LES DOSSIERS TECHNIQUES

AIDE A LA CONCEPTION D'UN CENTRE INFORMATIQUE SECURISE

De l'avant projet à la mise en service

Août 1996

Commission Techniques de Sécurité Physique

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30, Rue Pierre Sémard – 75009 Paris
Mail : clusif@clusif.asso.fr Web : http://www.clusif.asso.fr

REMERCIEMENTS

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

ALBINHAC Alain	
ALLOUËT Jean-Marc	
AUZAT Jacques	**G.I.E.. COMMERCIAL UNION FRANCE**
BEAUMARD Alain	**CNPP (Centre National de Prévention et de Protection**
BERGERON Robert	**CAP GEMINI**
BLANC-GARIN Jacques	**BG CONSULTANT**
DE CADEVILLE Anne	**C.N.A.M.T.S.**
GUERIN Claude	**COMPAGNIE GENERALE DE GEOPHYSIQUE**
LANGUEDOC Charles	
MATHE Joël	**APAVE OUEST**
NICOU Pierre	**3M FRANCE**
PELTIER Noëlle	
REFFRAY Alain	**EXPLOITIQUE**
WEISS Christophe	**APL FRANCE**

TABLE DES MATIERES

0. PREAMBULE

Les progrès continus de la technologie ont, en quelques années, modifié le paysage du monde informatique ainsi que le comportement des utilisateurs en regard de la sécurité du système d'information. Cette double évolution a marqué l'architecture des centres informatiques.

Les premières salles abritant les ordinateurs des années 60, pesant cinq tonnes et dont la seule UC occupait cinq pièces, n'ont rien de comparable avec les sites informatiques actuels plus petits et plus fonctionnels, construits à partir de critères et contraintes spécifiques locales.

Les années 70 ont été l'occasion pour les entreprises informatisées de développer les "Centres Vitrines" où l'informatique était considérée comme facteur de puissance et de prestige.

La prise de conscience dans la fin des années 80 des risques liés aux nouvelles technologies et aux nouvelles formes de criminalité (sabotage, fraudes, etc.) a favorisé l'émergence de "centres Blockhaus".

Les années 90 sont marquées par le souci pour les concepteurs d'intégrer les différentes architectures informatiques (sites centraux, micro-ordinateurs, informatiques personnelles, réseaux locaux, etc.). La spectaculaire percée d'architectures décentralisées de type client-serveur à base de serveurs, micro-ordinateurs, réseaux locaux d'entreprise font réapparaître des contraintes de sécurité physique dont nous étions en train de nous affranchir dans les systèmes centralisés.

Ces architectures provoquent trop fréquemment la répartition physique du système d'information dans des locaux plus ou moins sécurisés.

L'administration en est assurée par des utilisateurs dont ce n'est pas péjoratif de dire qu'ils ne sont pas toujours sensibilisés au vécu de la sécurité physique d'un système informatique.

Le niveau de protection doit être fonction des risques encourus par les entreprises et plus particulièrement de son environnement considéré a priori comme hostile (les différentes menaces liées à l'air, aux énergies, au feu, à l'eau, etc.).

Si, d'une manière générale, la sécurité des centres informatiques est mieux appréhendée dans les grandes entreprises que dans les Petites et Moyennes Entreprises, en raison de l'existence de structure "ad hoc", le problème majeur des entreprises est la difficulté d'aborder d'une manière globale la conception d'un centre informatique sécurisé, et ce dans une démarche participative associant l'ensemble des acteurs et experts.

1. INTRODUCTION

1.1 Objet du document

Ce document est destiné à aider le responsable (informaticien ou non) de la réalisation ou de l'aménagement d'un centre informatique sécurisé. Celui-ci, s'il n'a pas d'expérience dans ce domaine, est généralement démuni lorsqu'il doit faire construire ou aménager un nouveau centre.

Il doit permettre à ce responsable de se poser les bonnes questions (aspect didactique), de se focaliser sur les sujets essentiels et de les traiter dans le bon ordre (aspect méthodologique).

1.2 Domaines couverts

Ce document concerne principalement les aspects spécifiques de la réalisation ou de l'aménagement d'un nouveau centre informatique. Il ne peut prétendre se substituer au maître d'ouvrage et encore moins au maître d'œuvre. Il sert de guide didactique et méthodologique à l'informaticien responsable de la mise en place d'un nouveau centre informatique.

Ce document ne traite que l'aspect sécurité concernant la réalisation et l'installation d'un nouveau centre informatique, par opposition à la description de modes constructifs (calculs de dimensionnement, règles architecturales, etc.). C'est pour cela qu'il évoque aussi les conditions de sécurité dans lesquelles l'étude, la réalisation, l'installation et l'emménagement du centre devront être effectués.

1.3 Principes

Les principes de base qui ont guidé la réalisation de ce document sont :

- Son aspect didactique primordial,
- Son aspect méthodologique simple et pragmatique,
- Son utilisation par des non-spécialistes du domaine,
- Sa limitation à l'aspect sécurité,
- Sa complémentarité avec une analyse préalable de risques.

1.4 Concepts et Terminologie

Les concepts essentiels avec leur terminologie correspondante sont exposés succinctement afin que tous les lecteurs experts ou non aient les mêmes bases et le même langage avant de se plonger dans le corps du document.

➔ PROCEDURE : Manière spécifiée d'accomplir une activité.

➔ INSTRUCTION : Disposition formulant une action à mener.

➔ CONSIGNE : Application à des circonstances données d'une ou plusieurs instructions.

➔ PREVENTION : Ce qui permet de limiter la potentialité de sinistres concernant le fonctionnement de l'informatique.

➔ PROTECTION : Ce qui permet de limiter l'impact de sinistres concernant le fonctionnement de l'informatique.

➔ MAITRE D'OUVRAGE : Propriétaire juridique de l'ouvrage. De fait, plus généralement regroupé dans le vocable maîtrise d'ouvrage qui englobe les fonctions nécessaires à la définition des besoins, au financement de l'opération, au suivi de la réalisation, à la prise de possession de l'ouvrage, à l'exploitation du bâtiment.

➔ MAITRISE D'OEUVRE : Concepteur de l'ouvrage, il est en charge du contrôle de l'exécution. Le vocable Maîtrise d'œuvre sous-entend différentes fonctions : conception générale, conception architecturale, conception technique ou des structures, conduite d'opération générale, conduite partielle, gros oeuvre, second oeuvre, techniques. Le ou les maîtres d'œuvre ont toujours une responsabilité évidemment sur la finalité et la qualité de l'ouvrage

➔ CAHIER DES CHARGES : Ensemble des documents rédigés par le maître d'œuvre définissant la nature des travaux à exécuter par les intervenants individuels concourant au projet global.

➔ PROGRAMME : Ensemble de documents rédigés par le maître d'ouvrage exprimant les besoins et les contraintes à respecter. Ce document permet l'appel à Maître d'œuvre, et/ou Maître d'ouvrage pour son choix et de sa désignation.

2. PROJET ET ACTEURS

2.1 Facteurs déclenchants

La décision de se lancer dans un nouveau projet de construction d'un centre informatique peut avoir de nombreuses origines :

- Plan directeur informatique dégageant la nécessité de procéder à de nombreuses améliorations du système.
- Résultats d'un audit destiné à évaluer les performances du centre ou son niveau de sécurité.
- Nouvelle stratégie de l'entreprise.
- Fusion d'entreprises ou restructuration (y compris regroupement de Centres Informatiques).
- Changement ou évolution (technologie, taille, etc.) du système informatique.
- Contraintes externes (fin du bail, voisinage agressif, plaignant, etc.).
- Facteurs économiques (prix du m^2, opération immobilière, etc.).
- Gestion des ressources humaines et/ou Conditions de travail inadaptées.
- Sinistre important.
- Etc.

2.2 Orientation du Projet

Différentes options peuvent interférer sur le déroulement du projet :

- Le (ou les) facteur(s) déclenchant(s) va (vont) induire différents scénarios : modification du centre existant, extension du centre existant, déménagement vers un autre centre déjà aménagé ou à aménager, création d'un nouveau centre dans un immeuble existant ou encore création d'un centre de toutes pièces,
- En second lieu, et dans l'hypothèse où l'on ne se maintient pas sur le site existant, il est important d'arrêter l'option de la propriété pleine et entière ou celui de la copropriété (hébergement dans un site ou un immeuble existant) ou encore celui de la simple location. Dans cette dernière option, la liberté de manœuvre sera réduite,
- Il faudra enfin décider de faire appel ou non à des collaborations externes (voir liste au chapitre suivant). Dans l'hypothèse où ces collaborations seraient retenues, il conviendra d'en arrêter le degré d'implication. Il faut également se souvenir que l'efficacité de ces collaborations sera d'autant plus grande qu'elles interviendront tôt dans le processus d'élaboration du projet.

2.3 Différents acteurs

2.3.1 Acteurs de l'entreprise

Lors d'un projet d'une telle envergure, la plupart des fonctions de l'entreprise sont impliquées. Cependant on peut retenir les plus importantes, celles qui seront associées au déroulement de la totalité du projet et qui constitueront la base du comité de suivi du projet :

La Direction Générale.

Elle prend la décision et effectue les inévitables arbitrages entre les autres fonctions de l'entreprise. Elle représente souvent également les fonctions juridiques, économiques et financières de l'entreprise. C'est le pouvoir de décision et, par définition, le *maître d'ouvrage*.

Cette maîtrise d'ouvrage sera la plupart du temps déléguée soit à un cadre de l'entreprise sur des projets de taille ou de complexité réduite, soit à une société externe sur des projets d'envergure. Ce *maître d'ouvrage délégué* aura en échange le pilotage du comité de suivi de projet qui constitue, de fait, la véritable équipe de maîtrise d'ouvrage.

La Fonction Informatique.

Cette fonction a un rôle capital puisqu'elle doit produire le *cahier des charges*.

A ce titre, elle doit prendre en compte tous les problèmes d'interfaces entre la fonction informatique et les différentes fonctions utilisatrices. Cet aspect revêt une acuité toute particulière si le site informatique se sépare physiquement du reste de l'entreprise.

Dans le cas de projets de type "ré-aménagement" (par opposition à des projets de grande envergure), et en l'absence de fonction immobilière (Cf. plus loin), c'est fréquemment le Responsable de la Fonction Informatique qui est amené à assumer la fonction de maître d'ouvrage délégué.

La Fonction Organisation.

Lorsque cette fonction existe, c'est elle qui devra se préoccuper des conséquences physiques et organisationnelles de la distribution de l'informatique dans l'ensemble de l'entreprise. Cette fonction interviendra régulièrement dans la résolution des problèmes d'interfaçage entre la fonction Informatique et les différents utilisateurs. En l'absence de Fonction Organisation, c'est souvent à la Fonction Informatique qu'il incombera de spécifier ces aspects.

La Fonction Immobilière.

Lorsque cette fonction existe, c'est à elle que revient logiquement la délégation de maîtrise d'ouvrage dans la mesure où elle aura ensuite en charge la gestion de l'immeuble. Elle sera également associée en amont au choix des options propriété/copropriété etc. (voir § 2.2 ci-dessus). Il conviendra cependant de prendre garde au caractère spécifique de cette construction et de ne pas sous-estimer les spécificités de l'informatique.

La Fonction Sécurité.

Son rôle est évident quand il s'agit de la construction d'un centre sécurisé.

Les Partenaires sociaux (CE, CHSCT). Les meilleures chances de ne pas nourrir un conflit résident dans leur implication, très tôt, dans le projet. Par exemple, si ce dernier implique un déménagement, il faut prendre en compte rapidement les aspects sociaux : transport, restauration,

etc. De même, les partenaires sociaux doivent être associés à la détermination de nouvelles conditions de travail éventuellement imposées par des contraintes de sécurité plus draconiennes.

D'une façon plus générale, l'élaboration d'un tel projet doit s'appuyer sur un groupe de quelques personnes motivées, ouvertes au dialogue, et qui acceptent la remise en cause de positions pourtant jusque-là considérées comme inébranlables. Cela est d'autant plus important que l'entreprise pourra être amenée à faire appel à des conseils externes dont le rôle principal est d'apporter une vision nouvelle des problèmes.

2.3.2 Acteurs externes

Le nombre de ces acteurs dépend de la stratégie de l'entreprise. Certains sont cependant incontournables. La liste ci-après n'est pas exhaustive. Des circonstances particulières peuvent en effet conduire à faire appel à des partenaires très spécialisés. Les plus rencontrés sont les suivants :

- Promoteur, Aménageur ou Propriétaire,
- Investisseurs -,
- Maîtrise d'ouvrage déléguée (éventuellement),
- Bureaux de contrôle,
- Cabinet de Coordination Sécurité Chantier,
- Cabinet(s) de conseil,
- Architecte,
- Maîtrise d'oeuvre,
- Bureaux d'études,
- Assureurs,
- Interlocuteurs liés à l'environnement réglementaire (Permis de construire, Installations classées, Pompiers, etc.);
- France Télécom, EDF, La Poste, etc,
- Constructeurs (entreprise générale, ensemblier, etc.),
- Fournisseurs de matériels informatiques et d'équipements techniques,
- Fournisseurs du câblage.

3. MISSIONS, BESOINS ET ENJEUX DU CENTRE

Avant d'entamer l'ensemble des tâches de réalisation ou de (ré) aménagement du centre, il y a lieu de procéder à un certain nombre de réflexions préliminaires quant à ses missions futures et aux contraintes auxquelles il sera soumis.

