EMMANUEL **BESLUAU**

Préface de **Dominique Guinet**

Management de la Continuité d'activité

Assurer la pérennité de l'entreprise : planification, choix techniques et mise en œuvre

2e édition

ISBN: 978-2-212-12820-8

EYROLLES

Préface

Alors jeune ingénieur commercial IBM, j'étais en rendez-vous avec le Directeur du service informatique d'une grande banque régionale. Véritable chef d'orchestre, celui-ci avait la réputation de diriger son exploitation comme des cuivres : avec fermeté. Ce jour-là, il avait décidé de montrer, « devant IBM », à son premier violon d'homme système comment il convenait de tester les compétences d'un nouveau musicien. Une imprimante fut amenée, accompagnée d'un « listing » couvert de notes accessibles aux seuls initiés. L'impétrant fut mis à l'épreuve et dut réparer l'instrument récalcitrant.

Il y réussit fort bien ! Mais c'est au moment où il rendit l'instrument nouvellement accordé au chef d'orchestre que je me suis demandé comment procéder lorsque c'est tout l'orchestre qui ne fonctionne plus…

Aujourd'hui, la reprise d'activité est un thème d'actualité pour nos entreprises. En effet, un événement, petit ou grand, virus ou volcan, peut provoquer l'arrêt total ou partiel de l'activité. Au-delà d'un plan de reprise informatique, il faut que les activités clés aient été identifiées au préalable pour pouvoir remettre l'entreprise en route de manière optimale suite à un sinistre. Dans le cas d'une fusion acquisition, par exemple, cela sera déterminant pour définir une stratégie « *Load and Go* » – où seules les données sont reprises - par rapport à une stratégie « *Clone and Go* » où le processus sélectionné est repris en l'état.

Dans tous les cas, les risques associés requièrent l'analyse d'experts. La perception du risque est alors liée à la confiance portée à l'expert et à la capacité de l'équipe de direction à délimiter l'étendue géographique et fonctionnelle du risque, là encore, au-delà de la reprise de la production informatique.

En parallèle, les entreprises constatent l'émergence de nouvelles contraintes liées à la réglementation, à la concurrence et à l'accès aux ressources. Ces contraintes rendent nos entreprises plus vulnérables et nécessitent un véritable management de la continuité d'activité de l'entreprise et de ses partenaires.

Dans un environnement marqué par l'innovation et la performance, il est bon de disposer d'un éclairage averti et de méthodes éprouvées pour approcher le problème et tenter de se préparer. L'ouvrage d'Emmanuel Besluau propose des pistes réalistes. Il est pragmatique et adaptable à de nombreuses situations.

D'une part, il insiste sur ce qui doit être la préoccupation d'une Direction générale, quelle que soit la taille de l'entreprise : la *connaissance de ses activités critiques, de ses processus clés*. Sans cette connaissance précise et actualisée, il est en effet

difficile d'espérer atteindre la résilience nécessaire et illusoire de planifier les reprises indispensables.

D'autre part, cet ouvrage passe en revue les moyens techniques – notamment informatiques – qui permettent une meilleure résistance au sinistre, tout en restant lucide quant à la mise en œuvre effective de ces dispositifs sur le terrain. Celle-ci reste en effet tout particulièrement dépendante d'une bonne attribution des responsabilités et du bon enclenchement des actions en cas de sinistre.

Enfin, cet ouvrage est probablement l'un des premiers à mentionner des principes de *gouvernance de la continuité* et à détailler des moyens progressifs pour exprimer une *politique de continuité* et la traduire dans la réalité. Emmanuel Besluau associe ainsi technologie, méthode et contrôle dans une vision d'ensemble rigoureuse et inspirée par la pratique.

Ce dernier point est très important ; en effet, la prise en compte récente par de grands ERP des processus permettant de gérer la responsabilité sociétale de l'entreprise (RSE) montre qu'au-delà de l'élaboration et de la mise en œuvre effective d'un plan de reprise d'activité, ce concept de *gouvernance de la continuité* répond aux nouvelles exigences portées par les analystes financiers, les clients et les salariés au titre du développement durable.

Dominique Guinet
Ancien Ingénieur Commercial IBM
Directeur du Développement Durable, Bayer France

Préface

à la première édition (2008)

Il est toujours trop tard, quand le sinistre arrive, pour mettre en œuvre un plan de continuité d'activité... Un proverbe chinois illustre ce propos : « les tuiles qui protègent de la pluie ont toutes été posées par beau temps ».

Enfin un ouvrage complet, pratique et documenté sur la continuité d'activité, en français de surcroît !

Ayant moi-même vécu en entreprise des situations de sinistre, je peux témoigner de la nécessité d'être préparé à de telles situations, malheureusement plus fréquentes qu'on ne le croit. Un jour, la salle informatique de la banque dans laquelle je travaillais a brûlé. Nous n'avions aucun plan, ni rien de prévu dans une telle situation, à l'exception d'une sauvegarde externalisée.... La banque aurait dû disparaître. Or c'était en 1977, et l'informatique n'avait pas l'importance vitale qu'elle possède à présent. La banque a pu redémarrer, au prix fort, dans les cinq jours suivants, grâce à des locaux et des moyens fournis par un constructeur. Nous ne sommes revenus à une situation normale que six mois plus tard.

Après ce sinistre, qui avait enfin décidé la direction générale à mettre en place des solutions de secours et un plan associé, j'ai pris conscience de la valeur qu'il faut attribuer à une bonne préparation et aux démarches du type de celles présentées dans ce livre pratique.

En outre, dans ma vie professionnelle, j'ai côtoyé et conseillé de nombreux responsables d'entreprise. Tous m'ont fait part de leur souhait d'y voir enfin plus clair dans la démarche visant à mettre en place de manière pragmatique le management de la continuité d'activité dans leur entreprise. En effet, la mise en place d'un plan de continuité est un projet atypique. C'est un projet transverse qui prend en compte globalement toutes les activités et processus de l'entreprise.

Le Club de la Continuité d'Activité réunit tous les acteurs œuvrant dans ce domaine. Il a pour missions de partager les points de vue et retours d'expérience, de parfaire la maîtrise des solutions et de pérenniser la place du management de la continuité dans l'entreprise. Par là, il joue un rôle moteur auprès des organismes de normalisation et du législateur.

Le Club de la Continuité d'Activité accueille avec intérêt tout ce qui peut contribuer à développer les bonnes pratiques, comme le fait cet ouvrage. Riche d'une expérience très diversifiée de la production informatique, Emmanuel Besluau connaît bien tout ce que l'on peut attendre des technologies. Son approche, qui présente à la fois les principes d'organisation et les architectures techniques, se révèle très intéressante et assez unique.

Nul doute que ce livre contribuera à faire avancer la prise de conscience sur ce sujet important qu'est la continuité d'activité.

François TÊTE
Président du Club de la Continuité d'Activité
www.clubpca.eu

Table des matières

Partie I – L'entreprise dans un monde de risques

Partie II – L'entreprise élabore son plan de continuité

Partie III – L'ingénierie de la continuité

Partie IV – La gouvernance de la continuité

Avant-propos

Un grand nombre d'entreprises ne survivraient pas à une interruption de leur système d'information pendant seulement trois jours. À l'heure où les sinistres semblent se multiplier, des approches nouvelles, organisationnelles et techniques, se sont développées pour faire face aux conséquences et assurer la permanence des activités jugées critiques de l'entreprise.

Le management de la continuité d'activité permet ainsi de rendre l'entreprise plus résiliente dans un monde de risques. Autrefois limitée à la « gestion de crise » ou considérée comme une sous-partie de la gestion des risques ou de la sécurité, cette approche commence à s'imposer comme une discipline à part entière.

Or les observateurs s'accordent à considérer que la continuité d'activité n'a pas actuellement en France l'attention qu'elle mérite de la part des directions générales. En effet, focalisée sur des analyses de risques théoriques, l'entreprise néglige souvent l'impact réel des sinistres potentiels et ne connaît pas les processus les plus critiques. En l'absence de ces considérations, toute atteinte à l'intégrité des moyens vitaux de l'entreprise est souvent chèrement payée par incapacité à réagir efficacement face à l'imprévu.

Certes, quelques plans de reprise d'activité existent ici ou là et l'on peut louer les pionniers qui s'y consacrent. Malheureusement, il s'agit le plus souvent de scénarios trop simples, centrés sur quelques moyens autrefois identifiés comme vitaux et conçus sans vision d'ensemble. En outre, des directions de l'entreprise ont tendance à mettre en place des solutions locales qui, en l'absence d'une vision d'ensemble sur les services essentiels, laissent des lacunes importantes. Dans un monde où les moyens techniques se multiplient et se banalisent, les quelques investissements consentis pour la continuité peuvent ainsi apparaître comme inadaptés si l'on considère la faiblesse de certains maillons organisationnels.

Confiance exagérée dans une technologie fragile, défiance désabusée pour les dispositifs d'organisation utiles, le vécu de la continuité d'activité en France reste largement insatisfaisant. Une prise de conscience des apports réels du management de la continuité d'activité s'impose : c'est l'objectif de cet ouvrage, qui aborde les aspects méthodologiques aussi bien que la mise en œuvre concrète en s'appuyant sur des exemples et situations vécues édifiantes.

Enfin, il est important de mentionner une tendance apparue dernièrement : alors que les sinistres importants sont devenus plus fréquents, disposer d'un plan de continuité d'activité (PCA) valorise l'entreprise et rassure actionnaires, clients et fournisseurs. L'absence de démarche de continuité, dans un contexte où l'entreprise dépend de plus en plus d'éléments technologiques exposés, apparaît plus que jamais comme un signe d'insouciance ou d'incompréhension des enjeux modernes qui veulent que l'entreprise maîtrise correctement ses activités essentielles.

À qui s'adresse cet ouvrage ?

Cet ouvrage intéresse tout professionnel concerné par la continuité d'activité : les directions générales y découvriront comment structurer leur approche, les responsables du plan de continuité y trouveront un cadre de travail avec des recommandations, tandis que les directeurs métier y gagneront une idée plus claire de leurs responsabilités et de leur rôle en matière de continuité. Quant aux spécialistes techniques, ce livre leur fournit nombre d'indications et de recommandations leur permettant de mettre en œuvre la continuité au niveau technique.

Structure de l'ouvrage

Afin de ne négliger aucun aspect stratégique, organisationnel ou technique, cet ouvrage se présente en quatre volets, qui guideront pas à pas les différents acteurs et responsables vers une gestion efficace de la continuité d'activité en entreprise.

