adista

# Les gestes qui sauvegardent vos données

## Impliquer toutes les parties prenantes

# **Sauvegarde et restauration**
# anticiper l'imprévisible

L'imprévisible devient pour les organisations de tous types une réalité. Cyberattaques, catastrophes naturelles, erreurs humaines…elles font face à une multitude et à une diversité de risques qui peuvent survenir à tout moment et sans avertissement.

La restauration d'un système d'information après une attaque ou un incident est l'un des moments les plus délicats et exigeants auquel vous pourriez faire face. Ce processus mettra à l'épreuve vos capacités de résiliences IT et organisationnelles. Un grand nombre d'organisations réalisent trop tard qu'elles auraient dû créer et évaluer régulièrement leur plan de reprise.

Pour vivre le redémarrage souhaité de vos activités, **il est crucial que vos directions métiers et vos collaborateurs partagent une culture commune de la gestion du risque, avant, pendant et après**. Une préparation adéquate et une vigilance continue de tous sont les clés pour naviguer dans un paysage numérique de plus en plus périlleux.

**C'est l'objet de ce document :** vous confier quelques règles et concepts qui, bien appliqués, vous aideront à définir des périmètres et des stratégies adaptées pour avoir l'assurance de disposer de données saines et récupérables dans les meilleurs délais et assurer ainsi la pérennité de votre organisation.

- **Veeam Platinum Cloud & Service Provider**
- **Veeam Gold Value-added Reseller**

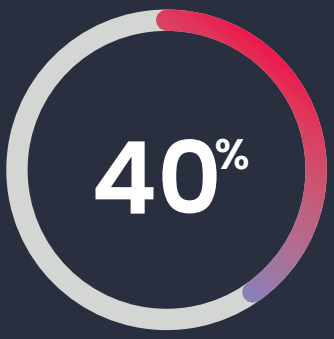
Les solutions Veeam, leader mondial des solutions de sauvegardes, associées au savoir-faire adista assurent la disponibilité des données de nos clients et par conséquent, la continuité d'activité , en protégeant leur système d'information où qu'il soit, dans un contexte où l'hybride prévaut.

Les données représentent un capital vital pour une entreprise. Il faut donc les choyer, et s'assurer qu'elles seront bien protégées ou du moins récupérables, en cas de défaillance technique ou de cyberattaques.

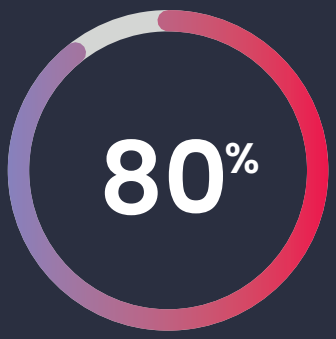
Les cyberattaques sont au cœur de l'actualité. Avec la multiplication des menaces de type ransomwares notamment mais pas seulement, jamais le besoin de sauvegarder ses données n'a été aussi grand.

## LA RESTAURATION DES DONNÉES SUITE À UNE CYBERATTAQUE : DES CHIFFRES ALARMANTS

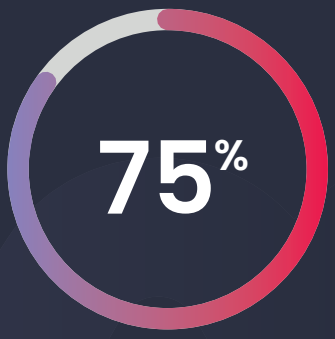
*Source : E-book « Tendances des ransomwares en 2024 » de notre partenaire Veeam*




**des données de production ont pu être chiffrées par des cybercriminels lors des attaques par ransomware**




**des entreprises n'ont pas de Plan de Reprise d'Activité**




**des administrateurs de sauvegarde estiment qu'une réorganisation complète de leur système est nécessaire**

## Les cyberattaquants veulent vos sauvegardes

De la même manière que votre équipe de prévention prévoit une sauvegarde saine et récupérable, le cyberattaquant a pour objectif de vous empêcher de restaurer vos propres données. Malheureusement, dans un bien trop grand nombre d'attaques, les attaquants réussissent à vous priver de votre capacité à vous sauver.

Chiffres issus du rapport "Veeam Data Protection Trends 2024" - 1200 réponses collectées auprès de décideurs et responsables informatiques d'entreprises de la la région EMEA.

