



SOIPP



# Guide de sauvegarde ultime pour les entreprises:

**soyez toujours prêt !**

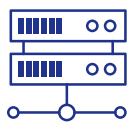
Une stratégie de cybersécurité robuste n'est pas une option, mais une nécessité. Quelle que soit la taille de votre entreprise, la protection de vos données, de votre infrastructure et de votre réputation est cruciale. Ce guide vous aidera à élaborer un plan de protection fiable pour protéger vos ressources numériques contre les pertes accidentelles, les cyberattaques ou les catastrophes naturelles.



## Élaborez un plan d'action

### Checklist d'une stratégie de sauvegarde professionnelle

- Identification des données critiques : déterminez quelles données sont les plus importantes pour votre entreprise.
- Choisissez les bons outils : sélectionnez les solutions de sauvegarde qui répondent aux besoins et au budget de votre entreprise.
- Appliquez la règle de sauvegarde 3-2-1 : assurez-vous que plusieurs copies de vos données soient stockées dans des lieux différents.
- Automatisez et surveillez : configurez des sauvegardes automatisées et une surveillance régulière.
- Testez régulièrement : effectuez des restaurations tests pour vous assurer de la fiabilité de vos sauvegardes.
- Sécurisez vos sauvegardes : chiffrez vos données et utilisez des mesures de sécurité renforcées.



## Les bases de la sauvegarde

Les sauvegardes de données sont votre première ligne de défense contre les attaques de ransomware, les suppressions accidentelles et les pannes système. L'une des bonnes pratiques est de suivre la règle de sauvegarde 3-2-1 :

- Conservez trois copies de vos données : une copie principale et deux copies de sauvegarde supplémentaires.
- Stockez deux copies sur différents supports : utilisez une combinaison de disques durs, de SSD et de stockage cloud.
- Conservez une copie hors site : stockez une sauvegarde dans un lieu sécurisé et distant pour vous protéger de tout dommage physique.
- En implémentant cette règle, vous réduisez les interruptions d'activité, maintenez la productivité et évitez les pertes financières dues aux défaillances matérielles, aux attaques par ransomware ou aux suppressions accidentelles.



## Élaborez une stratégie de sauvegarde pour votre entreprise

### Données clés à sauvegarder:

- Données client : informations, coordonnées et enregistrements des transactions.
- Documents financiers : factures, reçus et relevés bancaires.
- Informations confidentielles : secrets commerciaux, propriété intellectuelle et documents internes.

### Outils pour les entreprises:

- Solutions cloud : Acronis, Google Drive et Microsoft OneDrive proposent un stockage cloud évolutif et sécurisé.
- Serveurs de qualité professionnelle : les serveurs sur site fournissent des solutions de sauvegarde robustes et fiables.
- Systèmes hybrides : combinez le stockage cloud et le stockage physique pour une approche équilibrée.

### Automatisation et surveillance:

- Automatisez les sauvegardes : vos données sont ainsi sauvegardées automatiquement en continu sans intervention manuelle. Vous réduisez le risque d'erreur humaine et vos sauvegardes restent à jour.
- Surveillance : vérifiez régulièrement vos systèmes de sauvegarde pour vous assurer qu'ils fonctionnent correctement. Utilisez des outils de surveillance pour recevoir des alertes en cas d'échec d'une sauvegarde.



## Éviter les erreurs de sauvegarde les plus courantes

### Se baser sur une seule méthode:

- Risques : dépendre exclusivement du stockage cloud ou physique rend votre entreprise vulnérable. Le stockage cloud peut être compromis, et le stockage physique peut être endommagé ou perdu.
- Solution : utilisez une approche multicouche pour la sauvegarde, combinant stockage cloud et stockage physique.

### Oublier de tester vos sauvegardes:

- Risques : les sauvegardes irrécupérables fragilisent votre stratégie de sauvegarde.
- Solution : testez régulièrement vos sauvegardes pour vous assurer qu'elles sont effectivement récupérables. Effectuez des tests de restauration pour vérifier l'intégrité de vos données.

### Négliger la cybersécurité:

- Risques : des utilisateurs non autorisés pourraient accéder à vos sauvegardes non chiffrées.
- Solution : chiffrez vos données de sauvegarde et utilisez des mots de passe forts et uniques. Implémentez l'authentification multifacteur pour renforcer la sécurité.



## Conseils pour les restaurations d'urgence

### Que faire en cas de sinistre:

- Évaluer les dégâts : déterminez l'ampleur de la perte de données.
- Activer votre plan de sauvegarde : retrouvez la sauvegarde la plus récente et commencez le processus de restauration.
- Surveiller la restauration : assurez-vous de la restauration correcte des données et du fonctionnement de tous les systèmes.

### Collaborez avec votre MSP:

- Assistance de votre MSP (fournisseur de services managés): en tant que MSP, nous vous aiderons à restaurer vos données, de l'évaluation initiale à la restauration finale. Nous vous aiderons également à affiner votre stratégie de sauvegarde pour éviter toute future perte de données.



## Amélioration et formation continues

### Ayez toujours une longueur d'avance:

- Mettez régulièrement à jour votre plan de sauvegarde : il est important de revoir et d'actualiser votre stratégie de sauvegarde, car les technologies et les menaces continuent d'évoluer. Restez informé des dernières solutions de sauvegarde et des bonnes pratiques.

### Formation des collaborateurs:

- Sensibilisez votre équipe : veillez à ce que tous vos collaborateurs comprennent l'importance des sauvegardes et sachent comment utiliser les outils dédiés de manière efficace. Organisez régulièrement des sessions de formation pour que tout le monde soit informé et préparé.

### Commentaires et audits:

- Recueillez des commentaires : incitez vos équipes à donner leur avis sur les processus de sauvegarde. Leurs retours d'expérience peuvent vous aider à identifier les domaines à améliorer.
- Effectuez des audits réguliers : réalisez des audits régulièrement pour évaluer l'efficacité de votre stratégie de sauvegarde. Identifiez les éventuelles lacunes et apportez les ajustements nécessaires.



## **Votre entreprise est-elle à même de sauvegarder ses données efficacement ?**

**Faites notre test:**

- Sauvegardez-vous vos données au moins une fois par semaine ?
- Vos sauvegardes sont-elles automatisées ?
- Conservez-vous une copie de vos sauvegardes hors site ?
- Avez-vous élaboré un plan de sauvegarde ?
- Testez-vous régulièrement vos sauvegardes ?
- Avez-vous mis en place une formation à la cybersécurité pour vos collaborateurs ?
- Si vous avez un plan de sauvegarde, est-il mis à jour régulièrement ?

**Si vous avez répondu « Non » à l'une de ces questions, vos données sont en danger. Contactez-nous dès aujourd'hui pour obtenir de l'aide et vous assurer que votre entreprise est parée à toute éventualité.**



**N'attendez pas d'avoir subi une perte de données pour apprécier l'importance des sauvegardes.** Protégez les données de votre entreprise dès aujourd'hui !  
Contactez-nous pour obtenir l'aide ou les conseils de nos experts.

**SOIPP**

Email : [contact@soipp.com](mailto:contact@soipp.com)

Téléphone : +33494302080

<https://www.soipp.com>