- La première partie est consacrée à un sujet essentiel souvent négligé dans les études de continuité : le risque. Comment en prendre conscience et déterminer les faiblesses de l'entreprise ? Et surtout, comment limiter, d'une part l'exposition au risque et d'autre part les conséquences encourues ?
- Partant d'une approche plus traditionnelle quoique rénovée, la deuxième partie décrit comment construire les équipes et attribuer les missions pour obtenir un plan de reprise efficace et comment organiser les tests et exercices pour qu'il le reste. Des canevas précis de plannings et de campagnes de tests réutilisables y sont fournis.
- En troisième partie est proposé un tour d'horizon technologique et informatique qui décrit les différents mécanismes en jeu, en relativisant leur apport et en insistant sur les moyens montrant le meilleur retour sur investissement. Les ressources humaines, dont la criticité est apparue avec la pandémie de la grippe H1N1, sont aussi traitées.
- Enfin, après l'analyse, l'élaboration du plan et l'étude des moyens techniques et humains disponibles, la quatrième partie traite des aspects essentiels de gouvernance supervisant la mise en œuvre de la continuité, à travers la prise de conscience nécessaire, les décisions de politique et le contrôle indispensable à mettre en place.

Remerciements

Je remercie mes collègues du Duquesne Group et tout particulièrement René Dugué et Donald Callahan, qui m'ont poussé à consacrer le temps nécessaire à cet ouvrage. Je tiens aussi à décerner une mention spéciale aux différents clients accompagnés durant ces années et qui m'ont souvent fourni de la matière pour ce livre. Certains se reconnaîtront sans doute dans les quelques anecdotes qui y sont rapportées.

Chapitre 3

Le développement d'une stratégie de continuité

Au cours des analyses présentées dans les deux chapitres précédents, l'entreprise a fait le point sur les risques qu'elle encourt et a déterminé ses activités critiques, dont la perte lui causerait les dommages les plus forts. Les délais de reprise et les temps d'immobilisation maximum acceptables de ces activités ont été étudiés et sont désormais connus.

Il reste maintenant à effectuer les actions préventives nécessaires et à prévoir les modalités de reprise pour que les exigences des activités critiques puissent être remplies. C'est l'objet de ce chapitre, qui explique comment déterminer ces actions et comment définir la manière dont la continuité d'activité est assurée dans l'entreprise. Tout ce dispositif constitue la stratégie de continuité de l'entreprise.

Les aspects techniques de ce chapitre ne sont qu'esquissés, afin de ne pas nuire à son déroulement ; ils seront abordés plus en profondeur dans la troisième partie de cet ouvrage.

Produire une stratégie de continuité est un travail nécessitant cinq phases principales d'étude et de décision.

1. Dans une première phase, à partir de l'analyse d'impact sur les activités (BIA – voir le chapitre 2) qui a précédé, les besoins en termes de reprise sont affinés et déterminés précisément.
2. Au cours de la deuxième phase, on passe en revue les solutions possibles et réalistes.
3. La troisième phase permet de déterminer les délais inhérents aux solutions proposées en rapport avec les exigences formalisées durant l'analyse d'impact pour chaque activité.
4. La phase quatre consiste à réaliser une étude de coût et faisabilité sur les solutions possibles.
5. Enfin, la phase cinq mène à une conclusion et à une prise de décision : la stratégie est prête et documentée.

Cette stratégie servira de fondement au développement du plan de continuité proprement dit.

Phase 1 – Expression des besoins en termes de reprise

Cette première étape est réalisée à partir des conclusions de l'analyse d'impact sur les activités (BIA). Elle se focalise exclusivement sur les processus jugés critiques.

> **Vocabulaire**
> Dans la suite de ce chapitre, les mots *processus* et *activités* sont employés indifféremment.

Exigences des processus critiques

Dans la liste des ressources associées aux processus critiques (établie normalement lors du BIA), on reprend les différents paramètres de reprise que sont les MTD (temps maximal d'interruption admissible), WRT (temps nécessaire à la récupération du travail), RTO (délai cible de récupération des moyens de travail) et RPO (délai cible de récupération des données).

On y ajoute, le cas échéant, les besoins supplémentaires en cas de crise. Il s'agit principalement de besoins en personnel – définition de l'équipe de gestion de crise nécessaire pour le ou les processus considérés – ainsi qu'en moyens matériels tels que :

- un site de secours (ou des bureaux) d'où la crise sera gérée ;
- des moyens de communication ;
- des possibilités d'accès (doubles de clés, cartes magnétiques, etc.).

Ces points sont précisés et détaillés dans le chapitre 4.

Étude des besoins

Pour chaque processus critique, les besoins sont listés et classés en catégories. Ce classement se révèle en effet utile pour pouvoir confier l'étude des divers besoins à des équipes différentes. On pourra, par exemple, reprendre les catégories de besoins suivantes :

1. bureaux et locaux de travail ;
2. systèmes, infrastructures et locaux informatiques ;
3. données et enregistrements critiques ;
4. production industrielle et fabrication.

La gestion de ces listes réclame un soin particulier, de manière à suivre au plus près les évolutions du terrain.

Les ressources humaines, lorsqu'elles sont considérées dans le cadre d'un sinistre externe (non pandémique), figurent de fait dans la première rubrique (les bureaux et chaises étant pour des employés…).

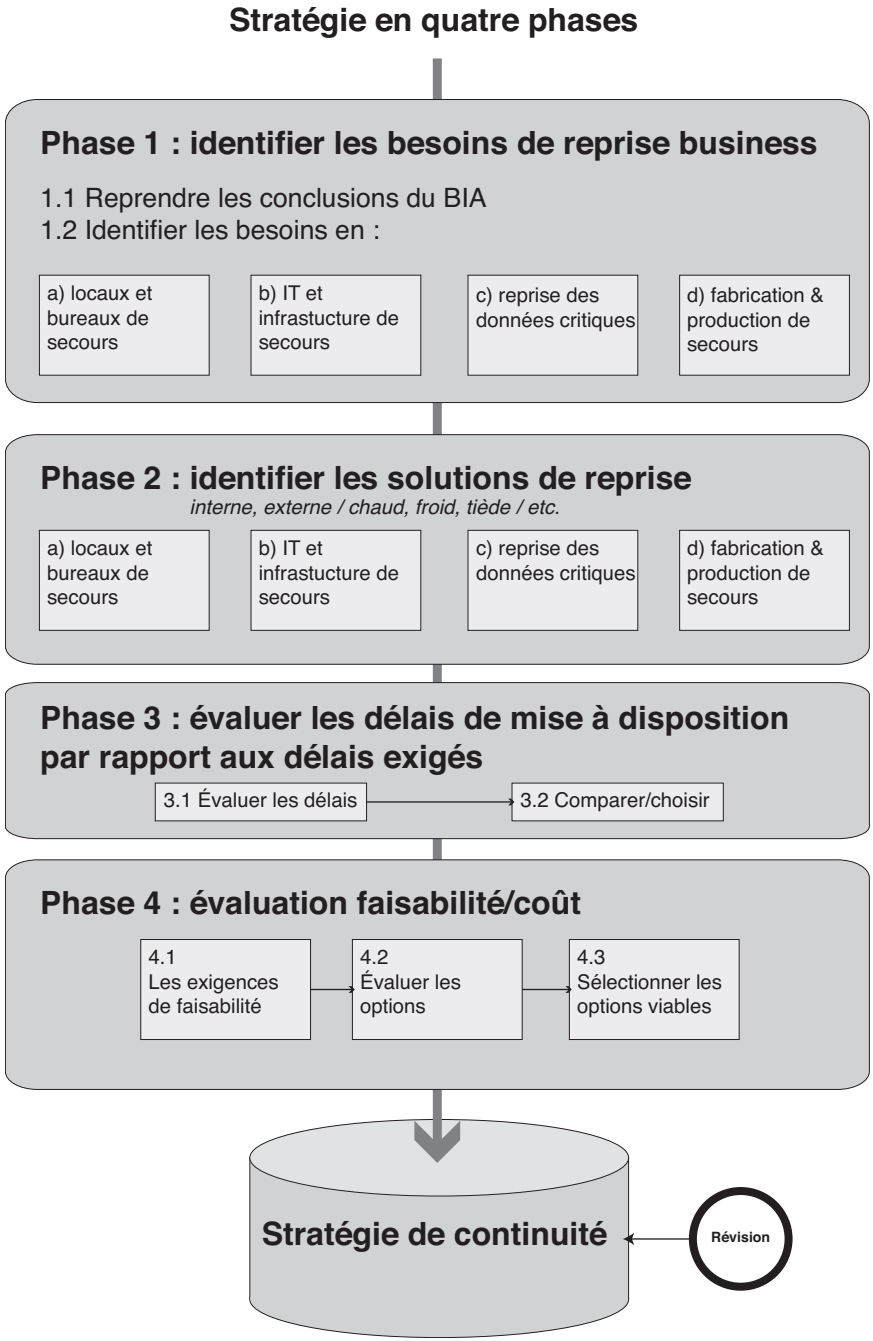

Figure 3-1 : Schéma synoptique de la démarche en quatre phases

En revanche, s'il s'agit du sinistre de pandémie, qui a pour caractéristique principale de ne toucher que les êtres humains, il est recommandé de définir un plan spécial pandémie (voir chapitre 11).

1. Bureaux et locaux de travail

On classe dans cette catégorie les besoins concernant :

- les locaux généraux – situation et nature (par exemple : est-il possible d'utiliser une salle dans un hôtel ? à quelle distance du site sinistré ? aura-t-on besoin d'utiliser des bureaux provisoires mobiles ?) ;
- le mobilier de bureau et meubles divers ;
- les moyens de communication ;
- les fournitures (papiers, stylos, etc.) ;
- des locaux particuliers (locaux réfrigérés ou coffre fort, par exemple) ;
- des formulaires spéciaux (pour faciliter la saisie par écrit, par exemple) ;
- le matériel informatique de bureau (PC avec licences adéquates, imprimantes, etc.).

On indiquera, quand il y a lieu, la tolérance acceptable sur ces moyens.

2. Systèmes, infrastructures et locaux informatiques

Cette catégorie comprend les besoins en termes de :

- locaux informatiques – taille, emplacement et caractéristiques techniques ;
- fournitures électriques nécessaires ;
- capacité de refroidissement et de filtrage de l'air ;
- serveurs de stockage ;
- bandothèques et robots dérouleurs de bandes magnétiques ;
- connexions pour les télécommunications, débits, taux de transfert, etc. ;
- imprimantes spécifiques et alimentation en papier associée ;
- systèmes d'exploitation, sous-systèmes, bases de données, middleware ;
- outils de reprise et de restauration de données ;
- licences d'utilisation associées ;
- postes de travail ;
- PC avec licences adéquates et imprimantes individuelles associées.

La précision s'impose sur la plupart des éléments de cette liste, qui doivent être correctement spécifiés (type, version, mises à jour, niveau, etc.). Il faut en effet assurer une cohérence et une compatibilité optimales de l'ensemble.

3. Données et enregistrements critiques

En complément de la catégorie précédente, il convient de considérer les besoins en documents, données et toute autre information nécessaire à l'activité.

Données informatiques

Classiquement, on étudie les aspects suivants, généralement gérés dans diverses entités de l'entreprise :

- les sauvegardes informatiques (correctement effectuées sur les points de reprise applicative, de manière à pouvoir être chargées et exploitées sur le site de secours) ;
- les lieux où ces sauvegardes doivent être conservées (hors sites) ;
- les formats de ces sauvegardes (média, types de cassettes ou de disques, outils de sauvegarde, formats des enregistrements, contraintes diverses) ;
- les regroupements logiques des éléments sauvegardés (lots de cassettes cohérents, valises regroupant ces lots, etc.) ;
- éventuellement, les moyens logistiques pour acheminer les sauvegardes sur les sites (taxi, camionnette, etc.).

