

LES BONNES PRATIQUES POUR BIEN SAUVEGARDER SES DONNÉES

PARTIE 2

Chiffrement des sauvegardes

Une sauvegarde non chiffrée peut exposer des informations sensibles en cas de perte, de vol ou d'accès non autorisé.

- Chiffrer toutes les sauvegardes, particulièrement celles conservées hors site ou dans l'infonuagique.
- Utiliser des algorithmes de chiffrement robustes, comme AES-256.
- Gérer et protéger les clés de chiffrement séparément des sauvegardes.
- Documenter la procédure de déchiffrement. Sans celle-ci, la sauvegarde pourrait devenir inutilisable.

Gestion des versions

- Conserver plusieurs versions d'un même fichier dans le temps.
- Définir une politique de rétention claire.

Par exemple :

- 7 jours de sauvegardes quotidiennes;
- 4 semaines de sauvegardes hebdomadaires;
- 12 mois de sauvegardes mensuelles.

→ Cette pratique permet notamment de récupérer des données altérées ou corrompues dont le problème n'est découvert que plusieurs jours ou semaines plus tard.

Erreurs fréquentes à éviter

- ✗ Sauvegarder uniquement sur le même appareil ou au même endroit.
- ✗ Ne jamais tester la restauration.
- ✗ Oublier de sauvegarder les configurations (pare-feu, serveurs, applications).
- ✗ Ne pas chiffrer les sauvegardes transportées ou conservées hors site.
- ✗ Ignorer les alertes d'échec des sauvegardes.
- ✗ Dépendre exclusivement d'une procédure manuelle.
- ✗ Conserver les clés de chiffrement au même endroit que les sauvegardes

Tester régulièrement la restauration



Une sauvegarde non testée est une fausse sauvegarde.

- Effectuer des tests de restauration complets au moins une fois par trimestre.
- Vérifier l'intégrité des fichiers à l'aide de sommes de contrôle.
- Simuler un scénario réel de sinistre.
- Documenter les résultats des tests.
- Mesurer l'objectif de temps de reprise (RTO), soit le temps réel nécessaire pour restaurer les données.

Protection contre les rançongiciels

- Maintenir des sauvegardes immuables, impossibles à modifier ou à supprimer pendant une période déterminée.
- Conserver une copie hors ligne complètement déconnectée du réseau.
- Activer le versionnage dans les solutions infonuagiques.

Documentation et procédures

Rédiger et maintenir à jour un plan de sauvegarde comprenant :

- les données sauvegardées et leur emplacement;
- les supports utilisés;
- la fréquence et le type de sauvegarde;
- les personnes responsables;
- la procédure de restauration détaillée.

De plus :

- intégrer les sauvegardes au Plan de reprise d'activité (PRA) ou au Plan de continuité des activités (PCA);
- former le personnel concerné;
- revoir régulièrement la documentation afin qu'elle demeure à jour.

RÉCAPITULATIF : CHECKLIST DE BASE

- | | |
|--|--|
| ☐ Règle 3-2-1 respectée | ☐ Politique de rétention définie et appliquée |
| ☐ Sauvegardes automatisées | ☐ Procédure de restauration documentée |
| ☐ Sauvegardes chiffrées | ☐ Responsable des sauvegardes identifié |
| ☐ Copie hors site ou infonuagique active | ☐ Alertes d'échec configurées et surveillées |
| ☐ Copie hors ligne disponible (protection rançongiciels) | |
| ☐ Test de restauration réalisé au cours des 90 derniers jours | |