Backups: sauvegarder les données

Dans ton futur métier, tu vas gérer des données critiques : fichiers d'entreprise, configurations serveurs, bases de données, documents personnels d'utilisateurs, etc. Une panne, une erreur humaine ou un ransomware peut tout faire disparaître en quelques secondes. Ton rôle est d'éviter que la perte de données devienne un problème. Pour cela, il existe des principes, des méthodes et des bonnes pratiques de sauvegarde que **tout technicien** doit maîtriser.

Exploration

L'objectif de ce cours est de t'expliquer **pourquoi les backups sont indispensables**, **comment ils fonctionnent**, et **comment les réaliser correctement**.

Objectifs du cours

À la fin de cette leçon, tu dois être capable de :

- comprendre pourquoi une sauvegarde n'est pas une option mais une obligation ;
- identifier les risques liés à l'absence de sauvegarde ;
- expliquer ce qui distingue une vraie sauvegarde d'une simple copie ;
- appliquer les bonnes pratiques de base ;
- présenter la méthode **3-2-1** et une alternative moderne.

Pourquoi faire des sauvegardes ?

Une sauvegarde sert à **pouvoir restaurer** des données perdues, corrompues ou chiffrées. Les causes les plus courantes sont :

- une panne matérielle (disque dur, SSD, NAS, serveur) ;
- une erreur humaine (suppression accidentelle, formatage) ;
- un logiciel malveillant (cryptovirus / ransomware) ;
- un vol, un incendie, une inondation ;
- des erreurs logicielles (mise à jour ratée, corruption).

> On dit dans le métier:

> 👉 « UNE DONNÉE EXISTE RÉELLEMENT UNIQUEMENT SI ELLE EST STOCKÉE À AU MOINS DEUX ENDROITS DIFFÉRENTS. »

> « IF IT ISN'T IN AT LEAST TWO PLACES, IT DOESN'T EXIST. »

> « LES DONNÉES QUE TU N'AS PAS SAUVEGARDÉES SONT DES DONNÉES QUE TU AS CHOISI DE PERDRE. »

C'est le principe de **REDONDANCE**

Sauvegarde vs copie

Ce n'est **pas** parce que tu copies un fichier sur une clé USB que tu as fait un backup.

Une **bonne sauvegarde** doit :

- être indépendante de l'original ;
- être impossible à modifier par accident ;
- pouvoir être restaurée intégralement ;
- être régulière ;
- être testée.

Une simple copie ne protège pas :

- si tu modifies ou supprimes un fichier original, la copie peut être écrasée ;
- si ton PC se fait infecter, la clé USB branchée sera aussi chiffrée ;
- si ton bureau brûle, original + copie disparaissent ensemble.

Les 5 informations essentielles à retenir

1. Un backup doit toujours être **séparé** de l'original.
2. Tu dois multiplier les copies (pas une seule !).
3. Tes sauvegardes doivent être **régulières** et **automatisées**.
4. Tu dois **tester** au moins une restauration pour vérifier que tout fonctionne.

5. Une bonne stratégie utilise la **méthode 3-2-1** ou une variante moderne équivalente.

La règle 3-2-1

C'est la méthode la plus utilisée aujourd'hui :

- **3 copies des données** :
  - les données originales (sur l'ordinateur ou serveur)
  - deux sauvegardes différentes
- **2 supports différents** :
  - par exemple : un disque local + un NAS
  - ou un SSD + un cloud
  - ou un NAS + des bandes
- **1 copie hors site (off-site)** :
  - cloud sécurisé
  - NAS dans un autre bâtiment
  - coffre physique

👉 Cela protège à la fois contre les pannes locales, les erreurs humaines et les catastrophes physiques.

Variante moderne : la règle 3-2-1-1-0

Adaptée à l'ère des ransomwares.

Elle ajoute :

- **1 copie immuable** (WORM, snapshot verrouillé, cloud immuable) → impossible à modifier ou supprimer même par un virus
- **0 erreur** → test régulier des restaurations + vérifications d'intégrité

> C'est la règle recommandée dans les environnements professionnels (entreprises, écoles, institutions publiques).

Bonnes pratiques du métier

- Utilise des **sauvegardes incrémentielles** ou **incrémentales** (plus rapides, moins lourdes).
- Automatise tes backups pour éviter les oublis.
- Sépare les droits : un ransomware ne doit pas pouvoir effacer les backups.
- Définis une **politique de rétention** (ex : garder 30 jours, 6 mois…).
- Documente où se trouve chaque copie.
- Prévois un plan B si un support tombe en panne.
- Utilise le chiffrement si les données sont sensibles.

Exemples concrets

- Un utilisateur supprime un dossier important → restauration depuis l'incrément de la veille.
- Un SSD tombe en panne → restauration depuis un NAS + copie cloud.
- Un ransomware chiffre la machine + le NAS → restauration depuis la copie immuable déconnectée.

Synthèse (à retenir absolument)

- Une donnée non sauvegardée **sera perdue un jour**.
- Une bonne sauvegarde doit être **séparée, multiple et testée**.
- La méthode **3-2-1** est la base.
- La variante **3-2-1-1-0** est la référence moderne contre les cyberattaques.
- Ton rôle est de garantir la disponibilité des données, même en cas de catastrophe.

- Bien insister sur la différence entre « je copie un fichier » et « je fais une sauvegarde ».
- Montrer que **la menace principale aujourd'hui est le ransomware**, ce qui justifie la copie immuable.
- Rappeler que **la restauration** est plus importante que la sauvegarde elle-même.