# 3 questions

## à Gilles Noël et Jean-Félix Chevassu

Directeur des Offres Cloud et Directeur des Offres cybersécurité d'adista

**Quelle est la valeur ajoutée d'une politique de sauvegarde ?**


Réduire la sauvegarde à la simple notion de copie de données, c'est passer à côté de l'essentiel. Car l'important n'est pas la sauvegarde mais les données qu'elle préserve. Les données sont au cœur des enjeux business et réglementaires, au cœur de l'innovation et de la compétitivité. Assurer leur disponibilité, leur intégrité et leur remise à disposition à travers des test réguliers, doit vous permettre d'assurer votre continuité d'activité même en mode dégradé.


Vos sauvegardes sont des cibles prioritaires pour les attaquants, pour vous laisser sans solution de secours. Si vous êtes en mesure de restaurer vos données à partir de vos sauvegardes sans avoir à payer la rançon, non seulement vous économisez des coûts immédiats, mais vous protégez également la réputation de l'entreprise en montrant qu'elle est capable de gérer efficacement les crises. Votre politique de sauvegarde peut même devenir un avantage concurrentiel.

**Selon le rapport "Veeam Data Protection Trends 2024", environ 80% des entreprises n'ont pas de véritable plan de reprise d'activité (PRA) en place. Comment expliquer ce chiffre ?**

Beaucoup de dirigeants hésitent à investir dans des solutions dont la rentabilité est difficile à démontrer tant qu'ils n'ont pas subi de désastre. La mise en œuvre d'un PRA peut être coûteuse et nécessiter des ressources importantes, tant humaines que financières. Les entreprises peuvent avoir d'autres priorités plus immédiates et négliger la mise en place d'un PRA. J'aime prendre l'image du parachute de secours. Ce n'est que le jour où vous en avez besoin que vous réalisez son caractère vital.

Malgré la multiplication et la médiatisation des incidents, bon nombre pensent qu'ils ne seront pas touchés. « Ça n'arrive qu'aux autres, nous n'avons jamais eu de problème ». Ce faux sentiment de sécurité impacte la culture d'entreprise. Les personnes responsables de la sécurité du SI se retrouvent encore trop souvent seules face à ces sujets, avec des ressources limitées. Plus vous avez de personnes impliquées et formées, avec des mises à jour de leurs compétences, plus vous mettez les chances de survie de votre côté.

## Au-delà de la perte de données, quels sont les risques cachés d'une cyberattaque ?

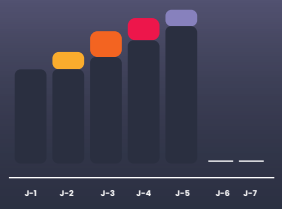
L'un des principaux risques est l'interruption pure et simple de l'activité due à une paralysie de ses systèmes critiques et les pertes financières qui en découlent. Dans ce cadre, on sous-estime le risque et les coûts des litiges juridiques avec ses parties prenantes, par exemple pour des fabrications non-honorées. Et si en plus des données sensibles sont compromises, l'entreprise peut être tenue responsable et faire face à des poursuites et des amendes, notamment en cas de non-conformité à la législation (RGPD, NIS2, DORA, etc.).

Une cyberattaque peut aussi créer un climat de stress, d'incertitude voire de défiance au sein de l'entreprise. Pourquoi la cyberattaque a fonctionné ? Est-ce dû à un manque d'investissements pour sécuriser le SI ? Pourquoi la restauration des sauvegardes est-elle si fastidieuse ? Ces questions sont légitimes et leurs réponses impactent directement la réputation de l'entreprise, la productivité et le moral des équipes.

Précisons aussi qu'en cas d'attaque réussie, se remettre sur pied et renforcer la sécurité pour prévenir de nouvelles attaques peut avoir un coût considérable. Je ne peux que recommander un Bilan d'Impact sur l'Activité (BIA) pour identifier et hiérarchiser au préalable les services critiques et ressources essentielles : ceux qui doivent continuer coûte que coûte, ce qui peuvent attendre une demi-journée ou une journée et les autres.

