

Sauvegardes : la règle du 3-2-1

La seule assurance qui fonctionne contre le ransomware, le vol, l'incendie et l'erreur humaine.

12 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/sauvegardes

Panne de disque, ransomware, erreur de manipulation, vol, incendie : les causes de perte de données sont nombreuses, et une seule suffit. La sauvegarde est votre dernière ligne de défense — à condition qu'elle soit bien conçue, automatisée et testée. Ce guide couvre la méthode complète : quoi sauvegarder, selon quelle architecture, avec quels outils selon votre taille, à quelle fréquence, et comment vérifier que tout cela fonctionnera le jour J.

1. De quoi une sauvegarde doit protéger

Une bonne stratégie se conçoit en listant les scénarios — chacun élimine certaines architectures :

- La panne matérielle : un disque meurt, sans préavis — le scénario le plus banal
- L'erreur humaine : fichier écrasé, dossier supprimé, mauvaise manipulation découverte trois semaines plus tard (d'où l'importance de conserver des versions anciennes)
- Le ransomware : chiffre tout ce qu'il atteint, y compris les sauvegardes connectées au réseau — d'où l'exigence d'une copie hors ligne
- Le vol et le sinistre physique (incendie, dégât des eaux, foudre) : emporte l'original ET la sauvegarde posée sur la même étagère — d'où la copie hors site
- La défaillance d'un prestataire cloud : compte piraté, service fermé, erreur de leur côté — d'où l'intérêt de ne pas tout confier au même acteur

2. La règle 3-2-1 (et sa version renforcée)

- 3 copies de vos données : l'original + deux sauvegardes
- 2 supports différents : par exemple un NAS local + un cloud de sauvegarde
- 1 copie hors site : dans un autre lieu physique que l'original

La version renforcée : 3-2-1-1-0

Elle ajoute deux exigences nées de l'ère du ransomware : 1 copie hors ligne ou immuable (déconnectée du réseau, ou verrouillée en écriture — impossible à altérer même avec des droits administrateur volés), et 0 erreur aux tests de restauration. Pour une entreprise, c'est ce standard qu'il faut viser.

BON À SAVOIR

Un montage simple et robuste pour une TPE/PME : sauvegarde automatique quotidienne des postes et du serveur vers un NAS local (restauration rapide), doublée d'une copie chiffrée envoyée chaque nuit vers un cloud de sauvegarde avec versions immuables (protection ransomware et sinistre). Coût : quelques dizaines d'euros par mois.

3. Définir le périmètre : quoi sauvegarder

L'inventaire est l'étape que tout le monde saute — et la cause n° 1 des mauvaises surprises. Passez en revue :

- Les fichiers de travail : serveur de fichiers, mais aussi les documents stockés localement sur les postes
- Les logiciels métier et leurs bases de données : facturation, comptabilité, CRM, paie — vérifiez la procédure de sauvegarde propre à chaque application
- La messagerie : Microsoft 365 et Google Workspace ne garantissent qu'une rétention limitée — la sauvegarde des boîtes reste votre responsabilité
- Le site web et sa base de données, chez l'hébergeur ET hors de l'hébergeur
- Les configurations : pare-feu, box, NAS, licences et clés — indispensables pour reconstruire vite
- Les données des outils SaaS annexes : agenda, notes, outils de gestion de projet

ATTENTION

La synchronisation cloud (OneDrive, Google Drive, Dropbox) n'est PAS une sauvegarde : elle réplique instantanément les suppressions et le chiffrement d'un ransomware vers toutes les copies. Elle protège contre la panne d'un poste, pas contre la perte de données. Une vraie sauvegarde conserve des versions indépendantes et historisées.

4. Les solutions selon votre taille

Indépendant ou très petite structure

Un logiciel de sauvegarde sur chaque poste vers un disque externe (débranché après chaque sauvegarde) + un abonnement de sauvegarde cloud automatique. L'essentiel : que rien ne repose sur une action manuelle quotidienne.

TPE (2 à 10 postes)

Un NAS en RAID comme cible centrale, alimenté automatiquement par les postes et le serveur, avec réplication nocturne chiffrée vers un cloud de sauvegarde. Activez les instantanés (snapshots) du NAS : ils permettent de remonter le temps après une erreur ou un début de chiffrement.