Là encore, la plus grande précision est indispensable, car ces aspects ne tolèrent pas l'approximation. Une cassette manquante ou une sauvegarde effectuée à la mauvaise date provoqueraient, par exemple, l'impossibilité de restaurer les données.

Données non informatisées

Le bureau « sans papiers » étant loin d'être généralisé, il est par ailleurs indispensable de référencer tous les dossiers papiers, microfiches, disques optiques, etc.,utilisés dans l'activité de tous les jours ou vitaux en termes de conservation.

Il faut ici prendre en compte tout ce qui est conservé sur le site, dans les bureaux, armoires ou en sous-sol, sans oublier les sites d'archivage. À ce propos, une réflexion sur ce sujet peut se révéler utile pour faire évoluer la politique de gestion et d'entreposage de ces documents.

4. Production industrielle et fabrication

Bien que ces aspects se situent à la marge de cet ouvrage, citons ici les besoins concernant :

- les équipements de production critiques (machines, stocks de pièces intermédiaires, etc.) ;
- les produits cruciaux à conserver en stock (produits finis, semi-finis ou matières premières, etc.) ;
- des locaux alternatifs permettant de fabriquer en tout ou en partie et de poursuivre la production, en précisant leurs caractéristiques.

> **Remarque générale**
>
> • Ces listes doivent faire l'objet d'une attention minutieuse.
>
> • Elles doivent être remplies et détaillées par des spécialistes choisis en fonction de chaque cas.
>
> • Elles évoluent au cours du temps : les tests et la maintenance du plan (voir les chapitres 6 et 13) veilleront sur ce point à conserver leur pertinence.

• La gestion du changement dans le système informatique doit veiller à bien tenir à jour ces configurations.

Phase 2 – Étude des options possibles pour la reprise

Afin de répondre aux besoins de reprise exprimés, on étudie un certain nombre d'options envisageables. Ces options doivent être analysées sans idées préconçues sur le fait qu'elles seront finalement retenues ou pas. Il est en effet toujours plus intéressant d'explorer toutes les solutions, sans a priori.

Les classements permettant de structurer la démarche, dans le domaine de la continuité d'activité comme pour toute autre analyse, ces options peuvent une fois encore être regroupées en différentes catégories. L'exclusion éventuelle d'une catégorie, pour quelque raison que ce soit, n'interviendra que plus loin dans la démarche.

Catégories d'options ouvertes

Deux classements sont proposés ici, selon que l'on considère le fournisseur de l'option (interne, externe, etc.) ou son degré de préparation.

En fonction du fournisseur

Un premier classement peut être effectué en fonction du fournisseur de l'option.

- **Options internes** : il s'agit d'options qui engagent l'entreprise avec ses propres ressources et moyens, par exemple : un site de bureaux de secours appartenant à l'entreprise. Le fournisseur est donc interne à l'entreprise.
- **Options contractuelles auprès de fournisseurs** : dans ce cas, on fait appel à un fournisseur externe avec lequel un contrat a été conclu. Sur ce point, on peut noter le développement d'accords d'un type particulier : les accords de réciprocité entre confrères.
- **Options impliquant des employés** : c'est un cas particulier à étudier, impliquant les employés de l'entreprise (les employés peuvent travailler depuis leur domicile par exemple). Il vaut mieux avoir prévu ce cas de figure dans les accords d'entreprise ou, éventuellement, dans le contrat de travail. Le « fournisseur » est alors d'un type un peu particulier, puisqu'il s'agit de l'employé. Si cet employé est un prestataire, on pourra se reporter au cas précédent (fournisseur externe).

En fonction du degré de préparation

On peut également classer les différentes options en fonction de leur niveau de préparation et, par conséquent, de leur rapidité de mise à disposition.

- **Options toutes prêtes** : tout est prêt pour prendre le relais en cas de sinistre, les divers moyens sont disponibles, réservés et à jour. C'est en général une option rapide à mettre en œuvre, mais coûteuse.

- **Options prévues** : un accord a été passé avec un fournisseur ou un autre site de l'entreprise pour que les moyens soient mis à disposition dans un délai convenu. C'est souvent le cas dans les situations contractuelles avec une entreprise de secours ou dans les accords de réciprocité avec des confrères, par exemple. Pour cette option, les délais de mise en œuvre sont d'ordre moyen.
- **Options au cas par cas** : rien de particulier n'est prévu a priori, mais on sait que, si le besoin se fait sentir, on y répondra par une action particulière en interne ou une commande en externe. Rien n'empêche d'ailleurs de préparer cette commande. C'est en général l'option la moins coûteuse, mais aussi la moins sûre.

De façon similaire, on classera aussi les moyens informatiques selon leur degré de préparation opérationnelle. Traditionnellement, on parle alors de moyens de secours *à froid* (peu préparés), *tièdes* (préparés) ou *chauds* (prêts à l'usage).

Ventilation des options selon les catégories

Le tableau suivant donne un exemple de ventilation des catégories d'options retenues.

Tableau 3-1 : Ventilation des options retenues dans les différentes catégories

	Interne	Externe	Employés
Froid	Site précâblé à 200 km	Non retenu	Travail à domicile
Tiède	Site de développement activable	Contrat avec une société d'infogérance pour les serveurs Unix	PC prééquipé à domicile
Chaud	Non retenu	Contrat de haute disponibilité sur les applications X et Y	Non retenu

On constate dans cet exemple que les solutions froides retenues ne font pas l'objet de contrats sur le marché et que seule la solution chaude est réalisée avec un prestataire externe.

L'élaboration de tableaux de ce type permet la discussion et la prise de décision durant les réunions de suivi.

Options envisagées

En fonction des besoins exprimés et des catégories d'options définies précédemment, il devient possible de lister et d'analyser les options les plus susceptibles de donner satisfaction. Encore une fois, cela consiste à se livrer à un exercice d'imagination des solutions qui pourraient convenir. Il ne s'agit pas

pour autant de rêver et de s'éloigner de la réalité technologique et financière : les avantages et inconvénients des options listées seront jugés plus loin (phase 3).

On adoptera la même segmentation que pour l'expression des besoins :

1. bureaux et locaux de travail ;
2. systèmes, infrastructures et locaux informatiques ;
3. données et enregistrements critiques ;
4. production industrielle et fabrication.

1. Bureaux et locaux de travail

Le tableau ci-après donne un exemple d'options envisageables qui seront étudiées pour les locaux et bureaux, classées en fonction de leur fournisseur.

Tableau 3-2 : Options pour les locaux et bureaux

Locaux et bureaux		
Catégorie	**Option**	**Description**
Solution contractuelle avec fournisseur externe	Site mobile	Site mobile de secours livré en un lieu prévu, et en général prééquipé en mobilier, téléphones et postes de travail.
	Salles de réunion d'hôtel	Hôtel prévu à l'avance.
	Site fixe	Site de secours en un lieu donné, proposé en tant que service par un prestataire, également prééquipé.
Solution interne à l'entreprise	Autre site de l'entreprise	Site de secours dormant ou pas, prééquipé ou non.
Recours à l'employé	Travail à la maison	L'employé travaille depuis son domicile et peut éventuellement accéder au système informatique, téléphonique, etc.

2. Systèmes, infrastructures et locaux informatiques

De même, le tableau suivant traite des options concernant les sites informatiques de secours, plus ou moins équipés des matériels et systèmes nécessaires. Ces options sont ici encore classées en fonction de leur fournisseur (interne, accord externe, offre commerciale). La description des sites doit correspondre au plus près à une réalité constatée et/ou réalisable.

Tableau 3-3 : Options pour les sites informatiques

Sites informatiques de secours		
Catégorie	**Option**	**Description**
En toute propriété	Site distant appartenant à la société	Site de secours de la société, en un lieu déterminé prévu et en partie préparé.
	Site mobile	Site mobile de secours livré en un lieu prévu, en général prééquipé en mobilier, téléphones, postes de travail ou serveurs, réseaux, etc.
Accord avec un tiers	Accord de réciprocité avec un confrère	Chacun réserve de la place à l'autre en cas de sinistre.
Offre commerciale	Site dédié (offre du marché)	Site de secours dédié, proposé en tant que service par un prestataire, plus ou moins prééquipé.
	Site partagé (offre du marché)	Site de secours partagé, proposé en tant que service par un prestataire, plus ou moins prééquipé.

On peut aussi constituer d'autres tableaux abordant un sujet spécifique pour lequel une décision s'impose, comme le niveau de préparation des sites (voir le tableau suivant).

Tableau 3-4 : Niveaux de préparation possibles pour les sites informatiques de secours

Sites informatiques de secours		
Catégorie	**Option**	**Description**
Non préparé	Site froid	Site de secours non équipé en matériel informatique mais disposant de moyens pour en accueillir (alimentations électriques, air conditionné, chauffage, eau, sprinklers, lignes télécoms, faux-planchers et passage de câbles, etc.).
Prévu	Site tiède	Site de secours déjà équipé de certains moyens informatiques nécessaires, mais pas de tous, nécessitant donc d'être complété dans un certain délai ; demande une préparation.
Prêt à l'emploi	Site chaud	Site de secours dont l'équipement est très proche de celui du site à secourir.

Pour chaque option envisagée, on peut présenter les niveaux que l'on souhaite étudier (froid, tiède, chaud).

3. Données et enregistrements critiques

En ce qui concerne les données et enregistrements critiques, une attention particulière doit être portée à la capacité à reconstruire les données opérationnelles. Pour plus de précision sur les aspects techniques, on se reportera à la Partie III de cet ouvrage.

Tableau 3-5 : Options pour les données critiques

Données critiques		
Catégorie	**Option**	**Description (voir partie III)**
Fréquence des sauvegardes	Continu	Sauvegarde en continu par réplication à distance
	Quelques minutes	Cliché (*snapshot*) toutes les 3 minutes, par exemple (stockage en réseau NAS)
	Jour	Sauvegarde une fois par jour
	Semaine	Sauvegarde une fois par semaine
	Mois	Sauvegarde une fois par mois
Type de sauvegarde	Complète	Complète, sur tous les fichiers
	Incrémentielle	Uniquement ce qui a été modifié depuis la sauvegarde précédente
	Différentielle	Uniquement ce qui a changé depuis la dernière sauvegarde complète
Technologie de sauvegarde	Miroir distant (*remote mirroring*)	Copie de disque à disque, par contrôleur, par exemple
	Propagation de log de SGBD	Le système de gestion de base de données propage son journal sur un site distant
	Bandes	Copie sur bandes stockées hors site

Afin de faciliter la prise de décision, il est également possible de mentionner les avantages et les inconvénients de chaque option. On se reportera au chapitre 8 pour plus de précision sur ces points.

Enfin, cette analyse ne doit pas omettre les dossiers non informatiques que l'on peut dupliquer, mettre dans des armoires ignifuges ou conserver en double sur deux sites, par exemple.