# Les différents types de sauvegarde

## Sauvegarde complète




**Toutes les données sélectionnées sont intégralement sauvegardées à chaque opération**

Restauration rapide et simple car les données sont disponibles à un seul endroit. Fiabilité accrue car chaque jeu de sauvegarde est indépendant

En fonction du volume, consommation d'espace de stockage important. Temps de réalisation de la sauvegarde important

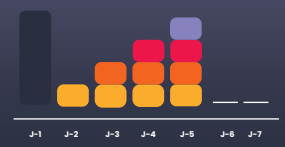
## Sauvegarde incrémentielle


**Seules les données modifiées ou ajoutées depuis la dernière réalisation (complète ou incrémentielle) sont sauvegardées à chaque opération**

Rapidité d'exécution et faible consommation d'espace de stockage pour les sauvegardes complémentaires

Temps de restauration allongé en fonction de l'ancienneté de la donnée. Nécessite de relire tous les points de sauvegarde antérieurs (lecture de la complète + tous les points de sauvegarde)

## Sauvegarde différentielle

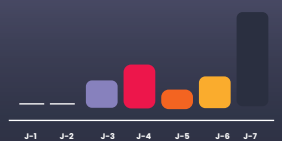



**Seules les données modifiées depuis la dernière sauvegarde complète sont sauvegardées à chaque opération**

Temps d'exécution d'une sauvegarde plus rapide que la méthode complète. Temps de restauration améliorée (lecture de la complète + du dernier point de sauvegarde)

Avec le temps, consommation d'espace de stockage important

## Sauvegarde reverse incrémentielle




**Toutes les données sélectionnées sont intégralement sauvegardées à chaque opération**

Restauration rapide et simple car les données sont disponibles à un seul endroit. Fiabilité accrue car chaque jeu de sauvegarde est indépendant

En fonction du volume, consommation d'espace de stockage important. Temps de réalisation de la sauvegarde important

# Les différents moyens de sauvegarde

### Stockage externe / NAS

**Équipement de stockage physique permettant de conserver une copie des données**

+ Temps d'accès et débits rapides
+ Capacité de stockage évolutif

− Risque de pannes matérielles

### Bandes magnétiques

**Équipement de stockage physique permettant de conserver une copie des données**

+ Radio coût / volume sauvegardé faible
+ Longue durée de vie

− Gestion des équipements pour utiliser les bandes
− Sensibilité à l'environnement ambiant

### Stockage Cloud

**Service en ligne permettant le stockage des données sauvegardées sur des serveurs distants via Internet**

+ Pas d'investissement à prévoir
+ Facilité de mise en place

− Dépendance à l'accès Internet. Exigences réglementaires pour certaines activités
− Coût financier à long terme

# Bien distinguer sauvegarde et PRA

La sauvegarde se concentre principalement sur la protection des données, en ciblant les données et fichiers spécifiques grâce à des copies précises. Son temps de reprise dépend des sauvegardes disponibles et de leur fréquence. En revanche, le PRA vise le rétablissement complet des opérations, couvrant une infrastructure globale, y compris les systèmes, réseaux, applications et données. Il est conçu pour gérer des sinistres majeurs et repose sur des délais de reprises définis (RTO et RPO) pour assurer la continuité d'activité.

# PCA, PRA, PCI, PRI et PCC :
## Définitions et complémentarités

De l'opérationnel à l'IT en passant par la communication, ces plans forment les fondations d'une résilience robuste.

### PCA (Plan de Continuité d'Activité)

Le PCA garantit la continuité des opérations même en cas de crise majeure, comme une catastrophe naturelle ou une cyberattaque. Il permet de maintenir les activités critiques en mode dégradé, assurant ainsi que les fonctions essentielles de l'entreprise restent opérationnelles. Le PCA inclut des procédures et des ressources nécessaires pour gérer les interruptions et minimiser les impacts sur les opérations.

### PRA (Plan de Reprise d'Activité)

Le PRA rétablit les opérations après un incident, tel qu'une panne de système ou une perte de données. Il peut fonctionner indépendamment ou en complément du PCA, en se concentrant sur la restauration rapide des services et des infrastructures pour revenir à un état normal. Le PRA inclut des stratégies de récupération des données, des tests réguliers et des plans de communication pour coordonner les efforts de reprise.