PME (10 postes et plus)

Une solution de sauvegarde centralisée et supervisée (avec alertes en cas d'échec), incluant serveurs, postes, machines virtuelles et messagerie, avec copie immuable hors site et rapports réguliers. À ce niveau, la supervision par un prestataire se justifie pleinement : une sauvegarde qui échoue en silence pendant trois mois est un scénario classique.

5. Fréquence et rétention

- La fréquence découle d'une question simple : combien d'heures de travail pouvez-vous accepter de perdre ? Une sauvegarde par nuit signifie jusqu'à une journée perdue ; les données critiques (facturation, production) peuvent justifier des sauvegardes en continu ou toutes les heures
- La rétention (combien de temps garder les versions) doit couvrir les erreurs découvertes tard : conservez par exemple 30 jours de versions quotidiennes, 12 semaines de versions hebdomadaires, 12 mois de versions mensuelles
- Attention aux obligations légales : certaines données (comptabilité, paie) ont des durées de conservation imposées — la sauvegarde doit les respecter

- Chiffrez les sauvegardes, surtout celles qui partent hors site — et conservez la clé de chiffrement en lieu sûr, hors du système sauvegardé

6. Tester : le protocole qui change tout

Une sauvegarde non testée est une hypothèse, pas une protection. Les tests se planifient comme le reste :

- Chaque mois : restaurer quelques fichiers pris au hasard, vérifier leur intégrité et noter le résultat
- Chaque année : un test de restauration complète — remonter un serveur ou un poste entier depuis la sauvegarde, et chronométrer : ce temps est votre vrai délai de reprise (RTO)
- Après chaque changement d'infrastructure : re-vérifier que les nouvelles machines et applications sont bien dans le périmètre
- Surveiller les rapports : tout échec de sauvegarde doit générer une alerte lue par quelqu'un — l'échec silencieux est le piège mortel

L'essentiel à retenir

- 01 Appliquer la règle 3-2-1, avec une copie hors ligne ou immuable
- 02 Inventorier le périmètre : postes, serveurs, messagerie, site web, logiciels métier
- 03 Automatiser entièrement — aucune action manuelle quotidienne
- 04 Chiffrer les copies hors site et sécuriser la clé
- 05 Définir une rétention qui couvre les erreurs découvertes tard (30 jours minimum)
- 06 Tester une restauration de fichiers chaque mois
- 07 Réaliser un test de restauration complète chronométré une fois par an

Questions fréquentes

OneDrive/Google Drive sauvegarde déjà mes fichiers, pourquoi payer autre chose ?

Ces services synchronisent : toute suppression ou chiffrement se propage immédiatement à toutes les copies. Leur corbeille et leur historique de versions offrent un filet limité (durées courtes, restauration en masse laborieuse). Une sauvegarde dédiée conserve des versions indépendantes, historisées et restaurables en bloc — c'est un autre métier.

Un RAID sur mon NAS, est-ce une sauvegarde ?

Non. Le RAID protège contre la panne d'UN disque, c'est de la disponibilité. Il ne protège ni de la suppression, ni du ransomware, ni du vol, ni de l'incendie, ni de la panne du NAS lui-même. Un NAS en RAID est une excellente cible de sauvegarde, pas une stratégie complète.

À quelle fréquence sauvegarder ?

Posez la question en termes de perte acceptable : si perdre une journée de travail est supportable, une sauvegarde nocturne suffit. Si perdre plus d'une heure de facturation est critique, il faut des sauvegardes horaires ou continues sur ces données-là. Rien n'oblige à une fréquence unique : les données critiques peuvent être sauvegardées plus souvent que le reste.

Combien ça coûte ?

Pour une TPE : un NAS correct s'amortit sur des années, et la sauvegarde cloud coûte de quelques euros à quelques dizaines d'euros par mois selon le volume. À comparer au coût d'une journée d'arrêt complet de l'entreprise — et au fait qu'une PME sur deux ne survit pas à une perte totale de ses données.

Pour aller plus loin

Cybermalveillance.gouv.fr — bonnes pratiques de sauvegarde — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

ANSSI — Guide d'hygiène informatique (mesure sauvegardes) — cyber.gouv.fr/publications/guide-dhygiene-informatique

Vos sauvegardes tiendraient-elles le choc ?

Mise en place, tests de restauration, plan de reprise : nous rendons votre activité résiliente, à votre échelle.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr