GLOSSAIRE

Appel à Financement n°2- Fonction « Stratégie de continuité et de reprise d'activité »



Historique du document – Suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V0.1	15/07/2025	Équipe programme CaRE	Version initiale
V.1.0	06/052026	Équipe programme CaRE	Mise à jour : définition de "Bouton rouge" et de "SI mutualisé"

Table des matières

Principe de base *4*

Le modèle 3-2-1 ..... *5*

Définition 5

Intégrité et immuabilité dans la sauvegarde *8*

Principe 8

En synthèse 8

RTO et RPO *9*

Définition 9

Exemple 9

Schéma 10

Politique, plan de sauvegarde et procédure de restauration *11*

Politique de sauvegarde et de restauration 11

Plan de sauvegarde 12

Description du processus 13

Procédure de restauration *14*

Définition 14

Objectif 14

Contenu 14

Les types de sauvegardes *15*

Sécurisation des sauvegardes *17*

Comptes de sauvegarde 17

Authentification multi facteur (MFA) 17

Principe du moindre privilège 17

Gestion des comptes à privilèges 17

Chiffrement des données 17

Isolation des sauvegardes 17

Contrôle d'accès basé sur les rôles (RBAC) 18

Surveillance et audit 18

Mises à jour et correctifs 18

Surveillance de l'efficacité des sauvegardes *19*

Statut des sauvegardes 19
Fréquence des sauvegardes 19
Volume des données sauvegardées 19
Durée des sauvegardes 19
Intégrité des données 19
Alertes et notifications 19
Historique des sauvegardes 20
Conformité de la politique de sauvegarde 20
Surveiller l'intégrité des données 21
Utiliser des empreintes numériques (hashing) 21
Mettre en place de politiques de sécurité strictes 21
Comparer régulièrement l'état des données 21
Vérifier l'intégrité après chaque sauvegarde 21
Tester régulièrement 21
Surveiller les journaux d'événements 21
Les tests de restauration 22
Quelques bonnes pratiques liées aux bonnes pratiques de restauration des données 22
Test technique 23
Test fonctionnel 23
Test de processus métier 23
Perte d'une salle machine 24
Sauvegardes externalisées 25
Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité 25
Quelques bonnes pratiques 26
Glossaire 29

Les sauvegardes

PRINCIPE DE BASE [1]

Par essence, la sauvegarde des systèmes d'information[2][3] est une pratique essentielle en cybersécurité[4]. Elle consiste à créer des copies des données et des différents systèmes pour les protéger.

Son objectif initial était prévu pour pallier des pertes opérationnelles comme les pannes matérielles, des dommages sur les systèmes d'information.

Aujourd'hui, la **sauvegarde est un élément indispensable de la réponse aux incidents de sécurité**, agissant comme dernier rempart.

Pour cela, elle doit s'appuyer sur des points essentiels à intégrer dans la politique de sauvegarde :

- **Architecture du système de sauvegarde** : Le système doit être isolé dans un réseau distinct de celui de la production pour minimiser les risques de propagation d'incidents.
- **Les objectifs de récupération** : Il faut établir des objectifs de temps de récupération (RTO) et des objectifs de point de récupération (RPO) pour déterminer combien de temps et combien de données peuvent être perdues sans impact majeur sur l'organisation.
- **Intégrité et immutabilité** : Les sauvegardes doivent pouvoir être externalisées et rendues immuables pour garantir qu'elles ne peuvent pas être modifiées ou supprimées par des attaquants.

[1] *ANSSI, les essentiels : sauvegarde des systèmes d'information*
[2] *ANS, Règles de sauvegarde des systèmes d'information de santé*
[3] *ANSSI : sauvegarde des systèmes d'information*
[4] *CNIL : Sécurité : Sauvegarder*

LE MODELE 3-2-1

Définition

La règle de sauvegarde 3-2-1 est une stratégie de protection des données visant à garantir l'intégrité et la disponibilité des informations critiques de l'établissement.

Trois copies de vos données

Il est essentiel de pouvoir disposer de trois copies des données sauvegardées : la sauvegarde initiale et deux copies supplémentaires. Cette redondance réduit le risque de perte de données en cas de défaillance d'un ou plusieurs supports.

Deux types de supports différents

Les sauvegardes doivent être stockées sur au moins deux types de supports différents, comme un disque dur externe ou un service de stockage en ligne en plus du stockage initial. L'utilisation de différents supports protège contre les défaillances spécifiques à un type de support.

Une copie hors site ou hors ligne

Au moins une copie de sauvegarde doit être stockée, dans un emplacement physique différent de celui des données originales, ou hors ligne, c'est-à-dire non connectée à un réseau. Cela protège les données contre les cyberattaques ou les catastrophes locales, comme les incendies ou les inondations.

Quelques exemples de copie hors ou hors ligne :

Type	Architecture	Fonctionnement	Remarque
Sauvegarde sur bande magnétique	**Serveur de sauvegarde** : Connecté au serveur de production pour effectuer les sauvegardes. **Bibliothèque de bandes** : Stocke les bandes magnétiques contenant les sauvegardes. **Site distant** : Les bandes sont transportées physiquement vers un site distant sécurisé.	- Les données sont copiées du serveur de production vers le serveur de sauvegarde - Les données sauvegardées sont transférées sur des bandes - Les bandes sont transportées et stockées dans un site distant sécurisé	- Protection contre les cyberattaques, car les bandes ne sont pas connectées au réseau. - Longue durée de vie des bandes.