3.1 Principales étapes préliminaires

3.1.1 Diagnostic de l'organisation existante

Lorsqu'on réalise un nouveau centre informatique, et quel que soit le facteur qui a déclenché la prise de décision, on doit finalement optimiser le fonctionnement du centre. En préalable à l'écriture du dossier d'expression des besoins, il est donc important de pratiquer un diagnostic de la situation existante (à moins qu'une étude ne soit déjà disponible).

Ce diagnostic doit mettre en évidence, pour chacune des activités informatiques, les éventuelles anomalies ou insuffisances actuelles de fonctionnement ou d'organisation (par exemple sur le plan de l'efficacité, du coût, de la qualité), les remèdes que l'on peut y apporter à l'occasion de la prise en charge du nouveau centre, et les dispositions concrètes à mettre en oeuvre. Cette analyse doit concerner :

- Les Etudes et le Développement, la Maintenance des applications.
- L'exploitation.
- Les activités diverses informatiques ou para informatiques.

3.1.2 Analyse des flux

L'analyse préalable des flux doit ensuite permettre d'étayer ultérieurement l'organisation physique du centre. Cette analyse doit porter sur **les flux physiques** :

- Circulation des documents de saisie (bordereaux, etc.).
- Lieu de stockage et de consommation des fournitures.
- Circulation des documents édités (listings, mailings, etc.).
- Etc.

Elle doit également porter sur **les flux logiques** :

- Communication entre les éléments du système,
- Communication avec d'autres systèmes du site,
- Communication avec l'extérieur du site,
- Etc.

Enfin, elle doit porter sur **les flux humains** :

- Accès et circulation des différentes catégories de personnel du centre.
- Fonctions nécessitant l'accès de personnels extérieurs au centre.
- Idem pour les personnels extérieurs à l'entreprise.

- Etc.

Cette analyse des flux est importante, notamment sur le plan de la productivité (limitation de la complexité) et de la sécurité (par exemple, vérification de la capacité à fiabiliser et sécuriser les chemins majoritaires, recherche d'un cloisonnement "stratifié" ou "concentrique", etc.).

3.1.3 Attribution des rôles

Il est indispensable, pour le bon déroulement du projet, de préciser les rôles, attributions et responsabilités des différents acteurs : qui est responsable de quoi ? Qui est l'interlocuteur de qui ? Qui assiste aux différentes réunions ? Comment la communication sera organisée entre les différents acteurs ?

Simultanément, dans le cadre de la construction d'un centre sécurisé, on peut également recommander instamment la mise en pratique, par les différents acteurs des concepts d'Assurance Qualité. La construction d'immeuble s'accompagne de plus en plus souvent de la mise en place de plan d'Assurance Qualité par les différents intervenants.

3.1.4 Analyse des besoins futurs en ressources humaines

Le dossier d'expression des besoins mettra probablement en exergue des besoins jusque-là insatisfaits. Il sera nécessaire de s'assurer que les compétences existent. Si ce n'est pas le cas, il conviendra de prévoir des recrutements ou des formations. Ces opérations devront être entreprises suffisamment tôt pour que les compétences soient disponibles au moment de la prise en charge du centre.

Ceci concerne les aspects informatiques (mise en place de procédures ou de logiciels de sécurité) mais également les aspects relatifs aux installations techniques elles-mêmes, dont la surveillance et/ou la maintenance devront éventuellement être assurées par du personnel de l'entreprise.

Les points précédents étant établis, on peut commencer à rédiger ce que les Informaticiens appelleraient le "Cahier des Charges"(1) du centre à construire ou à (ré) aménager.

Ce travail est l'apanage direct et exclusif du responsable informatique, et il représente sa contribution essentielle au succès du projet; en effet, personne ne peut (et ne doit) se substituer à lui pour fournir les réponses aux questions soulevées, puisqu'elles relèvent spécifiquement de son métier, et tout travail approximatif à ce niveau aura des conséquences majeures sur la viabilité de la réalisation complète. Il est d'ailleurs du devoir d'un responsable informatique de s'étonner ouvertement et avec insistance, (si par hasard ou par négligence de mandarinats) on ne vient pas lui poser de telles questions ! On peut identifier trois grandes parties, détaillées dans les pages suivantes:

- La définition des fonctions du centre, et des contraintes auxquelles il sera soumis.
- Les besoins techniques et humains qu'il devra satisfaire.
- Les objectifs de Qualité et de Sécurité qui lui seront fixés.

(1) Le terme "Cahier des Charges" est en effet compris autrement par les métiers du bâtiment (Cf. Définitions au § 1.4), ce qui permet une occasion de plus de quiproquo ... Dans la mesure du possible, on parlera donc plutôt de "Dossier d'Expression des Besoins".

3.2 Fonctions, Évolutions et Perspectives

3.2.1 Destination du centre

La première tâche consiste à définir clairement quelle est la destination finale du centre; en effet, les implications au niveau sécurité (fonction des enjeux) et évolutivité notamment seront très différentes selon le cas. Sa mission peut par exemple d'être :

- Un centre principal ou complet, ou centre secondaire.
- Un centre de secours ou miroir.
- Un centre de production répartie, ou à spécialisation fonctionnelle.
- Un centre automatique ou télé-piloté.
- Etc.

3.2.2 Fonction du centre

Il faut ensuite spécifier quelles seront les missions fonctionnelles précises de ce centre :

- Traitement d'informatique collective, et/ou
- Hébergement de serveurs, et/ou
- Impression / façonnage, et/ou
- Avec ou sans noeud et frontaux de télécommunications, et/ou
- Avec ou sans hébergement de services études / développement, et/ou
- Avec ou sans cohabitation avec d'autres services (locaux administratifs, production...).

3.2.3 Possibilité d'extension et d'adaptation

Il sera nécessaire de réfléchir aux évolutions les plus probables du centre :

- Est-il prévu une montée en puissance en plusieurs phases ?
- Quelles sont les évolutions prévues sur le plan fonctionnel (extension de personnel, missions) ?
- Quelles sont les évolutions prévues sur le plan organisationnel (effectifs de personnel, encombrement et autres contraintes liées aux matériels) ?

3.2.4 Contraintes géographiques

Il faut également identifier les caractéristiques du (ou des) site(s) géographique(s) sur lequel (ou lesquels) il est possible (ou obligatoire) de situer le centre, et en tirer les conclusions correspondantes sur le plan de la sécurité :

- Risques naturels (inondations, mouvement de terrain, zones orageuses ...),
- Risques de voisinage (pollutions, contaminations, extension de mouvements sociaux etc.).

La notion de site dédié ou partagé, et la notion de propriété des locaux auront également un impact quant au programme Sécurité du centre (circulation fréquente de personnels n'appartenant pas au centre, degré de liberté dans le choix des dispositions constructives, ...).

3.3 Besoins Généraux

Le site d'implantation du centre étant réputé choisi, on peut enfin procéder au recensement des exigences fonctionnelles :

3.3.1 Nomenclature des locaux

On détermine tout d'abord, en fonction des missions du centre définies plus haut, la nomenclature des zones fonctionnelles qu'il doit comporter :

- Salle(s) machines,
- Salle(s) pupitreurs (avec ou sans unités de sauvegarde),
- Bandothèque,
- Bureau préparation et local supervision,
- Salle transmissions de données,
- Salle télécommunications vocales,
- Salle imprimantes/façonnage,
- Local stocks consommables,
- Atelier (maintenance sur site des PC et petits matériels, pièces de rechange,...),
- Local alimentation EDF ou Tableau Général Basse Tension (TGBT),
- Local technique onduleur / groupe ou batteries,
- Local technique climatisation et/ou aérothermes,
- Tête de ligne de télécommunication,
- Bureau pour les équipes de développement,
- Sanitaires en zone à accès contrôlé,
- Etc.

3.3.2 Contraintes techniques

On procède ensuite à l'inventaire de tous les matériels informatiques devant, à terme, être hébergés par le centre; pour chacun d'eux, on identifiera (au moins) les paramètres suivants :

- Encombrement et poids des matériels informatiques et des stocks,
- Distances maxi et mini entre composants du système informatique,
- Types de tensions et fréquences des configurations : (230V/400V-50Hz-208V/440Hz - 208V/60Hz)
- Régime de neutre / mise à la terre,
- Types de refroidissement des matériels (air, autre fluide),
- Etc.

De la même façon, on fait l'inventaire des personnels (localisation, circulation), et de leurs besoins sur le plan des conditions thermiques, de l'éclairage, etc. A l'issue de ces inventaires, on peut procéder à l'établissement de premiers bilans (superficie, bilans électriques et thermiques).

3.3.3 Contraintes logistiques

On procède ensuite à l'identification des contraintes logistiques inhérentes à la localisation du centre:

- Quelle est la disponibilité des services publics (eau de ville, égouts, télécommunications, EDF, chauffage urbain ...) ?
- Quelle est la proximité des secours, et quels sont les chemins d'accès correspondants ?
- Quelles sont les possibilités d'accès pour la livraison des matériels et des fournitures ?
- Comment s'organise le stationnement des véhicules ?
- Le centre est-il susceptible d'être générateur de nuisances pour le voisinage (bruits d'aérothermes, allées et venues nocturnes ...) ?
- Etc.

3.3.4 Contraintes organisationnelles

On évalue et on documente ici les exigences résultant du diagnostic organisationnel et des études de flux établis au début de l'étude, examinés dans la perspective de la topologie du centre :

- Quelles sont les circulations majoritaires des personnes, fournitures et matériels ?
- Quelle est la disposition optimale correspondante des locaux (optimisation des flux et de l'ergonomie, cloisonnement des risques, stratification des contrôles d'accès ...) ?
- Quelle est la situation du centre par rapport aux services utilisateurs ?
- Quels sont l'organisation et les besoins de communications des différents services ?
- Etc.

3.3.5 Contraintes humaines

Il y a lieu évidemment de recenser tous les éléments qui devront être traités, sur le plan humain, tant au niveau de la future prise en charge du centre que du déménagement :

- Quels sont les effectifs et les catégories socio-professionnelles des personnels concernés ?
- La Culture d'Entreprise a-t-elle (ou doit-elle avoir) des retombées sur la conception du centre ?
- Quelle est la proximité des moyens de transport, de restauration, etc. ?
- Quel sera le degré d'acceptation du transfert par les personnels ? Y a-t-il lieu de procéder à des actions préliminaires (information, négociations...) ? Le transfert aura-t-il des effets sur le contrat de travail ? ...
- Quelles sont la proximité et la qualification des premiers secours ?
- Quels seront les impacts du (et sur le) voisinage ?
- Quel est le degré d'ergonomie/confort recherché ?

3.3.6 Contraintes de planification

De façon à établir l'ordonnancement des travaux, il faut également procéder à l'identification des principaux points de repère dans le temps :

- Date de début des travaux,
- Date de livraison du site (réception provisoire + mises à niveau),

- Date de livraison des matériels et des services,
- Date de mise en service,
- Date d'évacuation des locaux actuels,
- Phasage de déménagement,
- Etc.

3.3.7 Contraintes financières

Il faudra enfin déterminer si l'opération doit être contenue à l'intérieur de limites budgétaires prédéterminées, tant au niveau de la prise en charge que du coût d'exploitation; si c'est le cas, on devra procéder à une première ventilation par poste (achat du terrain, achat des immeubles ou loyers, coût de construction des infrastructures, coût du déménagement, frais temporaires en double...), et étudier les mesures possibles d'économie.

3.3.8 Contraintes réglementaires et juridiques

Ce poste est généralement en dehors de la zone de responsabilité et de compétence du responsable informatique; il sera également indispensable que soient identifiées en amont toutes les contraintes réglementaires pouvant peser sur le projet :

- Plan d'occupation des sols,
- Cahier des charges de la zone concernée,
- Règles d'urbanisme,
- Réglementations diverses,
- Normes internes ou externes,
- Règles de l'art,
- Code du travail,
- Eventuellement, réglementation IGH (Immeuble de Grande Hauteur),
- Etc.

3.4 Objectifs de sécurité

Enfin, il est nécessaire d'identifier clairement, dès le début du projet, les objectifs de qualité et sécurité (tant au niveau de la disponibilité que de la confidentialité) qui sont fixés au centre; ceci conditionnera en effet le degré de résistance des différents dispositifs de sécurité (tant au niveau de la prévention des incidents que de leur résolution) :

3.4.1 Performances, qualités et conditions d'exploitation du centre

Quelles sont les plages de fonctionnement nominal de l'informatique (traitements par lots, traitements transactionnels) par exemple 24h/24 - 365j/an sans coupure, ou bien 24h/24 - 365j/an avec coupures programmées possibles pendant ou hors jours ouvrables ?

Quels sont les horaires de présence des opérateurs ?

Quelles sont les conditions de remise en service sur pannes ?

Quels sont les taux de disponibilité ou d'indisponibilité acceptables des installations : fréquence admissible et MTBF, temps maximum de réparation et DOWNTIME ponctuel et/ou cumulé ?

Dans quelles conditions peuvent s'effectuer un chargement ou une évolution du système en exploitation (avec ou sans coupure, jours ouvrés ou non) ?

Etudier les impacts de ces différentes dispositions au niveau des procédures des niveaux de redondance (matériels et personnels) requis, du degré de sophistication requis pour les systèmes de téléalarme, des besoins d'accès hors heures ouvrables, etc.