4. Production industrielle et fabrication

Pour la production et la fabrication industrielles, là encore, de nombreuses solutions sont susceptibles d'être proposées à l'étude.

Tableau 3-6 : Options pour les équipements de production

Équipements et ressources critiques de production		
Catégorie	**Option**	**Description**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	L'équipement est acquis lorsque le sinistre a lieu.
	Acquisition des pièces détachées	Acquisition des pièces en fonction des besoins après le sinistre
Préétabli	Contrat de service pour le sauvetage et la restauration	Contrat pour sauver et restaurer tous les équipements endommagés, souscrit, avant le sinistre, auprès d'un fournisseur externe.
	Maintien d'un stock de secours pour les pièces critiques sur un site distant	Le stock de pièces critiques est maintenu sur un site de secours à distance avant le sinistre.
	Maintien d'équipements de secours pour les équipements critiques, sur un site distant	Les équipements critiques sont maintenus sur un site de secours à distance avant le sinistre.
Stock de secours de matières premières	Maintien dans un entrepôt de secours des stocks de matières premières ou produits intermédiaires nécessaires durant la reprise	Ces matériels et produits sont stockés à l'avance sur un site distant.
Site de production alternatif	Utilisation d'un site distant de la société, vide	Site équipé de certains moyens : alimentations électriques, chauffage, sprinklers, air conditionné, etc.
	Réparation, reconstruction du site sinistré	Le site endommagé est reconstruit ou réparé, totalement ou partiellement.

Comme dans les autres analyses, un compromis est établi entre ce qui est souhaitable et ce qui est réalisable.

Phase 3 – Confrontation des options aux exigences métier

Une fois toutes les options possibles passées en revue, celles-ci devront être confrontées aux exigences de chaque activité, telles qu'elles ont été définies dans l'analyse d'impact (BIA). En éliminant les options non compatibles avec les besoins exprimés, notamment en termes de délais, cette phase permet de procéder à une première sélection, avant d'effectuer une évaluation multicritère (coût/faisabilité).

Cette confrontation se fait en deux étapes.

1. Les options listées précédemment sont passées en revue pour déterminer leur rapidité de mise en œuvre ou « délai d'activation » en cas de sinistre.
2. Ce délai de mise en œuvre est alors comparé aux besoins émis par les métiers sur leurs activités critiques, permettant ainsi de retenir les options donnant satisfaction.

Importance de la confrontation

Très souvent dans l'entreprise, les responsables de moyens ont déjà plus ou moins réfléchi à la continuité des moyens dont ils ont la charge et ont réalisé des actions, des plans divers. En particulier, on a souvent affaire aux cas suivants :

- des responsables de sites informatiques (mais pas seulement) qui ont prévu des sites de secours plus ou moins adaptés ;
- des responsables de systèmes informatiques qui ont mis en place des solutions de résilience permettant par exemple des copies de données à distance ;
- des responsables d'exploitation qui font des sauvegardes régulières et conservent des cartouches en lieu sûr ;
- des équipes de support qui ont prévu des débordements sur un prestataire externe au cas où elles seraient surchargées.

Toutes ces actions sont intéressantes et doivent être prises en considération. Elles ont cependant le tort, la plupart du temps, d'être déconnectées des besoins métier, par absence de BIA préalable.

La confrontation dont il est question ici est une action indispensable de comparaison entre les besoins exprimés par les processus critiques et la réalité mise en œuvre par les gestionnaires de moyens. Aussi curieux que cela puisse paraître, cette confrontation n'est que très rarement exécutée. Or elle est nécessaire pour détecter cinq types de situations assez courantes :

- **la surprotection** : les mécanismes de résilience ou de reprise assurent une disponibilité qui va au-delà de ce que les métiers demandent ;
- **la sous-protection** : telle application n'est pas considérée comme critique par les exploitants alors qu'elle a été déclarée comme telle lors du BIA ;
- **la lacune** : la protection d'un ensemble applicatif est correcte, mais un maillon essentiel pour les métiers est laissé pour compte (par exemple, un nouveau module mis dans un environnement qui n'est pas aussi fiable que le reste) ;
- **le « tout en interne »** : une solution externe chez un prestataire serait possible à peu de frais ; or les exploitants internes mettent en place des solutions résilientes coûteuses ;

- **le vieillissement** : le plan de reprise d'activité (PRA) prévu permet de reprendre l'activité d'un mainframe IBM. Or dans les faits, depuis quinze ans, ce mainframe est marginalisé : 150 serveurs sont apparus en salle, sans être pris en compte par le PRA.

La confrontation aux exigences émanant des analyses d'impact doit donc être réalisée avec une vision d'ensemble sur les moyens et les besoins des métiers. Elle ne doit pas d'ailleurs se restreindre aux moyens gérés par l'entreprise et doit s'ouvrir aux services proposés en dehors de l'entreprise par des prestataires spécialisés…

Définition des délais d'activation

Cet aspect est fondamental car, en cas de sinistre et d'activation de l'option considérée, il convient de se conformer aux exigences de délai imposées alors que le chronomètre court.

Les options listées précédemment sont étudiées afin de mettre à jour les diverses préoccupations ou problèmes de réalisation potentiels, ce qui permet d'aboutir, pour chacune d'entre elles, à l'évaluation de leur EAT (*Expected Availability Time*) ou « délai moyen d'activation ».

En effet, si ce délai moyen d'activation est supérieur aux exigences métier, cela nécessitera de revoir l'option, en l'éliminant ou en l'améliorant.

Par souci de cohérence, la même segmentation que lors des autres phases est retenue pour étudier les différents paramètres d'activation des options.

1. Bureaux et locaux de travail

Le tableau ci-après présente, pour les options citées en exemple, les obstacles principaux à une mise à disposition rapide.

Tableau 3-7 : Difficultés prévisibles pour chaque option envisagée

Locaux et bureaux		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Solution contractuelle avec fournisseur externe	Site mobile	Distance à parcourir, conditions de circulation (météo, trafic), encombrements pour un convoi exceptionnel.
	Salles de réunion d'hôtel	Si le sinistre est régional, tous les hôtels sont pris ou sinistrés.
	Site fixe	Distance, conditions de circulation et d'accès.
Solution interne à l'entreprise	Autre site de l'entreprise	Idem, en ajoutant les causes communes (par exemple, les grèves).
Recours à l'employé	Travail à la maison	Difficultés de mise en place de la solution technique pour les employés et la sécurité.

Il est aussi intéressant d'étudier d'autres aspects, tels que ceux liés au degré de préparation opérationnelle ou à l'ouverture des locaux et bureaux de secours, ainsi que du centre de crise (voir le chapitre 4).

Tableau 3-8 : Difficultés à envisager pour la préparation des locaux, bureaux et centre de crise

Locaux, bureaux et centre de crise		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Niveau de préparation opérationnelle	Site froid	Préparer le site, le configurer, installer, connecter, etc. Les tâches peuvent s'avérer très longues.
	Site tiède	Les compléments, les paramétrages et les connexions peuvent prendre du temps (1 jour ?).
	Site chaud	Normalement disponible rapidement si c'est bien géré (quelques heures).

Remarque : disponibilité des sites

Le centre de crise (voir le chapitre 4) est encore plus sensible que les autres types de locaux. Il doit être ouvert le premier.

Tableau 3-9 : Préoccupations lors du déclenchement

Locaux, bureaux et centre de crise		
Catégorie	**Option**	**Préoccupations ou problèmes potentiels**
Méthode de recours	Préétabli	Normalement c'est une solution préparée donc rapide. Attention aux évolutions non reportées. Il faudra faire des tests.
	Préarrangé	Bien, si les engagements sont tenus. Prévoir du temps et des ressources humaines aguerries pour les installations, configurations, paramétrages, etc.
	Cas par cas	Selon les circonstances et types de besoins, les ressources peuvent mettre du temps à se mettre en place. À réserver au matériel standard ?

2. Systèmes, infrastructures et locaux informatiques

Pour les options concernant les sites informatiques de secours, plus ou moins équipés des matériels et systèmes nécessaires, on s'attachera à des préoccupations telles que celles présentées dans les tableaux ci-après. Les difficultés mentionnées doivent permettre rapidement de retenir ou d'éliminer une option.

Tableau 3-10 : Difficultés prévisibles pour chaque option envisagée

Matériel sur les sites informatiques de secours		
Catégorie	**Option**	**Préoccupations et délais**
En toute propriété	Site distant appartenant à la société	La distance du site, l'état des routes, le temps pour y aller peuvent avoir un effet sur les délais.
	Site mobile	Idem, en ajoutant les connexions réseau à effectuer.
Accord avec un tiers	Accord de réciprocité avec un confrère	Les délais dépendent ici de la préparation ou non du site, de la réaction du partenaire (qui peut, dans les cas extrêmes, avoir lui-même subi un sinistre), de la distance et de l'état des routes, etc.
Offre commerciale	Site dédié (offre du marché)	La distance, le besoin de personnel sur place influencent les délais.
	Site partagé (offre du marché)	Site utilisé en totalité ou en partie, conséquences de l'occupation par d'autres clients, éloignement et facilité d'accès.

Tableau 3-11 : Difficultés à considérer pour la préparation des sites de secours

Matériels sur le site de secours		
Catégorie	**Option**	**Préoccupations et délais**
Niveau de préparation opérationnelle	Site froid	Il faut équiper le site : problèmes d'acquisition d'équipements, de démarrage, d'installations diverses, de paramétrages, qui peuvent aller jusqu'à 7 jours.
	Site tiède	Les équipements supplémentaires et les installations puis les paramétrages peuvent prendre de 1 jour à 5 jours.
	Site chaud	Normalement disponible rapidement (de 15 minutes à quelques heures).

3. Données et enregistrements critiques

En ce qui concerne les données et enregistrements critiques, une attention particulière sera portée à la rapidité de reconstruction des données opérationnelles. Rappelons que les moyens techniques utilisés sont expliqués plus en détail dans la partie III.

Tableau 3-12 : Caractéristiques et délais pour chaque option concernant les données critiques

Données critiques		
Catégorie	**Option**	**Problématique et délais**
Fréquence des sauvegardes	Continu	Convient aux RPO courts (quelques heures).
	Quelques minutes	RPO de quelques minutes.
	Jour	RPO = 1 jour.
	Semaine	RPO = une semaine.
	Mois	RPO = un mois.
Type de sauvegarde	Complète	Demande peu de bandes et peu de temps pour restaurer.
	Incrémentielle	Demande le plus de bandes et de temps pour restaurer.
	Différentielle	Entre les deux précédents.
Technologie de sauvegarde	Miroir distant (*remote mirroring*)	Peut permettre des RTO et RPO voisins de zéro, si complet.
	Routage de transactions	Idem, avec retour en arrière possible.
	Grappe (*cluster*) à distance campus et SAN	Typiquement : RTO < 30 minutes et RPO < 8 heures.
	Propagation de log de SGBD	Dépend du traitement de la log sur site distant ; dans les meilleurs cas : RPO et RTO < 30 minutes.
	Bandes	Bandes proches ou non du lieu de restauration ; selon le temps d'acheminement, RPO et RTO se comptent en jours.
Site de stockage distant	Site commercial	Considérer la distance et l'accessibilité, le rangement des bandes, la facilité à les regrouper et à les retrouver rapidement, délais pour prévenir le fournisseur.
	Site interne	Idem, en ajoutant les compétences en local ou à déplacer.

