

TRANSFORMATION NUMÉRIQUE

Sauvegarde et résilience

Sauvegarde et résilience



Une fois que vous avez adopté les différents produits et services sur site et cloud abordés précédemment, il est essentiel de définir la manière dont vous allez protéger ces données en cas de catastrophes ou d'autres incidents qui les mettraient en danger. L'établissement d'une entreprise résiliente commence par vos systèmes d'information.

Les sauvegardes doivent être considérées comme un élément de votre stratégie globale de cybersécurité et de résilience. Trop souvent, les entreprises ne pensent pas assez à une protection solide des données par le biais de sauvegardes. Pourtant, ces dernières constituent le moyen le plus fondamental dont disposent les entreprises pour protéger leurs systèmes d'information et leurs données.

En cas de catastrophe, votre dernière ligne de défense est votre sauvegarde ! Qu'il s'agisse d'une catastrophe naturelle telle qu'un ouragan ou une éruption volcanique ou d'un incident d'origine humaine où vos données sont compromises ou rendues inaccessibles, votre sauvegarde, de par sa nature, vous fournit une copie autonome de vos données que vous pouvez utiliser pour redémarrer votre activité.

Cela est de plus en plus important à mesure que le monde évolue vers une ère plus mobile ou de télétravail, ce qui signifie que les entreprises déploient des applications cloud pour la productivité et les processus opérationnels.

Les produits Software as a Service (SaaS) basés sur le cloud sont généralement négligés, car ils sont souvent exploités dans des lieux hautement sécurisés et ne sont pas soumis aux risques naturels que nous connaissons habituellement dans les Caraïbes. Ce n'est pas le cas, comme le montre le tableau suivant fourni par Microsoft :

Sauvegarde et résilience

	Responsabilité	SaaS	PaaS	IaaS	Sur site
La responsabilité est toujours conservée par le client	Informations et données	Client	Client	Client	Client
	Appareils (mobiles et PC)	Client	Client	Client	Client
	Comptes et identités	Client	Client	Client	Client
La responsabilité varie selon le type	Infrastructure d'identité et d'annuaire	Partagée	Partagée	Client	Client
	Applications	Microsoft	Partagée	Client	Client
	Contrôles du réseau	Microsoft	Partagée	Client	Client
	Système d'exploitation	Microsoft	Microsoft	Client	Client
La responsabilité est transférée au fournisseur de services cloud	Hôtes physiques	Microsoft	Microsoft	Microsoft	Client
	Réseau physique	Microsoft	Microsoft	Microsoft	Client
	Centre de données physique	Microsoft	Microsoft	Microsoft	Client

 Microsoft
  Client
  Partagée

Source : [Microsoft](#)

Les données, les appareils (PC et smartphones) et les comptes sont sous votre entière responsabilité. En ce qui concerne les données, cela implique également qu'il est de votre responsabilité de veiller à ce qu'elles soient protégées contre la perte.

Pour les données stockées localement, la règle suivante est considérée comme la meilleure pratique :

La règle « 3-2-1 » :

Trois copies des données doivent être stockées sur **deux** types de supports, dont au moins **un** situé hors site.

Adressez-vous à vos spécialistes informatiques locaux qui peuvent vous fournir le matériel et l'expertise nécessaires pour sauvegarder vos données en toute sécurité.

Sauvegarde et résilience



Suivez les étapes ci-dessus pour concevoir et mettre en œuvre un plan de sauvegarde résilient.

1. Faites l'**inventaire** des ordinateurs et des autres appareils connectés au réseau (imprimantes, disques, routeurs, etc.). Faites l'inventaire de tous les logiciels utilisés, tels qu'Office, Photoshop, Quickbooks, etc., ou de tout autre logiciel utilisé dans le cadre des activités de votre entreprise. Notez le fournisseur, la date d'achat, la date de fin de garantie, le coût et la durée de vie prévue.
2. **Évaluez les risques** en utilisant le modèle fourni dans la section relative aux ressources de ce site. L'évaluation déterminera quelles parties du système informatique sont les plus vulnérables et donc les plus importantes à sauvegarder pour assurer la résilience.
3. **Définissez les objectifs de point et de délai de récupération** (voir l'encadré sur les définitions). Attention, des objectifs plus courts sont plus complexes et plus coûteux à mettre en œuvre !
4. **Définissez votre politique de sauvegarde** en utilisant comme point de départ le modèle fourni dans la section relative aux ressources de ce site.
5. **Mettez en œuvre votre stratégie de sauvegarde** conformément à la politique que vous avez définie. N'hésitez pas à faire appel à un expert local pour vous aider à la mettre en place. Contrôlez régulièrement vos sauvegardes pour vous assurer de leur bon fonctionnement.
6. **Réviser votre politique de sauvegarde tous les 6 mois** ou si vous apportez une modification majeure au logiciel ou au matériel utilisé dans l'entreprise. Par exemple, si vous changez de logiciel de comptabilité, vous devez réviser votre politique dans le cadre de la procédure de changement de logiciel afin de garantir la résilience de vos sauvegardes.