3.4.2 Conditions d'entretien et de maintenance

Quel est le degré de sécurité - sûreté souhaité (contre qui ou quoi souhaite-t-on être protégé ? Pendant combien de temps ? Quel est le coût potentiel d'un incident ? Quel budget Sécurité peut-on mettre en face ? ...)

Quelle politique veut-on adopter en ce qui concerne la sophistication et la centralisation des moyens de sécurité (Gestion Technique Centralisée) ?

A qui veut-on confier les missions de surveillance/gardiennage et celles de maintenance (personnels internes ou externes, télésurveillance et téléalarme, infogérance, etc.) ?

Sous quelle forme (présence durant heures ouvrables, astreintes, etc.) ?

Que se fixe-t-on comme politique de redondance et de secours ?

Quels sont les impacts de ces dispositions au niveau des procédures de notification, des contrôles d'accès et de circulation, etc.

3.4.3 Supervision technique

Quels seront les rôles dévolus au personnel d'exploitation du centre ?

Quels seront les rôles dévolus au personnel du poste de garde, du poste de contrôle technique, du poste de sécurité (ou de télésurveillance) ?

Quelles seront les fonctions gérées par un éventuel système de GTC (Gestion Technique Centralisée) ?

Déduire de ces choix les besoins organisationnels correspondants (procédures, descriptions de fonctions, rattachement hiérarchiques, modes de compte-rendu, formation, etc.).

4. MENACES ET PARADES

Ce chapitre a pour objectif de passer en revue les différentes menaces pouvant peser sur un Centre Informatique, et d'évoquer un certain nombre des parades pouvant être intégrées dès les phases initiales du projet d'aménagement (ou de réaménagement) de ce Centre.

Les menaces passées en revue dans ce document sont :

Les parades énumérées dans les pages suivantes n'ont en aucun cas l'ambition d'être obligatoires (puisque les parades doivent, par principe, être sélectionnées essentiellement en rapport direct avec la potentialité des menaces et l'ampleur des enjeux), ni exhaustives, ni suffisamment détaillées pour permettre une sélection en l'état. Il sera donc essentiel, au moment de la définition détaillée des parades à mettre effectivement en place sur un Centre donné, de procéder à une analyse réaliste des menaces, puis de se référer à une ou plusieurs des sources ou entités qualifiées dans les domaines considérés (confrères possédant l'expérience nécessaire, professionnels des métiers concernés, cabinets de conseil spécialisés, organismes professionnels tels que le CLUSIF ou l'APSAD, etc.).

4.1 Dégâts des eaux

4.1.1 Types d'incidents

Les incidents pouvant conduire à un dégât des eaux peuvent être de nature diverse :

- Inondations,
- Défaut d'étanchéité (façades, toitures),
- Débordement ou panne des systèmes d'évacuation
- Infiltrations,
- Rupture de conduites,
- Fuite de condensateurs de climatisations,
- Déclenchement intempestif de sprinklers,

- Etc.

Les conséquences de ce type d'incident peuvent être par exemple :

- Des courts-circuits électriques
- Une détérioration du matériel et des fournitures
- L'inhibition de certaines alarmes
- Une corrosion progressive
- Des risques d'électrocution
- Etc.

4.1.2 Parades

Un certain nombre de mesures (dites "de prévention") permet d'éviter que des incidents tels que ceux listés ci-dessus ne surviennent :

- Choix de l'implantation du site (ou tout au moins des salles les plus critiques) en prenant en compte ce risque (éviter sous-sols et rez-de-chaussée pour les risques d'inondations, et les derniers étages pour les risques d'infiltration par les toits; éviter les façades extérieures, surtout au vent dominant, pour éviter les ruissellements par les façades, etc.),
- Limitation des apports d'eau en salle (climatisations hors salle -ou, pour le moins, traitées spécifiquement-, choix judicieux de l'emplacement des sanitaires, etc.),
- Choix des cheminements de toutes les conduites (sous pression ou non) à moindre risque,
- Conception d'un drainage efficace du bâtiment,
- Etc.

D'autres mesures (dites "de protection") peuvent être intégrées dans la conception du Centre :

- Surdimensionnement et doublement des équipements d'évacuation critiques (pompes de relevage etc.)
- Surélévation des équipements informatiques critiques,
- Mise en place de bacs de rétention (+ alarmes) sous tous les équipements ou conduites susceptibles de fuir,
- Toutes conduites apparentes; dans la mesure du possible,
- Disponibilité de plans des circuits, avec identification claire des systèmes de coupure,
- Existence de systèmes de détection d'humidité,
- Existence de systèmes de détection et de localisation des fuites,
- Mécanismes de coupure automatiquement des fuites,
- Evacuation d'eau par drainage ou pompage,
- Prise en compte des contraintes logistiques nécessaires au basculement sur les installations informatiques de secours,
- Etc.

Pour toutes ces mesures (et il en sera de même pour la plupart des autres menaces), ces parades ne seront vraiment efficaces que dans le cadre d'une approche organisationnelle adéquate, notamment au niveau de la cohérence de la chaîne DETECTION-ALARME-INTERVENTION.

4.2 Destructions par le feu

4.2.1 Types d'incidents

Les incidents pouvant conduire à une destruction totale ou partielle par le feu peuvent être d'origine accidentelle (court-circuit, mégot oublié dans une poubelle, manipulation de produits inflammables, incident lors de travaux de soudure...) ou malveillante (un simple jerrican d'essence suffit).

Les conséquences de ce type d'incident sont en général très graves, et peuvent être fatales à l'entreprise, car les moyens informatiques peuvent être rendus hors service pour une durée très longue. On est en général confronté à :

- Une destruction partielle ou totale du site informatique,
- La mise hors service des équipements de traitement, même en cas de sinistre limité (périmètre de sécurité inaccessible, contamination, dégâts des eaux successifs à l'extinction de l'incendie, mise hors service des équipements de sécurité...)
- Un endommagement de la connectique,
- Une contamination par les fumées, aux effets pervers durables,
- Des risques personnels importants,
- Etc.

4.2.2 Parades

Au niveau de la conception d'un Centre, les mesures de prévention permettant d'éviter que de tels désastres ne surviennent ou ne s'étendent, sont par exemple les suivantes :

- La prise en compte des risques extérieurs (éviter le voisinage d'entités à risque),
- Une conception et une maintenance rigoureuses des installations électriques,
- L'absence de stockage de matières inflammables sur le Centre et aux abords immédiats,
- Une bonne gestion des stocks et déchets d'emballage et de façonnage (localisation, évacuation),
- Un compartimentage efficace des locaux en fonction des risques et enjeux,
- La réduction des risques de courts-circuits (séparation courants forts et courants faibles)
- La gestion de tous les chemins de propagation de feu (limitation des cloisons vitrées, choix judicieux des huisseries, confection soignée des passages de câbles et conduites, existence de clapets automatiques dans les gaines de climatisation, asservissement des climatisations et prises d'air...),
- La prise en compte, dans la définition des périmètres à accès protégés, des possibilités d'actions de mise à feu malveillantes (parois ou baies en limite de propriété),
- Etc.

En ce qui concerne les mesures de protection, on pourra se référer utilement à l'ouvrage "*LA PROTECTION CONTRE L'INCENDIE DES EQUIPEMENTS INFORMATIQUES*" du CLUSIF ; dans les grandes lignes, ces mesures recouvrent la mise en place de système de détection et protection conformes aux règles de l'APSAD, l'utilisation de matériaux de construction à faible pouvoir calorifique, l'asservissement des moyens de climatisation et des alimentations électriques, etc.

En outre, il y a aura lieu de prendre en compte, dès la conception du Centre, les contraintes logistiques nécessaires au basculement sur les installations informatiques de secours.

Pour ce chapitre particulièrement, la cohérence de la chaîne DETECTION-ALARME-INTERVENTION est déterminante, son efficacité étant, dans le meilleur des cas, aussi faible que le plus faible de ses maillons (il est parfaitement illusoire de mettre en place un système de détection sophistiqué, si personne ne sait interpréter les alarmes et/ou ne sait comment intervenir). En outre, un certain nombre de mesures organisationnelles (non liées directement à la conception du Centre, mais plutôt à sa prise en charge) seront décisives :

- Etablissement de procédures de réactions internes et externes vis-à-vis de l'incendie, rigoureuses et régulièrement testées,
- Conduite des actions de formation correspondantes, avant même la fin de l'emménagement sur le Centre,
- Respect draconien des interdictions de fumer,
- Surveillance des interventions extérieures (permis feu, etc.),
- Dépoussiérage régulier des plénums, de faux-plancher et de faux-plafond par une société spécialisée,
- Choix judicieux des issues de secours et des moyens correspondants à mettre en place (sans compromettre les impératifs de contrôle des accès),
- Etc.

4.3 Coupures électriques

4.3.1 Types d'incidents

Les incidents pouvant aboutir à une interruption de l'alimentation électrique de tout ou partie du Centre peuvent être d'origine interne (par exemple court-circuit ou surcharge) ou externe (perturbations EDF) ; elles peuvent être aussi bien accidentelles (erreur de manipulation lors d'interventions sur les installations électriques ou au branchement d'un nouvel équipement) que malveillantes (sabotage d'un poste de transformation Basse Tension).

Les conséquences de ce type d'incident peuvent être graves, car on peut aboutir à un arrêt complet du Centre, pouvant même entraîner une mise hors service de certains mécanismes de sécurité. En outre, la brutalité de l'arrêt peut avoir des conséquences sur l'intégrité des données.

4.3.2 Parades

En ce qui concerne les mesures de prévention et de protection, on pourra se référer utilement à l'ouvrage "*ALIMENTATION ELECTRIQUE DES SYSTEMES INFORMATIQUES*" du CLUSIF ; ce document explicite un certain nombre de règles élémentaires relatives à :

- La conception et le dimensionnement des installations conformes aux normes et aux préconisations des professionnels du métier et des constructeurs informatiques, incluant notamment la mise en place de protections sélectives par équipement,
- L'homogénéité des installations,
- La redondance équilibrée des moyens de secours et des sources d'alimentation.

On pourra en outre, comme dans tous les cas où l'on peut être confronté à des menaces de malveillance, veiller à ce qu'aucun équipement sensible ne soit accessible de l'extérieur, par exemple inclusion des Tableaux Généraux Basse Tension (TGBT) dans le périmètre à accès et circulation contrôlés).

4.4 Défauts de climatisation

4.4.1 Types d'incidents

Les incidents, pouvant être à l'origine d'un dysfonctionnement ou d'une interruption des fonctions de climatisation, sont par exemple :

- Une coupure de l'alimentation EDF,
- Une coupure de l'alimentation d'eau (pour les climatisations à eau perdue)
- Une panne ou un dysfonctionnement des installations de climatisation,
- Une fuite d'origine accidentelle ou malveillante du fluide,
- Un sabotage des installations, particulièrement au niveau des mécanismes d'évacuation des calories (aérothermes par exemple),
- Les effets du rayonnement solaire direct,
- Etc.

Les conséquences de ce type d'incident peuvent être par exemple :

- Une hausse de température localisée ou généralisée dommageable aux équipements (dilatations, chocs thermiques...),
- Un vieillissement prématuré des composants,
- Fréquemment, la nécessité de l'arrêt des matériels informatiques en attendant la remise en route des installations,
- Une détérioration des batteries de secours
- Etc.

4.4.2 Parades

Tant en ce qui concerne les mesures de prévention que de protection, on pourra se référer à l'ouvrage technique du CLUSIF sur la climatisation des équipements informatiques, qui passe en revue les points suivants :

- Etude du système de climatisation en fonction de l'ensemble du Centre,
- Mise en place impérative d'une redondance sur toute la chaîne climatique,
- Etude soigneuse de l'alimentation électrique des équipements frigorifiques,
- Mise en place de protections contre les rayonnements solaires directs,
- Etc.

En outre, il pourra être nécessaire de considérer la mise en place de processus cohérents de détection des défauts, la définition et la construction d'asservissements permettant de limiter la détérioration des équipements (mise hors tension automatique des unités de traitement), l'inclusion de tous les éléments critiques (vannes, aérothermes, bâches de réserve...) dans le périmètre à accès et circulation contrôlés, la disponibilité permanente d'un stock de secours des composants essentiels, etc., Enfin, il faudra prendre en compte tous les aspects organisationnels, non directement liés aux dispositions constructives du Centre, mais plutôt à sa prise en charge :

- Disponibilité permanente de documentations adaptées,
- Souscription d'un contrat de maintenance efficace,
- Rédaction et test des procédures d'intervention,

- Etc.

4.5 Incidents de télécommunication

4.5.1 Types d'incidents

Quelques-unes des situations pouvant se produire sont par exemple :

- Une rupture de liaisons de télécommunication (internes ou externes),
- Un dysfonctionnement de centraux téléphoniques,
- Des perturbations,
- Des intrusions logiques,
- Des sabotages,
- La panne ou la destruction d'un équipement,
- Etc.

Les conséquences de ce type d'incident peuvent être par exemple :

- Des interruptions de service,
- Des problèmes d'intégrité (mascarades, implantation de bombes logiques, altération des programmes ou données...),
- Des problèmes de confidentialité (interceptions, rejeux...)
- La désactivation de dispositifs de sécurité (télésurveillance),
- Etc.

4.5.2 Parades

Les mesures de prévention permettant d'éviter que de tels incidents se produisent sont par exemple les suivantes :

- La protection efficace des têtes de lignes et locaux de télécommunication,
- La protection des liaisons extérieures (gainages, grillages, avertisseurs...),
- Le choix soigneux du type de câbles utilisés (blindage),
- La pose enterrée des liaisons extérieures,
- La séparation des cheminements courant forts / faibles,
- Etc.