Sur tous ces points, le chiffrage devra être précis et validé par les hommes de l'art. L'enjeu consiste ici à détecter les points à problèmes, qui peuvent se révéler bloquants ou, au contraire, à susciter une amélioration.

Il faut aussi noter que la plupart du temps plusieurs solutions cohabiteront et que, pour une activité donnée de l'entreprise, c'est la plus pénalisante qui sera ressentie au final par les usagers.

Là encore, les données papier ou enregistrées sur disque optique numérique (DON) feront l'objet d'une considération particulière.

4. Production industrielle et fabrication

Enfin, voici un exemple de préoccupations concernant les solutions envisageables pour les moyens de production de l'entreprise.

Tableau 3-13 : Difficultés prévisibles pour chaque option envisagée

Équipements et ressources critiques de production		
Catégorie	**Option**	**Préoccupations et délais**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	Si l'équipement n'est pas disponible et pas standard, il faudra attendre (des mois) ou sinon l'acquérir à l'avance et l'entreposer.
	Acquisition des pièces détachées	Les pièces de rechange ont-elles été réservées par le fabricant pour la maintenance ? Sont-elles accessibles ? Sinon : refabrication, donc délais élevés.
Pré-établi	Contrat de service pour le sauvetage et la restauration	Difficultés de mise en œuvre du contrat dues à des effets collatéraux du sinistre (incendie rendant les locaux inaccessibles, émanations toxiques).
	Maintien d'un stock de secours pour les pièces critiques sur un site distant	Le temps de récupération dépend de la distance, de l'état des transports, de l'emballage des pièces et de la logistique.
	Maintien d'équipements de secours pour les équipements critiques, sur un site distant	Idem, en ajoutant les compétences nécessaires pour maintenir ces équipements en état et redémarrer.
Stock de secours de matières premières	Maintien dans un entrepôt de secours des stocks de matières premières ou produits intermédiaires nécessaires durant la reprise	Le temps de récupération dépend de la distance, de l'état des transports, de l'emballage des matières et de la logistique. Les produits finis stockés peuvent-ils être expédiés au client depuis le site de secours sans impact pour les clients ?
Site de production alternatif	Utilisation d'un site distant de la société, vide	Attention au degré de préparation du site.
	Réparation, reconstruction du site sinistré sur place	Délais dépendant du temps à évaluer les dommages, à monter le dossier assurance, à évaluer les réparations et à les déclencher avec les contrats adéquats, tout en respectant les consignes de sécurité.

Les défauts ou faiblesses constatés peuvent conduire à rechercher l'amélioration des offres dont l'entreprise dispose sur le marché. Ils nécessitent souvent des ajustements dans les options, qui se traduisent par une révision des contrats.

Comparaison aux exigences et sélection des options

Une fois le délai moyen d'activation déterminé, celui-ci est comparé aux besoins chiffrés précédemment par les différents paramètres de reprise : MTD, RTO, RPO et WRT. Cette comparaison permet de sélectionner les options les mieux adaptées ; les options non convenables sont alors éliminées. Notons que, dans certains cas, les options sont réétudiées dans le but d'accélérer ou de faciliter leur activation. Les autres options, elles, sont retenues et passées au crible de l'étude de faisabilité et coût faisant l'objet de la phase 4.

Le tableau suivant donne, à titre d'exemple, la liste des options précédentes qui sont ici éliminées, en précisant la raison de cette élimination.

Tableau 3-14 : Options éliminées pour les locaux et bureaux (1)

Locaux et bureaux		
Catégorie	**Option**	**Raison de non-sélection**
Solution contractuelle avec fournisseur externe	Site mobile	La distance à parcourir, les conditions de circulation (météo, trafic), les encombrements pour un convoi exceptionnel sont rédhibitoires.
Activation	Cas par cas	Selon les circonstances et le type de besoins, les ressources peuvent prendre trop de temps à être mises en place.
Niveau de préparation	Site froid	Les tâches de préparation du site, de configuration, d'installation, de connexion, etc.,peuvent être très longues.

Tableau 3-15 : Options éliminées pour les sites informatiques de secours (2)

Sites informatiques de secours		
Catégorie	**Option**	**Raison de non-sélection**
En toute propriété	Site mobile	Sur routes surchargées, cette solution est impossible à réaliser, sans parler des difficultés de connexions réseaux à effectuer.
Offre commerciale	Site partagé (offre du marché)	Le site peut être utilisé en totalité ou en partie, l'occupation par d'autres clients, l'éloignement et la difficulté d'accès rendent cette option trop incertaine.
Niveau de préparation	Site froid	Il faut équiper le site : problèmes d'acquisition d'équipements, de démarrage, d'installations diverses, de paramétrages ; cela peut aller jusqu'à 7 jours voire plus.

Tableau 3-16 : Options éliminées pour les données critiques (3)

Données critiques		
Catégorie	**Option**	**Raison de non-sélection**
Fréquence des sauvegardes	Mois	RPO = un mois. Délai trop long, même pour les applications peu exigeantes.
Type de sauvegarde	Incrémentielle	Demande le plus de bandes et de temps pour restaurer.
Technologie de sauvegarde	Routage de transactions	Technologie non maîtrisée en interne.
	Grappe (*cluster*) à distance campus et SAN	Technologie non conforme à l'architecture choisie.

Tableau 3-17 : Options éliminées pour les équipements de production (4)

Équipements et ressources critiques de production		
Catégorie	**Option**	**Raison de non-sélection**
À acquérir quand le besoin apparaît	Acquisition de l'équipement	Si l'équipement n'est pas disponible et pas standard, il faudra attendre (des mois) sinon l'acquérir à l'avance et l'entreposer.
Préétabli	Contrat de service pour le sauvetage et la restauration	Difficultés de mise en œuvre du contrat dues à des effets collatéraux du sinistre (incendie rendant les locaux inaccessibles, émanations toxiques...).
Site de production alternatif	Réparation, reconstruction du site sinistré sur place	Délais trop longs en raison du temps nécessaire à évaluer les dommages, à monter le dossier assurance, à évaluer les réparations et à les déclencher avec les contrats adéquats, tout en respectant les consignes de sécurité.

Phase 4 – Étude de coût et faisabilité

Certaines options ont été éliminées en phase précédente. Les autres, après quelques aménagements, ont été retenues et font maintenant l'objet d'une étude d'évaluation. Elle se déroule classiquement en trois étapes :

1. la détermination des critères pour l'évaluation ;
2. le chiffrage des options selon les critères ;
3. les pondérations et choix d'options.

Enfin, une proposition de choix est réalisée pour la phase 5.

Critères d'évaluation

Ces critères doivent être appropriés au problème abordé. Concrètement, on aura souvent besoin d'évaluer les options sur les points suivants :

- **la facilité ou difficulté de mise en place** de l'option, en fonction des efforts de réalisation et des investissements demandés ;
- **la facilité ou difficulté d'activation** de l'option (une fois en place) – en effet, l'effort d'activation (au moment du sinistre ou au moment des tests) peut être important et dissuasif ;
- **le coût de la mise en place** (une fois, puis récurrent), en tenant compte des divers paramètres ;
- **le coût de l'activation** (là encore, pour une activation réelle ou lors des tests) ;
- **le niveau de qualité** permis par l'option – certaines options de type « mode dégradé » peuvent en effet être acceptables lors d'un sinistre pour certaines activités, mais pas pour d'autres ;
- **la sécurité** inhérente à l'option – l'option ne doit pas représenter une brèche béante en sécurité ; tout risque sur ce point doit être documenté afin de fixer les limites acceptables ;
- **la maîtrise ou le contrôle opérationnels** sur l'option – il est possible qu'une dépendance de tiers trop forte sur certaines applications sensibles soit inacceptable ;
- **la maîtrise technique** sur l'option – là encore, l'absence de compétences en interne ou la dépendance trop forte de compétences externes peuvent être considérées comme rédhibitoires.

Pour une bonne lisibilité et afin de faciliter la décision, on se fixera un nombre limité de critères (pas plus de cinq, par exemple).

Les différents responsables techniques de l'entreprise doivent être mis à contribution sur ces points, surtout lorsqu'il s'agit d'évaluer des options qui vont les impliquer ou les mettre en concurrence avec des prestataires extérieurs à l'entreprise.

Chiffrage des options

Une fois les critères définis, ils sont évalués pour chaque option retenue. Cela peut se faire par une note de 0 (mauvais) à 3 (très bon), comme l'illustre le tableau ci-après.

Tableau 3-18 : Évaluation des options sur des critères d'effort, de qualité, de maîtrise, de coûts et de sécurité

Matériels sur site de secours (0 = défavorable à 3 = très favorable)						
Catégorie	**Option**	**Effort**	**Qualité**	**Maîtrise**	**Coûts**	**Sécurité**
En toute propriété	Site distant	1	3	3	2	3
Accord avec un tiers	Accord de réciprocité avec confrère	2	2	1	3	1
Offre commerciale	Site dédié	3	3	2	1	3
Niveau de préparation	Site tiède	2	2	2	2	2
	Site chaud	3	3	2	1	3

Ce travail de chiffrage est à effectuer sur toutes les options qui ont été retenues jusque-là. Il peut être demandé à plusieurs personnes responsables dans des services différents et fera l'objet de discussions et d'itérations jusqu'à obtention d'une vision partagée. En général, ce chiffrage s'appuie sur des données factuelles et ne devrait pas provoquer trop de divergences de point de vue.

On peut ne pas discuter à ce stade de l'importance des différents critères. Cela permet de scinder l'approche en deux parties : une qui se concentre sur le choix des critères, et l'autre qui se focalise sur leur évaluation.

Sélection d'options

Les différents critères sont alors pondérés et les options les mieux notées retenues.

Considérons l'exemple précédent concernant le site de secours informatique :

- Dans l'hypothèse où seuls comptent l'effort et la sécurité (et donc pas le coût, ni la maîtrise, ni la qualité), alors le choix se portera sur les deux options suivantes :
  - Offre Commerciale / Site dédié
  - Niveau de préparation / Site chaud
- Si, en revanche, le coût et la maîtrise sont mis en avant, alors le choix se fera sur le site distant en toute propriété.

Toute pondération de l'ensemble des critères est bien évidemment possible et on obtient, à la fin de cette étape, une liste d'options retenues.

Phase 5 – Mise au point de la stratégie de continuité

Une réunion de validation peut être organisée pour avaliser les décisions ou pour les cibler d'avantage lorsque le nombre d'options ouvertes est élevé.

