérateur la mise en place d'un message personnalisé préenregistré fournissant les nouvelles modalités d'appel.

4.3 Le sauvetage des locaux et des équipements

Dans le cas d'un sinistre matériel (incendie, dégâts des eaux, ...), il convient de préserver au mieux ce qui peut être sauvé afin de faciliter le retour ultérieur sur site ou de récupérer des données sur des supports endommagés.

Les dispositifs suivants doivent en particulier être étudiés :

- le gardiennage du site sinistré, afin d'éviter des vols ou des actes de vandalisme et pour préserver les éléments de preuves éventuels ;
- le recours à des sociétés spécialisées dans le sauvetage de locaux et d'équipements : en cas d'incendie, par exemple, de nombreux équipements peuvent être endommagés par des fumées et vapeurs corrosives, une intervention rapide permet de placer ces équipements dans une atmosphère contrôlée et de freiner la progression de la corrosion. Un nettoyage peut ensuite être entrepris ;
- le recours à des sociétés spécialisées dans la reconstitution d'information (archives inondées, disques endommagés).

Au minimum, on maintiendra à jour dans le Plan de Secours Informatique une liste des sociétés susceptibles d'intervenir.

4.4 Les sauvegardes / restaurations

Le plan de sauvegardes / restaurations est un dispositif essentiel du Plan de Secours Informatique. Il doit garantir la restauration des informations et des outils stratégiques en toutes circonstances par des moyens adaptés et des procédures rigoureuses d'exécution et de contrôle. La nature des supports et les règles d'utilisation et de préservation sont primordiales à la qualité des sauvegardes et surtout de leur restauration.

4.4.1 Les types de sauvegarde

Les sauvegardes peuvent être différenciées selon leur utilisation et leur mode de réalisation.

En fonction des destinations, il y a lieu de distinguer les sauvegardes de production des sauvegardes de recours. Les premières sont destinées à faire face à un incident courant d'exploitation tel que l'écrasement d'un fichier. Elles doivent être accessibles rapidement et peuvent donc être stockées sur le site d'exploitation. Les secondes sont destinées à faire face à un sinistre majeur nécessitant le recours à des moyens externes. Elles doivent notamment permettre de faire face à une destruction du site d'exploitation et seront donc impérativement acheminées sans délais sur un site distant. Les sauvegardes de recours (ou encore de « dernier recours ») doivent être absolument fiables et ne seront utilisables que sur autorisation spéciale de la structure de crise. Afin de garantir leur fiabilité et leur intégrité, elles doivent être réalisées selon des procédures de sécurité renforcées (procédures de sauvegardes sécurisées et différentes des procédures de sauvegardes d'exploitation, contrôles renforcés, sécurité renforcée des transferts et des lieux de stockage).

Une troisième catégorie de sauvegarde peut être considérée pour l'archivage. Dans le cas de l'archivage, les exigences de délais de reprise sont en général plus faibles que pour les deux autres catégories mais le caractère de preuve doit souvent y être préservé.

Enfin, il est toujours prudent d'effectuer une sauvegarde avant toute opération réputée dangereuse sur un disque (maintenance par exemple ou changement de release) ou sur l'ensemble de la configuration.

Plusieurs modes de réalisation des sauvegardes sont envisageables :

- sauvegarde physique ;
- sauvegarde logique.

4.4.1.1 Sauvegarde physique

Il s'agit de la sauvegarde volume par volume de tout ou partie des données.

Elle est utilisée pour la restauration d'un disque après un incident d'exploitation (atterrissage de tête, problème d'arrêt intempestif, ...). Il est souhaitable que ces sauvegardes fassent l'objet d'une durée de conservation étudiée. Elles peuvent également être utilisées dans le cadre d'un plan de secours si la configuration de secours est identique et si le matériel le permet.

Le recours à la technologie de disques RAID permet également de faire face à ce type d'incidents d'exploitation par une redondance des données sur des disques différents et grâce à des dispositifs de remplacement de composants sans arrêt de la production.

4.4.1.2 Sauvegarde logique

Il s'agit de la sauvegarde par entités logiques.

4.4.1.2.1 Sauvegarde logique complète

Elle est essentiellement utilisée pour reconstituer le système d'information sur une configuration de secours plus ou moins réduite par rapport à la configuration d'origine. Son principal avantage est de faciliter la synchronisation des données mais en contrepartie sa durée d'exécution est longue. Il convient de s'assurer de la cohérence des niveaux système, application et données restaurées.

4.4.1.2.2 Sauvegarde incrémentale

Elle consiste à sauvegarder des fichiers qui ont été modifiés entre deux moments identifiés.

Ce type de sauvegarde est souvent indispensable si une sauvegarde complète journalière est trop longue ou impossible.

Elle nécessite une organisation (logicielle ou manuelle) facilitant le repérage des supports et des fichiers sauvegardés.

La sauvegarde incrémentale est rapide mais ne doit pas être utilisée sur une longue période, car il y a des risques d'incohérence. Il faut alors pouvoir disposer d'une sauvegarde complète dont l'ancienneté ait encore un sens pour les utilisateurs. Ce type de sauvegarde est fréquemment associé à la sauvegarde complète.

4.4.1.2.3 Sauvegarde applicative

Il s'agit de la sauvegarde de l'ensemble des fichiers, nécessaires à la bonne exécution ou à la bonne reprise d'une application.

Ce type de sauvegarde permet d'assurer la cohérence des informations, notamment dans le cadre d'un plan de secours lorsqu'on a décidé la reprise totale ou partielle d'une application. Il faudra éventuellement prévoir des procédures spécifiques de sécurité (convoyage, conservation, scellement, audit, ...) en fonction de l'importance stratégique de l'application.

Ces sauvegardes sont liées au cycle de production et leur fréquence sera directement fonction du nombre de traitements exécutés.

4.4.1.2.4 Journalisation

La journalisation consiste à créer un journal de toutes les opérations de mises à jour effectuées sur un fichier.

En cas de problème sur le fichier, la dernière sauvegarde sera restaurée et on appliquera tous les mouvements de mises à jour enregistrés dans le journal.

Les SGBD disposent en général de procédures de journalisation. Cependant, dans certains cas, il peut être nécessaire de prévoir cette journalisation au niveau du développement de l'application.

En fonction de la fréquence de mise à jour de la base, et du temps acceptable de reconstitution des données, les journalisations peuvent être à périodicités différentes (quotidiennes, hebdomadaires, ...).

La difficulté des procédures de journalisation réside dans la synchronisation entre la sauvegarde générale et le démarrage d'un nouveau journal. Cette difficulté est particulièrement aiguë dans le cas d'un service 24 h sur 24.

Les journaux peuvent faire l'objet d'une sauvegarde spécifique afin de restaurer des données plus fraîches.