Quelques-unes des mesures matérielles permettant de maintenir ou rétablir rapidement le service, même si un incident se produit, sont, par exemple :

- Le doublement des liaisons de télécommunication sur deux centraux distincts (si possible), ou au moins, si les liaisons sont critiques, la souscription d'un abonnement avec chemins d'accès distincts,
- Le doublement de tous les équipements critiques,
- Le recours à des liaisons satellites (éventuellement en secours de liaisons terrestres),
- Le recours à des opérateurs redondants, partiellement ou totalement privés,

- La vérification de l'accessibilité des chemins de câbles (et la disponibilité de la documentation correspondante),
- La protection contre la foudre de toutes les installations de télécommunication (Cf. chapitre suivant),
- La mise en place de moyens de détection des écoutes en ligne, etc.

4.6 Foudre

4.6.1 Types d'incidents

On peut distinguer des situations résultant de foudre "directe", celles où la foudre tombe sur un élément du Centre, et les situations de foudre "indirecte", celles où la foudre est tombée en un point pouvant être assez éloigné du Centre, mais "remonte" ou rayonne jusque dans le Centre (terres électriques, alimentation EDF, circuits de télécommunications, réseaux de télécommande ou de télésurveillance internes, câblage terminaux, etc.). Dans tous les cas, on aboutit à des surtensions violentes et/ou l'émission de champs électriques intenses.

Les conséquences de ce type d'incident peuvent être par exemple :

- Une perturbation des traitements des données informatiques, consécutive aux perturbations des champs électriques,
- La destruction des circuits électriques et/ou électroniques,
- La mise hors service de dispositifs de sécurité,
- L'électrocution de personnels.

4.6.2 Parades

Les mesures de prévention permettant d'éviter que de tels incidents ne se produisent sont par exemple les suivantes :

- Le choix de l'implantation du Centre en dehors de zones à risque,
- L'absence de dispositions constructives susceptibles d'attirer la foudre,
- La mise en place, dans les zones exposées, de câbles ne permettant pas la remontée de la foudre (fibres optiques),
- Dans le même esprit, la segmentation des installations (raccordement des équipements par modems à isolement galvanique),
- Etc.

Certaines mesures de protection sont abordées dans l'ouvrage "*ALIMENTATION ELECTRIQUE DES SYSTEMES INFORMATIQUES*" du CLUSIF :

- Construction d'une "cage maillée" autour des installations critiques (on utilise souvent, improprement, les termes de "Cage de Faraday" ; ces dernières sont effectivement efficaces contre la foudre directe, mais elles sont plutôt destinées à protéger des champs électromagnétiques, et leur prix est beaucoup plus élevé),
- Mise en place de paratonnerres (dans le cadre d'études bien spécifiques),
- Installation de para surtenseurs de puissance adaptée,
- Installation de parafoudres,

- Etc.

4.7 Intrusions physiques

4.7.1 Types d'incidents

La pénétration et la circulation sur le Centre de personnes non autorisées peuvent conduire à des vols de matériels (critiques ou non), des pertes de confidentialité (vol ou copie de documents ou sauvegardes, mise en place de bretelles d'écoute), ou encore des malveillances ou sabotages (avec éventuellement mise hors service des mécanismes de sécurité).

4.7.2 Parades

Au niveau de la prévention des intrusions, on peut noter :

- La mise en place de protections passives par une ou des enceintes étudiées en fonction des risques (solidité des cloisons, mise en place de blindages, conceptions de type "bunker"...),
- La limitation du nombre de baies ouvrant sur l'extérieur, et leur renforcement soigneux et homogène,
- Le choix judicieux de l'implantation, du type et de la surveillance des issues de secours,
- La mise en place de mécanismes de contrôle des accès évolués et rigoureux,
- Etc.

Les mesures de protection comprennent par exemple :

- Les systèmes de surveillance vidéo,
- Une protection active par détection de présence, avec un report des alarmes vers un PC de surveillance 24h/24h,
- Etc.

Il faut bien sûr noter de mettre en place toutes les mesures organisationnelles, non liées directement à la conception du Centre, mais qui seront décisives dès sa prise en charge :

- Ne pas laisser à la vue des visiteurs non concernés les matériels les plus critiques,
- Mettre en place un système d'identification des visiteurs (donc une banque d'accueil adéquate),
- Mettre en oeuvre des procédures généralisées d'interception des visiteurs non identifiés,
- La mise en place de dispositifs antivol sur les matériels les plus tentants ou les plus critiques,
- etc.

4.8 Phénomènes électrostatiques et électromagnétiques

4.8.1 Types d'incidents

On peut être confronté à deux types d'incidents notablement différents :

- Des situations où le Centre est affecté par des rayonnements ou des accumulations de charges parasites d'origine externe (phénomènes atmosphériques, émissions radios ou radars accidentelles ou malveillantes, proximité de machines tournantes puissantes, appareils électriques à décharges tels que des éclairages luminescents, néons...),
- Des situations de type malveillant, où les rayonnements électromagnétiques émis par les matériels de traitement du Centre sont captés par des parties tierces, dans le cadre de tentatives d'atteinte à la confidentialité.

Les conséquences du premier type de situation peuvent être par exemple des dysfonctionnements (souvent apparemment aléatoires) des matériels de traitement, et éventuellement une perte d'intégrité des informations stockées sur des supports magnétiques, tandis que le second type de situation peut entraîner des conséquences aussi graves, puisque, outre les risques de divulgations d'informations confidentielles, on peut être confronté à des scénarios de mascarade ou de "rejeu" aboutissant par exemple à des détournements de fonds ou de sabotage logique.

4.8.2 Parades

Les mesures de prévention permettant d'éviter les incidents du premier type (accidentel) sont par exemple les suivantes :

- Le choix judicieux du site du Centre (éloignement d'émetteurs radio ou radar puissants),
- Le choix de l'emplacement des matériels et supports les plus critiques (loin de blocs tournants puissants tels que des machineries d'ascenseurs ou des machines industrielles pour les problèmes d'induction, loin des conducteurs aériens ou souterrains à haute tension...),
- Le choix de moyens d'éclairage étudiés (éclairages luminescents à starters antiparasités),
- Un raccordement correct à la terre de tous les matériels (évacuation des charges électrostatiques),
- Le blindage adéquat de tous les conducteurs véhiculant des intensités élevées,
- Un choix judicieux des revêtements (non accumulation des charges),
- Le maintien du degré hygrométrique,
- Le bannissement dans les endroits les plus critiques des matériaux et éléments générateurs de charges (les corbeilles en plastique, et même les fauteuils à roulettes aux postes les plus critiques, tels que dans "l'atelier" de préparation/réparation des micros, etc.),
- Egalement le bannissement total de tout moyens de fixation de nature magnétique (aimants, tableaux...),
- Etc.

Les mesures de prévention pour les situations de type malveillant sont par exemple :

- Le choix de l'emplacement des matériels les plus critiques (loin des parois et des voies d'accès,...)
- Le traitement anti-compromission des entrées/sorties.

Les dispositions constructives basées sur la création de Cages de Faraday sont à la fois des mesures de prévention, dans la mesure où elles évitent que l'on puisse capter les émissions du Centre, et des mesures de protection, dans la mesure où elles permettent de protéger le Centre alors même qu'il est situé dans une zone de rayonnement.

4.9 Pollutions ou contamination

4.9.1 Types d'incidents

Les incidents pouvant conduire à une pollution ou à une contamination d'un Centre sont, par exemple :

- L'existence de vapeurs corrosives,
- La présence de poussières (environnement, travaux, éditions massives...),
- Les conséquences induites d'un incendie (fumées, vapeur d'eau),
- Les conséquences d'un attentat,
- Etc.

Les conséquences de ce type de situation peuvent par exemple être :

- Une altération ou destruction plus ou moins progressive des circuits internes des machines informatiques,
- Des dysfonctionnements consécutifs à un taux (ou des caractéristiques) de poussières non conforme avec les spécifications des constructeurs,
- Un échauffement anormal des équipements dû à la baisse d'efficacité des mécanismes de ventilation,
- Un déclenchement intempestif du système d'extinction incendie,
- Des risques de court-circuit,
- Un dérèglement des systèmes de régulation d'hygrométrie,
- Une augmentation des risques d'incendie (accumulation de poussières de cellulose par exemple,)
- Etc.

4.9.2 Parades

Les mesures permettant d'éviter que de tels incidents se produisent sont par exemple les suivantes :

- Un choix approprié du site du Centre (absence de voisinages générateurs de vapeurs corrosives ou poussiéreuses),
- Un filtrage approprié des apports d'air neuf,
- Une limitation des apports d'air neuf au strict nécessaire,

- Un cloisonnement des circulations d'air en cas d'incendie (portes coupe-feu, clapets automatiques dans les gaines de climatisation...),
- D'une façon générale, surveillance de l'étanchéité des cloisons et des huisseries,
- Des dispositifs de nettoyage adaptés (aspiration centralisée),
- Un fonctionnement sous atmosphère neutre et en surpression,
- Un isolement (y compris au niveau des plénums) des zones génératrices de poussières (locaux d'impression et de façonnage),
- Un choix pertinent de tous matériaux de construction et revêtements (ne générant ni ne retenant de poussières),
- La peinture anti-poussières des surfaces sous faux-plancher,
- Etc.

Les mesures de protection sont plutôt du ressort de la prise en charge du Centre que des dispositions constructives :

- Professionnalisme des intervenants de nettoyage (entreprise spécialisée),
- Moyens utilisés (pour éviter le recyclage des poussières),
- Cohérence de ces nettoyages (plénums sous faux-planchers et faux-plafonds), et fréquences (au moins annuel)
- La mise en place de protections avant travaux,
- Le respect des interdictions de fumer,
- Etc.

4.10 Inaccessibilité du Centre

4.10.1 Types d'incidents

Cette situation peut résulter de circonstances d'ordre accidentel ou malveillant :

- Catastrophe naturelle,
- Moyens de transport hors service,
- Mouvements sociaux internes et externes,
- Manifestations ou émeutes,
- Attentats,
- Mise en place de cordons de sécurité par les autorités,
- Etc.

Les conséquences de ce type d'incident peuvent être par exemple :

- Arrêt du centre du fait de l'impossibilité des personnels d'exploitation d'y accéder,
- Destruction ou mise hors service d'équipements sensibles,
- Impossibilité de faire fonctionner le site par occupation des locaux,
- Etc.

4.10.2 Parades

Les mesures de prévention permettant d'éviter la survenance de telles situations sont par exemple :

- Le choix approprié du site du Centre (hors zone inondable ou susceptible d'être l'objet de séismes ou glissements de terrains, multiplicité des chemins d'accès, identification des barrières de dégel possibles, choix de régions et/ou de voisins réputés peu susceptibles d'être l'objet de mouvements sociaux et/ou d'actes de terrorisme,...),
- Limitation à l'essentiel des accès au Centre (ce qui exclut les visites de prestige, et encourage la spécialisation du site aux seuls usages du Centre),
- Absence d'affichage ostensible de l'identité et des missions du Centre,
- La protection du Centre contre l'intrusion (méthodes actives et passives),
- La protection au moins aussi évoluée de tous les éléments essentiels au fonctionnement du Centre (TGBT et groupes électrogènes, condenseurs, entrées d'apport d'air...)
- Etc.

Une mesure de prévention d'ordre organisationnel pourra consister à faire que l'accès au Centre ne soit pas essentiel à son fonctionnement (télépupitrage).

Les mesures de protection sont également plutôt du domaine organisationnel, puisqu'elles sont essentiellement basées sur la pertinence du Plan de Secours.

Il peut cependant éventuellement y avoir certaines implications au niveau des dispositions constructives (accessibilité des locaux de stockage des sauvegardes et des fournitures critiques, idem pour les possibilités de basculement réseau).

5. DEROULEMENT DU PROJET

5.1 Prémices

Les facteurs déclenchants sont ressentis (§2.1), la décision est prise : il faut faire quelque chose!

Les acteurs sont identifiés (§2.3) et, comme l'informaticien n'est pas plus un homme du bâtiment que le responsable des moyens généraux n'est un informaticien, il est dès lors urgent de prendre le temps nécessaire.

Nota : La démarche que nous allons dérouler est une démarche de construction à neuf sur un site vierge. Il faut l'adapter à une réhabilitation ou à un complément technique. Il ne s'agit que de prendre en compte l'existant comme une contrainte à intégrer.

Puisque le point de non-retour est atteint, le responsable informatique va devoir oublier son existant; ce n'est pas un modèle, il est tellement vieux, exigu, sale, il tombe tellement souvent en panne...

On a vu au chapitre 3 que la première démarche est celle de l'expression des besoins. A l'issue de ce document, l'informaticien avait rédigé un "programme". Ce n'est pas au sens informatique qu'il faut l'entendre, ce n'est pas un ordinateur qui l'exécutera mais une équipe d'hommes. Le responsable informatique est dès lors aux prises avec le redoutable exercice de rédiger un document synthétique, clair et même court, qui définit ses besoins sans introduire de solutions.

Besoin exprimé en terme de surface, de puissance de flux et de stock, d'homme et de poste de travail, d'horaire. Besoin à exprimer également en terme fonctionnel et, bien évidemment, au plan de la disponibilité, de l'intégrité et de la confidentialité.