Type	Architecture	Fonctionnement	Remarque
Sauvegarde sur disque dur externe	**Disque dur externe** : Connecté au serveur de production pour effectuer les sauvegardes. **Site distant** : Les disques durs sont transportés physiquement vers un site distant sécurisé.	- Les données sont copiées du serveur de production vers le disque dur externe - Les disques durs sont transportés et stockés dans un site distant sécurisé	- Facilité de transport et de stockage. - Coût relativement faible.
Sauvegarde air-gap (isolation physique)	**Serveur de sauvegarde** : Connecté au serveur de production pour effectuer les sauvegardes. **Stockage Air-Gap** : Unité de stockage physiquement isolée du réseau principal. **Déconnexion physique** : Le stockage Air-Gap est déconnecté du réseau après chaque sauvegarde. **Sauvegarde initiale :** Les données sont copiées du serveur de production vers le serveur de sauvegarde**.** **Transfert vers le stockage Air-Gap :** Les données sont ensuite transférées vers l'unité de stockage Air-Gap. **Déconnexion :** Une fois le transfert terminé, l'unité de stockage Air-Gap est physiquement déconnectée du réseau, empêchant tout accès non autorisé.	- Les données sont copiées du serveur de production vers le serveur de sauvegarde - Les données sont transférées vers une unité de stockage isolée - Après chaque sauvegarde, l'unité de stockage est physiquement déconnectée du réseau	- Les données sont protégées contre les cyberattaques, car elles ne sont pas accessibles via le réseau. - En cas de sinistre affectant le réseau principal, les données sauvegardées restent intactes et accessibles.
Sauvegarde cloud sans connexion physique	**Serveur de sauvegarde** : Connecté au serveur de production pour effectuer les sauvegardes. **Cloud public/privé** : Les données sont transférées vers un service cloud. **Déconnexion physique** : Les données sont déconnectées du réseau après la sauvegarde.	- Les données sont copiées du serveur de production vers le serveur de sauvegarde - Les données sauvegardées sont transférées vers le cloud - Après la sauvegarde, les données sont déconnectées du réseau pour plus de sécurité	- Accès rapide aux données en cas de besoin. - Protection contre les sinistres locaux.

Type	Architecture	Fonctionnement	Remarque
Sauvegarde hybride (cloud et local)	**Serveur de sauvegarde :** Connecté au serveur de production pour effectuer les sauvegardes. **Disque dur externe** : Stocke une copie locale des sauvegardes. **Cloud public/privé** : Stocke une copie distante des sauvegardes.	- Les données sont copiées du serveur de production vers le serveur de sauvegarde - Une copie des données sauvegardées est stockée localement sur un disque dur externe - Une copie des données sauvegardées est transférée vers le cloud	- Redondance accrue. - Protection contre les sinistres locaux et les cyberattaques. - Cout de restauration pouvant être élevé.

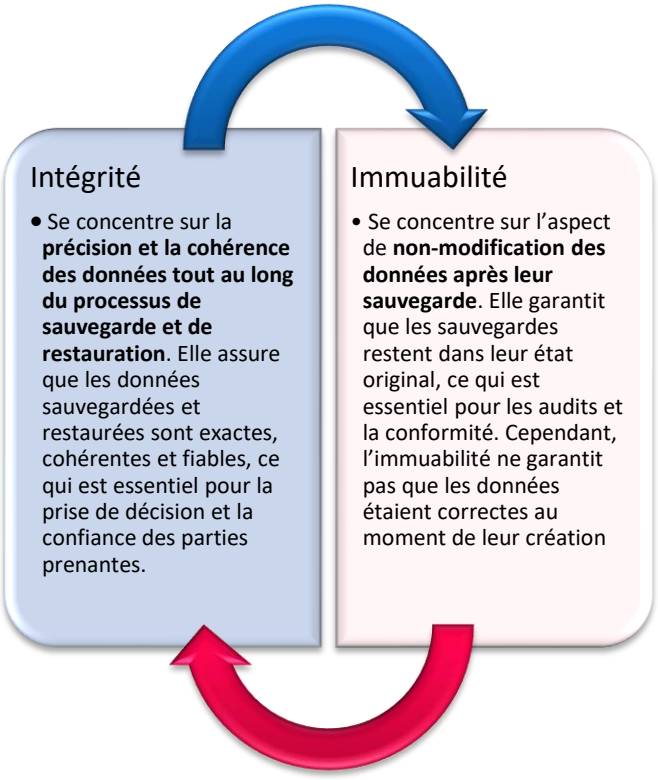
INTEGRITE ET IMMUABILITE DANS LA SAUVEGARDE

Principe

Dans le cadre de la règle 3-2-1, il est important de garantir l'intégrité des données sur l'une des copies de sauvegarde. Pour des raisons de performance et de durée d'analyse, ce contrôle d'intégrité est effectué sur la 3ème copie (le « 1 »), qui peut être hors ligne ou hors site. Ces contrôles s'appliquent généralement aux bases de données et aux machines virtuelles.

En synthèse

Dans une politique de sauvegarde et de restauration, il est essentiel de combiner l'intégrité et l'immuabilité des données pour une protection complète. L'immuabilité assure que les sauvegardes restent inchangées et disponibles dans leur état original, tandis que l'intégrité garantit que les données sauvegardées et restaurées sont précises, cohérentes et fiables. Ensemble, ces deux concepts créent un environnement de données sécurisé et conforme aux exigences réglementaires. Cependant, l'immuabilité ne garantit pas l'intégrité des données. Les deux notions doivent être gérées de manière complémentaire pour assurer une protection et une fiabilité maximales des données.



RTO ET RPO

Avant de définir les plans de sauvegarde et les procédures de restauration, il est important de comprendre l'importance de ces deux indicateurs clés dans la gestion des sauvegardes.

Définition

- **RTO (Recovery Tome Objective *ou objectif de délai de reprise*)** est le délai maximal acceptable pour la restauration d'une fonction ou d'un service après une interruption. Cela signifie que c'est le temps maximum pendant lequel un établissement peut tolérer l'indisponibilité d'une fonction ou d'un service avant que cela n'ait des conséquences fortes sur ses activité.

- **RPO (Recovery Point Objective ou point de récupération des données)** est le point maximal acceptable de perte de données en cas d'interruption. En d'autres termes, c'est la quantité maximale de données que l'établissement peut se permettre de perdre entre deux sauvegardes.

Ces deux indicateurs sont essentiels pour élaborer un Plan de Reprise d'Activité (PRA) et minimiser l'impact des incidents sur le fonctionnement de l'établissement.