4.4.2 Les techniques de duplication, de sauvegarde et de restauration

Le choix des techniques de sauvegarde / restauration dépend à la fois des exigences fonctionnelles (fraîcheur des données à restaurer, délais de mise à disposition, cohérence entre les ensembles de données restaurées) ainsi que des contraintes techniques (délais d'acheminement sur le site de secours, volumes à restaurer, performances des outils de sauvegarde et de restauration). La combinaison de ces objectifs et contraintes conduit à envisager les différentes techniques suivantes :

4.4.2.1 la réplication ;

La réplication consiste à dupliquer les informations sur des disques distants de manière à pouvoir alléger la phase de restauration, voire de s'en dispenser. Les mises à jour sont transmises à intervalles réguliers sur le site distant, puis intégrées à la copie de secours des disques de production. Les différentes solutions de réplication diffèrent selon la fréquence d'envoi des mises à jour et le délai de rétention avant mise à niveau des supports de secours.

Il est important de noter qu'en cas d'altération des données de production, les données sur le site de secours sont également altérées. Cette solution ne dispense donc pas d'une sauvegarde périodique de recours dont le contenu devra être garanti.

4.4.2.1.1 Cas 1 : la réplication immédiate

Ce mode de réplication est directement assuré par le système, l'application ou le SGBD. Il permet de répercuter instantanément une modification de donnée sur l'environnement de production et sur celui de secours.

La perte de données est dans ce cas nulle ou quasi nulle et le délai de reprise ne dépend que du niveau de préparation des serveurs et du réseau.

4.4.2.1.2 Cas 2 : Les mises à jour sont transmises à intervalles réguliers

Les mises à jour sont transmises à intervalles réguliers (quelques minutes à plusieurs heures) sur le site de secours, soit comme précédemment par l'application ou le SGBD, ou par un dispositif spécifique (logiciel de sauvegarde évolué, transmission des journaux de mise à jour). L'application des mises à jour sur les supports de secours peut également être différée, avec une autre périodicité (exemple : mise à niveau quotidienne après validation d'un état stable des données de production). En cas de sinistre, et selon la nature de celui-ci, les dernières mises à jour reçues peuvent être appliquées pour limiter la perte d'information (sous réserve du maintien de la synchronisation des données).

4.4.2.2 la sauvegarde classique.

La sauvegarde de recours classique consiste à dupliquer les informations (systèmes, applications et données applicatives) sur des supports amovibles acheminés sans délai sur un site de stockage éloigné et sécurisé. Sa durée de conservation est le temps optimal entre la nécessité d'une remise à jour (traitement, réexploitation) et la capacité à réaliser l'opération (temps de traitement, cohérence logiciel et matériel).

Les contraintes logiques, techniques, volumétriques et financières nécessitent fréquemment d'organiser le plan de sauvegarde en mixant les différentes solutions. Par exemple, sauvegarde physique pour les disques systèmes, incrémentale pour les batchs, logique et journalisation pour les bases.

Il convient de prêter une attention particulière à la synchronisation des données et des systèmes et applications lors des sauvegardes et des opérations de restauration. Il est nécessaire par exemple de préciser dans la restauration, les patchs de l'éditeur qui doivent être appliqués.

La gestion des supports de sauvegarde et des procédures de restauration peut être automatisée par l'utilisation d'un logiciel spécialisé de sauvegarde / restauration couplé à un robot.

ADEQUATION RISQUES / SAUVEGARDES

UTILISATION	CATEGORIE			LIEU DE STOCKAGE		DUREE DE CONSERVATION	
	SAUVEGARDE		ARCHIVAGE				
	PRODU-CTION	RECOURS		SUR SITE	HORS SITE	TEMPO-RAIRE	LONGUE DUREE
Incident d'exploitation	X			X		X	
Remise à disposition d'applicatifs	X			X			X
Audit	X ou X		X	X ou X		X	X
Remise à disposition légale			X	X ou X			X
Sinistre		X			X	X ou X	

Tableau 1 : Adéquation risques / sauvegardes

4.4.3 La synchronisation des données

La synchronisation des données est un problème important à traiter dans un plan de sauvegardes / restaurations. Un moyen simple pour le résoudre est de stopper les mises à jour sur l'ensemble des informations à synchroniser, pendant toute la durée des sauvegardes. Cette solution est malheureusement de moins en moins praticable car la fenêtre utile pour réaliser les sauvegardes est souvent insuffisante, voire nulle.

D'autres solutions doivent alors être envisagées :

- la réplication (cf. ci-dessus) ;
- la technique du « snapshot », offerte par certains outils (SGBD, logiciels de sauvegarde, ...) et qui consiste à figer un état des fichiers à un instant « t » et de réaliser ensuite la sauvegarde à partir de cet état, tout en autorisant la poursuite des mises à jour des fichiers.

4.4.4 Les solutions de sauvegarde / restauration.

A ce jour, il existe deux grands types de moyens de sauvegardes que sont :

- les moyens centralisés ou «propriétaires » qui sont mono-système d'exploitation ;
- les systèmes de sauvegarde en architecture distribuée sur le mode client serveur et capables de fonctionner dans des environnements multi-systèmes.

Compte tenu de l'évolution des architectures informatiques dans ces dernières décennies, les systèmes ouverts dominent le marché actuel.

4.4.4.1 Architectures dites "centralisée"

La particularité de ces systèmes de sauvegardes tient au fait qu'ils sont aussi bien capables de générer des sauvegardes physiques (un disque, un ensemble de disques ou un serveur complet) que des sauvegardes logiques. Ils sont pilotés par un des serveurs dont ils assurent la sauvegarde et permettent de constituer des supports bootables, très utiles en cas de reconstitution complète d'un serveur. Selon les configurations et le volume des données à traiter, ces systèmes de sauvegardes sont reliés à des périphériques du serveur qui les héberge ou à des robotiques plus ou moins complexes.

4.4.4.2 Architecture « distribuée » ou client / serveur

Le système de sauvegarde est en principe installé sur un serveur dédié auquel sont rattachés une ou plusieurs robotiques en mode canal ou réseau. L'ensemble des sauvegardes est géré au niveau d'un catalogue (objet très sensible) qui doit lui-même être régulièrement sauvegardé.

Les serveurs à sauvegarder sont reliés aux serveurs de sauvegarde soit par le réseau d'entreprise, soit via un réseau dédié à ce besoin, et le logiciel client est installé sur chacun d'entre eux. Dans le premier cas, il convient de bien dimensionner le réseau afin de ne pas perturber les opérations courantes.

Le déclenchement des sauvegardes peut être :

- soit piloté par le serveur de sauvegardes lui-même à travers son planificateur de tâches (déclenchement temporel) ;
- soit par l'agent du client qui peut être conditionné par un événement interne ou externe (sauvegardes événementielles). Exemple : déclenchement d'une sauvegarde avant ou après un traitement précis.

Les sauvegardes sont dites logiques (fichier par fichier, ou répertoire par répertoire) et sont décrites le plus souvent de manière explicite, ce qui implique un plan de sauvegarde rigoureux et des moyens de contrôle appropriés. Les sauvegardes peuvent être totales ou incrémentales. Ces systèmes de sauvegarde ne sachant pas générer de supports dits « bootables », il faut stocker indépendamment des données, les moyens de reconstituer chaque système d'exploitation, ainsi que le serveur et le logiciel de sauvegarde eux-mêmes.

