

# Garantir la continuité de votre activité : Le protocole de sauvegarde infaillible

---

## Gouvernance et planification stratégique

- Maintenir un inventaire à jour des actifs numériques critiques et définir des priorités selon leur criticité métier.
- Définir le RTO (Recovery Time Objective) : le délai maximal acceptable pour restaurer l'activité après un incident.
- Définir le RPO (Recovery Point Objective) : la quantité maximale de données qu'il est acceptable de perdre.

## Architecture et intégrité des données

- Appliquer la règle du 3-2-1 : conserver au moins 3 copies des données, sur 2 supports différents, dont 1 copie hors site.
- Isoler les sauvegardes du réseau principal via l'air-gap ou la sauvegarde immuable pour contrer les ransomwares.
- Chiffrer systématiquement les sauvegardes au repos et en transit pour garantir la confidentialité.
- Inclure les configurations des équipements réseau (firewalls, switches) et les images systèmes (OS) dans le périmètre de sauvegarde.

## Sécurisation des accès

- Appliquer le principe du moindre privilège pour limiter les accès aux systèmes de sauvegarde.
- Généraliser l'authentification multi-facteurs (MFA) pour tous les accès aux infrastructures de sauvegarde.

## Maintenance et validation opérationnelle

- Tester mensuellement la restaurabilité des données et la validité des sauvegardes via des exercices grandeur nature.
- Documenter précisément la procédure de restauration et conserver une version papier ou hors-ligne accessible en cas d'indisponibilité totale des systèmes.