### PCI (Plan de Continiuité Informatique)

Spécifique aux services informatiques, le PCI est une composante du PCA. Il vise à garantir la disponibilité continue des systèmes informatiques et des données en cas de perturbation. Le PCI inclut des mesures de sauvegarde, des redondances de systèmes et des procédures de basculement pour assurer que les services informatiques critiques restent accessibles.

### PRI (Plan de Reprise Informatique)

Le PRI redémarre les systèmes informatiques après un incident, en complément du PCI. Il se concentre sur la récupération rapide des systèmes et des données pour minimiser les temps d'arrêt. Le PRI inclut des procédures de restauration, des tests de récupération et des plans de communication pour assurer une reprise coordonnée et efficace des services informatiques.

### PCC (Plan de Communication de Crise)

Assure une communication claire et efficace avec les collaborateurs, les clients, les partenaires et les autorités en cas de crise. Souvent négligé, mais crucial, le PCC permet de gérer la perception publique et de maintenir la confiance des parties prenantes. Il inclut des protocoles de communication, des messages pré-rédigés et des canaux de communication dédiés pour diffuser rapidement des informations précises et cohérentes.

**Indispensable : suivre la règle du**

# 3-2-1-1-0

*La règle du 3-2-1-1-0 est une stratégie essentielle pour assurer la sécurité et la résilience des données en matière de sauvegarde. Elle définit des bonnes pratiques pour minimiser les risques de perte de données en cas de sinistre ou de panne.*

**3 = Conservez 3 copies de vos données :** Il s'agit de la copie primaire (originale) et de 2 copies de sauvegarde

**2 = Stockez les sauvegardes sur 2 types de supports différents :** Utiliser deux supports de stockage distincts permet de limiter les risques liés à un même type de défaillance.

**1 =Gardez au moins 1 copie hors site :** Stocker une copie des données dans un autre lieu (physique ou distant) permet de se protéger contre les incidents locaux (incendie, vol, panne matérielle).

**1 = Positionnez 1 copie hors-ligne :** Une des sauvegardes doit être conservée dans un état tel qu'elle ne puisse pas être facilement altérée ou compromise en la déconnectant physiquement (un disque dur externe débranché) ou en la rendant immuable (pas de possibilité de modification ou de suppression, même par un administrateur).

**0 = Zéro erreur lors des sauvegardes :** Cette extension récente à la règle vise à garantir que les sauvegardes soient exemptes d'erreurs. Elle repose sur la vérification régulière des sauvegardes pour s'assurer qu'elles fonctionnent, sur des tests de restauration pour valider l'intégrité et la fiabilité des données sauvegardées, et sur l'utilisation d'outils de surveillance pour détecter toute corruption ou défaillance des sauvegardes.

La règle du 3-2-1-1-0 est une approche simple, mais robuste pour sécuriser vos données. Elle garantit non seulement la disponibilité des sauvegardes grâce à la redondance, mais aussi leur intégrité grâce aux vérifications régulières.

## Recommandations complémentaires

**Définir son périmètre de sauvegarde :** La sauvegarde doit être adaptée à l'entreprise, à son fonctionnement, à ses caractéristiques : volume de données, vitesse de l'évolution des données, quantité d'information que l'on accepte de perdre, durée de conservation de l'information… C'est tout un périmètre qu'il faut définir.

**Définir sa périodicité :** Il s'agit également de mettre en place une périodicité de sauvegarde en adéquation avec les besoins de l'entreprise. La périodicité va dépendre de la criticité et de la fréquence de modification des données.

# Plans de Continuité et de Reprise :
## Anticiper en continu et dépasser la résilience IT

Bien que les stratégies de sauvegarde de données soient essentielles pour protéger les informations critiques, elles ne suffisent pas à elles seules à garantir la résilience d'une entreprise face aux incidents majeurs. En effet, l'absence de plans de continuité d'activité (PCA) et de reprise d'activité (PRA) expose les entreprises à des risques financiers et réputationnels considérables.

Si leur mise en œuvre peut certes être complexe, représenter un certain investissement par rapport à d'autres projets et nécessiter des ressources humaines importantes, c'est bel et bien le non-alignement entre directions métiers et le manque de vision partagée autour de la planification qui fait déjà prendre un énorme risque à toute organisation.

