

Tester ses restaurations : le rituel qui valide tout le reste

Une sauvegarde jamais restaurée est une croyance. Le protocole de test complet : quoi, quand, comment, et quoi noter.

7 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/test-restauration

Toutes les histoires de sauvegardes tournent autour du même moment de vérité : la restauration. C'est là qu'on découvre le disque plein depuis des mois, le dossier critique hors périmètre, le mot de passe de chiffrement que personne n'a, ou les 30 heures nécessaires là où le métier en tolérât 4. Le test de restauration transforme la croyance en certitude — et c'est un rituel simple, à condition d'être protocolisé. Voici le protocole.

1. Les trois niveaux de test

- Le test fichier (mensuel, 15 min) : restaurer quelques fichiers pris au hasard — dont un ancien (30+ jours) pour valider la profondeur d'historique — et vérifier leur intégrité en les ouvrant
- Le test applicatif (semestriel) : restaurer une base ou un périmètre métier (la compta, un dossier client complet, une boîte email) et vérifier que l'application l'exploite
- Le test complet (annuel, chronométré) : remonter un serveur ou un poste entier depuis zéro — machine de test ou environnement virtuel — jusqu'à l'état « on peut travailler »

2. Le chronomètre : la donnée qui pilote

Le test complet produit LE chiffre stratégique : votre délai de restauration réel. Comparé au RTO fixé par le métier, il valide ou invalide toute l'architecture : 30 heures mesurées pour un RTO de 4 heures = décision à prendre (restauration locale plus rapide, serveur de secours, réplication). Sans mesure, cette conversation n'a jamais lieu — jusqu'au sinistre.

CAS CONCRET

Découvertes typiques d'un premier test complet, par ordre de fréquence : le débit — restaurer 2 To depuis le cloud prend des jours sur une connexion ordinaire (d'où l'intérêt de la copie locale pour la vitesse ET du cloud pour la survie) ; la clé de chiffrement introuvable ; le serveur restauré qui ne démarre pas sans une configuration jamais documentée ; le logiciel métier qui exige une réinstallation dont personne n'a les licences. Chaque découverte à froid est un sinistre évité.

3. Protocoliser : la fiche de test

- Une fiche par test : date, périmètre testé, qui a testé, durée, résultat, anomalies, actions correctives — cinq lignes suffisent
- Varier les cibles : ne pas toujours restaurer le même dossier de démonstration — le hasard révèle les trous de périmètre
- Tester aussi les restaurations « exotiques » : la boîte 365, le site web, la configuration du pare-feu — tout

ce qui figure au périmètre

- Faire tester par le suppléant de temps en temps : la procédure que seul UN cerveau sait exécuter est un homme-clé de plus
- Ces fiches sont de l'or en audit, pour l'assureur et pour les exigences clients : la sauvegarde « prouvée » vaut plus que la sauvegarde déclarée

4. Automatiser ce qui peut l'être

- Les alertes d'échec de sauvegarde lues chaque jour restent le socle (voir supervision) — le test valide, l'alerte surveillance
- Les solutions professionnelles savent vérifier automatiquement l'intégrité, voire démarrer la sauvegarde en machine virtuelle et prouver le boot par capture d'écran — demandez ces fonctions à votre prestataire
- L'automatisation complète le rituel humain, elle ne le remplace pas : seul le test humain vérifie que ce qui est sauvegardé est bien ce dont le MÉTIER a besoin

L'essentiel à retenir

- 01 Instaurer le test fichier mensuel (15 minutes, fiche remplie)
- 02 Restaurer un périmètre applicatif chaque semestre
- 03 Chronométrer un test complet annuel et le comparer au RTO
- 04 Varier les cibles et faire tester le suppléant
- 05 Archiver les fiches de test (audit, assurance, clients)
- 06 Activer les vérifications automatiques disponibles

Questions fréquentes

Restaurer sur quoi, sans casser la production ?

Jamais par-dessus la production, toujours à côté : un dossier « restauration-test » pour les fichiers, une machine de test ou virtuelle pour les systèmes (la virtualisation rend le test complet accessible même sans matériel de rechange), un compte de test pour les boîtes. Le prestataire dispose généralement d'un environnement dédié — c'est une question à lui poser.

Qui doit réaliser ces tests : nous ou le prestataire ?

Le prestataire opère, l'entreprise vérifie : les tests techniques figurent idéalement au contrat d'infogérance (avec les fiches en preuve), et le référent interne exécute lui-même le test fichier mensuel — quinze minutes qui maintiennent la compétence en interne et contrôlent la prestation. Le test entièrement délégué sans preuve revient à la croyance de départ.

Un échec au test, ça arrive souvent ?

Aux premiers tests : très souvent — c'est précisément leur intérêt, et il n'y a aucune honte à découvrir un trou à froid. Périmètre incomplet, historique trop court, durée irréaliste et clé mal gardée sont les quatre troupilles classiques. Un échec de test est une réussite du processus : notez, corrigez, re-testez. Le seul vrai échec est celui découvert le jour du sinistre.

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 — 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