GUIDE PRATIQUE

La sauvegarde de données : une assurance incontournable

INFORSUD
TECHNOLOGIES
Solutions et impulsions pour l'avenir

Il ne viendrait à l'idée d'aucun automobiliste responsable de rouler sans assurance tant les risques sont importants. En matière de sauvegarde de données, le principe est le même : dans une économie digitalisée, comment peut-on imaginer un système d'information sans le moindre filet de sécurité ?

S'il est toujours possible de reconstituer un système d'information (matériels et logiciels) en cas d'incident majeur ou suite à une attaque, les données perdues le seront définitivement.

- Quelles sont les risques et les conséquences potentielles d'une perte de données ?
- Comment mesurer la valeur de ses données et définir sa stratégie de sauvegarde ?
- Comment faire les bons choix dans un objectif bénéfices / risques adapté à son contexte ?
- Sur quels critères baser son plan de restauration des données ?

Ce guide pratique a pour objectif de vous aider à faire les bons choix en matière de sauvegarde et de restauration de vos données, que vous optiez pour une stratégie interne ou déléguée auprès d'un prestataire informatique.

Pourquoi sauvegarder ses données informatiques ?

Dans le contexte d'un monde toujours plus digitalisé, les données hébergées ou transitant dans le système d'information font partie intégrante du capital des organisations, privées comme publiques. Elles doivent dès lors faire l'objet d'une analyse et d'une gestion des risques, au même titre que tout autre actif.

Les enjeux associés aux données

Face à cette dépendance aux données, les organisations sont soumises à deux dangers majeurs :

- **La perte de données :** en raison de suppressions volontaires ou involontaires, de corruption criminelle (attaques) ou accidentelle (panne ou pertes des supports de stockage, sinistre, etc.)
- **L'atteinte à l'intégrité des données :** c'est le risque d'altération des données. Assurer l'intégrité des données, c'est se donner les moyens de garantir l'exhaustivité, la précision, l'exactitude et la validité des données durant tout leur cycle de vie.

Les principales conséquences de la perte ou d'une atteinte à l'intégrité d'une donnée

- Temps de travail perdu des collaborateurs.
- Atteinte à l'image de marque.
- Erreurs de processus, sur les chaînes de production, sur les commandes, sur les factures, etc.
- Arrêts de production.
- Perte d'informations clés : commerciales (fichier prospects / clients), administratives et financières (comptabilité, contrats…).
- Disparition ou dégradation de connaissances, savoir-faire, de secrets de fabrication, etc.

Si la majorité des organisations se relèveront facilement de quelques heures de travail perdues, les conséquences financières d'une perte de données critiques peuvent s'avérer importantes, peuvent conduire à la fragilisation à plus ou moins court terme de l'organisation, voire à des cessations d'activité.

BON À SAVOIR

Ne pas confondre sauvegarde, archivage et rétention

La sauvegarde est la réplication d'une donnée sur un support (bande, disque, cloud) pour la restaurer en cas de besoin.

L'archivage combine la suppression d'une donnée de son emplacement initial et la conservation de cette donnée à un autre emplacement, afin de pouvoir la retrouver sans encombrer l'outil principal. Exemple : l'archivage de données comptables de plus de 5 ans permet d'alléger l'ERP, mais de retrouver la donnée au besoin.

À noter que l'archivage peut lui-même disposer… d'une sauvegarde !

Rétention : c'est le temps de conservation d'une donnée « supprimée » dans un outil spécifique, sans qu'elle le soit réellement. C'est le principe de la « corbeille » : avant qu'elle ne soit vidée, il est possible de restaurer les données qui y ont été déposées. Dans la plupart des cas, il est possible de configurer manuellement la durée de rétention.

Attention : la rétention ne doit pas être confondue avec « le temps de rétention légale » d'une donnée (en principal ou archivée). Exemple : 5 ans pour des documents à portée fiscale.

À RETENIR

- **Le système d'information et ses données sont aujourd'hui au cœur du bon fonctionnement des organisations, privées ou publiques.**
- **La perte ou l'inaccessibilité à des données peut entraîner des conséquences plus ou moins graves pour les organisations.**

Données : criticité, cartographie et temporalité

Toutes les données n'ont pas la même valeur ni la même criticité dans le temps. Pour autant, toute perte, aussi mineure soit-elle, est préjudiciable pour l'organisation.