Exemple

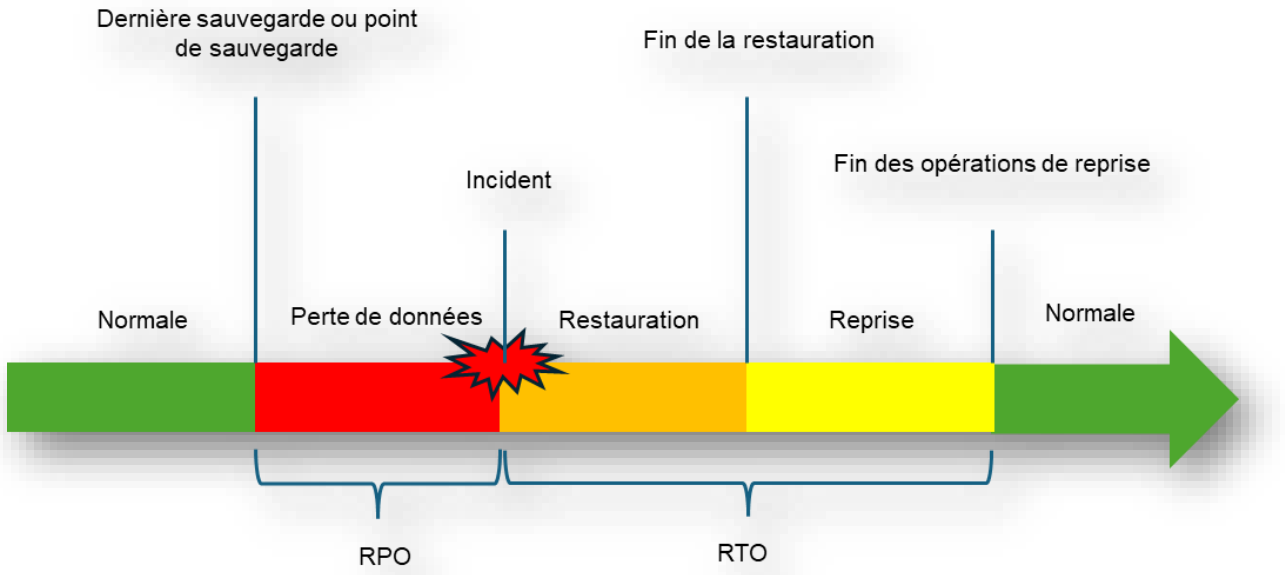
Supposons qu'un incident se produise à 12h00 :

- **RTO** : Si le RTO est de 2 heures, les systèmes doivent être restaurés et opérationnels d'ici 14h00.

- **RPO** : Si le RPO est de 4 heures, les données générées jusqu'à 8h00 doivent avoir été sécurisées. Les données générées entre 8h00 et 12h00 peuvent être perdues.

Schéma

Ce schéma représente les étapes essentielles du processus de sauvegarde et de récupération des données en cas d'incident.



Explications détaillées

- ***Normale*** : La situation initiale où tout fonctionne normalement et les données sont sauvegardées régulièrement.
- ***Dernière sauvegarde ou point de sauvegarde*** : Le dernier point de sauvegarde avant l'incident.
- ***Incident*** : Un événement imprévu qui entraîne une perte de données.
- ***Perte de données*** : La période pendant laquelle les données ne sont pas sauvegardées et sont donc perdues en raison de l'incident.
- ***RPO (Recovery Point Objective)*** : L'objectif de point de récupération, indique la période maximale acceptable de la perte de données, s'étendant du dernier point de sauvegarde à l'incident.
- ***Restauration*** : La phase de récupération des données à partir des sauvegardes disponibles.
- ***RTO (Recovery Time Objective)*** : L'objectif de temps de récupération, représente la durée maximale acceptable entre la survenance de l'incident et le retour à la normale'.
- ***Reprise*** : La phase où les opérations normales reprennent après la restauration des données.
- ***Fin de la restauration et opération de reprise*** : Le moment où la restauration et les opérations de reprise sont terminées. Les opérations normales peuvent reprendre.

POLITIQUE, PLAN DE SAUVEGARDE ET PROCEDURE DE RESTAURATION

La politique de sauvegarde et de restauration[5], et le plan de sauvegarde sont hiérarchiquement liés et complémentaires. La politique de sauvegarde établit le cadre stratégique et les objectifs globaux de la sauvegarde des données, tandis que le plan de sauvegarde traduit ces directives en actions concrètes et opérationnelles. En d'autres termes, la politique de sauvegarde définit le "quoi" et le "pourquoi", tandis que le plan de sauvegarde détaille le "comment".

Politique de sauvegarde et de restauration

Définition

La politique de sauvegarde et de restauration est un ensemble de directives et de règles établies par un établissement pour protéger ses données critiques. Elle définit les principes généraux et les objectifs de la sauvegarde des données, incluant la fréquence des sauvegardes, les types de données à sauvegarder, les méthodes de sauvegarde, les emplacements de stockage, et les mesures de sécurité à appliquer. La politique de sauvegarde vise à garantir la disponibilité, l'intégrité et la confidentialité des données, tout en assurant la conformité aux exigences réglementaires et la continuité des opérations.

Objectif

L'objectif principal d'une politique de sauvegarde et restauration est de **protéger les données et les systèmes critiques** contre des incidents tels que la perte ou la corruption de données. Cela nécessite la réalisation de sauvegardes régulières, la mise en place de procédures de restauration en cas d'incident, et l'assurance que les données peuvent être restaurées rapidement et efficacement en cas de nécessité. En somme, il s'agit de garantir la continuité des opérations et la sécurité des informations essentielles.

Contenu

Une politique de sauvegarde et de restauration contient à minima les éléments suivants :

- Les typologies des données à sauvegarder (base de données, applications, serveurs, documents, ...).
- La hiérarchisation des données en fonction de leur criticité.
- La fréquence des sauvegardes en fonction de la criticité des données.
- La planification des sauvegardes en fonction de l'activité.
- Les responsabilités des personnels impliqués dans le processus des sauvegardes.
- Les mesures sécurité afférentes aux sauvegardes (chiffrement, contrôle d'accès).
- Les mesures sur la confidentialité et l'intégrité des données.
- Les exigences de conformité légale et réglementaire portant sur les sauvegardes (RGPD, CNIL, ...).
- La définition d'une stratégie claire de restauration en lien avec le Plan de Reprise d'Activité (PRA) et en tenant compte des principaux scénarios d'incidents (pannes, cyberattaques, erreurs humaines, catastrophes naturelles).

[5] *ANS : Règles de sauvegarde des systèmes d'information – Guide pratique technique – PGSSI-S*

- La réalisation régulière de tests de restauration pour s'assurer que les données peuvent être récupérées efficacement et que les procédures sont bien comprises par le personnel.
- La rédaction d'une procédure d'isolation d'urgence du système de sauvegarde en cas de suspicion de compromission ou d'attaque.
- A description des systèmes et des outils permettant une restauration rapide des données, minimisant ainsi les interruptions d'activité.

Plan de sauvegarde

Définition

Le plan de sauvegarde, quant à lui, est un document opérationnel qui détaille les procédures spécifiques et les actions à entreprendre pour mettre en œuvre la politique de sauvegarde. Il inclut des instructions précises sur la manière de réaliser les sauvegardes, les outils et technologies à utiliser, les responsabilités des différents acteurs, et les étapes à suivre pour restaurer les données en cas d'incident. Le plan de sauvegarde est conçu pour être un guide pratique permettant de garantir que les sauvegardes sont effectuées correctement et que les données peuvent être restaurées rapidement et efficacement.