L'informaticien pourrait utilement fixer, à ce stade, une note "Objectif" pour l'audit MARION. Cet audit serait à faire sur le projet à l'issue de l'étude. Cet usage pour rassurant qu'il est pour quelqu'un qui n'est pas des métiers du bâtiment, peut être à contrario déroutant pour ces derniers. En tout état de cause, cette solution nécessitera une grande maîtrise du bâtiment et de la méthode Marion pour l'auditeur en charge de contrôler l'objectif.

L'exercice que constitue un programme, si difficile soit-il, doit être parfait, même si, pour ce faire, il est nécessaire de faire appel à une aide extérieure : l'AMO (Assistance à Maîtrise d'Ouvrage). Certaines formations peuvent également constituer une aide appréciable.

Attention, une première règle : le centre informatique est un bâtiment spécial, il est l'affaire d'une assistance à maîtrise d'ouvrage spécialisée, faute de quoi les conseils risquent d'être vains, voire erronés et mener à l'échec.

Au fait, la DG est-elle consentante ou va-t-il falloir la bousculer ? En tout état de cause, pour argumenter et avoir les feux verts nécessaires, il faudra que le programme soit budgété :

- Coût des divers terrains,
- Coût des travaux tout frais annexes afférents inclus.

A ce stade, l'opération devra également être planifiée et vous n'oublierez pas que le bâtiment a ses vicissitudes : le béton a besoin de prendre, le plâtre de sécher, que la peinture se place après les enduits, ..., c'est-à-dire qu'il s'agit de faire un bâtiment.

Dès ces prémices, pour la rédaction du programme, le responsable informatique ne pourra pas être seul mais, un point important, fera par la suite gagner du temps : il devrait être le "patron", responsable de la maîtrise d'ouvrage, désigné par le Maître d'Ouvrage (propriété juridique), il sera dès lors le décideur éclairé indispensable à une opération bien menée.

Et puis, on n'oubliera jamais que, quel que soit le type d'opération, neuf, petit, réhabilitation, extension, modification, remplacement, etc., son bon ou mauvais fonctionnement rejaillira sur le service informatique. Il vaut donc mieux, pour le responsable informatique, qu'il se saisisse dès le départ d'un chapeau qu'on ne manquera pas de lui faire porter par la suite. Il pourra ainsi exercer réellement ses responsabilités et en accepter les conséquences en toute connaissance de cause.

5.2 Etude et conception générale

5.2.1 Choisir la maîtrise d'œuvre

Une fois encore, n'oublions pas que nous sommes dans le monde du bâtiment et qu'il va falloir s'inscrire dans ce contexte.

Un critère important dans le choix : l'identification des partenaires incontournables. Par exemple, si ce nouveau centre s'inscrit dans une opération immobilière plus importante telle que la construction générale d'un site, il faudra tenir compte du pouvoir de "Monsieur l'architecte de l'opération" qu'il soit de conception, de maîtrise d'œuvre d'exécution, dépendant et "flanqué" d'une entreprise générale. Une règle est dès lors indispensable pour le responsable de la maîtrise d'ouvrage du centre informatique, conquérir son espace de liberté car son intérêt particulier n'est pas l'intérêt général et il n'y a jamais fusion de l'un dans l'autre mais plutôt acceptation et respect mutuel.

Il va donc falloir concevoir et deux voies s'ouvrent à la maîtrise d'ouvrage :

■ ***LA MAITRISE D'OEUVRE***

C'est-à-dire choisir un partenaire qui fera corps avec le Maître d'Ouvrage, devenant le garant des intérêts face aux entreprises. Il sera responsable de la conception générale, du suivi de l'exécution et de la réalisation des objectifs.

■ ***LE CLE EN MAIN TOUT CORPS D'ETAT***

C'est-à-dire choisir une entreprise générale spécialisée qui aura la responsabilité de concevoir et réaliser l'ensemble des ouvrages aptes à répondre aux objectifs.

Les critères de choix vont être multiples. Aucun d'entre eux ne peut être considéré comme déterminant, nous vous en proposons quelques-uns en rappelant :

- Taille du site : plus un site est important, plus il se prête à une maîtrise d'œuvre.
- Partenaires habituels ayant donné toute satisfaction,
- Culture du Maître d'Ouvrage l'orientant naturellement vers une solution ou une autre,
- Simplicité des rapports avec la clé en main, une seule relation, un seul interlocuteur,
- Rigueur et contrôle permanent de la conception en Maîtrise d'œuvre mais une certaine lourdeur,
- Implication technique du Maître d'Ouvrage qui doit juger seul de la qualité de l'offre clé en main,

- Référence, professionnalisme et spécialisation de l'un comme de l'autre,
- Etc.

Et si la société propriétaire de l'ouvrage à construire comprend des services généraux, des directions de projets industriels ou autres ingénieries, le responsable informatique doit impérativement préserver son rôle et sa responsabilité quel que soit le titre qui lui sera donné.

5.2.2 Choix du bureau de contrôle

Dès ce stade, "flanqué" ou non d'une AMO, le Maître d'Ouvrage "éclairé" choisira son bureau de contrôle. Ce n'est pas trop tôt, c'est la loi et, qui plus est, c'est son intérêt car il trouvera là le garant de la solidité des ouvrages, de la sécurité des personnes et des biens. En plus, si le projet le justifie, il pourra confier à ce bureau de contrôle, hors missions réglementaires, une mission de contrôle de la sécurité physique du système d'information.

Si le Maître d'Ouvrage opte pour cette dernière solution, il veillera comme pour son concepteur, au professionnalisme et à la spécialisation dans le secteur de l'environnement informatique de son bureau de contrôle.

5.2.3 Consultation de concepteurs

Un appel à concepteur pourra être lancé sur une orientation soit Maîtrise d'Oeuvre, soit d'entreprise générale, voire pourquoi pas sur les deux axes.

L'appel sera officiel et formalisé suivant les règles si le futur centre dépend d'une administration, il serait préférable qu'il reste restreint pour éviter que les concurrents ne se découragent. Une consultation de 5 à 7 entreprises, semble un maximum encore raisonnable.

L'appel à conception sera lancé sur la base du programme complété par un règlement d'appel d'offre définissant les règles de la consultation :

- Nature des réponses : concours architectural, APS (Avant Projet Sommaire), Technique, budget de travaux, offre technique et financière complète pour une clé en main
- Forme des documents à remettre : schéma et plan, maquette ....
- Date de remise des offres.

A leur réception, l'analyse des offres est l'occasion non seulement de comparer techniquement et financièrement les offres mais aussi de les mettre à niveau, de faire expliquer telle solution, tel déchiffrage, de faire modifier ou compléter l'offre.

Une règle, une déontologie : respecter la propriété des offres, ne pas faire concourir une entreprise sur la solution d'une autre. Tomber dans ce travers, discrédite le Maître d'Ouvrage car tout se sait dans le bâtiment un jour ou l'autre.

Et puis, bien penser que vous avez affaire à des spécialistes qui ont réfléchi en terme d'homogénéité globale du projet et de cohérence pour la sécurité/sûreté. N'ayez pas la tentation du "patchwork", qui, pour une économie apparente souvent mesquine, finit par coûter très cher le jour du sinistre.

Enfin, n'oubliez pas dans cette phase, de voir l'aspect exploitation et maintenance :

Ne pas se faire vendre, par exemple, du "free-cooling" pour économiser de l'énergie et de l'EJP (Effacement des Jours de Pointe) pour réduire le prix de cette énergie sans vérifier le temps de

retour du surinvestissement. Dans certains cas, on a vu ce délai s'allonger à plus de 75 ans, ce qui n'est pas très sérieux.

5.2.4 Conception du centre informatique

Votre partenaire est choisi, vous entrez dans la phase de conception.

Le Maître d'Ouvrage trouvera pendant cette phase une aide appréciable de la part de son bureau de contrôle qui, par ses avis éclairés, orientera efficacement les choix et facilitera les arbitrages.

■ ***LA CONCEPTION AVEC UN MAITRE D'OEUVRE***

Lors de la consultation, beaucoup de choses ont déjà été réglées, de grandes lignes ont été tracées; nous sommes à un stade que nous qualifierons d'APS (Avant Projet Sommaire). Les plans ne sont que des esquisses, peut-être au 1/100ème mais il reste à définir réellement concrètement les solutions constructives, affiner les principes techniques, optimiser les solutions. Cette phase verra également la confirmation du budget de travaux et la réduction de la fourchette de tolérance des coûts.

Le Maître d'Oeuvre est le principal acteur de cette phase, mais le Maître d'Ouvrage exerce naturellement un contrôle, et il répond aux questions qui ne manqueront pas de lui être posées.

Maintenant, beaucoup de choses se précisent, le contact est pris avec les administrations et les concessionnaires, le bilan de puissance électrique se fige (sur la base des besoins précis que le Maître d'Ouvrage fournit). Les plans, les façades, les coupes se détaillent et un document descriptif synthétique décrit le bâtiment, le Maître d'Oeuvre prépare le permis de construire qui sera déposé en Mairie par le Maître d'Ouvrage. Tout le projet sera concrétisé par un document descriptif des travaux et de la fonctionnalité : l'APD (Avant Projet Détaillé).

■ ***LA CONCEPTION AVEC UNE ENTREPRISE CLE EN MAIN***

Le Maître d'Ouvrage a acheté un produit à réaliser décrit dans le devis descriptif fourni par l'entreprise. Tout n'est pas joué pour autant. C'est peut-être la méthode la plus délicate pour le Maître d'Ouvrage car la relation conflictuelle : "chose due et décrite par rapport au coût de la chose", entraîne l'entreprise vers des compromis parfois divergents des objectifs fonctionnels et sécuritaires.

Le Maître d'Ouvrage est donc seul face à l'entreprise clé en main qui définit les ouvrages, concrétise les plans, rédige le permis de construire qui est, là aussi, à déposer par le Maître d'Ouvrage.

Dans cette solution, c'est au Maître d'Ouvrage de vérifier l'évolution de l'étude. Celle-ci n'est ponctuée par un document intermédiaire que par une clause particulière du contrat qui n'aurait pas dû être oubliée, faute de quoi le Maître d'Ouvrage ne pourra que constater à posteriori le résultat.

5.2.5 Etudes d'exécution

Là encore, les deux options vont aboutir à des déroulements radicalement différents, mais vous pourrez être aidé par votre AMO et par votre bureau de contrôle.

■ ***LES ETUDES D'EXECUTION ET CHOIX DES ENTREPRISES AVEC UN MAITRE D'OEUVRE***

Soit vous aurez confié à votre Maître d'Oeuvre une mission dite de type M1 (conception détaillée) celui-ci réalisera un dossier d'exécution complet comprenant :

- APD (Avant Projet Détaillé),

- STD (Spécifications Techniques Détaillées),
- PEO (Plan d'Exécution des Ouvrages),
- Bordereau quantitatif estimatif avec quantités et métrés,

Soit vous avez confié à votre Maître d'Oeuvre une mission M2 (conception) celui-ci constituera :

- Le DCE (Dossier de Consultation des Entreprises) à partir des APD,
- Les pièces administratives en y joignant un cadre de bordereau quantitatif estimatif.

La part de conception des entreprises consultées sur la base des DCE découpés en lots sera évidement très différente de l'une à l'autre solution et dans le deuxième cas une dérive est possible.

Vous aurez peut-être convenu avec votre Maître d'Oeuvre de pratiquer une solution intermédiaire entre M1 et M2 figeant correctement le projet et garantissant la conception générale sans occasionner des coûts trop importants pour l'étude.

Le DCE constitué, vous consultez les entreprises lot par lot ou éventuellement regroupées, voire en entreprise générale. Attention vous entrez dans une phase conflictuelle (Maître d'ouvrage et Maître d'œuvre faces aux entreprises) et pour un bon contrôle, il est parfois souhaitable de maîtriser les lots et leurs interfaces.

Les entreprises répondent, vous ouvrez les plis et confiez à votre Maître d'Oeuvre l'analyse et la comparaison. Il vous remet un rapport d'AMO (Assistance à Maîtrise d'Ouvrage) comparant qualitativement, quantitativement et financièrement les offres et vous choisissez les entreprises qui exécuteront les travaux

A ce stade, on parlera de marché et d'ordre de service rédigé par le Maître d'Oeuvre et constituant les pièces contractuelles entre le Maître d'Ouvrage et les entreprises.

On va parler une dernière fois d'étude avec la phase d'étude d'exécution détaillée faite par les entreprises suivant la mission M1, M2 ou intermédiaire de votre Maître d'Ouvrage. Cette phase sera plus ou moins longue et importante.

- ***LES ETUDES D'EXECUTION ET CHOIX DES SOUS-TRAITANTS AVEC UNE ENTREPRISE CLE EN MAIN TOUT CORPS D'ETAT***

Sans clauses particulières convenues préalablement, ce stade échappe complètement au Maître d'Ouvrage. Ce qui simplifie considérablement sa vie tout en réduisant son pouvoir de contrôle.

Il est donc souhaitable d'avoir prévu un agrément des sous-traitants et un certain contrôle des prestations aux termes du contrat " clé en main ".

Dans un cas comme dans un autre, il faudra là encore avoir prévu l'intervention du bureau de contrôle et savoir l'imposer à sa maîtrise d'œuvre.

5.3 Chantier

Trêve de réflexion, le grand psychodrame est en place et c'est le premier rendez-vous de chantier.