C'est la raison pour laquelle il est impératif de sauvegarder la quasi-totalité des données critiques et /ou fonctionnelles évoluant au sein du système d'information :

- **Les données de travail :** fichiers bureautiques, fichiers clients, données d'applications métiers, e-mails, etc.
- **Les données de la DSI** (souvent oubliées) : les données d'Active Directory* sont, par exemple, essentielles car en cas de problème, l'absence d'annuaire utilisateurs et de leurs droits associés est au moins aussi perturbante pour l'activité que la perte d'informations métiers.

En revanche, les systèmes et tout ce qu'il est possible de retrouver facilement ou de télécharger (système d'exploitation, logiciel…) n'ont aucunement vocation à être sauvegardés, à l'inverse des éventuelles données de configuration.

La cartographie granulaire des données

Dans une organisation, chaque direction, chaque métier et chaque processus dispose de ses propres spécificités, besoins et contraintes. Dès lors, les risques, et surtout les conséquences, d'une perte de données sont très variables.

Il peut être tentant de considérer que toutes les données sont critiques et de leur appliquer les mêmes modalités de sauvegarde, selon le principe de « qui peut le plus peut le moins ». Mais le rapport coût-efficacité par rapport aux risques n'est pas équilibré.

Il est donc indispensable de réaliser une cartographie détaillée des données pouvant aller jusqu'à chaque machine et même chaque processus avant de déployer une politique de sauvegarde.

Le temps, élément de valeur de la donnée

La valeur d'une donnée peut fortement varier dans le temps, en fonction des cas d'usage dans lesquelles elle est appelée.

Par exemple, dans un système de monitoring, une donnée n'a de valeur qu'immédiatement et pour un temps court. Au contraire, un système de reporting financier a besoin de s'appuyer sur des données d'historique sur un temps long.

Dans tous les cas, la question à se poser pour chaque donnée est la suivante : **quelle quantité de données l'organisation est-elle en mesure de perdre sans risque majeur ?** La réponse à cette question va permettre de définir la fréquence des sauvegardes.

La fréquence des sauvegardes

La fréquence des sauvegardes dépend directement de la criticité des processus concernés. Par exemple, un site web vitrine, même lorsque des publications y sont régulièrement postées, n'a pas les mêmes contraintes qu'un site de vente en ligne, pour lequel la perte de données de commandes a un impact direct sur le chiffre d'affaires, sur l'image de l'entreprise, etc.

Pour les données les moins critiques, une sauvegarde quotidienne est conseillée. Pour les autres cas, la fréquence peut varier de quelques heures à quelques minutes, voire à une sauvegarde en temps réel. Et selon des modalités à spécifier selon l'organisation : copies distantes natives, sauvegardes en local puis centralisées la nuit, etc.

À RETENIR

- **Toutes les données, qu'elles soient critiques et fonctionnelles (hors fichiers systèmes et logiciels) ont vocation à être sauvegardées.**
- **A minima, une sauvegarde quotidienne est conseillée.**
- **La fréquence de sauvegarde est directement liée aux implications qu'engendre une perte de données entre deux sauvegardes.**

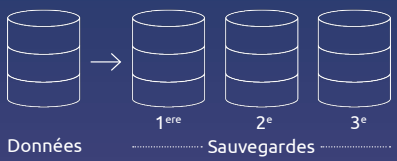
*Active Directory : service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.

BON À SAVOIR

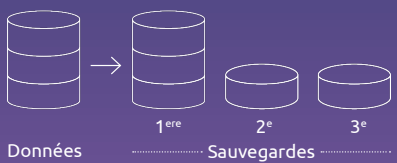
Faut-il sauvegarder tout, tout le temps ?

Les quantités colossales de données présentes dans les systèmes d'information impactent fortement la durée pour réaliser une sauvegarde. En fonction des usages, des périodes et de l'activité, une sauvegarde peut être complète, incrémentielle et différentielle.

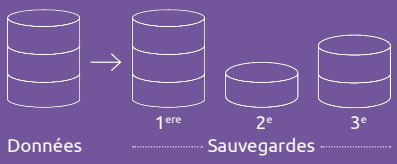
Sauvegarde complète : copie totale des données dans un nouvel espace de sauvegarde.



Sauvegarde incrémentielle : enregistre les données créées ou modifiées depuis la dernière incrémentielle. La restauration est complexe et longue car chaque incrémentielle est traitée individuellement.



Sauvegarde différentielle : enregistre les données créées et modifiées depuis la dernière sauvegarde complète et les cumule. Plus gourmande en espace mais plus simple et rapide à restaurer.



La sauvegarde externalisée : l'indispensable assurance des données

Comment sauvegarder les données ? Quels choix opérer pour obtenir les meilleures garanties de couverture de risque de perte de données ou d'altération de leur intégrité au meilleur coût ?