Objectif

Un plan de sauvegarde a pour but de mettre en œuvre la politique de sauvegarde et à garantir une récupération, dans les meilleurs délais, des données perdues ou corrompues. Pour cela, il est nécessaire de définir la valeur des deux indicateurs RTO et RPO.

Contenu

Un plan de sauvegarde contient à minima les éléments techniques suivant :

- Les logiciels, matériels utilisés pour réaliser la sauvegarde.
- Supports utilisés (stockage dédié, cloud, bande, ...)
- Les types de sauvegardes (complète, incrémentielle, différentielle, ...)
- La fréquence de réalisation des sauvegardes
- Le délai de rétention
- Le niveau de réplication
- Les procédures à suivre en cas d'échec du plan

Description du processus

Réaliser un état des lieux de l'existant

- Réaliser une analyse détaillée de l'environnement des systèmes d'information actuels.
- Identifier quels systèmes, applications et données sont essentiels et nécessitent une protection accrue.
- Évaluer les capacités existantes par rapport aux exigences futures prévues.

Définir les responsabilités

- Attribuer clairement les responsabilités de gestion et d'opération des sauvegardes à des individus ou équipes spécifiques.

Identifier les données prioritaires

- Classer les données en fonction de leur criticité et de leur importance pour l'activité de l'établissement.

Définir les méthodes de sauvegarde

- Sélectionner les méthodes et outils de sauvegarde adaptés aux besoins spécifiques (choix entre sauvegarde totale ou partielle).

Déterminer la fréquence des sauvegardes

- Définir un calendrier définissant la fréquence des opérations de sauvegarde pour garantir la sécurité sans gêner les activités courantes.

Choisir les emplacements de stockage

- Décider de l'endroit où les sauvegardes seront stockées (sur site, hors site, cloud).
- Assurer la redondance des sauvegardes pour éviter les pertes de données.

Tester les sauvegardes

- Effectuer des tests réguliers pour vérifier l'efficacité des sauvegardes et la capacité de restauration des données.

Documenter le plan de sauvegarde

- Rédiger un document détaillant toutes les étapes, procédures et responsabilités.
- Mettre à jour régulièrement ce document pour refléter les changements et les améliorations.

Réviser et améliorer le plan

- Réévaluer périodiquement le plan de sauvegarde pour l'adapter aux nouvelles menaces et aux évolutions technologiques.
- Apporter des améliorations continue en fonction des retours d'expérience et des tests effectués

PROCEDURE DE RESTAURATION

Définition

La procédure de restauration est un ensemble de directives détaillées qui décrivent les étapes à suivre pour récupérer les données à partir des sauvegardes en cas d'incident. Elle inclut les instructions pour identifier les données à restaurer, les outils et technologies à utiliser, les étapes de vérification de l'intégrité des données restaurées, et les responsabilités des différents membres de l'équipe. La procédure de restauration vise à minimiser les temps d'arrêt et à assurer une reprise rapide et efficace des opérations.

Objectif

Une procédure de restauration vise à garantir que les données peuvent être récupérées rapidement et efficacement après un incident, tout en maintenant leur intégrité et leur disponibilité. Elle permet également de se conformer aux exigences réglementaires, de coordonner les efforts des équipes, et de documenter le processus pour des améliorations futures.

Contenu

- **Identification** : Déterminer quelles données doivent être restaurées et à partir de quel point de sauvegarde en se référant aux indicateurs précisés dans le RTO et RPO.
- **Préparation** : S'assurer que l'environnement de restauration est prêt, ce qui peut inclure la vérification de l'intégrité des sauvegardes et la préparation du matériel ou des logiciels nécessaires.
- **Exécution :** Utiliser les outils ou logiciels appropriés pour restaurer les données à partir des sauvegardes.
- **Vérification** : S'assurer que les données restaurées sont intègres, complètes et fonctionnelles, et que le système fonctionne correctement après l'exécution la restauration.

LES TYPES DE SAUVEGARDES

Tableau comparatif des types de sauvegardes

Type de sauvegarde	Description	Avantages	Inconvénients
Complète	Effectue une sauvegarde intégrale de toutes les données sélectionnées	Facile à restaurer car toutes les données sont contenues dans la dernière sauvegarde réalisée	Prend du temps et nécessite une grande capacité de stockage
Différentielle	Effectue une sauvegarde des données qui ont changées depuis la dernière sauvegarde complète	Plus rapide que la sauvegarde complète et plus simple à restaurer qu'une sauvegarde incrémentielle	Prend plus de temps et d'espace qu'une sauvegarde incrémentielle
Incrémentielle	Effectue uniquement une sauvegarde des données qui ont été modifiées depuis la dernière sauvegarde (complète ou incrémentielle)	Rapide et nécessite moins d'espace de stockage	La restauration peut s'avérer complexe. Il faut restaurer la dernière sauvegarde complète et toutes les sauvegardes incrémentielles suivantes pour arriver au point de restauration souhaité.
Miroir ou réplication	Une copie des données, pour la redondance de celles-ci, est effectuée en temps réel	Permet une récupération rapide des données en cas de défaillance notamment matériel	Ne protège pas contre les suppressions involontaires de données ou de corruption. Les modifications apportées sur la source des données sont immédiatement répliquées. Nécessite de grande capacité de stockage.
Distante	Effectue une sauvegarde des données sur des serveurs distants	Accessible, automatisée et protège contre des incidents locaux	Dépend de la connexion internet, de la capacité réseau et des coûts induits par cette connexion

Type de sauvegarde	Description	Avantages	Inconvénients
Hors ligne	Sauvegarde des données sur des supports physiques externes non connectés (sauf le temps de la sauvegarde) ou le temps de la sauvegarde	Offre une protection robuste contre les risques cyber en assurant une immuabilité des données. Les données peuvent être restaurées rapidement. Les sauvegardes hors ligne sont inaccessibles aux ransomwares, réduisant ainsi le risque de perte de données critiques	Les sauvegardes hors ligne doivent être régulièrement mises à jour pour garantir qu'elles contiennent les données les plus récentes, ce qui peut nécessiter des ressources supplémentaires (humaines et matérielles) et générer des couts supplémentaires en termes d'infrastructure

SECURISATION DES SAUVEGARDES

Pour sécuriser les sauvegardes, voici quelques bonnes pratiques à suivre.