L'ensemble de la stratégie de continuité peut alors être documenté dans un rapport d'étude, qui peut se structurer comme suit :

Stratégie de continuité

1. Besoins de reprise
   - 1.1. Introduction, rappel du contexte BIA, cadrage
   - 1.2. Exigences des processus critiques
   - 1.3. Besoins pour la reprise
     - a. Segmentation (bureaux, locaux IT, données, autre)
     - b. Besoins en fonction de cette segmentation
     - c. Besoins communs
2. Options possibles
   - 2.1. Catégories d'options à étudier (internes, contractuelles, etc.)
   - 2.2. Options envisagées, en fonction de la segmentation
   - 2.3. Options éliminées et raisons de l'élimination
3. Confrontation aux exigences métier
   - 3.1. Délais d'activation
   - 3.2. Comparaison avec les besoins des métiers
   - 3.3. Options retenues avec argumentation
4. Étude de coût et faisabilité
   - 4.1. Critères retenus
   - 4.2. Chiffrage des options en fonction des critères
   - 4.3. Pondération et sélection des options
5. Compte rendu de la réunion de décision

L'ensemble de ces éléments, élaborés tout au long de l'étude décrite dans ce chapitre, est conservé dans un système documentaire. On pourra ainsi s'y reporter pour comprendre les décisions stratégiques qui ont été entérinées, en consultant le détail des attendus ou hypothèses qui ont conduit à ces décisions. Cela permet par ailleurs de vérifier si ces hypothèses sont encore valables ou non. Enfin, les auditeurs pourront facilement le consulter (voir le chapitre 14).

La réactualisation nécessaire de la stratégie

Cette étape importante qu'est l'élaboration d'une stratégie de continuité se heurte dans la réalité des entreprises à plusieurs écueils :

- Ce type d'approche a souvent été mené il y a cinq ou dix ans, et l'entreprise continue sur ses choix de l'époque, sans juger utile d'y revenir.
- La stratégie élaborée autrefois est victime de glissements successifs quasi imperceptibles : de nouveaux systèmes informatiques viennent remplacer les anciens et les questions concernant leur capacité de résistance au sinistre ne sont pas remises à l'ordre du jour.
- De nouveaux progiciels sont maintenant utilisés dans l'entreprise, sans que leur résilience fasse l'objet d'aucune considération dans les choix.

Bref, l'entreprise se trouve souvent dans une situation technique qui s'est complexifiée et qui n'a pas été envisagée dans la stratégie devenue progressivement obsolète.

> **Un choix de treize ans**
>
> La société APCL a souscrit, il y a treize ans, un contrat avec un prestataire pour disposer en région parisienne d'un centre de secours équipé d'un ordinateur de type mainframe. Ce contrat est toujours en vigueur et, chaque année, il est signé à nouveau à la suite d'une rencontre entre APCL et le prestataire.
>
> Lorsqu'à la suite d'un audit de PCA, un consultant externe vient visiter le centre informatique d'APCL, il constate avec stupeur qu'il y a dans ce centre plus de 450 serveurs de différents types... La stratégie de reprise de la société n'a pris en compte qu'un seul serveur sur les 450... celui qui était là il y a treize ans !
>
> Devant ce constat alarmant, APCL refait un BIA et conclut au fait que 45 serveurs au moins sont à reconsidérer dans sa stratégie et à inclure dans le contrat de secours.
>
> **Moralité** : BIA et stratégie sont à revoir régulièrement.

Il faut toujours réévaluer une stratégie ancienne et l'étalonner sur la réalité de l'entreprise. Pour cela, les points suivants sont à passer en revue :

- refaire la liste des applications critiques et des moyens sous-jacents en fonction des conclusions du BIA revu (voir le chapitre 2) ;
- étudier les moyens techniques sous-jacents à ces applications et les classer en catégories selon leur résilience ou les délais de reprise (du genre : immédiat, quatre heures, un jour, etc.) ;
- vérifier l'adéquation des deux : les caractéristiques des moyens techniques permettent-elles d'assurer la continuité requise ?
- détecter ainsi les écarts et élaborer des plans d'action pour les combler.

Ce n'est qu'au prix de ces vérifications très régulières que l'entreprise pourra avoir confiance en sa stratégie.

Chapitre 10

Le centre informatique

Avec les divers mouvements de consolidation des matériels informatiques de l'entreprise, le centre informatique se trouve dépositaire d'éléments très importants pour la disponibilité et la continuité des activités.

Le centre informatique lui-même possède une infrastructure particulière qu'il faut choisir et gérer avec soin afin de satisfaire aux objectifs de continuité de l'entreprise.

Choix du site

Idéalement au nombre de trois (primaire, secondaire et distant), les centres informatiques sont localisés sur deux sites : un premier site sur lequel sont organisés les centres primaire et secondaires en « duo » ou « campus » et un deuxième site à distance convenable, sur lequel on prévoit le centre de secours distant. On note actuellement une tendance à écarter un peu les centres primaire et secondaire (d'une trentaine de kilomètres quand on le peut) et à mettre le site distant à plus de 200 km des deux autres.

Cette dualité du premier site est un idéal que n'atteignent que les entreprises ayant un niveau d'exigence très élevé en matière de continuité d'activité. Les autres se contentent d'un site dit principal convenablement fiable selon leurs critères, doublé d'un site distant pour le secours.

Ce deuxième site à distance est considéré comme moins critique que le site principal. Toutefois, ce site distant est en réalité très souvent le site principal d'une autre branche de l'entreprise ou d'une autre société ; il est alors aussi critique que les autres. Le choix du site doit donc dans tous les cas de figure être effectué avec la plus grande attention, à base de critères raisonnés.

L'appréciation des risques présentée dans le chapitre 1 a donné une liste des principaux facteurs à prendre en compte, à laquelle on se reportera. Lors du choix d'un site pour y créer un centre informatique, il est ainsi possible de sélectionner un emplacement permettant de minimiser ces risques. L'approche est

tout de même délicate, car il faut trouver des compromis : un site idéalement situé, loin des tremblements de terre et des inondations, s'il est loin de toute ville agréable et de toute université risque fort de n'attirer aucun employé compétent ! Il faut donc graduer les exigences et peser le pour et le contre de critères potentiellement contradictoires.

Vulnérabilité du site

On se reportera sur ce point au chapitre 1. Néanmoins, lorsqu'il s'agit de choisir une nouvelle implantation, il est intéressant d'évaluer aussi la vulnérabilité des différentes solutions possibles.

Pour un désastre donné, la vulnérabilité d'un site se mesure en pertes financières, mais aussi et surtout en pertes humaines. Sur ce deuxième point, il faut considérer un certain nombre de facteurs, tels que :

- la densité de population dans la zone considérée ;
- la compréhension scientifique du risque ;
- le niveau d'éducation et de sensibilisation du public ;
- l'existence de systèmes d'avertissement, de communication, d'alerte ;
- la disponibilité ou non d'infrastructures de secours et leur degré de préparation ;
- le respect des règles de construction, les pratiques locales ;
- certains facteurs culturels déterminant la réaction du public.

Tous ces points peuvent en effet jouer sur les comportements et donc sur les conséquences du sinistre.

Attractivité du site

Le site envisagé doit attirer des collaborateurs (le site totalement vide étant une vue de l'esprit) et offrir un environnement propice aux activités. Ce sujet sort du thème de cet ouvrage, mais citons néanmoins :

- l'existence de collèges, de lycées, d'universités ou d'écoles d'ingénieurs à proximité ;
- la qualité de vie (voir par exemple les classements faits par certaines revues du genre « les villes où il fait bon vivre ») ;
- l'évolution des populations (en baisse ou en hausse) ;
- la facilité à se loger sur place (à l'hôtel ou en logement fixe) ;
- le droit du travail et la protection sociale (pour les sites à l'étranger) ;
- la connaissance ou non des caractéristiques des lieux (la notion de zone inondable, zone à risque, etc. existe-t-elle sur place ?) et leur suivi dans le temps.

La continuité d'activité est en effet aussi une affaire de compétence et de motivation du personnel.

Climat des affaires

Le site doit se trouver dans un environnement propice aux affaires. Cela concerne aussi bien la situation économique et politique, mais vu sous l'angle de la continuité d'activité, on observe les points suivants :

- la présence de compagnies d'assurance et d'offres de contrats convenables ;
- une fourniture de qualité pour l'électricité, la téléphonie, le réseau ;
- la proximité des points d'accès réseau, ou des points de présence pour la fibre optique à haut débit ;
- la facilité à acquérir un terrain plus vaste que le simple centre informatique ;
- le coût de l'immobilier pour le site et les collaborateurs ;
- la possibilité d'obtenir des offres de services de secours, d'hébergement informatique, de conseil, etc.

En particulier lorsque l'on a choisi l'étranger, ces points peuvent s'avérer déterminants pour la bonne mise en œuvre d'un plan de continuité.

Règles de précaution

À titre de précaution, certaines règles sont généralement admises et respectées pour le choix d'un site, quelle que soit la ville ou le pays :

- être situé à plus d'un kilomètre de toute voie ferrée, autoroute, voie de passage de cargos, usine classée à risque ou usine de traitement des eaux ;
- être situé à plus de cinq kilomètres de tout aéroport ;
- être assez éloigné d'émetteurs radio ou radars puissants (qui normalement n'acceptent rien à proximité) ;
- être à distance « suffisante » d'une centrale nucléaire (de l'ordre de 30 km, à apprécier selon les pays…) ;
- ne pas être trop éloigné d'un poste source électrique (moins de cinquante kilomètres), les défauts d'alimentation électrique étant souvent proportionnels à cette distance ;
- se tenir en dehors de toute zone inondable, loin de l'aval d'un barrage ;
- avoir accès facilement à l'eau potable et à de l'eau en général pour refroidir ou éteindre un incendie.

Bien évidemment, si ces règles sont valables lorsqu'on choisit le site, elles peuvent ne plus s'appliquer ultérieurement.

Il est souhaitable, dans la logique du plan de continuité, de déterminer les critères jugés valables par la direction, de leur accorder un certain poids, puis de les évaluer ou faire évaluer. Les notes obtenues permettent alors de départager les sites candidats.

Infrastructure du centre informatique

Le centre informatique accueille des éléments critiques tels que des serveurs, des réseaux, du stockage, etc. Il permet leur fonctionnement mais peut aussi provoquer des pannes diverses et variées dont certaines sont de mode commun (voir le chapitre 7) et donc préjudiciables à la continuité.

Éléments critiques

Les éléments du centre informatique pouvant connaître des pannes préjudiciables à la disponibilité sont nombreux : les contraintes en termes de fiabilité et de sécurité portant dessus sont à étudier soigneusement. On peut citer en particulier :

- la chaîne des alimentations électriques qui doivent être redondantes, protégées et que l'on doit pouvoir couper par sections ;
- les capacités à générer du courant électrique en cas de coupure (batteries, alternateurs, générateurs Diesel et cuves à fioul) doivent être dimensionnées correctement en puissance, qualité de courant et durée de production ;
- la climatisation doit être suffisamment fiable et adaptée aux calories à évacuer et sa maintenance ne doit pas nécessiter l'arrêt général ;
- les éventuels points chauds de la salle doivent être détectés et refroidis localement, la température des éléments sensibles (serveurs) surveillée ;
- les filtrations d'air doivent aussi maintenir le bon taux d'humidité ;
- les systèmes de sécurité d'accès et de surveillance vidéo doivent permettre la traçabilité des accès dans le respect des lois ;
- les systèmes de détection et de sécurité incendie peuvent éviter des dommages importants : leur bon état de fonctionnement doit être vérifié régulièrement ;
- les planchers et faux planchers doivent pouvoir supporter le poids des machines (qui évolue à la hausse) ;
- les canalisations d'eau doivent éviter toutes les zones où une fuite serait catastrophique ;
- les câbles électriques et de réseau SAN, IP, etc. doivent suivre des cheminements distincts ;
- les interventions de maintenance doivent pouvoir se faire en perturbant le moins possible l'ensemble ; dans certains cas, il faut prévoir des bipasses.