La résilience d'une organisation est sa capacité à faire face à l'imprévu, de quelque nature que ce soit. Elle dépasse l'indispensable résilience IT pour engager tous les métiers à « prévoir l'imprévu » ensemble.

## Témoignage client :
Refonte de l'hébergement et PRA

Domofrance
Groupe ActionLogement

**Contexte initial :** Domofrance disposait de trois datacenters non conformes aux normes, notamment en termes de sécurité, d'énergie et de climatisation, dont un situé dans une zone inondable. De plus, une partie de l'hébergement était infogérée par un éditeur offrant des niveaux de service insatisfaisants.

**Solution et projet :** Le projet a consisté à consulter plusieurs partenaires pour la construction d'une infogérance améliorée, en respectant les règles de marché public. L'objectif était de centraliser l'hébergement infogéré et celui des trois datacenters existants. Ce processus a inclus la sélection d'adista comme partenaire grâce à sa réputation et son sérieux.

**Technologie et mise en œuvre :** Pour la refonte de l'hébergement, Domofrance a opté pour une infrastructure hyperconvergente et de haute disponibilité. Le projet a duré environ un an de préparation, avec une attention particulière à l'architecture et aux outils technologiques.

**Résultats et avantages :** Le projet a permis de réaliser des économies significatives et d'améliorer les performances de l'infrastructure. Domofrance bénéficie désormais d'environ 40 indicateurs de niveau de service suivis scrupuleusement, avec des pénalités en cas de non-respect. La société teste annuellement son Plan de Reprise d'Activité (PRA), assurant une meilleure préparation en cas de sinistre.

**Conseils et recommandations :** Domofrance souligne l'importance d'une préparation minutieuse pour ce type de projet. Il recommande de prendre le temps nécessaire pour choisir les technologies appropriées et préparer le plan de migration, afin de garantir le succès du jour J.

## **RTO, RPO, WRT et MTD :**
## définir ces paramètres «business» essentiels

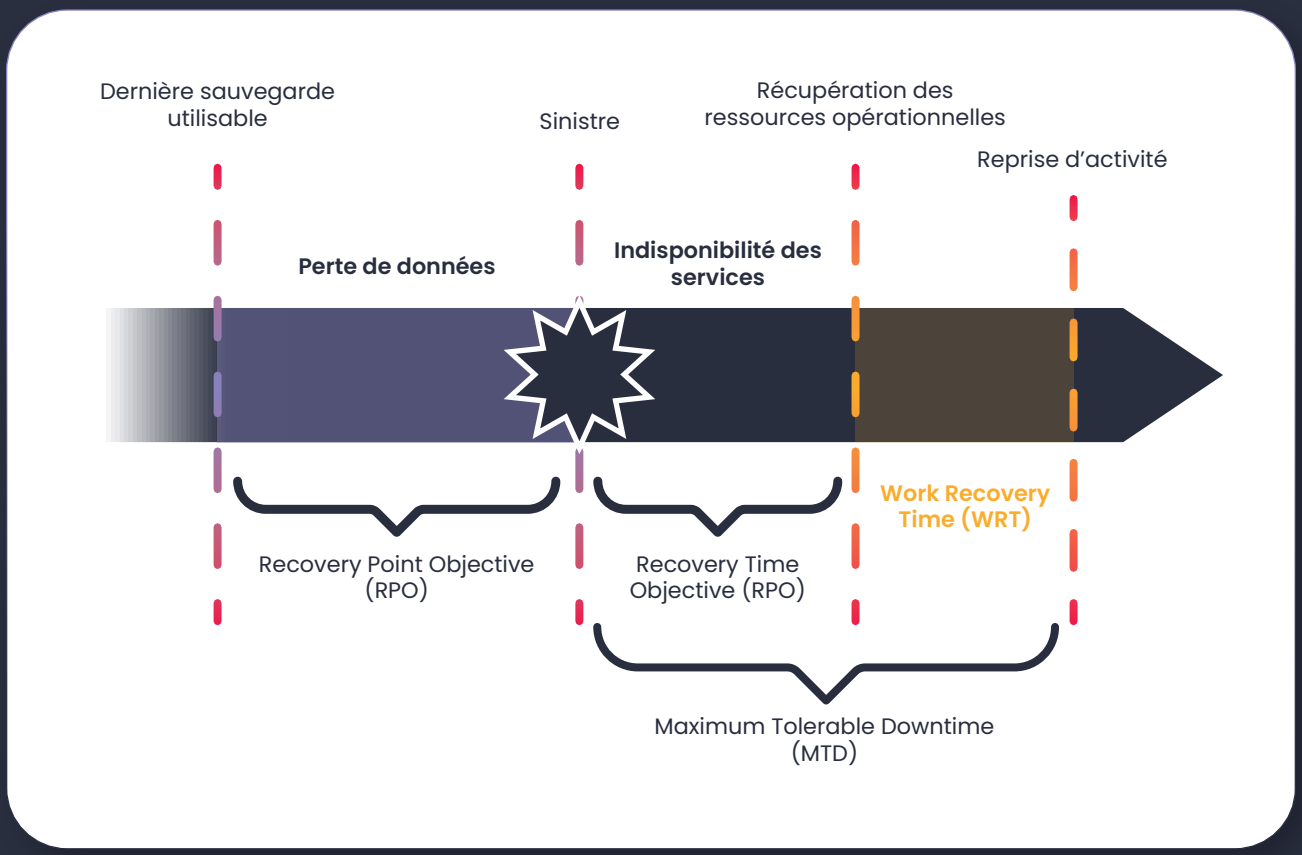
**Le RTO (Return Time Objective)** représente le délai maximal acceptable pour la restauration des fonctions critiques après une interruption, tandis que **le RPO (Recovery Point Objective)** définit la «fraîcheur» des données, la durée qui s'est écoulée entre le moment de la dernière sauvegarde ou du dernier état des données que vous pourrez exploiter pour remettre le Système d'Information en route et la survenance de l'incident.