Comptes de sauvegarde

Différencier la gestion les comptes utilisés par les matériels et logiciels de la sauvegarde de ceux gérer par l'Active Directory (AD) est une bonne pratique de sécurité pour plusieurs raisons :

- **Limiter les privilèges** : les comptes de sauvegarde doivent être configurés avec les privilèges strictement nécessaires à la réalisation des sauvegardes, réduisant ainsi les risques d'abus de privilèges.
- **Réduire les risques** : en cas de compromission d'un compte, les dommages sont limités à un domaine spécifique (AD ou sauvegarde) plutôt que de s'étendre à l'ensemble des systèmes.
- **Séparer les responsabilités** : cette séparation permet de mieux gérer et auditer les activités, en séparant clairement les tâches d'administration de l'AD des opérations de sauvegarde.
- **Protéger contre les attaques** : les attaques ciblent souvent les comptes à privilèges. En séparant la gestion des comptes, on diminue le risque que les sauvegardes soient affectées par une attaque visant l'AD.

Authentification multi facteur (MFA)

Utiliser une authentification multi facteur pour accéder aux systèmes de sauvegarde. Cela ajoute une couche de sécurité supplémentaire en exigeant plusieurs formes de vérification.

Principe du moindre privilège

Appliquer le principe du moindre privilège en limitant les accès aux sauvegardes uniquement aux personnes qui en ont réellement besoin. Réduire les droits d'accès au strict nécessaire.

Gestion des comptes à privilèges

Surveiller et gérer les comptes à privilèges de manière rigoureuse. Utiliser des solutions de gestion des accès à privilèges (PAM) pour contrôler et auditer l'utilisation de ces comptes.

Chiffrement des données

Chiffrer les données de sauvegarde, tant au repos qu'en transit, pour protéger contre les accès non autorisés en utilisant des algorithmes de chiffrement robustes.

Isolation des sauvegardes

Stocker les sauvegardes dans des environnements isolés, distincts des systèmes de production. Utiliser des zones réseau séparées pour minimiser les risques d'accès non autorisé.

Contrôle d'accès basé sur les rôles (RBAC)

Mettre en place un contrôle d'accès basé sur les rôles pour gérer les permissions de manière granulaire. Assigner des rôles spécifiques avec des droits d'accès définis.

Surveillance et audit

Surveiller en continu les accès aux systèmes de sauvegarde et réaliser des audits réguliers pour détecter toute activité suspecte. Configurer des alertes pour les tentatives d'accès non autorisées.

Mises à jour et correctifs

Maintenir les systèmes de sauvegarde à jour avec les derniers correctifs de sécurité. Cela permet de protéger contre l'exploitation des vulnérabilités connues.

SURVEILLANCE DE L'EFFICACITE DES SAUVEGARDES

Il ne suffit pas de simplement effectuer des sauvegardes régulières, il est tout aussi important de surveiller leur efficacité. La surveillance de l'efficacité des sauvegardes consiste à vérifier que les processus de sauvegarde fonctionnent correctement, que les données sont intégralement sauvegardées et qu'elles peuvent être restaurées rapidement et sans erreur en cas d'incident.

Statut des sauvegardes

- Vérifier si les sauvegardes ont été réalisées avec succès ou si elles ont échoué.
- Identifier les sauvegardes incomplètes ou corrompues
- En cas d'échec, mettre en œuvre des moyens de correction sur les erreurs rencontrées

Fréquence des sauvegardes

- Assurer que les sauvegardes sont effectuées selon le calendrier prévu (quotidien, hebdomadaire, mensuel).
- Comparer la fréquence réelle des sauvegardes avec la fréquence planifiée.

Volume des données sauvegardées

- Suivre la quantité de données sauvegardées à chaque cycle.
- Détecter toute variation anormale dans le volume des données.

Durée des sauvegardes

- Mesurer le temps nécessaire pour compléter chaque sauvegarde.
- Identifier les sauvegardes qui prennent plus de temps que prévu, ce qui pourrait indiquer des problèmes de performance.

Intégrité des données

(Cf. Surveiller l'intégrité des données)

- Vérifier que les données sauvegardées sont complètes et non corrompues.
- Utiliser des mécanismes de vérification d'intégrité pour s'assurer que les données peuvent être restaurées correctement.

Alertes et notifications

- Configurer des alertes pour les échecs de sauvegarde ou les anomalies détectées.
- Assurer que les notifications sont envoyées aux personnes responsables en temps opportun.

Historique des sauvegardes

- Maintenir un historique détaillé des sauvegardes effectuées, y compris les dates, heures et résultats.
- Utiliser cet historique pour analyser les tendances et améliorer les processus de sauvegarde.

Conformité de la politique de sauvegarde

- Vérifier que les sauvegardes respectent la politique définie (types de sauvegardes, délais de rétention, niveaux de réplication).
- Assurer la conformité aux exigences légales et réglementaires (RGPD, CNIL, etc.).

SURVEILLER L'INTEGRITE DES DONNEES

La sauvegarde des données est une composante essentielle de la stratégie de sécurité des systèmes d'information. Cependant, pour que ces sauvegardes soient réellement efficaces, il est essentiel de surveiller l'intégrité des données sauvegardées. La surveillance de l'intégrité des données dans le cadre des sauvegardes consiste à s'assurer que les informations sauvegardées restent exactes, complètes et non altérées depuis leur création jusqu'à leur restauration.

Utiliser des empreintes numériques (hashing)

- Générer des empreintes numériques (hashes) pour les fichiers sauvegardés.
- Comparer régulièrement ces empreintes avec celles des fichiers d'origine pour détecter toute modification.

Mettre en place de politiques de sécurité strictes

- Définir des règles claires pour l'accès et la modification des données sauvegardées.
- Limiter l'accès aux sauvegardes aux seules personnes autorisées.

Comparer régulièrement l'état des données

- Comparer l'état actuel des données sauvegardées avec un état connu et sûr.
- Utiliser des outils de surveillance pour automatiser ce processus.

Vérifier l'intégrité après chaque sauvegarde

- Effectuer des vérifications d'intégrité immédiatement après chaque opération de sauvegarde.
- Utiliser des outils de vérification d'intégrité intégrés aux solutions de sauvegarde.

Tester régulièrement

- Réaliser des tests de restauration périodiques pour s'assurer que les données peuvent être récupérées sans altération.
- Documenter les résultats des tests et ajuster les procédures si nécessaire.

Surveiller les journaux d'événements

- Analyser les journaux d'événements pour détecter toute activité suspecte ou non autorisée.
- Configurer des alertes pour les anomalies détectées dans les journaux.