En résumé, un centre informatique est un ensemble de technologies diverses qui doit avoir fait l'objet d'une étude d'ingénierie de conception visant à une bonne disponibilité et à une réparabilité aisée.

Référentiels et normalisation

Durant les années 2000-2005, des travaux concourants ont abouti à un ensemble de bonnes pratiques pour la conception et l'aménagement des centres informa-

tiques. Des comités d'utilisateurs ou de normalisation se sont penchés sur le sujet, tels que le *Uptime Institute* aux États-Unis ou la *Telecommunications Industry Association* (TIA), auteur de la norme TIA 942.

Ces travaux ont classé le niveau de service d'un centre informatique en quatre catégories (*tiers* en anglais), du plus faible au plus élevé. Le tableau suivant présente quelques caractéristiques de ces quatre catégories ou classes.

Tableau 10-1 : Les quatre classes du centre informatique, selon le Uptime Institute

Classes	Caractéristiques principales
1	– alimentation électrique sur une voie – refroidissement sur une voie – nombreux points uniques de défaillance – pas de générateur électrique si autonomie électrique de huit minutes – vulnérable aux intempéries – indisponibilité inférieure à 28,8 heures par an
2	– alimentation électrique sur une voie – refroidissement sur une voie – quelques composants redondants – générateur de secours – supporte 24 heures de coupure de courant – quelques critères de choix de site – salle informatique formellement séparée – indisponibilité inférieure à 22 heures par an
3	– alimentation électrique et refroidissement sur plusieurs voies dont une seule active – alimentation et refroidissement redondants – fournisseurs de service doublés – supporte 72 heures de coupure de courant – critères élevés de choix de site – résistance au feu : 1 heure – permet la maintenance à chaud (concurrente) – indisponibilité inférieure à 1,6 heures par an
4	– alimentation électrique et refroidissement sur plusieurs voies actives – composants généralement redondants – tolérance aux pannes – supporte 96 heures de coupure de courant – critères très exigeants de choix de site – résistance au feu d'au moins 2 heures – sécurité physique de haut niveau – équipe de maintenance présente 24h/24 7j/7 – indisponibilité inférieure à 0,4 heure par an

Bien évidemment, un site donné peut se trouver en classe 3 sur un thème et en classe 1 sur un autre. C'est cependant le plus bas (donc 1) qui l'emporte car la

chaîne de disponibilité prend la valeur du maillon le plus faible. Dans la pratique, nombre de fournisseurs ne pouvant prétendre complètement à la classe 4 (car il leur manque certains éléments) mais estimant être meilleurs que la classe 3 qualifient leur centre informatique de « 3+ ».

Il existe certaines différences d'approche et de contenu entre le U*ptime* I*nstitute* et la TIA 942. Pour plus de détails, se référer aux documents cités en annexe 2.

Lorsque l'entreprise a recours à un prestataire externe pour son centre informatique, elle a tout intérêt à spécifier dans son cahier des charges des références aux « classes » définies par ces normes.

Les principaux risques et leur parade

Un centre informatique est exposé, comme tout bâtiment, aux risques habituels que sont l'incendie, l'inondation, la foudre, etc. Le fait qu'il héberge des éléments critiques pour l'activité de l'entreprise et détienne des informations sensibles en stockage exige une démarche orientée dans deux directions :

- un niveau de protection ou de prévention élevé ;
- une capacité réelle à limiter les conséquences.

Lorsqu'on conçoit un centre à partir de zéro, il est possible de jouer sur les deux tableaux, et en particulier sur la prévention. Lorsque le centre existe déjà, en revanche, les menaces sont déjà présentes et il faut alors en limiter les conséquences éventuelles.

Incendie

Le feu, dans un centre informatique ou ses annexes, peut avoir des conséquences graves, dont certaines sont difficiles à percevoir immédiatement.

Dégâts

Les dégâts d'un incendie sont directs et évidents : pertes de stocks et de documents, destruction de biens et de réserves diverses, dommages causés par l'eau nécessaire à l'extinction du feu, locaux devenus impropres à leur usage, etc.

Mais d'autres dommages atteignent le centre informatique de façon beaucoup plus pernicieuse :

- affaiblissement de certaines structures du bâtiment telles que des poutres ou des murs ;
- destruction de cloisons ou vitrages, rendant nulles les isolations de zones à risque ;
- dégâts peu visibles dans les faux planchers, les gaines surélevées de passage de câbles, les systèmes de climatisation… ;
- détérioration importante des isolants des câbles, devenus impropres à leur usage et risquant de provoquer des courts-circuits ;

- problèmes dus aux fumées et émanations toxiques.

En outre, les incendies peuvent avoir des effets indirects qui s'apparentent à des pannes de mode commun : ainsi, si une coupure générale de l'alimentation électrique est requise et que les générateurs Diesel sont interdits de fonctionnement, aucun serveur ne pourra fonctionner. Si, de plus, la connexion réseau vers l'extérieur du site est hors service, ces situations peuvent mettre en danger toute action de reprise sur un site voisin ou éloigné et réduire ainsi à néant toute stratégie de continuité.

Parades

Les parades à mettre en place sont de plusieurs natures. Les listes données ci-après ne prétendent pas être exhaustives mais sont particulièrement adaptées au contexte du centre informatique.

Prévenir

Des actions élémentaires de respect de certaines règles se révèlent très efficaces en termes de prévention :

- ne pas laisser dans une zone à risque des cartons d'emballage, du polystyrène et autre combustible – lorsqu'une machine est déballée, son emballage doit être sorti de la salle et mis en un lieu prévu à cet effet ;
- organiser le stockage des réserves de papier pour imprimantes de manière à ne pas fournir de combustible au feu ;
- respecter les recommandations des constructeurs pour les alimentations électriques des machines et les sections de câblage ;
- inspecter les câbles électriques, changer immédiatement tout câble dénudé, toute connexion noircie ou suspecte ;
- faire respecter les interdictions de fumer (le mégot mal éteint est une cause importante d'incendie) ;
- réglementer l'usage des chauffages électriques d'appoint, des machines à café et de tout autre appareil qui maintient une température élevée ;
- éliminer de la salle informatique et de ses abords tout ce qui peut constituer un combustible ;
- respecter et faire respecter la réglementation en vigueur ;
- faire visiter les locaux par les services incendies (un expert des pompiers, par exemple) pour obtenir un état des lieux et éventuellement connaître les risques du voisinage ;
- séparer les cheminements de câbles conducteurs de courant fort de ceux transmettant du courant faible ;
- passer une fois par an l'aspirateur dans le dessous des faux planchers ;
- inspecter les goulottes de câbles en nettoyant tout ce qui n'a pas à s'y trouver.

Réagir

Dès les premières flammes, il faut réagir. Certaines réactions permettent de réduire les dégâts, voire d'arrêter le feu avant qu'il y ait sinistre. Les actions suivantes peuvent contribuer à encourager les bons comportements :

- mettre en place des extincteurs appropriés aux différentes natures de feux possibles, les garder en bon état par une maintenance régulière et indiquer clairement leur emplacement ;
- former régulièrement le personnel au bon usage des extincteurs avec des exercices pratiques ;
- mettre en place les détecteurs appropriés capables de déclencher l'alarme ;
- concevoir un déclenchement d'alarme correct, capable d'entraîner des actions telles que :
  - fermer des portes coupe-feu,
  - activer des systèmes d'extinction,
  - prévenir les secours,
  - ouvrir les verrous électroniques de portes pour permettre les évacuations,
  - alerter le personnel d'évacuation,
  - éventuellement, arrêter des machines sensibles ;
- s'équiper en systèmes d'extinction qui conviennent à l'environnement d'une salle informatique (gaz neutre non mortel, conforme aux normes) ;
- déterminer les éléments sensibles en cas d'incendie (cassettes, bandes, documents) et prévoir un stockage approprié (coffre ignifugé, par exemple) ;
- poser des affiches et communiquer sur le comportement à adopter en cas d'incendie ;
- faire des exercices d'évacuation du centre ;
- tester les équipements.

Dans tous les cas, la méthode la plus efficace consiste à détecter le plus tôt possible l'incendie, en prévenant des personnes formées qui organisent les actions prévues, tout en ayant sensibilisé le reste des employés.

Dégât des eaux

Sous cette appellation générique, on trouve des sinistres d'importance variable susceptibles d'affecter le centre :

- inondations avec des conséquences pouvant aller jusqu'à rendre un centre totalement inutilisable ;
- pluies importantes avec des ruissellements, des infiltrations de toiture ou de façade provoquant des dommages au bâtiment, aux machines et aux stocks en générant des infiltrations ;
- infiltrations ou fuites provoquant des dégâts que l'on ne découvre pas forcément tout de suite, mais qui détériorent des sous-ensembles du centre ;

- condensations localisées qui rongent des conduites, abîment lentement des revêtements ou des plafonds, provoquent des courts circuits.

Conséquences

Les effets des dégâts des eaux sont directs et indirects, de même que les parades seront immédiates et différées.

- **Effets directs** : la présence de l'eau empêchant toute activité dans le centre, il faut réagir immédiatement en pompant l'eau et en la déversant en contrebas, si c'est possible, ou dans un bac étanche ;
- **Effets indirects** : une fois l'eau évacuée, le centre connaît des moisissures, des courts-circuits, etc. ; il faut assécher les murs, détruire et reconstruire des cloisons, ôter et reposer les tapisseries, les moquettes, le câblage électrique et téléphonique – cela peut prendre plusieurs semaines pendant lesquelles le centre est inutilisable.

Les effets des dégâts des eaux peuvent aller bien au-delà de ce qu'on imagine en première analyse et il n'est pas rare de découvrir, une fois les eaux évacuées, des pannes diverses sur des systèmes qui ont été endommagés par un séjour dans l'eau ou par un simple degré d'humidité trop élevé.

Précautions à prendre

Lorsqu'on peut décider de l'implantation d'un centre, les précautions déjà mentionnées plus haut consistant à éviter toute zone inondable s'imposent. Pour tous les autres cas, il est intéressant d'envisager les solutions suivantes pour la prévention et la réaction en cas de sinistre :

- prévoir des bassins d'expansion situés plus haut que le centre et se fournir en pompes de relevage d'un bon débit ;
- drainer les alentours du centre et en améliorer l'étanchéité ;
- surélever la partie la plus sensible du centre ;
- ne pas faire passer de canalisations d'eau au-dessus d'éléments sensibles ;
- si le centre possède un système de refroidissement à eau, en prévoir la circulation en niveau bas ;
- prévoir des systèmes anti-fuite ou de coupure en cas de fuite sur les canalisations ;
- prévoir des bipasses et des pièges à froid pour pouvoir changer les vannes défectueuses ou certaines pompes sans avoir à tout interrompre ;
- pour tout système (climatiseur, canalisation froide) qui risque l'humidité ou la condensation, prévoir une récupération de l'eau ainsi produite par bac ou lèchefrite ;
- laisser les canalisations apparentes et accessibles de manière à ce qu'on puisse les inspecter facilement.

