Plan de secours

Un plan de continuité de service (PCS) contient à la fois un plan de secours informatique (PSI) et un plan de reprise d'activité (PRA).

Avant de commencer une étude de Plan de Secours Informatique, il faut donc définir le Plan de Continuité de Service pour faire valider par la Direction de l'entreprise, via un comité de pilotage, les activités concernées et les types de risques à prendre en compte.

I LE PLAN DE CONTINUITÉ DE SERVICE (PCS)

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

Il faut donc :

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

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

Il s'agit donc de répertorier pour chaque objet à risque un ou plusieurs risques significatifs, puis, pour chaque risque retenu, à étudier et décrire les conséquences directes de sa réalisation sur le système d'information. L'objectif est de réaliser un bilan des conséquences directes en termes :

- de durée d'indisponibilité des moyens (applications, services, ...) ;
- de perte d'information (dernières mises à jour, flux, archives, ...) ;
- de potentialité du risque qui sera soit directement attribuée, soit calculée.

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

Au regard de ces éléments, il sera dès lors possible d'envisager et d'évaluer des moyens de secours appropriés (PSI) et des scénarios de reprise (PRA) pour ramener l'impact estimé à un niveau acceptable.

II LE PLAN DE SECOURS INFORMATIQUE (PSI)

Après élaboration du plan de continuité de service, une étude des solutions doit être menée tant sur les aspects techniques que sur les aspects organisationnels. A l'issue de cette étude, un dossier de choix de solutions sera soumis aux instances de décision afin de définir le contenu définitif du Plan de Secours Informatique. A ce stade de l'étude, le chiffrage des solutions peut conduire à un ajustement des moyens demandés.

Un plan de secours est composé de dispositifs élémentaires (procédures techniques ou organisationnelles) dont l'activation dépendra de l'événement survenu et du contexte général.

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

- la mobilisation des ressources nécessaires :
  - ressources humaines : mobilisation des équipes d'intervention ;
  - réservation des moyens de secours (réquisition de moyens, alerte d'un prestataire externe, ...) ;
  - récupération des sauvegardes ;
  - récupération de la documentation ;
- le secours des équipements informatiques :
  - restauration des environnements système ;
  - adaptations techniques (le matériel de secours n'est pas toujours identique au matériel d'origine) ;
  - restauration des applications ;
  - validation des restaurations ;
- le secours des réseaux :
  - mise en place des équipements de secours ;
  - basculement sur liaisons de secours ;
  - paramétrage des différents équipements ;
- le secours de la téléphonie :
  - re-routage des appels ;
  - mise en place d'équipements de secours ;
  - paramétrage ;
- la reprise des traitements :
  - adaptations logicielles ;
  - adaptation des procédures d'exploitation ;
  - récupération de flux et synchronisation des données ;
  - traitements exceptionnels ;
  - validations fonctionnelles ;
- la reprise des activités des services utilisateurs :
  - tâches utilisateurs avant mise en place des moyens de secours ;
  - organisation d'un service minimum ;
  - travaux exceptionnels (procédures de contournement, rattrapages, ...) ;
- la communication de crise :
  - interne (personnel, autres entités, ...) ;
  - externe (clients, partenaires, public, ...) ;
- les dispositifs de post-reprise :
  - dispositifs préalables et d'accompagnement (assurance, remise en état des locaux, sauvetage des matériels, ...) ;

- dispositifs de retour à la normale (constituent un plan spécifique le plan de reprise d'activité ou PRA).

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

II.1 LA PARTIE ORGANISATIONNELLE DU PLAN DE SECOURS INFORMATIQUE

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

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

En cas de sinistre, on distinguera ensuite :

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

Le comité de crise doit être composé au minimum des Directions suivantes : Direction Générale, Principales Directions utilisatrices, Direction des Services Généraux et des Ressources Humaines, Direction Informatique, Direction de la Communication, Responsable du Plan de Secours. Le comité de crise prend les principales décisions concernant le secours.

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

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

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

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

II.2 LA PARTIE TECHNIQUE DU PLAN DE SECOURS INFORMATIQUE

La solution globale est la résultante de plusieurs solutions adaptées en fonction des exigences de reprise demandées et des pertes de données acceptées par les utilisateurs.

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

- le réseau local ;
- les accès réseau externes ;
- le cas particulier des accès Internet ;
- le secours de serveurs stratégiques devant assurer un service 24h / 24;
- le secours de serveurs pouvant supporter une indisponibilité de 24h;
- etc

Les critères d'évaluation d'une solution de secours peuvent être les suivants :

- le délai de reprise : le délai total de reprise est la somme des délais de déclenchement, temps de mise en œuvre (approvisionnement, restauration, tests, ...), et temps de re-synchronisation des données. Ce facteur, ainsi que la durée maximale de disponibilité des installations de secours sont des paramètres essentiels pour calculer les pertes d'exploitation résiduelles éventuelles, donc l'efficacité de la solution ;
- l'évolutivité de la solution : traduit sa capacité à prendre en compte les évolutions au sein de l'entreprise (architecture technique, organisation, enjeux, nouveaux risques, ...) ,
- les coûts : chaque type de solution entraîne un cortège de frais fixes, variables, récurrents.

II.2.1 DES STRATÉGIES DE SECOURS EN FONCTION DE LA DISPONIBILITÉ DEMANDÉE

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