LE GUIDE POUR LES TPE/PME

Sauvegardez et restaurez vos données en toute sécurité



Hexatel

SOMMAIRE

Sauvegardez et restaurez vos données en toute sécurité

01 La sauvegarde, une nécessité trop souvent négligé — p3

02 Les principales causes des pertes de données — p4

03 Quels impacts pour votre activité ? — p6

04 Les bases de la sauvegarde — p7

05 Les différents types de sauvegarde — p8

06 Les bonnes pratiques à adopter — p10

07 La méthode 3-2-1-1-0 — p11

08 Comment récupérer ses données après un incident ? — p13

09 Faire appel à un prestataire IT — p14

LA SAUVEGARDE, UNE NÉCESSITÉ TROP SOUVENT NÉGLIGÉ

Dans une entreprise, les données constituent la mémoire vivante de votre activité : coordonnées clients, devis, facture, contrats, plannings, outils internes... Sans ces informations, il devient rapidement difficile de poursuivre le travail dans de bonnes conditions.

Pour une TPE ou une PME, les données représentent à la fois un véritable moteur de croissance et une source de fragilité. Elles permettent de mieux connaître ses clients et de prendre des décisions éclairées. Mais cette dépendance au numérique expose aussi l'entreprise à différents risques : une panne, une erreur de manipulation ou une cyberattaque peuvent perturber, voire dans les cas les plus graves, à interrompre totalement l'activité.

Beaucoup de dirigeants de TPE/PME savent que leurs données sont précieuses, mais pensent encore que les pertes de données restent rares ou qu'elles ne concernent que les grandes entreprises. En réalité, c'est souvent l'inverse : les TPE/PME sont particulièrement exposées, car elles disposent généralement de moins de ressources pour anticiper et se protéger contre ces incidents.

Selon plusieurs études :



40%
des PME ont déjà perdu des données critiques

1/2
PME ne réalise pas de sauvegarde régulière

23
jours de délai en moyenne pour récupérer ses données après une attaque

16% des TPE-PME françaises ont déclaré au moins un incident informatique au cours des 12 derniers mois

Cybermalveillance, FranceNum

LES PRINCIPALES CAUSES DES PERTES DE DONNÉES

01 L’erreur humaine

C’est la cause la plus fréquente de perte de données, et souvent la plus sous-estimée. Une suppression accidentelle d’un dossier ou un copier/coller mal placé peuvent effacer des fichiers essentiels. Dans les petites structures, où plusieurs collaborateurs partagent les mêmes postes ou dossiers, ce type d’erreur est d’autant plus courant.

02 Les pannes matérielles

Aucun équipement informatique n’est totalement infaillible. Disques durs, serveurs ou ordinateurs possèdent tous une durée de vie limitée. Une panne matérielle, qu’elle soit liée à un disque défectueux, à un composant endommagé, à une surchauffe ou à de l’usure naturelle, peut entraîner la perte immédiate des données. Dans les TPE et PME, où les moyens techniques sont souvent limités, la défaillance d’un seul équipement peut rapidement bloquer l’ensemble de l’activité.

03 Les cyberattaques et les ransomwares

Les cyberattaques constituent aujourd’hui l’une des principales causes de perte de données pour les entreprises. Ransomwares, phishing ou intrusions malveillantes peuvent entraîner le chiffrement, la suppression ou le vol d’informations critiques en quelques minutes. Les TPE/PME sont particulièrement exposées, car elles disposent souvent de protections de sécurité moins avancées et de ressources internes limitées pour détecter et réagir rapidement aux incidents. Une seule attaque peut alors suffire à compromettre l’activité, la continuité des services et la confiance des clients.

LES PRINCIPALES CAUSES DES PERTES DE DONNÉES

04 Les sinistres et incidents physiques

Un incident matériel ou environnemental peut également détruire vos données du jour au lendemain. Un incendie, un dégât des eaux, une surtension électrique ou même un vol d'équipement peuvent mettre HS vos supports de stockage locaux. Ces événements sont imprévisibles et souvent dévastateurs, notamment lorsqu'aucune copie des données n'est conservée hors des locaux de l'entreprise. En cas de sinistre, seules les sauvegardes externalisées (dans le cloud ou sur un autre site) permettent de relancer rapidement l'activité.

05 Les incidents techniques ou logiciels

Une mise à jour défectueuse, un bug logiciel ou une mauvaise configuration d'un système peut provoquer une corruption de fichiers ou la disparition de certaines données. Dans les environnements informatiques peu supervisés, ces incidents peuvent passer inaperçus jusqu'à ce que les données soient déjà compromises.