Par ailleurs, il est important de tenir compte du fait que l'inondation mène la plupart du temps à une coupure électrique. Il est donc judicieux d'avoir conçu le

centre de manière à ce que les systèmes les plus sensibles soient mis hors d'atteinte de l'eau avec une alimentation par batteries et/ou générateur Diesel, eux-mêmes hors d'eau.

Dysfonctionnements électriques

L'alimentation électrique est indispensable pour tous les moyens informatiques du centre. Ses défauts sont ainsi fortement préjudiciables au bon fonctionnement des machines.

Défauts courants

Parmi les défauts courants de l'alimentation électrique, on peut noter :

- les variations de tension, les microcoupures ;
- les parasites ou courants induits (par les ballasts de tubes fluorescents, par exemple) ;
- des perturbations diverses en fréquence ou des défauts dus à des onduleurs de qualité médiocre ;
- les problèmes de références de potentiels multiples et d'électricité statique ;
- la foudre qui génère des courants pouvant avoir des conséquences destructrices à distance.

Les divers équipements réagissent de manière variable à ces défauts. Certains équipements industriels vont d'ailleurs eux-mêmes en générer. Si le centre est voisin d'une usine équipée de machines électriques (gros moteurs électriques, appareils de soudure électrique), il faudra être particulièrement vigilant.

Précautions à prendre

Parmi les précautions utiles à prendre, citons les actions suivantes :

- séparer les matériels sensibles comme les serveurs ou les routeurs de réseau des matériels perturbateurs (moteurs électriques, par exemple) ;
- prévoir des transformateurs ayant la puissance nécessaire ;
- généraliser la mise au neutre ;
- choisir des câbles de qualité et s'assurer que leur pose a été effectuée correctement ;
- prévoir des cheminements de câbles évitant les perturbations émises ;
- séparer le passage des alimentations nominales et de l'alimentation de secours (précaution générale contre les pannes de mode commun) ;
- vérifier régulièrement les connexions.

Moyens techniques

Pour améliorer la qualité du courant apporté en salle informatique, il est possible de recourir à des dispositifs tels que des onduleurs ou des moteurs électriques à volant d'inertie doublés de batteries. En général, ces moyens permettent

d'atténuer les défauts du courant d'origine publique et de pallier certaines coupures de courte durée (dix minutes).

Pour des coupures de plus longue durée, il faut avoir les moyens de générer soi-même du courant, via des générateurs Diesel ou à gaz. Les onduleurs à batterie doivent assurer le relais jusqu'à ce que ceux-ci entrent en action.

Quant à la foudre, elle nécessite une protection technique par paratonnerre en particulier. On utilise aussi les parafoudres pour protéger l'installation électrique et les lignes de transmission de données, la fibre optique étant à préférer dans ce cas.

Enfin, l'électricité statique peut se révéler dangereuse dans le cas des opérateurs intervenant sur les serveurs et touchant des éléments sensibles (cartes mères, processeurs) qui peuvent se trouver gravement endommagés. Il faut régler correctement l'hygrométrie de la salle, poser des revêtements antistatiques au sol et porter des vêtements en textiles ne produisant pas d'électricité.

Pour tous ces moyens techniques concourant à la bonne disponibilité du centre, il faut prévoir une surveillance correcte et un contrat de maintenance permettant la remise en route rapide, incluant des pièces de rechange si nécessaire.

Autres risques

Enfin, un centre informatique est exposé à d'autres risques encore que ceux qui ont été étudiés précédemment.

Défaut de climatisation

La climatisation peut tomber en panne, que ce soit en raison d'une coupure électrique (déjà mentionnée) ou pour des raisons plus particulières, telles que :

- des fuites de liquide réfrigérant ;
- des pannes de ventilateurs ou d'aéro-réfrigérant externe ;
- l'exposition à un rayonnement solaire direct trop élevé.

Dans tous les cas, la température monte et atteint des zones impropres au bon fonctionnement des machines, serveurs, stockage, etc. Les mesures préventives consistent alors à prévoir des redondances des systèmes de climatisation (de type n+1), à doubler les alimentations et à surveiller et maintenir ces systèmes.

En cas de défaillance totale, l'arrêt des machines sensibles ou responsables des plus gros dégagements de chaleur est à prévoir rapidement.

Il existe aussi un risque plus récent d'insuffisance chronique de refroidissement dans certains endroits de la salle informatique où sont concentrés certains serveurs qui dégagent plus de calories que la moyenne. La parade face à ce problème consiste alors à :

- ne pas remplir complètement les racks de machines ;
- disperser dans la salle les machines ou groupes de machines de ce type ;
- prévoir des compléments ponctuels de refroidissement aux points chauds.

Ces technologies, qui concentrent la puissance informatique et donc par la même occasion le dégagement calorifique, peuvent amener à repenser la conception de l'ensemble de la climatisation de la salle ou à aménager une salle particulière.

Ainsi, certains centres prévoient des salles spécifiques pour les hautes densités (mesurées en kVA/m² – kilo-Volt-Ampère par mètre carré), qui permettent d'aller au-delà de 5 kVA/m² par exemple. L'écoulement de l'air frais produit par la climatisation est contraint dans des allées dites « froides », afin d'évacuer les calories de manière plus efficace. Ce type de salles va se multiplier avec la généralisation des serveurs lames.

Intrusions de personnel

L'entrée dans le centre ne doit être réservée qu'au personnel habilité. Il existe en effet différents risques :

- vols de matériel, de sauvegardes ;
- mise sur écoute, pose de bretelles télécom ;
- vandalisme, destructions diverses.

Une protection efficace sera apportée par :

- des mécanismes de contrôle d'accès simples (gardien) ou sophistiqués (identification et authentification par carte, etc.) ;
- la traçabilité des personnes entrant sur le site (nom, prénom, jour, heure, personne visitée) ;
- la difficulté d'accès dans le centre (portes verrouillées, absence de baies vitrées) ;
- une vidéosurveillance des alentours du site ;
- la mise sous protection des éléments sensibles comme les tableaux électriques, les moyens de coupure divers ou les répartiteurs télécom, qui ne doivent pas être accessibles au premier venu ;
- une procédure de contrôle à la sortie des employés emportant du matériel ou des sacs pouvant en contenir.

Pollutions diverses

Normalement, ces aspects ont dû être pris en compte dans le choix du site sur lequel le centre est installé. Cependant, pour les centres situés dans des zones industrielles ou à proximité d'un site industriel, il existe certains risques liés à la pollution :

- émanation de gaz dangereux pour le personnel ou le matériel ;
- poussières de diverses natures ;
- eau impropre à son usage.

Toutes ces atteintes toxiques peuvent se traduire par des problèmes de santé, des dysfonctionnements de matériel, des risques de courts-circuits ou d'incendie, des déclenchements d'alarme intempestifs, etc.

La parade pourra être apportée par :

- des filtrations adaptées ;
- des portes coupe-feu ;
- des clapets dans les gaines de circulation d'air ;
- des zones en légère surpression ;
- une protection des réserves d'eau.

Les nouveaux centres : le cloud computing

Depuis peu se sont développés de nouveaux centres informatiques à base de technologies récentes et particulièrement destinés aux offres de « *cloud computing* ». Ces centres sont souvent exploités par des sociétés qui n'avaient pas pour vocation à l'origine d'offrir des services sur ce marché ; on peut citer ainsi un libraire en ligne (Amazon), un moteur de recherche (Google) ou encore un éditeur de logiciels qui offre ainsi ses produits « en ligne », Microsoft.

Voici les principales caractéristiques de ces centres en termes de matériel, de fonctionnement et d'utilisation.

Matériel

- L*e grand nombre de serveurs utilisés* : 40 000 serveurs, voire davantage, sont des chiffres souvent cités ; la recherche d'économies d'échelle est effectivement un point clé.
- L*a banalisation* : tous ces serveurs sont assez simples et quasi tous au standard de l'industrie dit x-86 (Intel en majorité ou AMD avec Windows et Linux).
- L'*interchangeabilité des matériels* : si un serveur est défaillant, il est assez aisé de le remplacer par un autre dans un temps court.

Fonctionnement

Concernant le fonctionnement de ces centres, on notera :

- le fait que les traitements se font sans conservation d'état (s'il y a une panne, on perd ce qu'on était en train de faire) ;
- le fait que le stockage des données a lieu avec conservation d'état (en cas de panne, on retrouvera des données assez récentes) ;
- la gestion « par paquets » de ces serveurs : pour ajouter de la puissance, on ajoute un lot de 200 serveurs complets, par exemple ;
- la densité assez forte des alimentations électriques, même si elle n'est pas dans les plus hautes valeurs pratiquées : il faut que le tout reste facile à réfrigérer avec des technologies courantes et banalisées.

Architectures

En termes de continuité d'activité, ce type de centre s'appuie essentiellement sur des architectures de secours de type n+1 (voir chapitre 7).

Utilisation

- L'utilisateur se connecte à ces serveurs à partir d'un site web d'accueil du prestataire : l'utilisateur configure ce qu'il souhaite à partir de cases à cocher.
- L'utilisateur peut choisir une configuration donnée sur une période courte (une heure, deux jours…) et paye à proportion.
- L'utilisateur choisit (en cochant) un niveau de disponibilité plus ou moins élevé ; cela a des impacts en terme d'architecture et de choix, par exemple, de serveurs couplés sur deux sites différents.

Perspectives

Il est intéressant de noter que ce type de site peut fort bien entrer dans une stratégie de continuité (voir chapitre 3) et permettre à une entreprise de trouver des moyens de secours activables aisément et à bon compte. Il faut pour cela que ses applications s'y prêtent, ce qui est loin d'être le cas général actuellement.

Par ailleurs, les fournisseurs d'offres en *cloud* qui s'appuient sur ces centres ont développé des outils qui permettent aux utilisateurs « d'aller se servir en puissance informatique » dans ces centres. Ces outils peuvent présenter des bogues et provoquer des pannes dites de mode commun (voir chapitre 7). Néanmoins, les taux de disponibilité annoncés sont de l'ordre de 99,95 %, ce qui est crédible avec deux sites couplés et tout à fait correct dans bien des usages.

Les experts considèrent que ces centres concentreront une portion de plus en plus importante de la puissance informatique mondiale.

On peut estimer aussi que les centres informatiques traditionnels (internes à l'entreprise) seront amenés à se concentrer sur des machines et des traitements non banalisés et souvent au cœur de l'activité de l'entreprise. L'entreprise aurait alors recours à ses propres centres pour son cœur de métier et au *cloud computing* pour tout le reste, le service informatique se transformant de plus en plus en intégrateur de services.