LES TESTS DE RESTAURATION

Quelques bonnes pratiques liées aux bonnes pratiques de restauration des données

La restauration des données est une étape clé dans la gestion des systèmes d'information, particulièrement en cas d'incident ou de sinistre. Pour s'assurer que les données peuvent être récupérées de manière efficace et sans erreur, ces tests permettent de vérifier que les procédures de sauvegarde et de restauration fonctionnent correctement et que les données peuvent être restaurées à leur état initial.

Planification des tests

- Établir un calendrier régulier pour effectuer des tests de restauration, incluant aussi bien des tests planifiés que des tests aléatoires pour simuler des situations réelles

Tests variés

- Effectuer différents types de tests, tels que des tests techniques, fonctionnels et de processus métier, pour couvrir tous les aspects de la restauration des données.

Documentation

- Maintenir une documentation détaillée des procédures de sauvegarde et de restauration, incluant les contacts clés et les étapes à suivre.
- Avoir un plan de restauration documenté et testé régulièrement pour s'assurer qu'il fonctionne correctement en cas de besoin.

Environnement de test

- Utiliser, si possible, un environnement de test qui reflète fidèlement l'environnement de production pour garantir que les résultats des tests sont représentatifs.

Analyse des tests

- Analyser les résultats des tests pour identifier les points faibles et les axes d'amélioration. Mettre en place des actions correctives basées sur ces analyses

Test technique

Objectif	Actions / Test	Critères de réussite
Vérifier que les sauvegardes et restaurations fonctionnent correctement au niveau technique.	Effectuer des sauvegardes et restaurations sur différents types de données et systèmes pour s'assurer de leur intégrité et de leur cohérence. Test unitaire des plateformes techniques : Vérification de chaque composant technique de manière isolée pour s'assurer qu'il fonctionne correctement. Tests de validation techniques : Connexion à la machine, connectivité réseau, ...	Les données doivent être sauvegardées et restaurées sans erreur, et les systèmes doivent fonctionner normalement après la restauration.

Test fonctionnel

Objectif	Actions / Test	Critères de réussite
S'assurer que les sauvegardes et restaurations répondent aux besoins fonctionnels de l'organisation.	Tester les sauvegardes et restaurations sur des applications spécifiques pour vérifier que toutes les fonctionnalités sont opérationnelles après la restauration.	Les applications doivent fonctionner comme prévu après la restauration, sans perte de donnée ou de fonctionnalité.

Test de processus métier

Objectif	Actions / Test	Critères de réussite
Vérifier que les sauvegardes et restaurations permettent de maintenir la continuité des processus métier.	Tester les sauvegardes et les restaurations en effectuant un ensemble de tests fonctionnels couvrant un processus métier.	Les processus métier doivent pouvoir être repris sans interruption après la restauration, et toutes les étapes doivent être validées fonctionnellement.

Perte d'une salle machine

Objectif	Actions / Test	Critères de réussite
Évaluer la capacité de l'organisation à récupérer ses données et à reprendre ses activités en cas de perte d'une salle machine.	Simuler la perte d'un datacenter, effectuer des tests de bascule vers un site distant (seconde salle, site de secours, etc.), et tester la restauration des données sur ce site.	Les données doivent être restaurées avec succès sur le site distant ou seconde salle machine, et les systèmes doivent être opérationnels pour permettre la reprise des activités.

SAUVEGARDES EXTERNALISEES

Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité[6]

L'Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité s'applique principalement aux marchés publics. Cependant, il peut également être utilisé par des entités privées si elles choisissent de s'y référer dans leurs contrats. En effet, le cahier des clauses simplifiées de cybersécurité est conçu pour sécuriser les systèmes d'information et les données associées dans tout type de marché, qu'il soit public ou privé

Cadre de sécurisation

Il fournit un cadre standardisé pour la sécurisation des systèmes d'information et des données associées dans les marchés. Cela inclut les technologies de l'information et de la communication, ainsi que les services annexes comme les extranets de commande et les services clients.

Obligations claires

Les clauses simplifiées de cybersécurité définissent clairement les obligations des titulaires de marchés et de leurs sous-traitants en matière de sécurité des systèmes d'information. Cela permet de s'assurer que tous les acteurs impliqués respectent les mêmes normes de sécurité.

Conformité réglementaire

En se référant à cet arrêté lors des appels d'offres ou des renouvellements de contrats, les établissements peuvent garantir leur conformité aux exigences réglementaires en matière de cybersécurité. Cela est particulièrement important pour les entités couvertes par le Référentiel Général de Sécurité (RGS) et la Politique de Sécurité des Systèmes d'Information de l'État (PSSI État).

Réduction des risques

En adoptant ces clauses, les établissements peuvent réduire les risques de cyberattaques et d'incidents de sécurité, en mettant en place des mesures préventives et des procédures de réponse adaptées[1].

[6] *Arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité*

Quelques bonnes pratiques

Exigences pour la sauvegarde

État des lieux initial

Effectuer un audit exhaustif de l'existant pour identifier les données critiques et les systèmes à sauvegarder. Cet état des lieux permet de comprendre les besoins spécifiques de l'établissement et prioriser les ressources en conséquent.

Définition des responsabilités

Définir précisément les responsabilités pour chaque aspect des sauvegardes et leur supervision. Une répartition claire des responsabilités élimine les risques de malentendus et garanti que chaque tâche et correctement prise en charge.

Méthodes de sauvegarde

Description : Définissez les méthodes de sauvegarde (complète, incrémentale, différentielle) et assurez-vous qu'elles sont adaptées à vos besoins.

Argument : Chaque méthode a ses avantages et inconvénients. Par exemple, les sauvegardes complètes sont plus sûres mais prennent plus de temps et d'espace.

Fréquence des sauvegardes

Définir la fréquence des sauvegardes en fonction de la criticité des données et de la fréquence de leur modification. Des sauvegardes fréquentes diminuent la perte de données en cas de problèmes, mais nécessitent plus de ressources.

Tests réguliers

Planifier et organiser des tests réguliers de restauration pour vérifier l'intégrité et la fiabilité des sauvegardes. Ces tests permettent de s'assurer les données peuvent restaurées correctement en cas de nécessité.

Supervision continue

S'assurer de la mise en place d'outils de supervision pour surveiller en temps réel l'état des sauvegardes et recevoir des alertes en cas de problème. La supervision permet de détecter rapidement les anomalies et de réagir avant qu'elles ne deviennent critiques.

Sécurité des données

S'assurer que les données sauvegardées sont chiffrées et stockées de manière sécurisée pour éviter tout accès non autorisé. La sécurité des données est essentielle pour protéger les informations sensibles contre les cyberattaques.