QUELS IMPACTS POUR VOTRE ACTIVITÉ ?

Outre le désagrément technique, la perte de données peut avoir de nombreuses conséquences. Une entreprise qui n'a plus accès à aucunes données se retrouve paralysée.



Les équipes ne peuvent plus travailler correctement

Les collaborateurs n'ont plus accès aux fichiers nécessaires pour accomplir leurs tâches : devis, factures, plannings, dossiers clients ou documents partagés. Certaines tâches devient impossible à réaliser.



Les clients s'impatientent et perdent confiance

Si les clients ne reçoivent pas leurs produits ou leurs réponses dans les temps, la relation de confiance peut être fragilisée. Les clients risquent de se tourner vers la concurrence et la réputation de votre entreprise sera entachée.



Les délais s'allongent et les ventes chutent

La facturation est bloquée, les commandes sont suspendues et les projets prennent du retard. Vos équipes doivent consacrer du temps à retrouver ou recréer des fichiers, au lieu de se concentrer sur leurs missions principales.



Vous perdez de l'argent et vous risquez des sanctions

Le ralentissement de votre activité et la plus faible productivité de vos équipes impacte directement votre chiffre d'affaires. Ces perturbations peuvent rapidement peser sur la trésorerie, d'autant plus que d'éventuelles sanctions réglementaires peuvent également s'ajouter.

Dans les cas les plus grave, la perte de données peut conduire à une interruption temporaire ou définitive de l'activité de l'entreprise. Selon la Fédération du E-commerce et de la Vente À Distance (FEVAD), **60% des PME qui subissent une perte massive de données ferment dans les 6 mois.**

LES BASES DE LA SAUVEGARDE

Avant de choisir une solution de sauvegarde, il est essentiel de comprendre ce qu'est réellement une sauvegarde et pourquoi elle est indispensable. Trop d'entreprises confondent encore la sauvegarde avec le simple stockage de fichiers ou la synchronisation dans le cloud.

Qu'est ce qu'est une sauvegarde ?



Une sauvegarde consiste à créer une copie des données importantes de l'entreprise et à la stocker dans un emplacement distinct de celui des données originales. L'objectif est simple : **pouvoir les restaurer en cas de perte, de corruption, de vol ou d'attaque.**

Contrairement à un simple transfert ou à un espace de stockage (comme un disque externe ou un service de partage en ligne), **une sauvegarde est automatisée, régulière et sécurisée.** Elle n'est pas une solution de confort, mais une assurance de continuité d'activité.

Les 3 piliers fondamentaux d'une sauvegarde

La sécurité

Les données doivent être chiffrées et protégées contre tout accès non autorisé. Une sauvegarde non sécurisée est aussi vulnérable qu'un document laissé sur le bureau

La redondance

Une seule copie ne suffit pas à garantir une sauvegarde efficace. Il faut multiplier les emplacements (local et distant) pour se prémunir des pannes ou sinistres

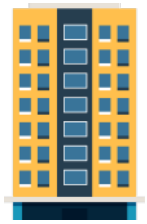
L'accessibilité

La sauvegarde doit pouvoir être restaurée rapidement. Il est inutile d'avoir une copie parfaite si elle est inaccessible au moment où l'entreprise en a besoin.

Une stratégie de sauvegarde solide,
c'est la garantie que votre activité ne s'arrête jamais.

LES DIFFÉRENTS TYPES DE SAUVEGARDE

Selon le lieu où les données sont sauvegardées



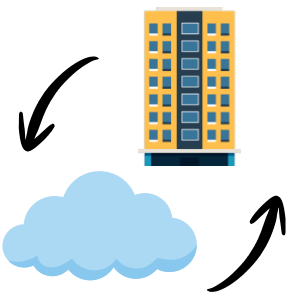
La sauvegarde locale

La sauvegarde locale se fait sur un support situé dans l'entreprise : serveur NAS ou disque dur externe par exemple. Elle permet une restauration rapide, mais reste vulnérable aux incidents physiques (vol, incendie, dégât des eaux...) La sauvegarde sur site est une bonne solution pour les TPE/PME, à condition d'être complétée par une copie externe ou cloud.



La sauvegarde externalisée (cloud ou hors site)

ici, les données sont copiées dans un datacenter ou dans le cloud. Cette solution protège mieux contre les sinistres locaux et permet d'accéder aux données même en cas de problème dans les locaux de l'entreprise. En cas de problème, la restauration est possible depuis n'importe où, à condition d'avoir une connexion Internet. Ce mode de sauvegarde est particulièrement adapté pour les TPE et PME car c'est une solution clé en main, fiable et sans contrainte technique.

