

mai  
2005

# GUIDE SSI

## Mettre en œuvre un plan de sauvegarde

### Fiche 5



Quelque soit la qualité des moyens de défense mis en œuvre (physique ou logiques) les données peuvent être altérées sciemment ou accidentellement.

Les données et les applications informatiques doivent être disponibles « à tout moment » lorsqu'on en a besoin, et doivent être conservées (sauvegardées) afin de pouvoir être récupérées (restauration) le moment voulu.

Il convient par conséquent de :

- Définir une politique de sauvegarde ;
- Définir des procédures de sauvegarde ;
- Définir des procédures de restauration ;
- Maintenir ces politiques et procédures.

### Politique de sauvegarde

Il n'y a pas de politique de sauvegarde universelle. Elle doit être définie en fonction du volume de données, de la quantité d'information que l'on accepte de perdre, et éventuellement de la durée « légale » de conservation de l'information.

→ Définir les périmètres à sauvegarder (services, matériels, sites, utilisateurs, ...)

→ Définir le type de données sauvegardées (fichiers utilisateurs, fichiers serveurs, documents contractuels, emails, bases de données, ...) Le contenu de la sauvegarde peut évoluer dans le temps avec l'ajout de nouvelles applications ou de données. Cette contrainte doit être prise en compte et il faut veiller à la complétude des sauvegardes régulièrement.

→ Fréquence/ périodicité de la sauvegarde, périodicité de la rotation des sauvegardes

- Principe de sauvegarde générique :

- Le support de sauvegarde journalière du lundi au jeudi est doublé et utilisé par alternance toutes les deux semaines.
- La sauvegarde mensuelle est conservée un an jusqu'au mois identique de l'année suivante.

- **Principe de sauvegardes spécifiques** : Des sauvegardes spécifiques peuvent être réalisées en parallèle pour des données sensibles comme les données financières de l'entreprise et conservées suivant les obligations légales (s'assurer que les applications ayant généré ces données soient également accessibles et que toutes les données soient bien identifiées, comme par exemple des petits outils de pilotage financier développés sous Excel en local, ou des fichiers sur les portables).

→ Définir le(s) lieu(x) et moyens de stockage des sauvegardes (lieux différents, armoires ignifugées, ...). Ne pas laisser les supports près de la machine. En cas de vol ou de sinistre, ces supports risquent en effet d'être également volés ou détériorés. Il est nécessaire de conserver les supports mensuels et annuels en dehors du site de l'entreprise. Conserver les supports hebdomadaires dans une localisation la plus éloignée possible de leur source et dans une armoire fermée (ignifugée de préférence).

## Procédures de sauvegarde

### Les différentes méthodes de sauvegarde

■ **Sauvegarde complète** : C'est une méthode de type « annule » et « remplace ». On écrase le contenu de sauvegarde par la nouvelle information. Méthode très sûre mais longue si le volume est important (par ex : la sauvegarde de gros volumes peut être supérieure à la durée de la nuit et empêcher le travail des utilisateurs le lendemain matin).

■ **Sauvegarde différentielle** : C'est une méthode qui sauvegarde toutes les informations qui ont été modifiées depuis la dernière sauvegarde complète.

■ **Sauvegarde mixte** :

Une sauvegarde journalière différentielle

+ une sauvegarde complète le vendredi

+ une sauvegarde mensuelle gardée un an

+ à chaque intervention technique (mise à jour, ...) sur un poste de travail ou un serveur, une sauvegarde complète (image de la machine) du poste ou du serveur réalisé par le prestataire.

■ **Sauvegarde incrémentale** : C'est une méthode qui ne sauvegarde que les informations qui ont été modifiées depuis la dernière sauvegarde enregistrée sur le support.

■ **Synchronisation d'équipements** : C'est une première méthode à mettre en place entre des équipements nomades et des postes fixes d'un utilisateur donné. Elle peut inclure autant les données d'agenda, de carnets d'adresses que de simples fichiers (fonction porte document) et s'active souvent manuellement.

■ **Pour des postes de travail en réseau, il existe des outils simples et efficaces de duplication automatique** (fonction « miroir ») vers un autre disque (serveur sur réseau par exemple) mais cette duplication ne garantit que les pertes dues à des pannes matérielles et ne protège pas contre les risques de virus.

## Test des sauvegardes

La procédure doit prévoir, avant de passer en mode de fonctionnement continu, de tester la bonne récupération des données afin de s'assurer du bon fonctionnement des sauvegardes.

## Vérification des sauvegardes

La procédure doit inclure le contrôle régulier d'un journal des sauvegardes afin de vérifier qu'aucune anomalie n'ait perturbé le bon fonctionnement des sauvegardes (support saturé par exemple).

## La mise en œuvre et les coûts

■ **Mise en œuvre par des ressources internes** avec acquisition des outils.

A titre d'exemple, pour une sauvegarde par poste, 1 disque dur externe sur port USB mobile de poste en poste (environ 300 €) ou 1 clé USB par poste (environ 100€/ poste) ou pour un système de sauvegarde en réseau de 20 postes, 2 serveurs (environ 5000€).

■ **Sous-traitance** à un prestataire de service informatique pour assistance et mise en œuvre.

A titre d'exemple, 2 jours d'expert (interne ou externe) avec la direction pour définir politique et procédures et 1/2 jour par an pour un audit du processus de sauvegarde.

■ **La sous-traitance à un prestataire (la sauvegarde à distance)**. Cette solution offre l'avantage de ne plus avoir à gérer le support physique des sauvegardes, ni la charge de travail associée car ils sont externalisés à un prestataire via un réseau haut débit. Il est nécessaire de bien définir la politique de sauvegarde et le contrat de prestation (s'assurer de la bonne adéquation de la prestation en cas de problème ; de la présence d'un cryptage adapté, les données se trouvant chez le prestataire ; de la santé financière de ce prestataire stratégique ; etc...)