Vous, Maître d'Oeuvre, "flanqué" de vos assistants (AMO et bureau de contrôle), tiendrez le rôle de producteur sans qui rien n'existe. Quant aux entreprises, elles seront acteurs, cameramen, scripts, machinistes, ou décorateurs. Le plateau est un terrain où il peut être de bon ton dans certains cas de

poser une première pierre. En tout cas il faudra respecter les usages du bâtiment qui permettent de cicatriser les conflits qui ne manqueront pas d'apparaître.

Bien sûr, le choix de la solution Maîtrise d'œuvre ou clé en main sera là aussi lourde de conséquences. Si la position du Maître d'Ouvrage pouvait apparaître désengagée de la phase de chantier dans la deuxième solution, il ne doit en aucun cas se désintéresser des travaux. En effet, les travaux sont l'occasion de connaître à fond son bâtiment, d'en apprécier les qualités et les défauts et peut-être d'en éviter certains à moindre frais.

Quelques conseils de comportement pour ceux qui ne connaissent pas l'ambiance bâtiment :

- On se méfie des escarpins dans la boue des chantiers et on prévoit des bottes,
- On n'accède pas sur un lieu de travail sans saluer les ouvriers, même si on est" grande gueule", ce qui est un bien dans ce contexte,
- On est toujours très respectueux du travail fait, même si c'est pour le faire défaire à la suite d'une erreur

N'oubliez d'ailleurs pas de tenir la vraie place du Maître d'Ouvrage qui n'intervient jamais directement sur le chantier mais qui passe toujours par le Maître d'Oeuvre, seul responsable de la qualité, de la cohérence et des délais. Mais n'hésitez jamais à demander ce qui se passe, pourquoi, comment, et dans quel but. L'intérêt que vous porterez flattera les personnes qui réalisent et l'interrogation du candide est toujours intéressante pour les spécialistes, elle remet les choses à leur vraie place.

Revenons au déroulement du chantier, ce sont d'abord les terrassements et VRD (voirie et réseaux divers) pour les fondations, gros oeuvre et structure. Dès le début, les lots techniques sont présents pour les alimentations, les incorporations et les réservations. Très vite , le second oeuvre intervient, serrurerie , menuiserie, et étanchéité assurent le "clos couvert". Les lots techniques interviennent à leur tour et se coordonnent avec les faux-plafond et les faux-planchers. Peinture, revêtement et finition s'enchaînent et s'intercalent. VRD et espaces verts termineront l'opération.

Pendant cette période, le Maître d'Oeuvre fera appel à toute sa capacité de coordination et le Maître d'Ouvrage, à tout son engagement et à son esprit de décision.

Plutôt que de suivre des recettes, il est préférable pour un Maître d'Ouvrage occasionnel de comprendre que la réussite de son projet doit passer par la cohésion avec son Maître d'Oeuvre et par la confiance éclairée, doublée d'un esprit de décision. Il sera conforté dans cette voie par la présence du bureau de contrôle qui, tout au long du chantier, exercera ses vérifications.

Un aspect formel existe pour cette phase de travaux, outre les derniers éléments d'étude d'exécution, c'est le compte-rendu du chantier. Une fois par semaine au moins, il est rédigé par le Maître d'Oeuvre et vous exigerez qu'il soit remis au plus tard 48 heures après le rendez-vous de chantier. C'est un document d'orientation indispensable, mais il ne modifie jamais les marchés, il ne peut en aucun cas constituer des avenants justifiant de plus ou moins values qui, elles, feront l'objet d'ordres de service rédigé par le Maître d'Oeuvre qui ne vous engageront qu'après votre signature (puisque vous êtes mandatés).

Un interlocuteur important est le CHSCT. Il sera nécessaire de suivre les procédures liées aux règles de chantier et au permis de construire, et d'en référer à cette assemblée.

Il est probable que vous serez amené à bousculer quelques délais de signature, tampon et autres exigences administratives en donnant votre parole. Il ne faut jamais se mettre en situation de ne pouvoir tenir cette parole car, si l'entreprise l'a accepté comme argent comptant, c'est dans votre intérêt et il faut que la régularisation conforme, soit donnée dans les plus brefs délais.

Dernier conseil :

- Participez aux réjouissances de chantier qui favorisent les relations souvent difficiles,
- Allez au gigot bitume,
- Organisez un mâchon pour le drapeau,
- Venez au méchoui de fin de chantier.

Imposez le respect des traditions : pénalité amicale et personnelle à chaque retard au rendez-vous de chantier pour alimenter la caisse noire, et si vous êtes dans ce cas, allez-y de votre obole.

C'est à ces occasions que l'on favorise la bonne volonté qui fait faire de grosses économies !

5.4 Réception des ouvrages

Une règle : avoir suffisamment bien travaillé avant, pour que cela ne soit plus qu'une formalité. Mais toujours est-il que nous en sommes là à une phase fondamentale par excellence, car elle constitue le transfert de propriété.

La réception ne peut juridiquement pas être partielle; elle est globale avec ou sans réserves; elle peut être refusée, si cela est formellement justifié. N'oubliez pas qu'une occupation des lieux vaut réception.

Un autre fait : quelle que soit la solution, clé en main ou Maîtrise d'œuvre, on arrive cette fois-ci au même résultat, à la même confrontation projet-réalité.

De par son côté global, la réception devra se préparer par des visites techniques préalables qui auront pour but de valider les ressources, leurs suffisances et leurs fonctionnalités.

Le Maître d'Ouvrage sera plus qu'aidé dans cette phase par son bureau de contrôle qui confirmera le respect des normes, des règlements et éventuellement la conformité aux objectifs de sécurité si la mission a été étendue.

Or, donc, vous avez procédé pendant la phase chantier à des recettes en usine avec essais de matériel électrique (onduleur/groupe électrogène), de matériel thermique (groupe froid/armoires de climatisation/...), il est aujourd'hui nécessaire de faire des essais globaux :

- Fonctionnement et asservissement réalisant les automatismes,
- Débit, pression, température, tension, fréquence...

Tous ces essais nécessiteront des procédures, des organisations, des moyens que devront fournir les entreprises et qui auront été prévus aux cahiers des charges de chaque lot. Ces essais seront formalisés par des comptes-rendus et seront toujours faits après les essais des entreprises. C'est seulement quand l'installation sera prête que vous recevrez favorablement la demande de réception que vous présentera l'entreprise ou que votre Maître d'Oeuvre vous transmettra.

Et c'est le grand jour, comme tout a été vu avant, la réception peut être prononcée, avec réserve si cela se justifie, sans réserve est plus rare et procède souvent de négligence.

N'oubliez pas, à cette occasion, que les DOE (Dossiers des Ouvrages Exécutés) font partie des marchés, que vous devez les exiger et qu'ils peuvent faire l'objet de réserves.

L'acte de réception est formalisé par un procès verbal de réception entre le Maître d'Ouvrage et l'entreprise. Le Maître d'Oeuvre, s'il existe, rédige ce procès verbal et le signe en tant que témoin. Le PV de réception mentionne les réserves.

Pour ce qui est des réserves, elles devront comporter un calendrier de levée pour éviter que les choses ne traînent exagérément. Il est aussi souhaitable de garder une retenue financière supplémentaire à la retenue de garantie cautionnable.

Vous devrez penser à vérifier les levées de réserves et en faire procès-verbal même si vous avez emménagé.

Un dernier point, lié au chantier, mais qui vous accompagnera longtemps après l'emménagement, les garanties :

- Garantie de parfait achèvement de 1 an,
- Garantie de bon fonctionnement de 2 ans,
- Garantie de solidité des ouvrages de 10 ans,
- Garantie en responsabilité civile de 30 ans.

Les garanties qui auront été prises dans les cahiers des charges des entreprises prendront effet à la date de réception des ouvrages.

6. EMMENAGEMENT ET PRISE EN CHARGE DU CENTRE

6.1 Emménagement dans les nouvelles installations

Les équipes qui ont eu dans leur carrière à affronter un déménagement ou un emménagement de leurs installations informatiques reconnaissent volontiers que l'on peut comparer cette expérience à un "sinistre planifié", tant il semble que la loi de Murphy (tout ce qui peut aller mal ...) veuille se vérifier avec la même insistance dans les deux cas.

Il semble donc possible d'extrapoler à un déménagement les règles d'or d'un bon Plan de Secours :

- Planification la plus fine possible,
- Mise en place et test préalable de tout ce qui peut l'être,
- Gestion centralisée de la "crise",
- Identification préalable de chemins de repli.

Les tactiques et modalités dépendent évidemment de la taille du Centre de Traitement en cause, de l'ampleur du déménagement (Informatique seule ou totalité de l'Entreprise), et du degré d'autonomie dans le temps dont dispose l'Informatique pour organiser son emménagement : date butoir pour fin de bail, date au plutôt de fin des travaux de préparation et/ou de prise de possession des nouveaux locaux (piège ! Quid des procédures de réception et de date contractuelle de prise en charge ?), durée maximum admissible de suspension des traitements etc.

6.1.1 Planification

D'une façon générale, les équipes informatiques savent bien identifier les tâches relatives au redémarrage de leurs systèmes; de leur côté, les Services Généraux pensent bien maîtriser les tâches de planification de logistique générale.

Bien évidemment, il arrive fréquemment que les (nombreux) problèmes qui se situent à la limite des deux univers soient sous-estimés ou tout simplement ignorés. Exemples : l'homme France Télécom et/ou l'installateur de la ferme principale (responsabilité Services Généraux) est déjà reparti (et ne reviendra pas) quand arrivera l'homme TRANSPAC (responsabilité Informatique); l'homme "Connectique Réseau Local" (responsabilité Informatique) arrivera évidemment longtemps après que les hommes "Marteau Piqueur" et "Tirage de Câble" (responsabilité Services Généraux) ne soient partis en week-end, mais cela n'est pas bien grave, puisque l'homme 'Téléphonie" (responsabilité Services Généraux) repassera derrière et fera quelques modifications à sa façon.

Une liste (ô combien non exhaustive !) de problèmes typiques concernant la simple gestion des déménageurs (problème qu'on ne rencontre même pas lors d'un sinistre + responsabilité Services Généraux + atmosphère "économies") peut être la suivante :

- Personnels non qualifiés (ou non équipés) pour la manutention et le transport de matériels informatiques (il est évident qu'une entreprise de déménagement en sous-effectifs ou surchargée qui doit faire appel à des personnels complémentaires de dernière minute la veille d'un week-end ne peut formuler aucune exigence quant à la qualification des dernières recrues (soins, aptitude physique, degré d'alcoolémie, compréhension du

français parlé et écrit, etc.); les promesses de mise à disposition de matériels de transport à suspension pneumatique - si on a pensé à l'exiger- disparaissent aussi souvent au dernier moment dans une ambiance de fait accompli détestable);

- Incapacité à maîtriser l'ordre de chargement des camions (et a fortiori leur déchargement); toutes les tentatives de planification dans ce domaine sont pratiquement vouées à l'échec, à moins d'affecter un superviseur individuel à chaque manutentionnaire, et de savoir résister à la frénésie générale en expliquant qu'on ira plus vite en allant plus lentement à des gens dressés au contraire.

Ce problème prend toute son ampleur lorsqu'on a à traiter un déménagement général et simultané de l'entreprise : on a alors toutes les chances pour que les postes de travail utilisateurs se retrouvent enfouis dans des cartons d'archives, faisant voler en éclats le doux rêve d'un lundi matin avec notre beau réseau local et tous ses postes testés à 100% .

Même lorsque l'informatique est seule à déménager, est-on bien sûr que le carton contenant ces câbles vitaux (que l'on a retiré en premier, puisque c'était la première chose qui nous tombait sous la main) n'arrivera pas en dernier, puisque c'était le premier carton mis au fond du premier camion qui est arrivé le premier au fond de l'entrepôt pour y passer la nuit ?

Il est certain que le meilleur PERT ne résiste pas longtemps à de tels traitements; si en outre on s'aperçoit sur le site de réception que par exemple :

- L'entreprise de nettoyage a consciencieusement fermé tous les bureaux, et que l'on ne sait pas qui a LE passe ... (mais cela ne freine pas vraiment les déménageurs, eux ils font un "tas" en attendant),
- L'autocommutateur ne fonctionne pas encore (ou déjà plus), ou bien le plan de numérotation est erroné, ou bien la liste n'a pas été faite, ou bien les numéros ne figurent pas sur les postes, ou bien on ne sait pas les faire fonctionner, ou bien on a repris les anciens postes mais ils sont encore dans les camions ... Les différents superviseurs n'ont plus alors qu'à se courir après, ce qui est bien vivifiant puisque les ascenseurs sont bloqués par les déménageurs,
- Les numéros de bureaux portés sur les cartons sont devenus partiellement illisibles (ou faux, les expéditeurs ayant travaillé sur une version du plan différente de celle du fabricant des plaques), ou bien les numéros portés sur les bureaux sont absents ou partiellement faux, le manutentionnaire, chargé de ces choses, ayant été kidnappé pour une tâche plus urgente ...

Ces problèmes de repérage ne seront malheureusement pas l'apanage des bureaux et de la téléphonie, l'Informatique elle-même aura son quota de problèmes lorsqu'il s'agira de la connexion des postes de travail, mais n'anticipons pas.

D'où **la règle n°1** : **S'occuper (irréprochablement) de ses propres affaires, mais aussi se mêler (inlassablement) des affaires des autres.**

6.1.2 Préparation

Selon un corollaire de la trop célèbre loi de Murphy, mentionnée plus haut, *"tout ce qui n'a pas été testé à 100% ne fonctionnera pas à 100%"*. Dans l'univers informatique où les choses sont souvent binaires, on peut extrapoler et dire que "ce qui ne fonctionne pas à 100% ne fonctionne pas du tout".