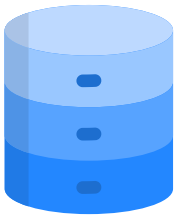


La sauvegarde hybride

La sauvegarde hybride combine les deux modes de sauvegarde présentés précédemment : une sauvegarde locale et une sauvegarde externalisée. Les données sont d'abord copiées en local pour garantir un accès rapide et une restauration immédiate en cas de problème mineur (panne d'un poste, fichier supprimé, etc.). En parallèle, une copie complète est envoyée automatiquement vers un espace distant, afin d'être protégée contre les risques de vol, incendie, dégât des eaux, cyberattaque... Ce modèle offre un niveau de protection plus élevé.

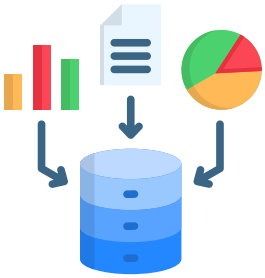
LES DIFFÉRENTS TYPES DE SAUVEGARDE

Selon l'étendue des données sauvegardées



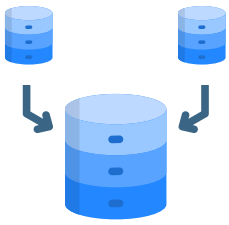
La sauvegarde complète

Elle consiste à copier l'ensemble des données à sauvegarder à chaque opération. C'est la méthode la plus simple et la plus fiable pour restaurer des fichiers, mais elle demande plus d'espace de stockage et plus de temps



La sauvegarde incrémentielle

Après une première sauvegarde complète, la sauvegarde incrémentielle enregistre uniquement les données modifiées depuis la dernière sauvegarde effectuée, qu'elle soit complète ou incrémentielle. Cette méthode est rapide et peu gourmande en stockage mais la restauration peut être un peu plus complexe.



La sauvegarde différentielle

Cette méthode se rapproche de la sauvegarde incrémentielle mais ne prend en compte que les sauvegardes complètes. En effet, la sauvegarde différentielle enregistrement toutes les données modifiées depuis la dernière sauvegarde complète. Cette méthode est plus rapide qu'une sauvegarde complète et plus simple à restaurer q'une sauvegarde incrémentielle. En revanche, elle utilise plus d'espace au fil du temps.

Pour les TPE-PME, la bonne pratique consiste souvent à combiner plusieurs méthodes de sauvegarde, par exemple une sauvegarde automatisée locale complétée par une sauvegarde externalisée. Cela permet de limiter les risques et de garantir une restauration rapide des données en cas d'incident.

LES BONNES PRATIQUES DE SAUVEGARDE

Définir une politique de sauvegarde claire

Déterminer quelles données doivent être sauvegardées, à quelle fréquence et sur quels supports.

Une politique claire permet d'éviter les oublis et de prioriser les données réellement critiques.

01





02

Automatiser les sauvegardes

En programmant vos sauvegardes à intervalles réguliers, vous éliminez le risque d'oubli humain.

Vous gagnez ainsi en sérénité et en constance, tout en assurant la continuité de votre protection.

Vérifier et tester les sauvegardes

Il est indispensable de tester régulièrement vos sauvegardes pour s'assurer que les fichiers sont complets, lisibles et exploitables

Le test peut être partiel ou total

03





04

Sécurisez les accès et le stockage

Il est crucial de chiffrer les données sauvegardées et de limiter les accès aux seules personnes autorisées.

Mots de passe forts, authentification à deux facteurs...

Documenter et former les équipes

En cas d'absence ou de départ d'un salarié, cette documentation garantit la continuité du processus

Une entreprise bien formée est plus réactive face aux incidents

05



LA MÉTHODE 3-2-1-1-0

La méthode 3-2-1-1-0 est aujourd'hui considérée comme une bonne pratique de référence pour sécuriser les sauvegardes de données. Elle repose sur 5 principes simples :



01 3 copies de données

Il est recommandé de disposer d'au mois trois copies de ses données : les données de production (celles utilisées au quotidien) et deux copies de sauvegarde. Si un fichier est corrompu ou supprimé, il reste ainsi toujours plusieurs versions disponibles pour le restaurer

02 2 supports de stockage différents

Les sauvegardes doivent être stockées sur au moins deux types de supports différents. Par exemple un serveur interne et ou stockage cloud. L'objectif est d'éviter qu'un même problème technique (panne de disque, défaillance matérielle...) n'affecte pas toutes les copies simultanément.

