

# Sauvegardes régulières

## De quoi parle-t-on lorsque que l'on évoque **les sauvegardes régulières** ?

Disposer de sauvegardes constitue le dernier recours en cas d'incident majeur ou d'attaque de type rançongiciel. Elles permettent une restauration & une reconstruction du SI ainsi que le redémarrage des activités de l'entreprise.

### Les points de vigilance :

Les données dites « personnelles », qu'elles soient relatives aux employés ou aux clients, nécessitent des **mesures de protection renforcées pour garantir leur intégrité, leur confidentialité, leur disponibilité et leur résilience** en application du règlement général sur la protection des données (RGPD). Les dispositifs juridiques de protection et de conservation des données s'appliquent quels que soient les objectifs du stockage (traitement ou sauvegarde).

De plus, il est nécessaire de **tester les sauvegardes** pour vérifier **leur fiabilité** avant qu'un potentiel acte malveillant se produise.

### Quelles sont les ressources mises à disposition pour vous aider à monter en compétences sur le sujet ?

- Sauvegarde des Systèmes d'Information de Santé ([PDF](#)) ;
- Sauvegarder et prévoir la continuité d'activité ([Site web](#)) ;
- Sauvegarde sécurisée de l'ANSSI ([PDF](#)).



### Les bonnes pratiques :

#### Identifier les données à sauvegarder :

- **Un inventaire** doit être préalablement réalisé pour recenser tous les systèmes d'information puis déterminer quelles données sont essentielles **à la poursuite de l'activité**. On distingue généralement les « **données métiers** » (fichiers client, données manipulées par les applications, etc.), des **données techniques** nécessaire à la reconstruction d'un SI. Il est ainsi requis de sauvegarder les sources d'installation, les licences, les fichiers de configuration des applications, les certificats, les clés, etc.

#### Rythme des sauvegardes :

- La fréquence des sauvegardes est à définir en fonction **des risques et de la fraîcheur de données souhaitées** lors d'une restauration (en cas d'incident, une sauvegarde quotidienne implique d'accepter une perte des données d'une journée).

#### Support à privilégier pour les sauvegardes :

- Pour plus de souplesse et de résilience, il convient de s'appuyer sur des sauvegardes en ligne mais également sur des sauvegardes déconnectées. Les sauvegardes en ligne, par exemple sur des disques réseaux (SAN/NAS) ou des services cloud permettent une fluidité et une agilité des sauvegardes. En revanche, elles sont exposées aux attaques informatiques, telles que les rançongiciels. Il est donc nécessaire de compléter le dispositif de sauvegarde par des sauvegardes dites « hors ligne » ou déconnectées. Il peut s'agir d'un support physique comme un disque dur externe, à déconnecter impérativement du système d'information à l'issue de la sauvegarde.

**La règle du « 3-2-1 » permet de se protéger contre des rançongiciels : 3 copies de sauvegarde, sur 2 supports différents dont 1 hors ligne.**