Un RTO trop long peut entraîner des pertes financières significatives dues à l'interruption prolongée des activités, tandis qu'un RPO mal défini peut conduire à la perte de données cruciales, impactant la prise de décision et la continuité des opérations.

Une remise en marche de vos services ne veut pas forcément dire que vos clients ou collaborateurs y auront accès. **Le WRT (Work Recovery Time)** définit le temps nécessaire pour rétablir effectivement vos services, en vérifiant les systèmes et les remettant en ligne après restauration durant la phase de RPO. Plus le WRT est long plus votre business est impacté.

La durée maximale pendant laquelle vos services peuvent être inopérant avant les conséquences ne deviennent vraiment inacceptables par votre organisation est la somme de votre RTO et du WRT. On l'appelle **le MTD pour Maximum Tolerable Downtime.**

**Les objectifs de reprise après sinistre**



Suivre la méthode

# M-E-R-C-I

pour une résilience by Design

*Rendre votre organisation plus résiliente ne se fait pas du jour au lendemain. Quelle que soit la taille de votre entreprise, vous disposez d'un fonctionnement, de process et d'outils qui vous sont propres. Disposez-vous d'une cartographie de l'existant ? Connaissez-vous la criticité de vos processus métiers ? Quelle est leur dépendance les uns vis-à-vis des autres ? Fixez le cap et projetez vos équipes vers la résilience by design avec M.E.R.C.I. une méthodologie en 5 étapes.*

## M : MANAGEMENT

A l'instar du RSSI et DPO, il est indispensable avant tout de nommer un RAR (Responsable des Activités Résilientes) qui doit disposer de bonnes connaissances des activités métiers de l'entreprise. Il assure le pilotage du projet, en coordination avec les métiers, la qualité, l'informatique et les prestataires externes.

## E : ÉLABORATION

Cette phase d'étude est constituée de l'analyse des risques et de la conception du système de résilience. Examinons le contenu de ces deux composantes.

**Analyse de risques :** Étude de contexte, définition du périmètre, identification des activités critiques, liste des sources de menaces, définition des critères de sécurité, définition des objectifs de continuité, cartographie du système, des processus, des ressources, et des applications.
Etude des événements redoutés, étude des scénarios de menaces.
Etude des risques, étude de mesures de sécurité
Exemple : il a été accepté de ne pas créer de site secondaire pour des raisons de coûts. Cependant, en cas de sinistre majeur dans la salle informatique principale, trois applications critiques doivent pouvoir repartir en moins de 72 heures (l'ERP / CRM, la messagerie et la comptabilité).