Plan de reprise d'activité

Intégrer les sauvegardes dans un plan de reprise d'activité pour garantir une continuité de service en cas de sinistre. La rédaction d'un plan de reprise d'activité permet de minimiser les interruptions de service et de reprendre rapidement les opérations normales.

Exigence dans le choix du prestataire ou de l'hébergeur

Pour choisir un prestataire ou un hébergeur fiable pour la gestion des sauvegardes et la supervision de votre système d'information, voici les prérequis essentiels à vérifier :

Certification et conformité

S'assurer que le prestataire dispose ou respecte un certain nombre de certifications et de règlements tels que la certification ISO 27001 ou le RGPD. Ce respect permet de garantir à minima que le prestataire respecte les normes de sécurité et de gestion des données.

Expérience et expertise

S'assurer de l'expérience du prestataire dans la gestion des sauvegardes et des systèmes d'information similaires à l'activité de l'établissement.

Infrastructure et technologie

Obtenir un descriptif de l'infrastructure technique du prestataire, y compris les centres de données, les technologies de sauvegarde utilisées et les mesures de sécurité en place à travers le Plans d'Assurance Sécurité (PAS). Une infrastructure robuste et moderne assure une meilleure fiabilité et sécurité des données.

Disponibilité et support

Vérifier les niveaux de service (SLA) proposés à travers le Plan d'Assurance Sécurité fourni par le prestataire, notamment le délai de rétablissement du service et les temps de réponse en cas de problème correspondent aux attendus de l'établissement. Par exemple, un support réactif et disponible 24/7 est important pour réduire et minimiser les interruptions de service.

Redondance et récupération

S'assurer que le prestataire propose des solutions de redondance et de récupération en cas de sinistre. La redondance des données et des systèmes garantit une continuité de service même en cas de panne majeure notamment sur les enjeux de la sauvegarde.

Sécurité des données

Vérifier les mesures de sécurité mises en place pour protéger les données, telles que le chiffrement, les pares-feux, et les contrôles d'accès. La protection des données sensibles est essentielle pour éviter les violations de sécurité et les pertes de données.

Références et avis

S'assurer des références et demander les avis d'autres établissements pour évaluer la réputation du prestataire. Les retours d'expérience peuvent donner une idée de la fiabilité et de la qualité des services proposés par le prestataire.

Flexibilité et évolutivité

S'assurer que le prestataire peut s'adapter à l'évolution des besoins de l'établissement et proposer des solutions évolutives. Une solution flexible permet de s'adapter aux évolutions de l'établissement sans nécessiter de changements majeurs.

Réversibilité

S'assurer que les données peuvent être récupérées sans pertes et réutilisées et ce, même après la fin du contrat avec le prestataire.

GLOSSAIRE

Terme	Définition	Traduction (Anglais)
Archivage	Stockage à long terme des données qui ne sont pas fréquemment utilisées mais doivent être conservées pour des raisons légales ou de conformité.	**Archiving**
Archivage des données	Processus de déplacement des données qui ne sont plus activement utilisées vers un emplacement de stockage à long terme.	**Data Archiving**
Authentification (*)	L'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.	**Authentication**
Autorisation	Processus de contrôle des droits d'accès aux données et aux ressources en fonction de l'identité de l'utilisateur ou du système.	**Authorization**
Bascule automatique	Processus de basculement automatique vers un système de secours en cas de défaillance du système principal.	**Failover**
Bouton rouge	Action rapide et facile, permettant d'isoler les serveurs de sauvegarde ou de déconnecter l'infrastructure de sauvegarde du reste du réseau, sur décision du RSSI ou toute personne habilitée.	**Emergency Isolation Capability**
Chiffrement (*)	Transformation cryptographique de données produisant un cryptogramme.	**Encryption**
Classement des données	Stratégie de stockage des données	**Data Tiering**
Cliché instantané	Copie instantanée de l'état des données à un moment donné, souvent utilisée pour les sauvegardes rapides et les restaurations.	**Snapshot**
Clonage	Création d'une copie exacte des données ou d'un système pour des tests ou des migrations.	**Cloning**
Compression	Réduction de la taille des données pour économiser de l'espace de stockage et améliorer la vitesse de transmission.	**Compression**
Copie en miroir	Réplication en temps réel des données sur un autre système ou emplacement pour assurer une disponibilité continue.	**Mirroring**
Cryptographie (*)	La cryptographie permet la transformation, au moyen d'un algorithme de chiffrement, d'un message clair en un message chiffré dans le but d'assurer la disponibilité, la confidentialité et l'intégrité des données échangées. Deux interlocuteurs peuvent ainsi échanger de manière confidentielle et sécurisée, pourvu qu'ils possèdent la clé leur permettant de chiffrer et/ou de déchiffrer leurs messages. La cryptographie sert aussi d'autres applications telles que l'authentification et la signature (numérique) des messages, ayant toutes pour finalité – chiffrement compris –	**Cryptography**

Terme	Définition	Traduction (Anglais)
	le traitement, le stockage ou la transmission sécurisée de données.	
Déduplication	Technique de réduction de la quantité de stockage nécessaire en éliminant les copies redondantes des données.	**Deduplication**
Destruction de données	Destruction sécurisée des données pour empêcher leur récupération.	**Data Shredding**
Enregistrement d'audit	Enregistrement détaillé des actions effectuées sur les données pour des raisons de sécurité et de conformité.	**Audit Trail**
Gestion d'instantané	Création de snapshots fréquents pour minimiser la perte de données en cas de sinistre.	**Snapshotting**
Gestion de version	Technique de gestion des versions multiples d'un fichier ou d'un ensemble de données pour permettre la récupération d'une version antérieure.	**Versioning**
Gestion du cycle des données	Stratégies et outils pour gérer les données depuis leur création jusqu'à leur destruction.	**Data Lifecycle Management (DLM)**
Hachage (*)	Fonction cryptographique qui transforme une chaîne de caractères de taille quelconque en une chaîne de caractères de taille fixe et généralement inférieure. Cette fonction satisfait entre autres deux propriétés :la fonction est « à sens unique » : il est difficile pour une image de la fonction donnée de calculer l'antécédent associé. La fonction est « sans collision » : il est difficile de trouver deux antécédents différents de la fonction ayant la même image.	**Hashing**
Haute disponibilité	Système ou composant qui est continuellement opérationnel pendant une longue période.	**High Availability (HA)**
Immuabilité	Propriété des données qui ne peuvent pas être modifiées ou supprimées après leur création, assurant ainsi leur protection contre les altérations non autorisées.	**Immutability**
Incrémentale pour toujours	Stratégie de sauvegarde où seules les modifications depuis la dernière sauvegarde incrémentielle sont sauvegardées en permanence, réduisant ainsi le temps et l'espace nécessaires pour les sauvegardes.	**Incremental Forever**
Intégrité (*)	Garantie que le système et l'information traitée ne sont modifiés que par une action volontaire et légitime.	**Integrity**
Journalisation	Enregistrement des modifications apportées aux données pour permettre une récupération précise en cas de besoin.	**Logging**
Masquage de données	Technique de protection des données sensibles en les remplaçant par des valeurs fictives tout en conservant leur format et leur type.	**Data Masking**
Mise en miroir de données	Réplication exacte des données sur plusieurs disques ou systèmes pour assurer la redondance et la disponibilité.	**Data Mirroring**