4.4.5 Les procédures, les tests, le suivi

Les sauvegardes doivent faire l'objet de procédures écrites par les techniciens. Les restaurations doivent également faire l'objet de procédures écrites qui précisent notamment les personnes habilités à les déclencher.

Ces procédures sont nécessaires mais nécessitent également d'avoir au quotidien :

- un tableau de bord du suivi des sauvegardes ;
- une remontée centralisée des alertes indiquant tout problème survenu lors des sauvegardes avec revue et prise en compte des alertes remontées selon des consignes écrites.

Ceci apporte une fiabilité aux sauvegardes et donc aux restaurations à faire en cas de sinistre.

Des tests périodiques de restauration (complets et / ou partiels) doivent être menés à intervalles réguliers afin de vérifier que les procédures sont suivies et à jour et que les sauvegardes fonctionnent bien. Ces tests feront l'objet de comptes-rendus et de suivi afin que tout dysfonctionnement soit corrigé.

4.5 Le secours des impressions et de la mise sous pli

Le secours des impressions et de la mise sous pli pose des problèmes spécifiques. Les moyens de secours ne sont en général pas fournis directement par les offreurs de secours informatique. Il convient soit d'étudier un secours interne, si plusieurs lignes d'impression / mise sous pli existent, en séparant physiquement ces différentes lignes, soit d'avoir recours à certains professionnels tels que les imprimeurs ou les sociétés réalisant des mailing. Ces solutions peuvent également contribuer à absorber la charge d'impression en période de pointe.

Comme pour le secours informatique, ces solutions doivent faire l'objet de contrat et être testées périodiquement.

D'autres points importants sont à prendre en compte :

- le stock d'imprimés ;

  Prévoir un stock d'imprimés à l'extérieur du site, en interne ou chez un fournisseur. Dans le cas d'un stock externe, il convient de surveiller les conditions de stockage du papier et de procéder à un roulement de manière à limiter le vieillissement du stock (qualité du support et maintien à jour des données imprimées).

  Dans certains cas, des impressions dégradées, sur papier vierge sont à envisager ;

- les aspects contractuels (sur la conservation des stocks, la mise à disposition des équipements, ... ;
- les relations avec les entreprises d'acheminement du courrier

  Il est important de prévoir à l'avance le circuit des documents en situation de secours. Le secours du courrier classique sera traité dans le cadre du Plan de Continuité d'Activité. Par contre l'envoi de masse de la production informatique doit être traité dans le Plan de Secours Informatique. Il convient notamment de se coordonner avec ces entreprises, surtout lorsque les volumes qui seront traités par le site de secours sont importants. Des

navettes pourront être organisées pour la livraison des éditions en interne ou vers des partenaires ;

- l'affranchissement ;
- les équipements spéciaux : prévoir le secours de machines à signer ;
- la confidentialité des documents produits ;
- ...

4.6 Le secours des accès au réseau Internet

4.6.1 Le raccordement au réseau Internet

L'accès au FAI (Fournisseur d'Accès à l'Internet) est le premier point de vulnérabilité pour le raccordement de l'entreprise à Internet. Différentes solutions peuvent être envisagées :

- deux raccordements distincts vers le même FAI (l'un maître et l'autre esclave) mais sur deux cartes réseaux différentes ;
- un raccordement vers deux FAI différents avec partage de charge sur les deux plans d'adressage IP ;
- un raccordement vers deux FAI différents (l'un maître et l'autre esclave) en réalisant, entre eux, un accord d'échange de trafic (dîte politique de « peering ») ainsi l'entreprise conserve le même adressage IP lors du basculement ;
- une redirection des flux Internet par le réseau interne de l'entreprise vers un autre point d'accès lors de la perte du lien principal.

4.6.2 Le reroutage des flux Internet

Lors de la mise en fonctionnement du site de secours, plusieurs solutions peuvent être envisagées :

- une connexion de secours vers le même FAI permettant de conserver le même plan d'adressage ;
- un nouvel accès à Internet complètement dé-corrélé de celui du site sinistré. Dans ce cas, une plage d'adresses IP correspondant au besoin du site de secours doit être réservée à l'avance et les DNS maîtres du domaine de l'entreprise doivent être mis à jour lors du redémarrage, avec le nouveau plan d'adressage.

4.7 Le contrat de secours

Quelle que soit la solution de secours retenue (interne, externe, repeuplement de salle blanche, ...), il est indispensable de formaliser les relations entre l'utilisateur des moyens de secours, et les entités qui mettront à disposition l'ensemble des moyens pour garantir la continuité de service (serveurs, réseau, postes de travail, ...).

Dans les développements suivants, on utilisera conventionnellement les termes de « souscripteur », « prestataire », et « contrat », étant donc bien entendu que cette relation peut s'appliquer à tous les cas de figure (clients / société de services, divisions ou établissements d'une même entreprise, entreprises utilisatrices liées par des engagements réciproques, ...).

Il faut en conséquence interpréter le texte suivant, dont certaines clauses peuvent ne pas avoir de signification ou doivent être extrapolées en fonction des moyens et relations prévus.

4.7.1 Objet du contrat

Le « Contrat » liant « prestataire » et « souscripteur » doit tout d'abord indiquer l'objet général de l'engagement des parties :

- nature des moyens mis à disposition et leurs conditions de mutualisation (environnement fixe ou mobile, avec ou sans télécommunications, ...) ;
- les situations ouvrant droit à la mise à disposition des moyens de secours (sinistre matériel, sinistre immatériel, écrêtage de charge, indisponibilités volontaires telles que migrations ou déménagements, conflit social, ...). Il est souhaitable que les exclusions soient explicitement mentionnées (formulation de type "tout sauf ...") ;
- les délais de base de mise à disposition des moyens de secours, et la durée maximale de mise à disposition ;
- etc.

4.7.2 Nature détaillée des « prestations »

Cette clause précise les moyens mis à disposition, leur lieu de mise à disposition (en cas de sinistre partiel, il peut être envisagé une clause spécifique prévoyant la livraison des équipements de secours par le prestataire chez le client) et les services additionnels qui sont éventuellement fournis. Par exemple, la « prestation » inclue-t-elle, le montage et la mise sous tension des matériels, la configuration du système (standard ou personnalisée), la connexion aux réseaux locaux et distants, le rechargement des données du « souscripteur », l'assistance d'ingénieurs et / ou de personnels d'exécution ?

Le problème du droit d'utilisation des logiciels sur site de secours doit être étudié en fonction des choix effectués.

On peut également détailler ici la durée de mise à disposition des moyens de secours (durée contractuelle de base, clauses de prolongation, montée en régime ou au contraire réduction progressive de la puissance de moyens mis à disposition, ...). Les clauses doivent évidemment être cohérentes avec les délais de réapprovisionnement et de reconstruction habituels à la technologie employée.

4.7.3 Procédure de déclenchement

Le « prestataire » doit préciser en détail les modalités de déclenchement des interventions (procédure, moyens employés - téléphone, fax, confirmation écrite - heures limites de prise en compte des appels, astreintes de jours fériés, ...).