D'où **la règle n°2** : **TOUT TESTER, de bout en bout, dans des conditions maximales de réalisme ; et même si à ce moment tout fonctionne, ce ne sera plus vrai le lendemain car :**

- les tests n'auront pas vraiment été faits en charge réelle (ô combien de climatisations et d'onduleurs qui, mis devant leurs vraies responsabilités !),
- les "dernières mises au point" auront bien sûr endommagé des choses qui fonctionnaient,
- des gens serviables (dont les premiers utilisateurs) auront déjà fait des "améliorations" pour se rendre utiles, mais sans avoir le temps de prévenir qui que ce soit.

Certaines grandes organisations vont même jusqu'à faire un déménagement "à blanc", une à deux semaines avant l'événement réel (d'une façon comparable à une répétition de Plan de Secours), avec simulation du chargement (dans des emballages poids et taille réelle), déplacement des camions, simulation du déchargement, basculement éventuel des télécommunications et des communications vocales, et bien sûr chronométrage complet.

D'où **la règle n°3** : **Croire en Descartes; il y a quelque temps, cet homme prétendait que l'on pouvait résoudre un gros problème a priori insoluble en le décomposant aussi longtemps que nécessaire en problèmes plus petits jusqu'à ce qu'ils soient solubles individuellement. Application à notre problème :**

- Dans toute la mesure du possible, dissocier le déménagement des utilisateurs de celui des informaticiens (ah mais, diront les Services Généraux, cela fera double dépense !); il vrai qu'il faudra, en plus de tous les autres soucis (retards de la nouvelle implantation par exemple) faire un montage télécommunication temporaire pour ceux qui n'ont pas encore déménagé, mais le jeu en vaut souvent la chandelle, tant en terme de sécurisation que de pression psychique sur les individus,
- Dans les grandes structures, au moins dissocier le déménagement des équipes de développement de celui des équipes d'exploitation, et mieux encore, dissocier le déménagement des équipes d'exploitation de celui des matériels centraux (en mettant en place des procédures de télépupitrage par exemple), ce qui permettra de sortir au moins une petite équipe de la tourmente,
- Mieux encore, utiliser à fond les potentialités des moyens de secours informatiques (dont dispose évidemment toute organisation informatique mature et sereine ...) en basculant par exemple sur les installations de son Centre de Secours pendant une période significative, et en ne rapatriant l'exploitation que lorsque les nouvelles installations, que l'on aura pu faire monter en régime graduellement, fonctionneront parfaitement.

6.1.3 Gestion de la crise

La création d'une "Cellule de Crise" pluridisciplinaire et équipée luxueusement en terme de moyen de communication et comportant une cellule de prise d'appels serviable et compétente paraît un élément essentiel de succès d'une opération de déménagement. Ses missions sont multiples :

- Limiter la frustration des utilisateurs en permettant un enregistrement immédiat et crédible de leurs appels,
- Augmenter l'efficacité des équipes d'intervention en sériant et regroupant les problèmes qui leur sont confiés et les protégeant des pressions psychologiques,
- Permettre une coordination et une vision globale du déroulement des opérations, permettant de régler immédiatement des conflits de priorité ou d'intérêt (ex. : intérêt Informatique = on modifie tout ce qu'il faut à tout prix pour que "ça marche" lundi matin, intérêt Services Généraux = on ne modifie rien pour que les corps de métiers n'en profitent pas pour justifier des dépassements phénoménaux, les utilisateurs survivront) et ultérieurement de pouvoir traiter d'une façon exhaustive et cohérente des problèmes éventuels de responsabilités fournisseurs.

6.1.4 Chemins de repli

Et si tout va mal, que fait-on ? A défaut d'y avoir songé préalablement, la décision est finalement laissée à des gens dont ce n'est pas la mission à des heures où ils devraient être au lit depuis longtemps (la fameuse climatisation vient de tomber en panne, bien sûr on ne sait pas comment elle fonctionne et on n'a pas le numéro de nuit de l'installateur, lequel n'a pas laissé de documentation, car lorsque son ouvrier a eu "achevé" son travail cet après-midi, il ne l'a surtout dit à personne, de peur qu'on veuille chipoter son oeuvre et/ou lui gâcher son week-end; et que faire si c'est cette coûteuse installation HALON qui vient de se déclencher d'une façon intempestive, mais on pense que ce n'est qu'un petit court-circuit ou défaut de l'installation, mais on n'est pas sûr, et de toute façon les bouteilles sont vides maintenant ?).

Alors ? La décision la plus tentante est de ne pas en prendre, de ne surtout pas annuler l'affaire et de continuer à laisser démonter les matériels à l'autre bout et de continuer à les laisser s'entasser ici (sans onduleur ou sans climatisation ou sans protection incendie ou avec contrôle d'accès débrayé), de ne pas basculer sur le Centre de Secours que l'on n'a, de toute façon, pas mis en "préchauffe".

Règles n°4, 5 et 6 : **Dresser une liste exhaustive des "horreurs" ayant la moindre chance de se produire, formaliser d'une façon draconienne les heures des "points de non-retour" et documenter les alternatives correspondantes (demi-tour, suspension, déménagement partiel, repli sur le Centre de Secours, activation des procédures dégradées...) et dresser la liste (avec le numéro de téléphone domicile) de tous les individus pouvant être indispensables ou utiles.**

La dernière règle : Garder son calme en toute circonstance, avant, pendant, et après...

6.2 Conduite et maintenance des installations

6.2.1 Documentation

En fin de réalisation et à l'issue de la réception du nouveau centre informatique, il est indispensable d'obtenir de la part des entreprises intervenantes les documents de fin d'affaire suivants :

- Le dossier d'ouvrage exécuté,
- Le dossier d'exploitation.

Il est à noter que la réalisation et la fourniture d'une documentation complète et cohérente sera facilitée par le choix d'un Maître d'Oeuvre ou d'un Ensemblier lors de la réalisation du projet. Nous ne saurions trop insister sur l'importance d'une telle documentation qui permettra un suivi et une évolution plus efficace du site.

Le dossier d'ouvrage exécuté comprendra notamment :

- Le plan de récolement des ouvrages,
- Les schémas électriques,
- Les matériaux utilisés,
- Les procès-verbaux de tenue et de résistance au feu,
- Les documentations des constructeurs,
- Etc.

Le dossier d'exploitation comprendra notamment :

- Les manuels d'entretien et de maintenance des différents équipements,

- Les documentations des constructeurs,
- Les manuels de conduite des installations,
- Les nomenclatures des pièces de rechange,
- Etc.

6.2.2 Conduite et gestion technique

Conduite du centre

La conduite du site sera d'autant plus aisée qu'elle reposera sur l'application de procédures et consignes claires et connues du personnel. (Cf. § correspondant). La participation des professionnels ayant conçu et réalisé les installations est indispensable à l'élaboration des consignes et procédures.

Gestion technique

En sus de la documentation technique et d'une formation adaptée, la conduite des installations sera facilitée par la mise en oeuvre d'une gestion technique spécifique. Cette gestion technique des informations relatives aux matériels d'environnement du centre informatique sera plus ou moins élaborée. Selon les besoins du centre, elle permettra de remplir les fonctionnalités suivantes :

a - Simple centralisation des alarmes

b - Visualisation des points de consignes et des états

c - Contrôle et commande sur site ou à distance des installations

Une gestion technique centralisée correctement conçue et réalisée permettra une conduite et une maintenance efficace du site. Elle sera notamment adaptée aux compétences des équipes internes au site. Les commandes à distance éventuelles devront être envisagées avec circonspection.

6.2.3 Maintenance des installations

Une maintenance régulière et efficace des installations techniques du centre informatique est essentielle au bon fonctionnement du site. Les points suivants sont à mettre en oeuvre :

- Choix des intervenants,
- Contrat de maintenance,
- Entretien préventif régulier et adapté,
- Suivi rigoureux des interventions de maintenance,
- Procédures d'intervention sur panne,
- Maintenabilité des installations prises en compte à la conception du site,
- Obligation d'entretien vis-à-vis des constructeurs et des assurances,
- Mise à jour des installations.

Choix des intervenants de maintenance

Ce choix sera fait sur la base des compétences et des références des intervenants proposant leurs services. Il pourra se porter :

- Soit sur une seule entreprise de services qui gérera l'ensemble des interventions de maintenance du site,

- Soit sur un certain nombre de sous-traitants spécialisés dans chacun des domaines techniques,
- Soit sur les équipes de maintenance internes au site quand elles existent et possèdent les compétences et disponibilités requises.

Les différents types de contrats de maintenance

Plusieurs possibilités contractuelles existent :

Le contrat entretien préventif seul, à savoir :

- Un certain nombre de visites d'entretien préventif,
- Pas de délai de dépannage,
- Pas de fourniture.

Le contrat entretien et dépannage, à savoir :

- Un certain nombre de visites d'entretien préventif,
- Délai d'intervention sur panne garanti,
- Pas de fourniture ou quelques petites fournitures d'entretien incluses (consommables).

Le contrat type garantie totale ou reconduction de garantie incluant :

- Les visites d'entretien préventif,
- Un délai garanti d'intervention sur panne,
- La garantie totale ou partielle des matériels.

Suivi des interventions

Un suivi rigoureux et systématique des interventions des équipes de maintenance est nécessaire pour identifier les dysfonctionnements éventuels, les mauvais entretiens, assurer la continuité de service du centre informatique et prévoir les pannes. Chaque intervention (panne ou entretien) devra faire l'objet d'un compte rendu signé par le responsable du site. Un point périodique avec le ou les responsables de la maintenance du site est à prévoir.

Sécurité des interventions

Lorsque des interventions, quelle qu'en soit la nature, sont réalisées par des entreprises extérieures, les dispositions prévues par l'arrêté du 20 février 1992 sont applicables.

Ce texte prévoit notamment l'établissement d'un plan de prévention destiné à régler les problèmes de sécurité posés aussi bien par l'entreprise utilisatrice que par l'entreprise intervenante.

En cas de travaux plus importants nécessitant le concours de plusieurs entreprises, le Maître d'Ouvrage doit appliquer le texte de décembre 1994 concernant la coordination des chantiers et l'application des PPSPS (Plan Particulier de Sécurité et de Prévention de la Santé).

Procédures d'intervention

Les procédures d'intervention sur les équipements techniques d'environnement devront être clairement établies et validées. Celles-ci seront particulièrement importantes pour les interventions nécessaires en dehors de la présence du personnel interne au centre informatique (identification, accès, durée, zones d'intervention, etc.)

Maintenabilité des installations

Bien que cela paraisse une évidence, bon nombre de centres informatiques sont conçus et réalisés sans avoir envisagé leur maintenance ultérieure. Il est donc nécessaire d'étudier ou de préconiser une maintenance aisée et sans risque pour la continuité de service du service informatique dès la conception du centre. Par exemple, il est dommage d'avoir à arrêter un centre informatique pour une maintenance nécessaire sur l'installation électrique ou la climatisation.

Nettoyage des installations

En plus du nettoyage de fin de chantier (généralement sommaire), un dépoussiérage soigné sera prévu avant l'installation des premières machines ; puis un entretien régulier (mensuel au minimum) au moyen d'un aspirateur muni d'un filtre ‘’absolue’’ ou d'une serpillière essorée doit être programmé.

Ce nettoyage peut être inclus dans le contrat de nettoyage général, mais il doit se dérouler sous la surveillance du personnel d'exploitation si l'entreprise n'est pas spécialiste.

De toute façon, un nettoyage complet des plenums du faux plancher et du faux plafond par une société spécialisée doit être planifié annuellement.

Cette opération doit inclure le dépoussiérage de toutes les parois et des machines, elle ne doit pas nécessiter l'arrêt de l'exploitation.

Obligation d'entretien des installations

Afin de bénéficier des clauses de garantie notamment, il est le plus souvent nécessaire de réaliser l'entretien préconisé par le constructeur des matériels. Par ailleurs, la réglementation et les compagnies d'assurance définissent certaines obligations d'entretien préventif dont il faut tenir compte.

Mise à jour des installations

Dans le cadre de la maintenance, la mise en oeuvre de fonctionnalités, omises lors du projet initial, permet d'optimiser le fonctionnement du centre, quand ce n'est pas d'en assurer le fonctionnement pur et simple. Par ailleurs, la mise à jour des installations est facilitée par une maintenance rigoureuse.

6.3 Fournitures

L'activité d'un centre informatique génère des mouvements de personnes et de fournitures dont la gestion courante n'est pas si aisée qu'il y paraît.

Qui ne s'est jamais trouvé avec la porte de la salle machine hyper-sécurisée laissée entrouverte par "l'inspecteur qu'est parti téléphoner" le jour où l'on fait visiter la salle à l'audit interne ?

Qui n'a pas eu de problèmes avec les équipes de techniciens télécommunications commandés par un autre service, venant intervenir sur la tête de câble et n'appréciant pas le fait que vous leur interdisiez l'accès sous prétexte que vous n'étiez pas au courant ?

Qui n'a pas eu de frisson en entendant l'inspecteur parler du "dégausseur" dont il va se munir pour régler le problème du dérouleur de bande magnétique ? Passons sur le chalumeau en salle machine, sur la brouette pleine de ciment roulant sur le faux plancher, sur l'électricien bricolant près du coup de poing en bandothèque, sur la porte d'accès laissée grande ouverte sur la rue pendant la livraison des imprimés ou d'une machine, etc.