**Conception des processus :** Selon les résultats de l'analyse des risques et des mesures de réduction des risques, cette étape permet de concevoir les mesures organisationnelles et techniques à mettre en œuvre dans chacun des services métier concernés.
Exemple, avec la description de deux processus :
Sauvegarde externalisée : identification des données à externaliser selon les niveaux de services définis (SLAs), choix de l'hébergeur, choix du logiciel de sauvegarde, définition des scénarios de test/ restauration, formation du personnel informatique, ...
Hébergement des trois applications critiques : méthodologie, accès distants, réhydratation des données, test, formation du personnel informatique.

## R : RÉALISATION

Cette phase est l'implémentation des processus définis en phase de conception.
Exemple avec l'utilisation de la technologie Veeam qui permet de répliquer les trois machines virtuelles on-premise au sein du datacenter de l'hébergeur, et création du repository permettant d'héberger les sauvegardes des données.

### C : CONTRÔLE

Cette phase concerne tout ce qui permet d'améliorer votre résilience, par des tests réguliers, des revues de conception, des retours d'expérience, des mesures d'indicateurs de satisfaction, l'identification des modifications applicatives éventuelles, la réalisation de tableaux de bord…
Exemple : test de bascule durant un week-end, accès distant via un client léger, test de bascule on-premise, mesures des temps d'accès.

### I : INFORMATION

Cette dernière phase est fondamentale car elle permet de mettre à niveau tous les interlocuteurs de l'entreprise : collaborateurs, clients, Direction, actionnaires, fournisseurs, assureurs… Elle a pour vocation de montrer la maîtrise de la résilience d'entreprise et donc de rassurer tout un écosystème. Elle est inscrite évidemment dans le processus de communication ad hoc.

## COMMENT MUSCLER SA STRATÉGIE DE REPRISE D'ACTIVITÉ ?

**Hybrider son Système d'Information**

C'est un fait : le Système d'Information est désormais hybride et utilise tout ou partie des caractéristiques des environnements On-premise, Cloud privé, Cloud public et Edge Computing. Loger les briques applicatives au meilleur endroit permet d'aligner le bon service au bon usage mais présente aussi l'avantage de répartir le risque.

En « éclatant » leur système d'information, les entreprises tirent parti des meilleures pratiques de sécurité propres à chaque environnement et peuvent bénéficier d'une résilience accrue face aux cyberattaques.

**Intégrer un site distant**

Un site distant protège contre les sinistres tels que les catastrophes naturelles, les incidents électriques, les pannes matérielles ou les incendies. La redondance géographique entre le site principal et le site distant divise les risques d'interruption en multipliant les points d'accès au système d'information. Il permet des sauvegardes fréquentes, renforce la sécurité des informations et inclut des protections supplémentaires contre les attaques. Un site distant peut être conçu pour être scalable et s'adapter ainsi aux évolutions de l'infrastructure principale et aux besoins croissants de l'entreprise grâce à des solutions de cloud intégrées.

**Éprouver et adapter son PRA régulièrement**

Votre Système d'information évolue constamment. Chaque modification peut potentiellement affecter la pertinence et l'efficacité du PRA. Plus vos tests seront réguliers, plus vos équipes seront familiarisées avec les procédures à suivre en cas de crise, réduisant ainsi le temps de réaction et minimisant les impacts négatifs sur l'entreprise.

# Parole d'expert

Brice Munier
Directeur de l'Infrastructure et de l'Innovation

**Quelles sont les innovations récentes qui révolutionnent la sauvegarde des données, et comment peuvent-elles en bénéficier ?**

Les dernières avancées en matière de sauvegarde des données transforment la manière dont les entreprises protègent et gèrent leurs informations. Ces innovations apportent plus de sécurité, de précision et d'automatisation aux processus de sauvegarde. **Voici trois évolutions majeures :**

**1. L'immutabilité des sauvegardes**
L'immutabilité consiste à verrouiller les sauvegardes pour une durée définie, empêchant toute modification ou suppression, même par un administrateur. Cette technologie protège les données contre les altérations accidentelles ou malveillantes, notamment en cas de cyberattaques telles que les ransomwares. Elle garantit ainsi l'intégrité des informations sauvegardées, même lorsque celles-ci sont stockées en ligne.