En particulier, le « contrat » doit comporter une liste exhaustive des représentants du « souscripteur » habilités à déclencher une intervention, ainsi que les procédures d'authentification et d'accusé de réception des appels.

Certains « contrats » peuvent comporter un déclenchement en deux temps (première alerte, déclenchant une « pré-chauffe » sur le site de secours, suivie d'une confirmation définitive du souscripteur, après qu'il ait fait l'inventaire détaillé des dégâts et parcouru ses procédures d'escalade).

4.7.4 Conditions de fonctionnement

Dans le cas de recours à un site fixe, le « Contrat » doit préciser clairement les heures d'ouverture de ce site, les procédures de sécurité et de contrôle d'accès, le plan d'accès, les moyens de parking, … Il peut être souhaitable de joindre au "contrat" tout ou partie du règlement intérieur du site, et de préciser les situations qui peuvent engager la responsabilité du « souscripteur ».

Dans le cas où le prestataire met une salle privative permanente à la disposition du client pour le secours de serveurs stratégiques, le contrat précisera les moyens de sécurité pour garantir la protection des équipements client (contrôle d'accès, sécurité incendie, alimentation électrique, ...) et pour assurer et sécuriser les échanges externes. Le contrat précisera également dans ce cas l'entité qui gère l'exploitation et, le cas échéant, le partage des responsabilités en matière d'exploitation de ses équipements.

4.7.5 Logistique

Le « contrat » doit prendre en compte les implications logistiques identifiées dans les plans de reprise (téléphone, télécopie, accès réseau, impressions, accès Internet, telex, secrétariat, hébergement des équipes du « souscripteur », installation et / ou stockage de matériels complémentaires, ...). Il faut en effet veiller à garantir la mise à disposition d'un minimum de confort à des équipes soumises à de très fortes pressions.

4.7.6 Tests et répétitions

Les solutions de secours n'ont de sens que si elles sont testées régulièrement. Il est donc essentiel que les parties se mettent d'accord sur une fréquence et un protocole de tests réguliers. Ces tests doivent faire partie intégrante du « contrat », et faire l'objet de comptes-rendus co-signés. Le contrat doit préciser les conséquences du non-respect de cette clause, que ce soit du fait du « prestataire » ou du « souscripteur ».

Certaines solutions de secours sont difficiles à tester (accords réciproques en l'absence de surcapacité, repeuplement de salle blanche, déplacement d'utilisateurs, perturbation de services), mais il faut s'imposer d'aller le plus loin possible. Une solution de secours impossible à tester augure mal d'une mise en œuvre réelle.

Chaque prestataire doit s'engager à assurer et tester l'interopérabilité avec les moyens des autres prestataires. Le contrat contiendra en annexe les coordonnées des contacts chez ces différents prestataires.

Il est conseillé d'assortir le « contrat » d'une clause de recette contractuelle, ne liant d'une façon durable prestataire et souscripteur qu'à l'issue de tests approfondis faisant l'objet d'un protocole contradictoire (adéquation de la configuration fournie, tests des interfaces et des réseaux, des impressions, ...).

4.7.7 Gestion de priorités

Sauf dans le cas de configurations « miroir », ou la totalité des équipements critiques est doublée, la majorité des moyens de secours est basée sur le partage par deux ou plusieurs entités d'un ensemble limité de matériels et installations.

Il est donc possible que ces entités souhaitent recourir simultanément à ces moyens, et il est essentiel de définir clairement des règles de priorités, pour être à même de résoudre d'emblée les situations de conflit d'accès. Elles doivent tenir compte au moins des éléments suivants :

- la cause de la demande d'intervention (sinistre total, partiel, écrêtage de charge, tests, anticipation en cas d'événement quasi certain, ...) ;
- le mode d'utilisation demandé / possible (exclusif, partagé) ;
- la durée de mise à disposition (tant la durée demandée que la durée maximale contractuelle restante à courir, car on peut mettre au point des systèmes à priorité décroissante dans le temps) ;

- dans le cas d'une relation client / fournisseur externe (bien que ceci puisse avoir une signification même dans le cas de relations internes), les catégories de clients pouvant entrer en compétition pour l'acquisition des ressources, et le jeu réciproque de ces relations contractuelles (client ponctuel, abonné service bureau, abonné repeuplement contre abonné service complet, ...).

Ces clauses de priorités peuvent prendre en compte la disponibilité éventuelle chez le « prestataire » de moyens de secours de deuxième niveau. Si ces moyens présentent des fonctionnalités inférieures à celles des moyens principaux, il peut y avoir lieu de définir les compensations qui seront garanties au « souscripteur » pour compenser la dégradation.

Elles peuvent, d'une façon symétrique, amener le « souscripteur » à enrichir son Plan de Secours (en développant des hypothèses du type « si le Centre de Secours de premier niveau n'est pas disponible, alors ... »).

4.7.8 Engagements et responsabilités

Le « prestataire » doit indiquer le nombre maximum de « souscripteurs » auxquels il peut s'engager à fournir assistance avec un environnement donné.

Dans le cas d'une relation client / fournisseur externe, cette notion revêt une importance particulière, car elle définit la probabilité du fournisseur de se trouver confronté à des situations de débordement, donc de conflits de priorité et par conséquent d'insatisfaction d'un ou plusieurs clients.

Ceci est d'autant plus grave que la totalité des fournisseurs externes de moyens de secours n'endosse que des engagements de moyens (ils mettent « tout ce qu'ils peuvent » à la disposition de leurs clients), et non des engagements de fin (en cas de sinistre, le fournisseur ne peut garantir qu'il pourra satisfaire un client déterminé, puisque ses moyens sont limités).

Il n'est pas possible de faire de recommandation quant au nombre optimal de sites pouvant être supportés : il s'agit en effet d'un équilibrage entre le coût de la prestation (inversement proportionnel au nombre de sites protégés), et la probabilité de « collision » de demandes d'intervention. Or ce dernier paramètre varie beaucoup en fonction de la technologie considérée (partageable ou non), de la qualité des actions de prévention de la clientèle, de la taille globale du prestataire (loi des grands nombres), de la psychologie de la clientèle (« mieux vaut un petit contrat que rien du tout », ou au contraire, recherche du « sur mesure »), ...

Le taux de mutualisation est à examiner systématiquement au cas par cas en fonction notamment de la technologie mise en œuvre (systèmes d'exploitation partageables ou virtuels, état moyen des délais de livraison pour des matériels neufs et d'occasion), du professionnalisme des partenaires, de la nature des risques couverts, de l'aggravation éventuelle des risques de l'entreprise (liés à son exposition à des malveillances, au montant de ses enjeux, à ses obligations éventuelles d'astreinte, à une accumulation de risques au niveau du prestataire, ... Voir le dernier paragraphe de ce chapitre).