Où sauvegarder ses données ?

- **Sauvegarde locale, dans le même bâtiment :** c'est le choix le plus simple mais aussi le plus risqué en cas de sinistre (incendie, dégât des eaux, etc.) car les données d'origine et leur sauvegarde peuvent disparaitre ou être détruites en même temps.
- **Sauvegarde locale, sur site (ou bâtiment) distinct :** l'absence de risque physique est ici remplacée par le risque logique, si les deux sites sont connectés. En effet, certaines cyberattaques sont capables d'utiliser les protocoles de transfert de fichiers, pour infecter les deux sites.
- **Sauvegarde externalisée :** déconnectée du site principal de stockage de la donnée, elle est le seul moyen de garantir l'intégrité des données sauvegardées. Ce qui inclut également les sauvegardes dans le Cloud, qui utilisent des protocoles de transfert propriétaires, qui en garantissent la sécurité.

Quels supports de sauvegarde ?

- **Sauvegarde sur bande :** malgré l'apparition de nombreuses autres technologies, l'écriture de données sur bande reste de loin la plus rapide et la plus robuste.
- **Disque dur mécanique :** c'est l'un des supports les plus économiques, mais l'écriture y est plus lente.
- **Disque flash :** le coût sensiblement élevé (environ 4 à 6 % plus cher au Go qu'un disque dur mécanique) de la technologie flash dissuade aujourd'hui de son utilisation. Néanmoins, sa rapidité d'accès aux données, sa durée de vie, sa stabilité ou encore sa consommation énergétique pourraient inverser cette tendance.

La responsabilité des sauvegardes

Véritable assurance tous risques pour l'organisation et sa résilience en cas de problème, la sauvegarde s'accompagne d'un **suivi permanent**, pour s'assurer de sa bonne réalisation :

- **Responsabilité interne :** sur site, il s'agit de s'assurer du bon déroulement de la sauvegarde sur le support retenu. En distanciel (dans le Cloud par exemple), le suivi des e-mails d'informations ou d'alertes doit être assuré quotidiennement.
- **Responsabilité déléguée :** dans le cadre d'un contrat de sauvegarde externalisée, la responsabilité de la gestion peut porter sur le prestataire, afin de limiter les risques de négligence. **Attention toutefois à faire appel à un prestataire en mesure de s'imposer une obligation de résultats (et pas seulement de moyens).**

POINT DE VIGILANCE

La question des débits (et des coûts) Internet

Face aux volumes toujours plus importants de données présentes dans les systèmes d'information, les débits réseaux peuvent compliquer les sauvegardes. Sachant par exemple qu'une sauvegarde incrémentielle porte en moyenne sur 10 % de la totalité des données d'une organisation.

En matière de réseaux professionnels, la fracture numérique est essentiellement pécuniaire. Quelle que soit sa localisation, une organisation pourra toujours bénéficier de réseaux haut débit, mais :

- Les coûts de raccordement peuvent coûter plusieurs milliers d'euros (voire des dizaines de milliers d'euros).
- Les coûts d'accès au réseau fibre reste bien plus élevé dans des villes de petite taille que dans une grande métropole.

À RETENIR

- **L'organisation et l'implémentation d'une politique de sauvegarde posent les questions de la localisation, des supports et de la responsabilité des sauvegardes.**
- **Au quotidien, la gestion des sauvegardes est à la fois chronophage et complexe. Et demeure critique : en cas de défaillance, les données ne pourront pas être restaurées.**
- **La sauvegarde externalisée, à savoir déconnectée du site principal, offre la meilleure garantie de protection des données.**

La restauration, véritable enjeu de la sauvegarde

La question de la restauration des données est au moins aussi importante que celle de la sauvegarde. À la suite d'un incident c'est d'elle dont va dépendre la capacité de rétablir un système informatique dans un état de fonctionnement correct, et donc garantir le mécanisme de reprise des services.

Il est indispensable de vérifier que la restauration des données sauvegardées fonctionne ainsi que le temps nécessaire pour la réaliser, avec des tests de restauration « à blanc » réguliers.

Le Recovery Time Objective et le Recovery Point Objectif

Pour faire les bons choix en matière de politique de sauvegarde et de restauration, il est nécessaire de réaliser une analyse de criticité des données et des processus métiers / opérationnels associés. Cette analyse repose sur deux mesures :

- **RTO, ou Recovery Time Objective :** l'objectif de temps de restauration consiste à définir la durée acceptable d'interruption d'un service, d'un processus. Le RTO est généralement le plus réduit possible pour les processus critiques et cœur de métier de l'organisation.
- **RPO, ou Recovery Point Objectif :** l'objectif de point de restauration est la durée maximale de données que l'organisation peut perdre en cas d'incident. Selon le secteur d'activité et les processus concernés, il peut varier de 0 (temps réel) à plusieurs heures.

