La sauvegarde des données n'est pas seulement une mesure technique, c'est un enjeu stratégique pour la continuité des opérations et la résilience de votre entreprise. En cas d'incident ce sont souvent les sauvegardes qui font toute la différence.

Cette liste de contrôle a été conçue pour vous aider à évaluer rapidement la maturité de votre organisation en matière de sauvegarde et de protection des données.

Cochez Oui, Partiellement ou Non pour chaque action afin d'identifier vos points forts et les éléments à améliorer.

L'objectif : vous aider à mettre en place des pratiques de sauvegarde simples, efficaces et adaptées à votre réalité.

	Oui	Partiellement	Non
Couverture des données			
Les données critiques de l'entreprise sont clairement identifiées			
Les serveurs sont inclus dans la stratégie de sauvegarde			
Les postes de travail critiques sont sauvegardés			
Les données cloud (Microsoft 365, Google Workspace, etc.) sont incluses			
Les applications de travail (comptabilité, ERP, CRM, etc.) sont sauvegardées			
La règle du 3, 2, 1			
Au moins 3 copies des données existent			
Les sauvegardes sont stockées sur au moins 2 types de supports différents			
Au moins 1 copie est hors site (site distant ou cloud sécurisé)			
Isolation et sécurité			
Les sauvegardes ne sont pas accessibles depuis les systèmes de production			
Les comptes ayant accès aux sauvegardes sont limités et contrôlés			
Les sauvegardes ne sont pas accessibles avec les mêmes identifiants que les utilisateurs			
Les accès sont protégés par authentification forte (MFA)			
Immutabilité			
Les sauvegardes sont immuables (non modifiables et non supprimables sur une période définie)			
Les politiques d'immutabilité sont documentées et connues			
Chiffrement			
Les données sont chiffrées en transit			
Les données sont chiffrées au repos			
Les clés de chiffrement sont gérées de façon sécurisée			
Fréquence et rétention			
La fréquence des sauvegardes est adaptée à la criticité des données			
Les périodes de rétention sont clairement définies			
La rétention respecte les obligations légales ou sectorielles (si applicables)			
Test de restauration			
Des tests de restauration sont effectués régulièrement			
Les restaurations sont documentées			
Les délais de restauration sont connus (RTO)			
Les pertes de données acceptables sont définies (RPO)			

Préparé par Riopel Consultant. Cette liste de contrôle est fournie à titre informatif uniquement et ne remplace pas les conseils personnalisés d'un professionnel, chaque infrastructure et chaque entreprise présente des particularités propres. Toute reproduction, en tout ou en partie, à des fins commerciales est strictement interdite sans l'approbation préalable de Riopel Consultant.

www.riopel-consultant.com
info@riopel-consultant.com
1-866-6RIOPEL (1-866-674-6735)

Surveillance et alertes			
Les sauvegardes sont surveillées			
Des alertes sont générées en cas d'échec			
Quelqu'un est responsable de vérifier et corriger les échecs			
Responsabilités et documentation			
Un responsable des sauvegardes est désigné			
La stratégie de sauvegarde est documentée			
Les procédures de restauration sont accessibles			
La solution est revue périodiquement			

Notes personnelles

Préparé par Riopel Consultant. Cette liste de contrôle est fournie à titre informatif uniquement et ne remplace pas les conseils personnalisés d'un professionnel, chaque infrastructure et chaque entreprise présente des particularités propres. Toute reproduction, en tout ou en partie, à des fins commerciales est strictement interdite sans l'approbation préalable de Riopel Consultant.

www.riopel-consultant.com
info@riopel-consultant.com
1-866-6RIOPEL (1-866-674-6735)