**2. L'analyse avancée des sauvegardes**
Les nouvelles solutions de sauvegarde ne se limitent plus à la simple conservation des données : elles les analysent pour détecter des anomalies. Par exemple, une augmentation soudaine de la taille des sauvegardes ou un changement de format peut révéler un problème potentiel. Ces systèmes peuvent aussi identifier des logiciels malveillants présents dans les sauvegardes, alerter les équipes informatiques et, si nécessaire, bloquer les sauvegardes compromises. Cette capacité d'analyse proactive permet d'améliorer la détection des menaces et de renforcer la sécurité globale.

**3. L'intelligence artificielle dans la gestion des sauvegardes**
L'intégration de l'intelligence artificielle (IA) dans les processus de sauvegarde permet d'optimiser la gestion des données. L'IA peut analyser les habitudes de sauvegarde et suggérer des améliorations, comme l'archivage automatique des données peu utilisées pour libérer de l'espace. Elle facilite également la vérification de l'intégrité des sauvegardes complexes, telles que celles impliquant plusieurs serveurs ou bases de données. Enfin, l'IA permet d'automatiser certaines tâches, comme la restauration de données, réduisant ainsi la charge de travail des administrateurs et accélérant la reprise d'activité.

Ces innovations redéfinissent les pratiques de sauvegarde en apportant un niveau accru de sécurité, une meilleure capacité de détection des anomalies et une automatisation avancée. Pour les entreprises, elles offrent une protection renforcée contre les cybermenaces, optimisent la gestion des ressources informatiques et facilitent la continuité des activités en cas d'incident.

# adista et Veeam

## Un partenariat stratégique pour la protection des données

Depuis plusieurs années, adista s'appuie sur Veeam comme partenaire clé pour développer des solutions de sauvegarde, de réplication et de gestion des données dans un environnement multi-cloud. Ce partenariat stratégique permet à adista d'offrir un large éventail de services à forte valeur ajoutée pour ses clients.

adista est certifiée Veeam Platinum Service Provider, le plus haut niveau du programme Veeam Cloud & Service Provider (VCSP). Cette distinction témoigne de l'expertise d'adista dans l'intégration de solutions complexes et sur mesure. Les équipes techniques et commerciales bénéficient d'une formation approfondie, garantissant une maîtrise complète des technologies Veeam.

En tant qu'interlocuteur unique, adista prend en charge l'intégralité du support client, de la conception à l'exploitation, assurant ainsi une prise en charge rapide et efficace. Cette approche intégrée simplifie les échanges et améliore la réactivité en cas d'incident.

Le partenariat entre adista et Veeam repose sur une relation de confiance durable. Cette collaboration a été récompensée par le Veeam Pro Partner Award du meilleur partenaire VCSP, reconnaissant l'expertise d'adista et son engagement à garantir la continuité d'activité des entreprises.

*« adista et Veeam sont partenaires de longue date. Nous avons grandi ensemble. Le Veeam Pro Partner Award salue un partenariat d'innovation, de croissance, et d'humains qui travaillent pour construire les choses ensemble. »*

***Ioanna MONNIER, Alliance Manager***

# À propos d'adista

adista transforme la technologie en levier de succès pour votre organisation. Avec une offre intégrée qui traverse l'IT, les télécommunications et la cybersécurité, adista s'engage à vous fournir des solutions personnalisées et innovantes qui répondent à vos défis spécifiques.

Notre approche, centrée sur l'expertise technique et une vision audacieuse du futur numérique, est animée par une volonté d'aller au-delà des attentes conventionnelles. En privilégiant une relation basée sur la transparence, la sincérité et une grande complicité, nous créons un environnement de confiance et de collaboration étroite avec nos clients, leur permettant d'exploiter pleinement le potentiel de leurs projets IT.

adista est plus qu'un fournisseur de services technologiques : c'est un partenaire stratégique engagé dans le succès et l'innovation continue de ses clients.

**Pour en savoir plus, rendez-vous sur www.adista.fr**

## Contactez-nous :


https://www.adista.fr/contact/

contact@adista.fr


markess by exægis

*Reconnu visionnaire dans le Blueprint Cloud Managed Services de Markess*

ISO/IEC 27001 Information Security Management

FRANCE BEST MANAGED COMPANIES Deloitte.

adista est une des marques opérationnelles du groupe inherent.