



COURS THEORIQUE –  
SAUVEGARDE DES DONNÉES,  
RGPD, CNIL, PCA ET PRA  
(Windows Server 2025)

# Enjeux de la Sauvegarde des Données Utilisateurs

- Les données utilisateurs sont critiques et sensibles.
- Indispensable de mettre en place une politique de sauvegarde adaptée.
- Objectifs:
  - Garantir la continuité de service.
  - Restaurer rapidement les données en cas de sinistre.
  - Se conformer aux obligations légales (CNIL, RGPD).

# Types de Données à Sauvegarder

- Profils utilisateurs (profils itinérants, AppData, documents).
- Partages de fichiers (DFS, dossiers de groupe).
- Bases de données, journaux, configurations système.

# Stratégies de Sauvegarde

- Sauvegarde complète: toutes les données à un instant T.
- Sauvegarde incrémentale: uniquement les données modifiées depuis la dernière sauvegarde.
- Sauvegarde différentielle: toutes les données modifiées depuis la dernière sauvegarde complète.

# Fréquence et Moyens de Sauvegarde

- Fréquence Recommandée:
  - Quotidienne pour les fichiers critiques.
  - Hebdomadaire pour les données archivées.
- Moyens de Sauvegarde:
  - Disques externes sécurisés.
  - NAS en réseau interne.
  - Sauvegarde cloud (avec chiffrement fort).
  - Volumes BitLockerisés.

# PCA et PRA

- PCA (Plan de Continuité d'Activité): maintenir un niveau minimum d'activité en cas d'incident.
- PRA (Plan de Reprise d'Activité): restaurer les services et données après un sinistre.

# Éléments Clés d'un PCA / PRA

- Cartographie des actifs critiques.
- RTO (Recovery Time Objective): délai de reprise.
- RPO (Recovery Point Objective): perte de données maximale tolérable.

# Bonnes Pratiques PCA/PRA

- Stocker les sauvegardes hors site ou chiffrées dans un coffre-fort numérique.
- Tester régulièrement les procédures de restauration.
- Documenter tous les scénarios de reprise.

# RGPD et CNIL : Sauvegarde des Données Personnelles

- RGPD (Règlement Général sur la Protection des Données) impose des obligations en matière de traitement et de sauvegarde des données personnelles.

# Principes Clés RGPD

- Minimisation: ne collecter que les données nécessaires.
- Sécurité: garantir l'intégrité et la confidentialité des données sauvegardées.
- Droit d'accès, de rectification et d'effacement.

# Obligations RGPD et CNIL

- Traçabilité des accès et des restaurations.
- Notification à la CNIL en cas de fuite de données.
- Mise en place d'un registre des traitements.

# Ressources Utiles

- CNIL: <https://www.cnil.fr/fr>
- RGPD: Règlement (UE) 2016/679

# Sécurisation des Sauvegardes – Bonnes Pratiques Cyber

- Chiffrer les sauvegardes: BitLocker, Veracrypt ou outils natifs.
- Limiter l'accès aux supports de sauvegarde: Administrateurs de confiance.
- Isoler les supports de sauvegarde: Stockage hors ligne ("air gap").
- Activer l'audit des restaurations.
- Utiliser des logiciels de sauvegarde certifiés: Veeam, Acronis, etc.
- Faire des tests réguliers de restauration: Ne pas tester = Ne pas sauvegarder.

# Mise en Oeuvre Technique sur Windows Server 2025

- Outil intégré: Windows Server Backup.

# PowerShell et Sauvegarde

- Installer la fonctionnalité: `Install-WindowsFeature -Name Windows-Server-Backup`
- Créer une sauvegarde: `wbadmin start backup -backupTarget:D: -include:C:\Users -quiet`
- Lister les sauvegardes: `wbadmin get versions`
- Restaurer: `wbadmin start recovery`

# Logiciels Tiers

- Veeam Backup & Replication (version Community gratuite pour serveurs limités).
- Acronis, Altaro, UrBackup, etc.

# Conclusion

- Sauvegarder les données n'est pas une option, mais une exigence légale, technique et sécuritaire.
- Le respect des normes RGPD, l'audit des accès, la redondance des sauvegardes et la préparation d'un PRA solide permettent d'assurer la résilience de l'organisation.



FIN DU COURS