L'objet n'est pas ici de dresser l'inventaire des contraintes de type poids au m^2 des imprimés, ni de mesurer la capacité de la cuve à fuel du groupe. L'objet est d'attirer l'attention sur les procédures qu'il conviendra de mettre au point, rédiger, "vendre" parfois pied à pied et enfin faire appliquer par des fournisseurs dont les populations intervenantes sont fort variées tant au plan culturel que caractériel. Ces procédures décriront les droits d'accès et condition de gestion de ces droits afin de garantir un bon niveau d'efficacité aux sécurités d'accès physiques nouvellement installées et souvent à grand frais.

Une approche en anneaux permettra d'inventorier les différents périmètres concernés :

- Périmètre externe type cour, jardin, propriété, etc.,
- Bâtiment, aile, étage,
- Salle de pilotage, bureaux techniques, équipes d'études, bureaux de direction,
- Ateliers de post-production, édition, façonnage, local d'imprimés,
- Salles machines, bandothèque, locaux télécoms, têtes télécoms, locaux techniques.

Une approche par typologie de l'accès permettra de cerner les mouvements susceptibles de s'opérer et d'identifier les catégories de procédures à prévoir :

- Par les entrées de personnels,
- Par les ascenseurs ou monte-charges,
- Par les ponts ou plateaux élévateurs,
- Par les trappes d'installation.

La destination du visiteur et de la fourniture a son importance :

- Salles sensibles,
- Bureaux sécurisés,
- Zones à libre circulation.

La cible de l'intervention et la fréquence sont prises en compte :

- Equipement logistique,
- Matériel ou équipement informatique ou télécoms,
- Visite d'un technicien ou d'un commercial,
- Opération régulière planifiable, permanente ou non,
- Opération irrégulière mais fréquente,
- Opération rare.

La nature des fournitures peut être prise en compte :

- Matériaux inflammables,
- Matériaux dangereux physiquement ou logiquement,
- Matériel lourd.

L'étude ordonnée de ces différents moyens d'inventaire permettra d'identifier les grandes catégories de procédures d'habilitations et de modes d'interventions auprès des fournisseurs.

6.4 Procédures, Instructions et Consignes

6.4.1 Organisation et responsabilités

Il s'agit de mettre en place un ensemble de mécanismes permettant d'assurer l'adéquation du centre avec sa mission. Cette mise en place s'effectue au travers d'une structure, chargée notamment d'initialiser et de suivre dans le temps toutes les procédures et consignes - ou instructions - de sécurité requises dans le contexte considéré.

La structure est plus ou moins légère, suivant que l'architecture informatique est circonscrite en un lieu ou répartie.

Il est nécessaire de définir clairement les responsabilités aux niveaux de l'élaboration, de la mise à jour, des tests et de l'application des différentes procédures et consignes - ou instructions - de sécurité

Les procédures (qui fait quoi ?) sont du ressort des Directions Fonctionnelles alors que les consignes - ou instructions - (comment le fait-on ?) le sont des Directions Opérationnelles.

6.4.2 Fonctionnement normal

Dans le cadre du fonctionnement normal d'un domaine de sécurité, les procédures constituent les règles générales d'organisation à respecter. Ces règles sont complétées par des consignes - ou instructions - spécifiques destinées à décrire un (des) ensemble(s) technique(s) et à expliquer son (leur) utilisation dont pourront découler des consignes à respecter dans des circonstances données. Cela concerne notamment les systèmes d'alimentation électrique, de climatisation, de détection/extinction incendie, de contrôle d'accès, etc.

6.4.3 Incidents

En cas d'incidents venants perturber le fonctionnement normal d'un domaine de sécurité, les consignes - ou instructions - doivent permettre de réagir rapidement :

- soit pour éviter qu'un sinistre ne se déclare, s'il en est encore temps,
- soit pour réduire l'ampleur et les conséquences d'un sinistre qui se serait déclaré.

Elles concernent particulièrement les incidents électriques, les défauts de climatisation, les débuts d'incendie, les fuites d'eau, l'intrusion et l'évacuation.

6.4.4 Contenu des instructions et consignes

Afin de répondre à leurs objectifs, il est souhaitable que les instructions et consignes comportent des dispositions en matière de PREVENTION, de DETECTION et d'ACTION.

6.4.5 Audit et contrôle

La vérification du respect des procédures incombe à la fonction AUDIT INTERNE, qui représente la (les) Direction(s) Fonctionnelle(s). Ses responsabilités en la matière doivent être définies, sachant que l'audit des procédures doit être réalisé au moins une fois par an.

Le contrôle des consignes - ou instructions - doit être effectué régulièrement et de manière dynamique par la Direction Opérationnelle concernée.

6.5 Formation et sensibilisation

Le facteur humain étant primordial, notamment en matière de sécurité, la formation et la sensibilisation du personnel (informatique) sont essentielles. Pour qu'elles soient suffisantes, elles doivent représenter au moins **5 jours par an et par personne**, dont au moins **3 jours** consacrés aux problèmes de sécurité. De plus, il est souhaitable que des réunions d'information générale concernant le fonctionnement du centre informatique aient lieu au moins **une fois par mois**. Il est donc nécessaire de mettre en place un plan de formation individuel comportant :

- Une formation initiale au moment du recrutement,
- Des formations périodiques, destinées au rafraîchissement des connaissances, à l'adaptation au changement et à l'évolution personnelle.

Ces formations seront complétées par une sensibilisation spécifique à la sécurité du centre informatique. La hiérarchie est responsable de la formation et de la sensibilisation du personnel placé sous son autorité.

Dans le cadre du plan de formation, elle doit identifier les besoins et prévoir la collaboration avec la DRH, les moyens nécessaires (humains, budgétaires, matériels) pour répondre à ces besoins.

Les différents domaines à traiter concernent :

- la connaissance des procédures et consignes - ou instructions - (cours magistraux),
- l'utilisation des systèmes de sécurité (cours pratiques),
- L'acquisition de réflexes préventifs (exercices),
- La motivation aux comportements adéquats et au respect des règles (sensibilisation).

Les actions de formation et de sensibilisation doivent faire l'objet d'un enregistrement régulier, afin d'en assurer le suivi avec la DRH et de lui permettre de contrôler la bonne réalisation du plan de formation.

Il ne faut jamais perdre de vue que les objectifs fondamentaux de la formation consistent à susciter une meilleure communication entre les hommes, en élaborant un langage commun et en partageant des connaissances. Cependant, elle doit être conçue, ordonnée et organisée en tenant compte des contraintes inhérentes à la sécurité :

- L'aspect non naturel de la démarche;
- La quasi-omniprésence de l'erreur humaine;
- La nécessité de convaincre en même temps que de former.

6.6 Assurances

Ce paragraphe est destiné à rappeler les principes généraux de l'assurance dans le contexte visé.

6.6.1 En phase de conception

Il est nécessaire de vérifier que tous les intervenants extérieurs présentent un certificat d'assurance, pour la période considérée et pour les activités pratiquées.

Cette précaution doit donc être prise en assurance de responsabilité générale ou spécifique (architectes, garantie décennale). Elle concernera notamment les architectes, ingénieurs d'étude, bureaux d'étude, métreurs, experts, contrôleurs techniques.

6.6.2 En phase de réalisation

Qu'il s'agisse de travaux neufs ou de travaux sur existant, il est préférable que le maître d'œuvre s'assure en "Tous risques chantier" pendant le chantier et en "Dommage Ouvrage" dès la date réglementaire d'ouverture des chantiers (DROC).

Certaines garanties complémentaires pourraient lui être utiles, notamment la garantie biennale (éléments d'équipement dissociables). Après réception totale ou partielle, l'assuré pourra également faire jouer la garantie de parfait achèvement.

6.6.3 En phase d'installation

Une garantie spécifique transport peut s'avérer nécessaire si l'assuré doit déménager son matériel.

S'il existe une période particulière entre la fin du chantier marquée par la réception, et l'installation effective, avec des risques spécifiques (vol notamment), on prévoira une couverture ad hoc.

6.6.4 En phase d'exploitation

L'assuré souscrira avant la mise en service des installations :

- **Un contrat multirisques** couvrant les dommages (incendie, explosion, attentats, vol, dégâts des eaux, catastrophes naturelles, etc.) à l'immeuble et à son contenu (bâtiment, infrastructures),
- **Un contrat TRi** (Tous Risques Informatiques) pour les matériels techniques (informatique et matériel d'environnement) avec les garanties reconstituées d'information et frais supplémentaires d'exploitation
- **Un contrat "Pertes d'exploitation"** dont la base dommage est constituée par les deux contrats précédents,
- **Un contrat Responsabilité Civile/Générale/Exploitation**.

Il peut, après étude, juger nécessaire d'acquérir des garanties complémentaires :

- Responsabilité Civile/Extension aux Risques Informatiques (ERI) - (audit de fonctionnement),
- Fraude informatique
- Attaque logique
- "Bonne fin de projet"
- "L'homme clé informatique"

7. CONCLUSION

A première vue, la lecture d'un tel document pourrait décourager les bonnes volontés, tant les difficultés potentielles ont été mises en évidence.

Au contraire, l'objectif en présentant les différents aspects du projet en regard de la sécurité, était de proposer un axe méthodologique de nature à aider le responsable informatique pendant son implication dans le projet, à toutes les phases d'évolution de celui-ci.

Ce document doit permettre d'éviter les grosses erreurs et d'être vigilant au bon moment, c'est pour cela qu'il faudra le lire et peut-être le relire pendant l'avancement du projet.

Il s'agit avant tout d'un document de vulgarisation qui ne saurait dispenser de l'assistance indispensable de professionnels expérimentés dans ce domaine très spécifique.

Enfin, il faut rappeler une nouvelle fois que ce document doit être associé aux autres publications du CLUSIF, construites dans le même esprit et susceptibles d'apporter des précisions essentielles pour la réalisation du projet, notamment en ce qui concerne les installations électriques, la climatisation, etc.

8. BIBLIOGRAPHIE

🕮 OUVRAGES GENERAUX

AFNOR, Sécurité Informatique, Protection des données, Eyrolles - 1983

FERRETI, LA MONT, Alarme, Texas Instruments - 1985

J-M. LAMERE, La Sécurité Informatique : Approche Méthodologique, Dunod - 1985

J-M. LAMERE, P. ROSE, J. TOURLY, Protection des Systèmes d'Information : Qualité et Sécurité Informatiques - Mise à jour permanente (LES REFERENTIELS DUNOD)

🕮 DOCUMENTS TECHNIQUES ETABLIS PAR L'APSAD

Télésurveillance Vol/Incendie

R 31 - Règle (mars 1989 et additif n°1 décembre 1995)

I 31 - Qualification des stations centrales de télésurveillance

- Règlement de qualification (octobre 1986 et additif n°8 août 1994)

K 31 - Qualification des stations centrales de télésurveillance

- Liste des stations centrales qualifiées (octobre 1995)

Détection d'Intrusion

R 51 - Règle d'installation (mai 1989) - Risques Courants

R 52 - Règle d'installation (septembre 1989) - Risques Lourds

R 53 - Règle d'installation (février 1993) - Risques Très Lourds

I 51 - Qualification d'installateurs "Risques Courants"

- Règlement de qualification (octobre 1988 et additif n°3 mai 1992)

I 52 - Qualification d'installateurs "Risques Lourds"

- Règlement de qualification (septembre 1992)

I 53 - Qualification d'installateurs "Risques Très Lourds"

- Règlement de qualification (octobre 1993)

K 51/52- Qualification d'installateurs "Risques Courants" et "Risques Lourds"

- Liste des installateurs qualifiés (octobre 1995)

K 53 - Qualification d'installateurs "Risques Très Lourds"

- Liste des installateurs qualifiés (en préparation)

Serrures de Bâtiment et Volets de Sécurité

H 61 - Serrures de bâtiments - Certification des matériels

- Règlement particulier de la marque A2P* (novembre 1991 et additif n°4 mars 1995)

H 62 - Fermetures de Bâtiments - Volets de Sécurité - Certification des matériels

- Règlement particulier de la marque A2P (janvier 1993 et additif n°2 février 1994)

J 61 - Serrures de bâtiment - Liste des matériels certifiés A2P (octobre 1995)

J 62 - Fermetures des bâtiments - Volets de sécurité -

- Liste de matériels certifiés A2P (octobre 1995)

Coffres-Forts, Portes fortes et Serrures de Coffres

H 71 - Coffres-Forts - Portes fortes - Serrures de coffres - Certification des matériels

- Règlement particulier de la marque A2P (février 1995)

J 71 - Coffres-Forts - Portes fortes - Serrures de Coffres

- Liste des matériels certifiés A2P (octobre 1995)

Marque A2P

H 0 - Règlement général de la marque A2P (avril 1985 et additif n°1 mai 1994)

🕮 PRESSE ET DIVERS

Revue "Face au risque" (n°232, 236, 243, 306, 313, ...)

Revue "Alarme, Protection, Sécurité"

Thèmes Techniques de la Méthode MARION-AP

Séminaire "Contrôle d'accès : Pourquoi ? Comment ? Quelles applications ? Quels moyens ? (CNPP - 13 Juin 1991).

Séminaire "Contrôle d'accès" (Les Rencontres d'Affaires - 3 et 4 Février 1993)