Terme	Définition	Traduction (Anglais)
Objectif de point de récupération (RPO)	Intervalle de temps acceptable pendant lequel les données peuvent être perdues en cas de sinistre.	**Recovery Point Objective (RPO)**
Objectif de temps de récupération (RTO)	Durée maximale acceptable pour restaurer les données et reprendre les opérations après un sinistre.	**Recovery Time Objective (RTO)**
Plan de Continuité d'Activité (PCA) (*)	Ensemble de procédures documentées servant de guides aux entités pour répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation.	**Business Continuity Plan (BCP)**
Plan de Reprise d'Activité (PRA) (*)	Procédures documentées permettant aux entités de rétablir et de reprendre leurs activités en s'appuyant sur des mesures temporaires adoptées pour répondre aux exigences métier habituelles après un incident.	**Disaster Recovery Plan (DRP)**
Plan de remédiation (*)	Plan visant à la reconstruction d'un SI à la suite d'une attaque.	**Remedial Plan**
Point de restauration	Moment précis dans le temps auquel les données peuvent être restaurées.	**Restore Point**
Politique de rétention	Règles définissant la durée pendant laquelle les sauvegardes doivent être conservées avant d'être supprimées ou archivées.	**Retention Policy**
Prévention de pertes des données	Stratégies et outils utilisés pour prévenir la perte ou le vol de données sensibles.	**Data Loss Prevention (DLP)**
Protection Continue des Données	Technologie de sauvegarde qui enregistre toutes les modifications des données en temps réel, permettant une restauration à n'importe quel point dans le temps.	**Continuous Data Protection (CDP)**
Récupération des données	Processus de récupération des données perdues, corrompues ou supprimées.	**Data Recovery**
Redondance	Duplication des données ou des composants pour augmenter la fiabilité et la disponibilité des systèmes.	**Redundancy**
Réplication de données	Copie des données d'un système à un autre en temps réel ou à intervalles réguliers pour assurer la redondance et la disponibilité.	**Data Replication**
Reprise après sinistre en tant que service	Service de reprise après sinistre externalisé fourni par un prestataire tiers.	**Disaster Recovery as a Service (DRaaS)**
Réseau redondant de disques indépendants	Technologie de stockage qui combine plusieurs disques durs pour améliorer la performance et/ou la redondance des données.	**Redundant Array of Independent Disks (RAID)**
Restauration	Processus de récupération des données à partir d'une sauvegarde en cas de perte ou de corruption.	**Restore**

Terme	Définition	Traduction (Anglais)
Restauration d'un système à nu	Processus de restauration d'un système complet, y compris le système d'exploitation, les applications et les données, sur un matériel vierge ou différent.	**Bare Metal Restore**
Restauration granulaire	Capacité de restaurer des éléments spécifiques, comme des fichiers individuels ou des e-mails, à partir d'une sauvegarde sans restaurer l'ensemble du système.	**Granular Recovery**
Retour en arrière	Processus de retour des opérations du système de secours au système principal après la résolution d'un sinistre.	**Failback**
Rotation des sauvegardes	Stratégie de gestion des sauvegardes en utilisant plusieurs supports de sauvegarde de manière cyclique pour optimiser l'espace et la sécurité des données.	**Backup Rotation**
Sauvegarde	Processus de copie des données pour les protéger contre la perte ou la corruption.	**Backup**
Sauvegarde à chaud	Sauvegarde effectuée pendant que le système est en ligne et en cours d'utilisation, permettant une disponibilité continue.	**Hot Backup**
Sauvegarde à froid	Sauvegarde effectuée lorsque le système est hors ligne ou inactif, minimisant les risques de corruption des données.	**Cold Backup**
Sauvegarde Cloud	Sauvegarde des données sur des serveurs distants via Internet, souvent fournie par des services de cloud computing.	**Cloud Backup**
Sauvegarde complète synthétique	Sauvegarde complète créée en combinant une sauvegarde complète initiale avec les sauvegardes incrémentielles suivantes, sans nécessiter une nouvelle sauvegarde complète.	**Synthetic Full Backup**
Sauvegarde des points d'accès	Sauvegarde des données des appareils individuels, comme les ordinateurs portables et les smartphones, pour protéger les données des utilisateurs finaux.	**Endpoint Backup**
Sauvegarde différentielle	Sauvegarde des données qui ont changé depuis la dernière sauvegarde complète.	**Differential Backup**
Sauvegarde en tant que service	Service de sauvegarde externalisé fourni par un prestataire tiers.	**Backup as a Service (BaaS)**
Sauvegarde hors site	Sauvegarde des données dans un emplacement géographiquement distinct pour protéger contre les sinistres locaux.	**Offsite Backup**
Sauvegarde incrémentielle	Sauvegarde des seules données qui ont changé depuis la dernière sauvegarde complète ou incrémentielle.	**Incremental Backup**
Sauvegarde sur bande	Utilisation de bandes magnétiques pour stocker les sauvegardes, souvent utilisée pour l'archivage à long terme.	**Tape Backup**
SI mutualisé	Un SI est considéré comme mutualisé lorsqu'il repose sur une instance unique, ou lorsque le même applicatif est déployé dans plusieurs établissements avec la même version, le même paramétrage et la même organisation.	**Shared Information System**
Somme de contrôle	Valeur calculée à partir des données pour vérifier leur intégrité lors de la transmission ou du stockage.	**Checksum**

(*) Les définitions sont issues du CyberDico[7] de l'ANSSI qui des mots, expressions et sigles du domaine de la cybersécurité. Il présente leur traduction ainsi que leur définition en français et en anglais.

[7] *ANSSI : CyberDico*