Dans tous les cas de figure, le « contrat » doit préciser les responsabilités du « prestataire » lorsqu'il n'est pas en mesure de respecter ses engagements, qu'il ait ou non appliqué rigoureusement les règles de priorité, et explicité les limitations de responsabilité qui peuvent en résulter.

Enfin, il est fréquent (et normal) que la responsabilité du « prestataire » soit dégagée au niveau de la qualité des programmes, données, procédures et sauvegardes du « souscripteur » (ce qui souligne à nouveau la quasi impossibilité pour un « prestataire » de s'engager sur des résultats).

4.7.9 Aspects financiers

La mise en place de moyens de secours représente le plus souvent des investissements importants, tant en temps qu'en matériel.

Il est donc nécessaire que les coûts associés soient clairement définis. Outre les coûts de développement des Plans de Reprise, il y a lieu d'identifier :

- les coûts d'abonnement éventuels qui doivent être pris en compte même en cas d'accords réciproques ou internes, car cet « abonnement » permettra de compléter les équipements pour pouvoir honorer les engagements. Dans le cas de fournisseurs externes, cet abonnement permettra de financer les équipements partagés, et de maintenir opérationnelle en permanence toute la structure d'accueil. Le coût est alors proportionnel à la configuration souscrite ;
- les coûts de déclenchement d'intervention (coût de préparation et de mise en œuvre des tests et interventions réelles) ;
- les coûts d'utilisation effective, pendant et après la durée contractuelle de base. Ils peuvent être liés à la puissance réellement consommée (et bien sûr à la durée d'utilisation). Il est fréquent de mettre en place des taux croissants dans le temps, qui encouragent le « souscripteur » à libérer au plus tôt les installations de secours. Ils peuvent également varier en fonction des plages d'utilisation.

La typologie de répartition de ces coûts varie beaucoup d'un type de prestation à l'autre : certains « contrats » peuvent avoir un coût d'abonnement élevé, mais par contre offrir une franchise au niveau des coûts de déclenchement et d'utilisation. A l'opposé, certaines solutions peuvent présenter des coûts d'abonnement limités, assortis de coûts d'utilisation - en test ou en réel- élevés.

L'ensemble de ces coûts peut être détaillé en termes de « prestation de base » et services complémentaires (aide au redémarrage, ...).

Par exemple, certains « contrats » (notamment avec des fournisseurs externes) peuvent être assortis de contrats d'assurance couvrant les coûts engendrés par une mise en œuvre réelle des moyens de secours (clauses dites de « Frais Supplémentaires » et éventuellement de « Reconstitution de Médias »). Il faut alors préciser le montant des capitaux garantis, déterminer qui prend la charge de l'assurance, et s'assurer que la clause couvre spécifiquement tous les frais liés à la mise en œuvre et à l'exploitation des moyens de secours lors du sinistre.

4.7.10 Evolution de la configuration

Les configurations informatiques changent rapidement. Il convient que le « contrat » vive avec elles, et prenne en compte les évolutions du « souscripteur » et éventuellement du « prestataire » (ce point, particulièrement évident, est souvent oublié par les accords réciproques formels et informels, qui sont le plus souvent basés sur une vague ressemblance des configurations au moment de l'accord, mais ignorent délibérément qu'elles vont probablement diverger très rapidement).

Il importe donc que le « contrat » précise la durée de sa validité « technologique », les dispositions qui sont prises pour se tenir au courant mutuellement des évolutions, des implications résultant de la nécessité de faire évoluer l'une et / ou l'autre des configurations.

4.7.11 Confidentialité

Il est d'usage que le « prestataire » et le « souscripteur » concluent un accord réciproque de confidentialité (particulièrement si le souscripteur souhaite être couvert face à des fraudes, malveillances, mouvements sociaux, ...).

Pour certains secteurs, cette notion de confidentialité peut même avoir un impact notable sur le déroulement des tests, et donc sur les coûts (par exemple, interdiction de recourir à des personnels externes pour la reconfiguration et le rechargement des données, destruction des supports magnétiques après usage, impossibilité d'utiliser des configurations et / ou réseaux partagés, ...).

4.7.12 Quelques recommandations

Les points les plus délicats de ces « contrats » sont les suivants :

- backup de deuxième niveau : le « prestataire » doit, dans toute la mesure du possible, disposer à son tour d'une solution de secours en cas d'indisponibilité de ses propres installations (suite à sinistre, débordement, mouvements sociaux, impossibilité d'accès, ...). Dans le même ordre d'idées, il est souhaitable que le prestataire s'engage à informer son (ou ses) souscripteur(s) de la survenance de toute situation l'empêchant d'honorer ses engagements de premier niveau ;
- accumulation de risques : il faut vérifier que le prestataire n'est pas dans une situation à forte probabilité de « collision » de demandes de mise en œuvre par exemple, les solutions de secours de type corporatif (GIE et autres) sont attirantes, mais une situation de mouvements sociaux sectoriels peut se révéler catastrophique. Il peut en être de même pour des accumulations de risques géographiques. Il est conseillé d'ajouter au contrat la définition d'un périmètre de sécurité à l'intérieur duquel le prestataire s'engage à fournir les moyens demandés, même en cas de « collision » ;
- limitation des responsabilités : comme indiqué plus haut, coût et degré de certitude de disponibilité sont deux paramètres opposés : une solution parfaitement fiable risque d'être d'un coût décourageant, ce qui aboutit à l'opposé du but recherché. Inversement, une solution « bon marché » peut être totalement illusoire ;
- transfert de moyens au prestataire : dans le cas où le contrat prévoit également la mise en oeuvre du secours avec les moyens mis à disposition par le client (logiciels, données, moyens humains, ...) il faut préciser les responsabilités, notamment vis-à-vis du respect de la réglementation .
- respect des règles de nombre d'abonnés et d'application des priorités : dans le cas de relations clients / fournisseurs externes, il est fréquent (et normal) que le prestataire refuse de divulguer l'identité de ses autres clients, puisqu'il peut être tenu vis à vis d'eux ainsi que mentionné, par des règles de confidentialité. Ceci peut être en contradiction avec la nécessité de transparence de la bonne application des engagements contractuels au niveau du nombre maximum d'adhérents, et de l'application rigoureuse des règles de priorité en cas de conflit d'accès. Il peut donc être souhaitable que le contrat identifie une tierce partie, tenue à la confidentialité, habilitée à auditer à tout moment la matérialité des services, le professionnalisme de la gestion des installations de secours, et le respect des règles contractuelles.

En conclusion, les « prestataires » ne pouvant en général endosser que des obligations de moyens, il appartient au « souscripteur » de s'assurer que la prestation fournie représente bien pour lui l'optimum entre la réduction de ses enjeux en cas de sinistre, le budget qu'il y consacre, et la vraisemblance de la solution mise au point.

