NOM: PRÉNOM: CLASSE:

MR ROLIN 2025

[SOFTWARE] Les principes des systèmes de sauvegarde et d'archivage

Objectifs
À la fin de cette séquence, l'apprenant sera capable de :

- Comprendre les enjeux de la sauvegarde et de l'archivage dans un environnement professionnel.
- Identifier les différents types de sauvegarde et leur fonctionnement.
- Décrire les supports, les technologies et les logiciels de sauvegarde utilisés en entreprise.
- Élaborer une stratégie de sauvegarde complète conforme aux bonnes pratiques.
- Mettre en œuvre, tester et documenter un processus de restauration fiable.
- Expliquer les obligations réglementaires liées à l'archivage et à la conservation des données.
- Intégrer la sauvegarde dans une démarche de sécurité informatique globale.

Introduction

La donnée est devenue l'un des actifs les plus critiques d'une organisation. Dans un environnement numérique interconnecté, chaque poste, serveur, ou application produit et manipule des volumes importants d'informations. Ces données sont essentielles au fonctionnement de l'entreprise : elles peuvent concerner la comptabilité, les clients, la production, ou encore les ressources humaines. Une perte accidentelle, une panne matérielle ou une attaque informatique peut compromettre la pérennité de l'activité. Le technicien de maintenance PC et réseau joue donc un rôle clé : il est à la fois garant de la fiabilité des équipements et responsable de la mise en œuvre de solutions de sauvegarde efficaces.

La sauvegarde et l'archivage ne sont pas de simples copies de sécurité : elles s'inscrivent dans une stratégie globale de gestion du cycle de vie des données, depuis leur création jusqu'à leur suppression définitive.
Comprendre leurs principes et leurs différences est indispensable pour assurer la continuité de service et la conformité aux obligations légales (RGPD, code du commerce, etc.).

Les enjeux de la sauvegarde et de l'archivage

La sauvegarde est une mesure de prévention. Elle permet de réduire les risques de perte de données liés à :

- une défaillance matérielle (disque dur, alimentation, carte mère)
- une erreur humaine (suppression involontaire de fichiers)
- un sinistre (incendie, inondation, vol)
- une cyberattaque (ransomware, virus, cryptage malveillant)

L'enjeu principal est la continuité de service. Les entreprises dépendent de leurs systèmes d'information ; un arrêt prolongé peut entraîner des pertes financières considérables.
De plus, certaines activités (banques, santé, administrations, etc.) sont soumises à des obligations réglementaires en matière de sauvegarde, d'intégrité et de traçabilité des données.

Les politiques de sauvegarde doivent donc répondre à deux paramètres essentiels :

- le RPO (Recovery Point Objective) : quantité maximale de données que l'entreprise peut se permettre de perdre
- le RTO (Recovery Time Objective) : durée maximale acceptable avant le retour à la normale après un incident.

Une bonne stratégie vise à réduire ces deux indicateurs au minimum, tout en maintenant un équilibre entre sécurité, coûts et performances.

Différence entre sauvegarde et archivage

Il est fréquent de confondre les deux notions, mais leurs finalités divergent :

Sauvegarde : elle permet la restauration rapide de données récentes en cas d'incident. Elle concerne des informations encore utilisées, souvent sur le court terme.

Archivage : il vise la conservation à long terme de données devenues inactives mais ayant une valeur historique, juridique ou administrative.

L'archivage ne sert pas à restaurer une machine, mais à retrouver un document ancien conforme à l'original.
Par exemple, une entreprise doit conserver les factures pendant 10 ans ; elles sont archivées, pas sauvegardées quotidiennement.

Critère	Sauvegarde	Archivage
Objectif	Restauration rapide	Conservation à long terme
Fréquence	Quotidienne / hebdomadaire	Occasionnelle / périodique
Données concernées	Actives	Inactives
Durée de conservation	Courte (jours à mois)	Longue (années)
Support	Disques, NAS, cloud	Bandes, serveurs dédiés, SAE
Gestion	Automatisée	Souvent manuelle ou planifiée

Les deux pratiques sont complémentaires : une donnée peut d'abord être sauvegardée régulièrement, puis archivée lorsqu'elle devient obsolète.

Typologie des sauvegardes

Les entreprises adoptent plusieurs types de sauvegardes selon leurs besoins :

1. Sauvegarde complète
    - Copie intégrale de toutes les données sélectionnées.
    - Simple à restaurer, mais très consommatrice en temps et en espace.
    - Souvent effectuée une fois par semaine, complétée par d'autres types les jours suivants.
2. Sauvegarde incrémentielle
    - Copie uniquement des fichiers modifiés depuis la dernière sauvegarde (complète ou incrémentielle).
    - Très rapide et économe en espace disque, mais la restauration nécessite l'ensemble des sauvegardes successives.
3. Sauvegarde différentielle
    - Copie des fichiers modifiés depuis la dernière sauvegarde complète.
    - Bon compromis entre rapidité et simplicité de restauration.
4. Sauvegarde continue (CDP)
    - Les données sont copiées en temps réel ou quasi réel, dès qu'une modification est détectée.
    - Utilisée sur les serveurs critiques ou les systèmes de production sensibles.

Le choix dépend de la taille du système, du réseau, et des contraintes métier.