Utilisez le modèle de plan de sauvegarde des données fourni dans les ressources pour élaborer votre plan. Adapté de [ce site](#) (en anglais), qui comprend des instructions supplémentaires.

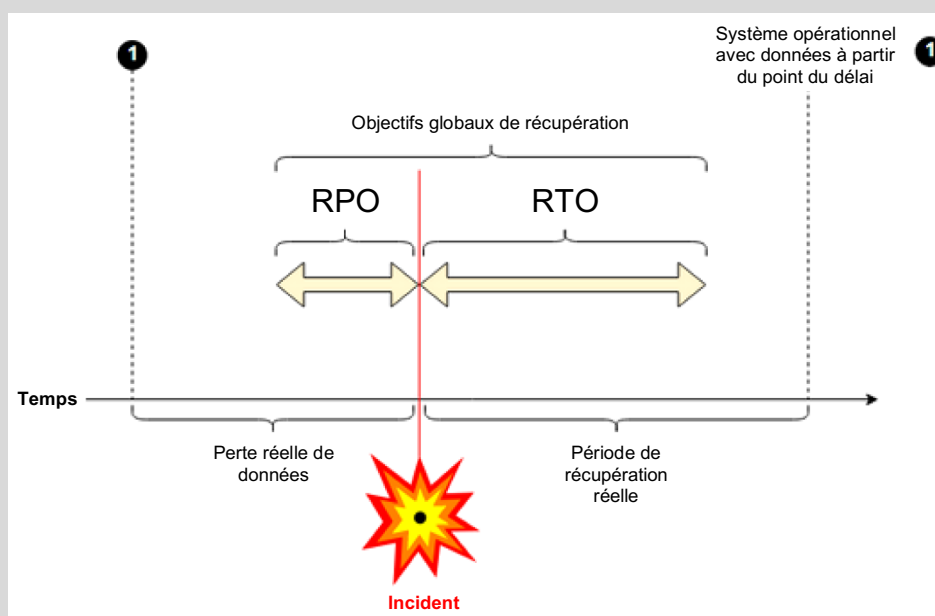
Sauvegarde et résilience

ENCADRÉ 1 : définitions

Politique de sauvegarde : les procédures et les règles visant à garantir que les données de l'entreprise sont sauvegardées et sécurisées de manière adéquate. Elle définit le type de sauvegardes, la fréquence et l'historique des sauvegardes accessibles en cas de catastrophe.

Objectif de point de récupération (RPO) : le RPO est le point maximum acceptable auquel les données peuvent être perdues. Par exemple, si des données peuvent être perdues pendant un jour, mais pas pendant deux jours, le RPO doit être fixé à un jour.

Objectif de délai de récupération (RTO) : le RTO est le délai maximum acceptable pour exécuter le processus de récupération afin de garantir que l'entreprise soit opérationnelle après une catastrophe.



Source : [Wikipédia](#)

Sauvegarde incrémentielle : ce type de sauvegarde ne contient que les fichiers modifiés depuis la dernière sauvegarde incrémentielle ou complète. Elle permet d'effectuer des sauvegardes plus rapidement, mais peut nécessiter plus de temps pour la récupération.

Sauvegarde complète : une sauvegarde unique qui contient toutes les données sélectionnées pour la sauvegarde.

Sauvegarde différentielle : une sauvegarde cumulative des données modifiées depuis la dernière sauvegarde complète. Elle est utilisée pour effectuer des sauvegardes plus rapidement, mais peut allonger le délai de récupération complète des données.