5 ANNEXE : FICHES GUIDES D'ANALYSE DES RISQUES

5.1 Locaux et infrastructure

Risques d'indisponibilité définitive

Menaces types	Conséquences à préciser	Parades à considérer[1]

Destruction totale (site ou bâtiment)	▪ Site et / ou services concernés
	▪ Durée d'interruption totale
	▪ Service dégradé
	▪ Perte d'information
	▪ Déplacement de personnel
		▪ Sauvegardes externes
		▪ Sites et moyens de secours
		  ▪ Informatique
		  ▪ Utilisateurs
		▪ Plans de reprise formalisés
		  ▪ Locaux
		  ▪ Equipements
		  ▪ Activités

Destruction salle informatique	▪ Idem Site et / ou services concernés
	▪ Durée d'interruption totale
	▪ Service dégradé
	▪ Perte d'information
	▪ Déplacement de personnel
		▪ Placer toutes les sauvegardes à l'extérieur de la salle
		▪ Local de secours
		▪ Secours des équipements
		  ▪ Interne
		  ▪ Externe
		  ▪ Livraison
		  ▪ Maintenance
		▪ Secours du câblage

Destruction d'un local nodal	▪ Fonctionnement dégradé du réseau local
	▪ Interruption des liaisons externes
		▪ Architecture sécurisée
		▪ Possibilité de reconfigurer via un autre LTE (local technique d'étage)
		▪ Kit d'urgence
		  ▪ Câbles
		  ▪ Matériels réseau

Destruction d'un local technique d'étage (LTE)	▪ Interruption temporaire du réseau dans les zones concernées
	▪ Service dégradé
	▪ Déplacement de personnel
		▪ Architecture sécurisée
		▪ Possibilité de reconfigurer via un autre LTE
		▪ Kit d'urgence
		  ▪ Câbles
		  ▪ Matériels réseau

[1] Toutes les parades à considérer ne peuvent être efficaces que si elles sont formalisées et régulièrement testées

Menaces types	Conséquences à préciser	Parades à considérer
Destruction de la médiathèque	▪ Perte d'archives ▪ Perte de sauvegardes ▪ Perte de données applicatives	▪ Externalisation d'une copie des informations sensibles (sauvegardes, archives légales) ▪ Etude des possibilités de reconstitution (récupération externe, trace papier) ▪ Copies sur disque

Destruction d'une zone utilisateurs ou d'une zone d'archivage (fonction du cloisonnement incendie)	▪ Perte de documents
	▪ Perte totale d'information (si sauvegardes locales)
	▪ Déplacement de personnel
	▪ Service dégradé
		▪ Sauvegardes extérieures à la zone
		▪ Secours des équipements locaux
		  ▪ Serveurs
		  ▪ Parc de PC / Imprimantes
		  ▪ Equipements spécifiques
		▪ Secours des supports physiques de flux et des dossiers (papier, disquette, …)
		  ▪ Copie externe
		  ▪ Numérisation
		  ▪ Possibilité de reconstitution
		▪ Locaux de secours utilisateurs

Destruction du système de climatisation	▪ Panne disque et détérioration de données ▪ Arrêt de serveurs ▪ Altération de supports ▪ Dans certains cas, indisponibilité de l'immeuble	▪ Redondance des équipements de climatisation (centrale eau glacée, armoires, …) ▪ Protection des locaux techniques (accès, incendie) ▪ Plan et moyens de secours pour les serveurs et applications indisponibles

Destruction d'équipement d'alimentation électrique (transformateur, armoire électrique, ...)	▪ Panne disque et détérioration de données
	▪ Arrêt de serveurs
	▪ Altération de supports
	▪ Indisponibilité de l'immeuble
		▪ Groupe électrogène régulièrement testés
		▪ Dédoublement des arrivées et postes de transformation électriques
		▪ Moyens de secours externes
		  ▪ Informatique
		  ▪ Utilisateurs
		▪ Contrat d'intervention rapide
		▪ Respect des charges d'utilisation recommandées par les constructeurs
		▪ Onduleur + arrêt sécurisé des machines

Menaces types	Conséquences à préciser	Parades à considérer
Destruction de l'onduleur général (ou dédié à une salle)	▪ Panne disque et détérioration de données ▪ Arrêt de serveurs	▪ Basculement sur le réseau (si possible automatique) ▪ Redondance de l'onduleur avec basculement automatique ▪ Sécurisation du local onduleur (accès, incendie, ...) ▪ Moyens de secours informatiques externes ▪ Contrat de maintenance prévoyant le remplacement dans un délai approprié

Tableau 2 : Locaux et Infrastructure (risque d'indisponibilité définitive des locaux)

Risques d'indisponibilité temporaire des locaux

Menaces types	Conséquences à préciser	Parades à considérer
Inaccessibilité temporaire sans destruction ▪ suite à menace (alerte à la bombe, pression sur le personnel, …)	▪ Arrêt des activités du site ▪ Inaccessibilité des consoles de pilotage ▪ Risque de détérioration des matériels	▪ Moyens de secours informatiques et utilisateurs externes pour un service minimum temporaire ▪ Sauvegardes externes ▪ Procédures d'alerte et mise en œuvre de mesures d'urgence
Inaccessibilité temporaire sans destruction ▪ suite à accident d'environnement	▪ Arrêt des activités du site ▪ Risque d'arrêt des équipements ▪ Risque de détérioration des matériels ▪ Risque de perte de données	▪ Moyens de secours informatiques et utilisateurs externes pour un service minimum temporaire ▪ Accès et pilotage distant ▪ Sauvegardes externes
Inaccessibilité temporaire sans destruction ▪ suite à non conformité des locaux	▪ Arrêt des activités du site	▪ Moyens de secours utilisateurs externes pour un service minimum temporaire ▪ Accès et pilotage distant
Inaccessibilité temporaire sans destruction ▪ suite à panne d'un système de sécurité	▪ Arrêt des activités du site	▪ Moyens de secours utilisateurs externes pour un service minimum temporaire ▪ Accès et pilotage distant
Blocage des accès suite à conflit social, sans arrêt des équipements	▪ Arrêt des activités du site ▪ Inaccessibilité des consoles de pilotage ▪ Risque d'occupation	▪ Moyens de secours utilisateurs externes pour un service minimum temporaire ▪ Impressions déportées ▪ Accès et pilotage distant ▪ Protection physique du bâtiment ▪ Stratégie d'anticipation d'une aggravation
Occupation des locaux suite à conflit social, sans arrêt des équipements (aggravation du risque précédent)	▪ Arrêt des activités du site ▪ Inaccessibilité des consoles de pilotage ▪ Risque d'arrêt des équipements ou d'actes malveillants	▪ Moyens de secours utilisateurs externes pour un service minimum temporaire ▪ Impressions déportées ▪ Accès et pilotage distant ▪ Protection physique des équipements critiques ▪ Procédures d'alerte et mise en œuvre de mesures d'urgence

Menaces types	Conséquences à préciser	Parades à considérer
Occupation des locaux avec arrêt des équipements (aggravation du risque précédent)	▪ Arrêt des activités du site ▪ Arrêt des équipements du site ▪ Risque de détérioration des matériels	▪ Moyens de secours informatiques et utilisateurs externes pour un service minimum temporaire ▪ Sauvegardes externes

Tableau 3 : Locaux et infrastructure (risques d'indisponibilité temporaire des locaux)