Supports et infrastructures de sauvegarde

Les supports physiques et logiques déterminent la fiabilité du système de sauvegarde :

- Disques durs externes / SSD : rapides et simples à utiliser, mais vulnérables aux chocs et pannes.

- NAS (Network Attached Storage) : solution réseau centralisée pour plusieurs postes, adaptée aux PME.
- SAN (Storage Area Network) : architecture dédiée aux grandes structures avec haut débit et réplication.
- Bandes magnétiques (LTO) : haute capacité (jusqu'à 18 To par cartouche), faible coût par Go, longévité >30 ans.
- Cloud (public ou privé) : stockage à distance, sauvegarde externalisée, redondance automatique.

Les entreprises combinent souvent plusieurs supports selon la règle du 3-2-1 :

3 copies des données, sur 2 supports différents, dont 1 copie hors site.

Cette approche réduit considérablement les risques liés aux sinistres physiques ou aux attaques ciblées.

Logiciels et solutions de sauvegarde

Le technicien doit connaître les outils courants :
- **Solutions grand public ou gratuites** : Cobian Backup, Duplicati, SyncBackFree.
- **Solutions professionnelles** : Veeam Backup & Replication, Acronis Cyber Protect, Backup Exec, DPM (Microsoft).
- **Solution personnalisée** : Script fait maison
- **Solutions intégrées** : Windows Backup, Time Machine (macOS), outils Linux (rsync, BorgBackup).

Critères de choix : compatibilité réseau, automatisation, compression, chiffrement, reporting, et support du cloud.
Les logiciels professionnels permettent de gérer plusieurs postes depuis une console centralisée et de planifier des politiques complexes.

Stratégie de sauvegarde et planification

Une stratégie efficace s'appuie sur trois piliers :

1. Planification – Déterminer la fréquence et le type de sauvegarde selon la criticité des données.
    - Journalière pour les fichiers dynamiques (bases de données, dossiers utilisateurs).
    - Hebdomadaire pour les sauvegardes complètes.
    - Mensuelle pour les archives système.
2. Automatisation – Réduire le risque d'erreur humaine via des tâches planifiées.
   Les outils modernes envoient des rapports par e-mail ou journalisent automatiquement chaque opération.
3. Vérification et tests – Une sauvegarde non testée est une sauvegarde inutile.
   Des tests réguliers de restauration garantissent la fiabilité du système et la conformité aux procédures de reprise d'activité.

Sécurité et protection des sauvegardes

La sauvegarde elle-même doit être sécurisée :
- Chiffrement des fichiers avec des algorithmes robustes (AES-256, RSA).
- Contrôle des accès : seules les personnes autorisées peuvent lancer ou restaurer une sauvegarde.
- Isolation : les sauvegardes critiques doivent être déconnectées du réseau (air gap) pour résister aux ransomwares.
- Journalisation : toutes les opérations sont tracées, datées, et signées numériquement.
- Mise à jour : les logiciels de sauvegarde doivent être maintenus à jour pour corriger les failles.

L’archivage : cadre légal et organisation

L’archivage en Belgique répond à des obligations légales précises.
Certaines durées minimales de conservation sont imposées :

- Documents comptables et pièces justificatives : 10 ans à partir de la clôture de l’exercice (Code des sociétés et des associations).
- Documents fiscaux et TVA : 7 à 15 ans selon le type d’opération (notamment immobilière).
- Documents relatifs au personnel : 5 ans minimum après la fin du contrat de travail.
- Contrats commerciaux : durée du contrat + 5 ans.

Les données personnelles doivent être conservées uniquement aussi longtemps que nécessaire à leur finalité, conformément au RGPD (Règlement général sur la protection des données).

Les documents peuvent être archivés sur support papier ou électronique, à condition que soient garanties :

- l’authenticité de l’origine
- l’intégrité du contenu
- la lisibilité pendant toute la période de conservation

Les formats d’archivage recommandés sont PDF/A, TIFF, XML ou tout format non modifiable reconnu.
L’archivage électronique structuré (SAE) assure :

- la valeur probante du document
- la traçabilité des opérations
- la sécurité et la conservation durable des données
- la destruction maîtrisée en fin de cycle

L’archivage s’intègre ainsi à la politique globale de sauvegarde et de conformité de l’entreprise.

Restauration et validation

Les tests de restauration servent à vérifier :

- la cohérence des fichiers restaurés
- la compatibilité des versions
- la rapidité de récupération
- le respect des objectifs RTO/RPO

Ces tests doivent être planifiés et documentés dans le PRA (Plan de Reprise d’Activité) ou le PCA (Plan de Continuité d’Activité).
Une restauration doit toujours être effectuée sur un environnement isolé avant réintégration en production.

Documentation et traçabilité

Un bon technicien doit produire une documentation claire :

- inventaire des systèmes sauvegardés
- fréquence et calendrier
- supports utilisés
- logs des sauvegardes et tests réalisés
- rapports d’incidents.

Cette documentation facilite les audits internes, la continuité de service, et la transmission des connaissances entre techniciens.

Conclusion

La sauvegarde et l’archivage constituent le socle de la résilience numérique d’une organisation.
Une bonne politique repose sur :

- une analyse précise des besoins
- des outils adaptés
- une automatisation fiable
- des tests réguliers
- une documentation complète

Le technicien de maintenance PC et réseau est au cœur de cette démarche : il doit assurer la disponibilité, la sécurité et la traçabilité des données au quotidien.