3-2-1 : la règle d'or pour ne pas perdre vos données

Le guide concret du DSI de PME pour protéger ses données contre les ransomwares et les sinistres, sans se ruiner.

> En tant que DSI ou Responsable Informatique, il y a une réalité qu'il faut accepter : la question n'est pas de savoir **si** vos serveurs vont tomber ou si vous allez subir une cyberattaque, mais **quand**. Face aux ransomwares de nouvelle génération qui ciblent activement les sauvegardes, la survie d'une entreprise ne tient pas à la qualité de ses pare-feu, mais à sa **capacité de restauration**.

La règle du 3-2-1-1-0

La règle classique 3-2-1 a évolué pour répondre aux menaces actuelles. Voici comment concevoir cette architecture :

3 Trois copies de vos données

Vous devez disposer de la copie de production et d'au moins deux copies de sauvegarde distinctes.

↳ Pourquoi ?

Statistiquement, la probabilité que trois systèmes indépendants tombent en panne simultanément est proche de zéro.

2 Deux supports de stockage différents

Ne stockez pas vos sauvegardes sur le même type de technologie que vos données actives. Production sur SAN, sauvegardes sur NAS dédiés ou bandes.

↳ Pourquoi ?

Éviter qu'une panne matérielle généralisée ou un bug de firmware n'affecte l'ensemble de votre écosystème.

1 Une copie hors-site (Offsite)

Au moins une copie stockée en dehors des limites géographiques de votre entreprise.

↳ Pourquoi ?

En cas d'incendie, de dégât des eaux ou de vol, vos sauvegardes locales disparaîtront avec vos serveurs. Le flux doit être chiffré de bout en bout.

1 Une copie hors-ligne, immuable (Air-Gapped)

Une copie déconnectée du réseau ou stockée sur un espace immuable — technologie WORM : *Write Once, Read Many*.

↳ Pourquoi ?

Un hacker avec des privilèges administrateur cherchera d'abord à détruire vos sauvegardes. Un stockage immuable empêche toute modification ou suppression, même par l'administrateur système.

0 Zéro erreur après vérification

Vos sauvegardes ne valent rien si vous ne pouvez pas les restaurer. Le « 0 » exige un contrôle automatique de l'intégrité et des tests de restauration périodiques.

↳ Le piège classique :

Un rapport « Backup Successful » ne garantit rien. Il faut programmer des restaurations à blanc de machines virtuelles dans un bac à sable pour valider que tout est exploitable.

RPO et RTO : les deux variables clés

- **RPO** (Recovery Point Objective) : quelle quantité de données acceptez-vous de perdre ? Une sauvegarde toutes les 24h + crash à 23h = 23h de perte.
- **RTO** (Recovery Time Objective) : combien de temps l'entreprise peut-elle rester à l'arrêt ? Restaurer 5 To via ADSL peut prendre plusieurs jours.

↳ La solution :

Dimensionner vos liaisons réseau et vos équipements de stockage en fonction de ces deux variables.

Pièges à éviter

NAS de sauvegarde accessible en partage réseau

Si votre NAS est monté en SMB/NFS accessible depuis les postes utilisateurs, un ransomware l'infectera en quelques secondes.

↳ La solution :

Isoler le réseau de sauvegarde sur un VLAN dédié, interdire l'accès direct, utiliser des comptes d'administration spécifiques sans relation avec l'Active Directory principal.

« Microsoft 365 sauvegarde déjà mes données »

C'est faux. Microsoft assure la haute disponibilité, mais applique un modèle de responsabilité partagée. La rétention par défaut n'est que de quelques jours.

↳ La solution :

Sauvegarder impérativement vos tenants SaaS (Teams, SharePoint, OneDrive, Exchange) vers une infrastructure tierce.

WiFeel : votre stratégie de sauvegarde infogérée

Mettre en place et maintenir une architecture 3-2-1-1-0 demande du temps et des compétences pointues. WiFeel conçoit et infogère votre politique de sauvegarde de bout en bout :

- **Audit initial** : analyse des flux de données, définition des RPO et RTO réels
- **Déploiement** : fourniture et sécurisation de NAS de sauvegarde (Synology), isolés sur VLAN
- **Externalisation Cloud** : transfert automatique vers des infrastructures cloud sécurisées et géographiquement distantes
- **Sauvegarde Microsoft 365 / Google Workspace** : protection des boîtes mails, SharePoint, Teams et OneDrive
- **Supervision 24/7** : alerte immédiate et intervention proactive en cas d'anomalie
- **Tests de restauration trimestriels** : validation réelle que vos serveurs critiques redémarrent en minutes, pas en semaines

Questions fréquentes

Qu'est-ce que la règle 3-2-1-1-0 en une phrase ?

Trois copies de vos données, sur deux supports différents, dont une hors-site et une hors-ligne ou immuable, avec des tests de restauration réguliers.

Microsoft 365 ou Google Workspace sauvegardent-ils déjà mes données ?

Non. Ces plateformes assurent la haute disponibilité, mais la récupération après suppression accidentelle ou piratage reste de votre responsabilité.

WiFeel peut-il reprendre une sauvegarde déjà en place ?

Oui. Nous auditons votre architecture existante et la faisons évoluer vers un standard 3-2-1-1-0 complet.

À quelle fréquence tester une restauration ?

Trimestriellement ou semestriellement pour les systèmes critiques. Un rapport de sauvegarde réussie ne garantit pas qu'un fichier sera exploitable.

Confier votre stratégie de sauvegarde à WiFeel, c'est transformer un risque cyber majeur en un sujet maîtrisé, audité et testé régulièrement.
Prenez rendez-vous sur www.wifeel.fr/rendez-vous

SAS WiFeel — 121 Chemin des Mésanges, 34160 Castries — p.belot@wifeel.fr — 06 15 64 50 00