03 Une copie externalisée

Au moins une sauvegarde doit être stockées hors site (dans le cloud ou dans un autre lieu physique). Cette précaution protège l'entreprise contre des incidents majeurs comme : un incendent, un dégât des eaux, un vol de matériel, un catastrophe dans les locaux.

LA MÉTHODE 3-2-1-1-0

04 Une copie immuable ou hors ligne

La méthode ajoute ensuite une copie immuable ou déconnectée du système principal.

Une sauvegarde immuable signifie qu'elle ne peut pas être modifiée ni supprimée pendant une période définie. Cela permet de se protéger contre les cyberattaques de type ransomware, qui cherchent souvent à chiffrer ou supprimer les sauvegardes avant d'attaquer les données.

Cette copie peut être stockée dans un cloud avec fonction d'immutabilité ou conservée sur un support hors ligne (non connecté en permanence au réseau).

05 Pas de problème de sauvegarde

Le dernier principe consiste à s'assurer que les sauvegardes fonctionnent réellement. Pour cela, il est essentiel de vérifier régulièrement l'intégrité des sauvegardes et de tester les procédures de restauration.

L'objectif est d'atteindre zéro erreur lors des tests de récupération, afin d'être certain que les données pourront être restaurées rapidement en cas d'incident.

COMMENT RÉCUPÉRER SES DONNÉES APRÈS UN INCIDENT

Lorsqu'un incident survient, la priorité pour l'entreprise est de retrouver rapidement l'accès à ses données afin de reprendre son activité dans les meilleures conditions. C'est précisément le rôle d'une stratégie de sauvegarde bien pensée.

01 Identifier l'origine de l'incident

La première étape consiste à identifier l'origine de l'incident et l'étendue des données impactées. Cela permet de déterminer quelle sauvegarde utiliser et d'éviter de restaurer des fichiers potentiellement corrompus ou infectés.

02 Procéder à la restauration

Une fois le diagnostic posé, l'entreprise peut procéder à la restauration des données à partir d'une sauvegarde récente.

Les solutions de sauvegarde modernes permettent souvent de restaurer les données rapidement afin de limiter l'interruption de l'activité. Certaines offrent également la possibilité de redémarrer temporairement un serveur directement depuis la sauvegarde, le temps de remettre en service l'infrastructure principale. Il est toutefois important de comprendre que la capacité de récupération dépend directement de la qualité de la stratégie de sauvegarde mise en place en amont.

03 Analyser les causes de l'incident

Après la restauration, il est recommandé de bien analyser les causes de l'incident et de renforcer vos mesures de protection afin d'éviter qu'une situation similaire ne se reproduise à l'avenir. Mettre en place des sauvegardes automatisées et une supervision des systèmes font partie des bonnes pratiques à envisager pour sécuriser durablement les données de l'entreprise.

FAITES APPEL À UN PRESTATAIRE EXTERNE

De nombreuses TPE et PME gèrent elles-mêmes l'hébergement et la sauvegarde de leurs données, souvent par manque de ressources ou par méconnaissance des risques. Elles considèrent que la sauvegarde est simple ou que faire appel à un prestataire serait trop coûteux. Pourtant, la perte de données est un **problème fréquent** : erreurs humaines, pannes matérielles, cyberattaques ou sinistres physiques peuvent rapidement interrompre l'activité, retarder les projets, nuire aux ventes et affecter la réputation de l'entreprise.

Pour rappel, **80 % des entreprises ont déjà subit au moins une fois une perte de données** et que 40 % des PME ont déjà été affectées par une attaque informatique ou un incident critique.

Faire appel à un prestataire spécialisé permet de **sécuriser ses données** de manière simple et fiable, de **bénéficier de solutions automatisées et testées**, et de **garantir une restauration rapide** en cas de problème. C'est aussi un moyen de profiter de l'expertise d'un professionnel en sécurité et conformité, tout en gagnant du temps, en réduisant les risques et en assurant sa continuité d'activité.

6 bonnes raisons pour externaliser votre sauvegarde

Plus de temps pour se concentrer sur son coeur de métier	Une restauration des données rapide en cas d'incident	Évite les investissements lourds
Une sécurité maximale des données	Une meilleure continuité d'activité	Un accompagnement en cas de crise

Hexatel

Un projet ? Une question ?

Nos équipes sont là pour vous accompagner à chaque étape de vos projets télécoms, réseaux et informatiques.

Contactez-nous sur notre site internet