5.2 Equipements informatiques et de télécommunication

Risques d'indisponibilité définitive

Menaces types	Conséquences à préciser	Parades à considérer
Destruction (accident ou malveillance)	▪ Perte de données ▪ Interruption temporaire ou définitive de service ▪ Dégradation de service ▪ Interruption de flux	▪ Redondance ▪ Mode dégradé ▪ Equipement de secours régulièrement testé ▪ Extension du contrat de maintenance ▪ Sauvegarde adaptée et complète ▪ Protection physique
Bris de matériel non remplaçable	▪ Perte de données ▪ Interruption temporaire ou définitive de service ▪ Dégradation de service ▪ Interruption de flux	▪ Idem destruction + ▪ Veille ▪ Stock de pièces de rechange ▪ Obtention des sources du système et des applications spécifiques ▪ S'assurer de la qualité de la maintenance ▪ Portabilité des applications
Vol	▪ Perte de données ▪ Interruption temporaire ou définitive de service ▪ Dégradation de service ▪ Interruption de flux ▪ Perte de confidentialité (données et savoir-faire)	▪ Idem destruction + ▪ Chiffrement des données sensibles ▪

Tableau 4 : Equipements informatiques et de télécommunication (risques d'indisponibilité définitive)

Risques d'indisponibilité temporaire

Menaces types	Conséquences à préciser	Parades à considérer
Panne, bris de matériel remplaçable, …	▪ Perte de données ▪ Interruption de flux ▪ Interruption temporaire de service ▪ Perte de confidentialité	▪ Procédure sécurisée de mise en réparation ▪ Contrat de maintenance avec obligation de résultat ▪ Stock de maintenance ▪ Optimisation de l'usage de l'équipement
Obsolescence	▪ Interruption temporaire ou définitive de service ▪ Dégradation de service ▪ Evolutions retardées ou impossibles	▪ Veille ▪ Portabilité des applications ▪ Stock de pièces de rechange
Saturation	▪ Interruption de flux ▪ Interruption temporaire de service	▪ Optimisation de l'usage de l'équipement

Tableau 5 : Equipements informatiques et de télécommunication (risques d'indisponibilité temporaire)

5.3 Système d'exploitation, applications, données et flux

Risques d'indisponibilité définitive

Menaces types	Conséquences à préciser	Parades à considérer
Perte d'un logiciel	▪ Interruption de service ▪ Interruption de flux ▪ Perte de données	▪ Sauvegarde haute sécurité des logiciels (scellement, tests périodiques de restauration) ▪ Conservation des supports d'origine et des différentes mises à jour ▪ Externalisation des sauvegardes de logiciels
Perte de données non reconstituables (effacement accidentel, erreur d'exploitation, virus, malveillance, destruction volontaire, erreur de paramétrage, ...)	▪ Interruption de service ▪ Interruption de flux ▪ Perte de données	▪ Sauvegarde haute sécurité des données ▪ Externalisation des sauvegardes

Tableau 6 : Système d'exploitation, applications, données et flux (risques d'indisponibilité définitive)

Risques d'indisponibilité temporaire

Menaces types	Conséquences à préciser	Parades à considérer
Interruption temporaire de flux par attaque logique (saturation réseau)	▪ Interruption temporaire d'activité	▪ Utilisation d'un autre moyen de transmission ▪ Surveillance du réseau

Perte de données reconstituables
(effacement accidentel, erreur d'exploitation, virus, malveillance, destruction volontaire, erreur de paramétrage, ...)
	▪ Interruption de service
	▪ Interruption de flux
	▪ Perte de données
		▪ Actions préventives
		  ▪ qualité de l'environnement d'exploitation
		  ▪ qualité de l'organisation de l'exploitation
		  ▪ lutte anti-virale
		  ▪ organisation globale de la sécurité
		▪ Procédures de reconstruction de données (à partir de documents originaux, d'autres fichiers, chez des clients ou partenaires)

Tableau 7 : Système d'exploitation, applications, données et flux (risques d'indisponibilité temporaire)

5.4 Services, fournitures et prestations extérieurs

Risques d'indisponibilité définitive

Menaces types	Conséquences à préciser	Parades à considérer
Disparition brutale d'un fournisseur ou d'un prestataire	▪ Arrêt du service ou de la fourniture ▪ Interruption d'approvisionnement ▪ Interruption de flux ▪ Perte de données	▪ Politique de diversification envers les fournisseurs ▪ Portabilité des services et prestations extérieurs ▪ Conformité aux standards du marché ▪ Service ou produit de substitution ▪ Fonctionnement en mode dégradé ▪ Veille et audit fournisseurs
Disparition d'un service ou d'un produit	▪ Arrêt du service ▪ Interruption d'approvisionnements (fournitures, énergie, matières premières, …) ▪ Interruption de flux de données ▪ Perte de données	▪ Exigence d'un plan de secours du fournisseur ▪ Services ou produits de substitution ou fonctionnement en mode dégradé ▪ Clause contractuelle prévoyant un préavis et / ou un service ou un produit de substitution ▪ Veille stratégique ▪ Disponibilité d'une documentation nécessaire au service ▪ Stock de secours
Arrêt imposé d'un service ou d'un produit (réglementation, embargo, conflit)	▪ Arrêt du service ▪ Interruption d'approvisionnements (fournitures, énergie, matières premières, …) ▪ Interruption de flux de données	▪ Veille ▪ Anticipation de l'arrêt ▪ Stock ▪ Communication de crise

Tableau 8 : Services, fournitures et prestations extérieurs (risques d'indisponibilité définitive)

Risques d'indisponibilité temporaire

Menaces types	Conséquences à préciser	Parades à considérer
Indisponibilité d'un service télécom souscrit auprès d'un opérateur	▪ Isolement total ou partiel d'un site (voix, données, …)	• Souscrire des engagements contractuels de qualité de service conformes aux exigences de service : ▪ garantie de temps de rétablissement assorti de pénalités, ▪ garantie de disponibilité ▪ sécurisation des moyens d'accès (doublement physique des infrastructures d'accès) ▪ mise en œuvre de solutions de repli (bascule sur ligne de secours, repli sur site de secours) ▪ Diversification des fournisseurs (routage automatique sur un autre opérateur)
Indisponibilité d'un service opérationnel contractualisé avec un prestataire extérieur (EDI, ISP, ASP…) Retard de livraison	▪ Interruption d'activité totale ou partielle ▪ Dégradation de service	▪ Souscrire des engagements contractuels de qualité de service conformes aux exigences de service. ▪ Certification ISO 9000 des services du fournisseur ▪ Si nécessaire, vérification d'existence d'un plan de secours et de rapports de tests. ▪ Diversification des moyens
Interruption prolongée de la fourniture en énergie électrique	▪ Interruption d'activité totale ou partielle ▪ Perte de données ▪ Dysfonctionnements au redémarrage	▪ Groupe électrogène régulièrement testé (fonctionnement et endurance) ▪ Dédoublement des arrivées et du poste de transformation électrique ▪ Moyens de secours externes ▪ Onduleur avec dispositif d'arrêt sécurisé des serveurs ▪ Garanties contractuelles sur le délai de rétablissement du service
Mauvaise qualité de la fourniture électrique (micro-coupures et surtensions)	▪ Perte de données ▪ Dégradation d'équipements ▪ Interruptions répétitives d'activité	▪ Mise en place d'interfaces de régulation entre l'arrivée et les équipements : ▪ interfaces dynamiques (groupes dynamiques avec volant d'inertie) ▪ interfaces statiques (transfor-mateurs d'isolement, régulateurs de tension, conditionneurs de réseau, onduleurs)