Les plans de reprise ou de continuité d'activité

C'est à partir de ces deux indicateurs que la stratégie de sauvegarde peut être déclinée, en fonction des données et des processus. Au-delà d'une simple sauvegarde des données avec restauration manuelle sur le site principal, le degré de criticité défini pourra conduire à définir :

- **Un Plan de Reprise d'Activité (PRA) :** en cas d'incident, une bascule manuelle est opérée vers le site de secours. La perte de données sera limitée à la dernière sauvegarde ou réplication, et l'arrêt d'exploitation au temps de bascule.
- **Un Plan de Continuité d'Activité (PCA) :** en cas d'incident sur le site principal, la bascule est opérée automatiquement sur le site de secours. La réplication de l'architecture et des données en temps réel évite les pertes de données et les arrêts de production.

POINT DE VIGILANCE

Déclencher un PRA : une décision stratégique

À l'inverse du PCA dont la bascule entre les deux sites est automatique dans un sens comme dans un autre, le retour au fonctionnement nominal après l'activation d'un PRA est long et complexe, En effet, le travail réalisé après la bascule sera enregistré sur le système secondaire. Un travail de comparaison puis de transfert de données entre le site secondaire et le site principal est à prévoir dans ce cas.

Avant de déclencher un PRA, il s'agit donc de bien peser le pour et le contre entre le temps de relance du site principal et le temps consacré au retour au fonctionnement nominal. C'est une décision qui revient à la direction générale, en concertation avec le partenaire informatique, dans son rôle et son devoir de conseil.

À RETENIR

- **La restauration des données est le point le plus crucial d'une politique de sauvegarde.**
- **Les temps de reprise et de pertes de données acceptables sont les principaux indicateurs de définition d'une stratégie de sauvegarde.**
- **En raison d'un retour au site principal long et complexe, la décision de déclencher un PRA relève de la direction générale.**

Sauvegarde de données : s'assurer d'être bien assuré !

La sauvegarde des données est à l'image d'une assurance tous risques : elle est indispensable, tout en espérant ne jamais en avoir besoin.

Pour autant, inutile d'être surassuré, au risque de dégrader le rapport bénéfices / risques. Un PCA sera, par exemple, surdimensionné pour un site Internet vitrine !

Reste ensuite une question cruciale : confier la stratégie de sauvegarde à l'interne ou s'appuyer sur un prestataire spécialisé ? Dans les deux cas, un certain nombre de critères est à évaluer avant de prendre une décision :

- Le volume de données à sauvegarder.
- La fréquence de sauvegarde.
- La nature des données à sauvegarder et le nombre de cas d'usage.
- Le débit Internet disponible, en upload pour la sauvegarde, en download pour la restauration (temps de redémarrage).
- La fiabilité, la sécurité et le besoin de supervision du site de sauvegarde (datacenter en propre ou partenaire).
- Les tests et la facilité de restauration.
- Le coût.
- La capacité et les compétences internes pour administrer les sauvegardes et gérer les restaurations le cas échéant.

Malheureusement, nombreuses sont les organisations qui ne prennent conscience de l'importance du déploiement d'une stratégie de sauvegarde de données qu'à la suite d'un incident.

INFORSUD Technologies

Solutions et impulsions pour l'avenir

Prestataire de services informatiques basé en Occitanie, nous accompagnons les entreprises et collectivités dans leur transformation digitale, avec une offre qui couvre tous leurs besoins informatiques : conseil et aide au choix, gestion des postes de travail et des infrastructures IT, hébergement infogéré en cloud, solutions de gestion et paie, cybersécurité et développements spécifiques.

Notre savoir-faire depuis plus de 35 ans, notre engagement quotidien et notre accompagnement de proximité nous permettent d'apporter des solutions adaptées aux besoins de nos 380 clients et l'impulsion technologique nécessaire pour qu'ils puissent se transformer durablement.

0 811 349 609
contact@inforsud-technologies.com
inforsud-technologies.com

Siège social
Causse Comtal
12340 Bozouls

Agence Tarn
Impasse des Crins
81990 Le Sequestre

Agence Haute-Garonne
2, rue Maryse Hilsz
31500 Toulouse