Tableau 9 : Services, fournitures et prestations extérieurs (risques d'indisponibilité temporaire)

5.5 Ressources humaines

Risques d'indisponibilité définitive

Menaces types	Conséquences à préciser	Parades à considérer
Disparition de personnel stratégique	▪ Perte de savoir-faire ▪ Arrêt temporaire ou définitif d'activité ▪ Blocage de système ou d'application (mot de passe, maintenance, exploitation, …) ▪ Blocage de décision	▪ Redondance des compétences sur les activités stratégiques ▪ Délégation de pouvoir ▪ Assurance VIP ▪ Documentation des tâches stratégiques ▪ Consignes de sécurité pour les déplacements en groupe ▪ Plan de remplacement d'urgence (recrutement, sous-traitance, …)
Départ de personnel stratégique	▪ Perte de savoir-faire ▪ Arrêt temporaire ou définitif d'activité ▪ Blocage de système ou d'application (mot de passe, maintenance, exploitation, …) ▪ Blocage de décision ▪ Dégradation de service ou sabotage lié aux conditions de départ	▪ Plan de remplacement avec période de recouvrement pour le transfert des connaissances. ▪ Redondance des compétences sur les activités stratégiques ▪ Documentation des tâches stratégiques ▪ Surveillance accrue du personnel démissionnaire et limitation des droits ▪ En cas de risque de malveillance, désactivation immédiate des droits de la personne (physiques et logiques)

Tableau 10 : Ressources humaines (risques d'indisponibilité définitive)

Risques d'indisponibilité temporaire

Menaces types	Conséquences à préciser	Parades à considérer
Conflit social	▪ Arrêt temporaire, total ou partiel d'activité ▪ Risque de blocage volontaire de locaux et / ou d'équipement (cf. fiche locaux et infrastructure)	▪ Politique sociale adaptée à la fonction informatique ▪ Externalisation des fonctions vitales ▪ Volant de personnel de secours externe à l'entreprise ▪ Locaux et moyens de secours externes et confidentiels
Difficultés de transport	▪ Arrêt temporaire d'activités du site ▪ Risque d'arrêt des équipements	▪ Mise en place de moyens de transport de secours (navettes, organisation du covoiturage, ...) ▪ Accès et pilotage distant ▪ Impressions déportées ▪ Moyens de secours utilisateurs externes pour un service minimum
Indisponibilité accidentelle massive du personnel (épidémie, contamination, …)	▪ Arrêt temporaire d'activités du site ▪ Risque d'arrêt des équipements	▪ Médecine préventive ▪ Maintenance préventive de la climatisation (changement des filtres, surveillance de la qualité de l'air) ▪ Volant de personnel de secours externe à l'entreprise

Tableau 11 : Ressources humaines (risques d'indisponibilité temporaire)

6 TABLE DES FIGURES ET TABLEAUX

7 GLOSSAIRE

PCA [correspond à BCP = Business Contingency Plan]

Plan de Continuité d'Activité. Il a pour but de garantir la survie de l'entreprise, en préparant à l'avance la continuité des activités désignées comme stratégiques. Il n'est pas limité au Plan de Secours Informatique.

PSI [correspond à DRP = Disaster Recovery Plan]

Plan de Secours Informatique. Sous-ensemble du PCA qui couvre les moyens informatiques. Il garantit la reprise des systèmes désignés comme critiques dans le temps minimum fixé. Il garantit également la reprise des données avec le minimum de perte fixé.

Plan de secours

Dans ce document, c'est un terme générique qui désignera soit le PSI, soit le PCA.

Délai de reprise [correspond à RTO = Return Time Objective]

C'est le délai total nécessaire entre l'arrêt de l'activité et la remise à disposition de l'informatique aux utilisateurs.

Degré de fraîcheur des données [correspond à RPO = Recovery Plan Objective]

Selon les besoins exprimés, le degré de fraîcheur des données correspond à la perte des données considérée comme acceptable entre l'arrêt de l'activité et sa reprise. Par exemple, au démarrage après sinistre, les données peuvent dater de la veille au soir, du matin ou de la minute du sinistre.

Comité de crise

Il est composé des responsables de chaque Direction utilisatrice concernée par le plan de secours. Il comprend également des membres de la Direction Générale, de la Direction des Services Généraux, de la Direction des Ressources Humaines, de la Direction de la Communication, de la Direction Informatique et des responsables du plan de secours. Son rôle est de se réunir en cas d'incident grave pour décider de déclencher ou non le plan de secours.

Salle de réunion du comité de crise

Désigne l'endroit où le comité de crise se réunit en cas de nécessité. Il est situé dans un périmètre proche de l'environnement ciblé par le plan de secours mais ne doit pas être adjacent à celui-ci. Il est en général équipé d'au minimum un téléphone, 1 fax et un coffre-fort dans lequel se trouvent les procédures du plan de secours.

Procédures techniques

Elles décrivent les actions à faire par la Direction Informatique au quotidien pour garder les moyens techniques de secours à jour. Elles décrivent également les actions à faire en cas d'activation du PSI ou à l'occasion des tests. Elle est écrite par la Direction Informatique.

Plan de test

Il permet dans un premier temps de valider ce qui a été mis en place par rapport aux besoins exprimés. Puis, à intervalle régulier il permet de garantir le caractère opérationnel du PSI.

Load Balancing

Solution technique, basée sur une duplication applicative et mettant en œuvre de 2 à n serveurs à des fins d'équilibrage de ressources. Cette technique permet de maintenir la disponibilité des applications en cas d'arrêt d'un ou plusieurs serveurs. L'intégrité des données est préservée par une propagation des mises à jour sur tous les serveurs. Toutefois, la session en cours est perdue en cas d'arrêt brutal du serveur en cours d'utilisation.

Dans le cadre d'un PSI, la possibilité de répartir ces machines sur deux sites géographiquement différents doit être étudiée.

Cluster de serveurs

Solution technique de secours s'appuyant sur 2 à n machines « en grappe » et partageant en commun l'ensemble des ressources nécessaires à maintenir la disponibilité des services. En cas d'arrêt brutal d'une ressource, seule la transaction en cours est éventuellement perdue.

Mirroring

Solution de secours s'appuyant sur des techniques de duplication en temps réel des données enregistrées, soit en mode synchrone, soit en mode asynchrone. La duplication des données d'un serveur peut être partielle ou totale, de préférence distante, selon le niveau de sécurité à atteindre et les contraintes techniques de l'environnement informatique.