# PROSIT 3

**Groupe :**

CARVAL Mathéo – Secrétaire
RABATEL Antonin – Tous

LUU Philippe - Animateur

BOUHAMED Allan – Secrétaire

# Contexte

Une semaine après leur attaque par rançongiciel, la société voisine Dupond & Dupont & Chaussai reste totalement bloquée. Leur prestataire Cloud ne respecte pas les SLA, la bande passante est insuffisante, et la restauration prendra plusieurs jours. Ils devront même repartir depuis des données archivées.

Marco, administrateur système de BERRIA, confirme que leur PRI/PCI était très insuffisant, malgré des serveurs en RAID 10.

Chez BERRIA, les sauvegardes reposent actuellement sur deux NAS, via des scripts PowerShell quotidiens. Cette solution est fonctionnelle mais limitée : elle ne respecte qu'en partie la règle du 3-2-1, n'offre pas de Cloud souverain et ne garantit aucun SLA, RPO ou RTO sérieux en cas d'attaque.

Marta souhaite désormais mettre en place une véritable stratégie de sauvegarde professionnelle, incluant une copie Cloud souveraine et un plan de restauration fiable. Elle demande à Léo d'étudier des solutions et de lister les étapes nécessaires à la création d'un nouveau plan de sauvegarde.

# Mots Inconnus

**Resilience** : capacité d'un système à continuer de fonctionner malgré une panne ou une attaque.

**PRI (Plan de Reprise Informatique)** : plan permettant de redémarrer les services après un incident majeur.

**PCI (Plan de Continuité Informatique)** : plan permettant de conserver un service minimal pendant l'incident.

**SLA (Service Level Agreement)** : engagements contractuels concernant un service Cloud (disponibilité, vitesse…).

**RPO (Recovery Point Objective)** : date/heure de la dernière sauvegarde acceptable → perte de données maximale.

**RTO (Recovery Time Objective)** : durée maximale pour restaurer un service.

**Restauration incrémentale** : restauration nécessitant toutes les sauvegardes depuis le dernier "full backup".

**Règle 3-2-1** :

- 3 copies
- sur 2 supports différents
- dont 1 stockée hors site

**NAS** : serveur de stockage en réseau.

**RAID 6 / RAID 10** : solutions de tolérance aux pannes (RAID ≠ sauvegarde).

**Cloud souverain** : Cloud hébergé en France ou UE respectant les lois européennes (OVH, Scaleway…).

**Débit de restauration** : quantité de données pouvant être restaurée par heure.

**Sécurité immuable (immutable backup)** : sauvegarde impossible à modifier par un attaquant.

# Problématique

Comment concevoir un nouveau plan de sauvegarde pour BERRIA garantissant la résilience du SI face à une attaque par rançongiciel, en respectant la règle 3-2-1, en assurant la souveraineté des données, et en atteignant des RPO, RTO et SLA acceptables pour l'entreprise ?

# Plan d'action

1. **Identification des données critiques**
   La première étape consiste à classifier les données selon leur criticité et leur impact sur l'activité.
   Il s'agit de déterminer quelles données sont indispensables à la continuité de service et lesquelles doivent être sauvegardées pour répondre à des obligations légales ou réglementaires.
   Cette analyse permet d'établir un périmètre clair et priorisé.
2. **Définition des objectifs de sauvegarde (RPO/RTO)**
   Nous définissons ensuite le RPO et le RTO pour chaque catégorie de données, en fonction de leur importance métier et de leur volumétrie.
   À partir de ces objectifs, nous choisissons les types de sauvegarde les plus adaptés, entre sauvegarde complète, incrémentielle ou différentielle, afin

d’équilibrer performance, rapidité de restauration et charge pour l’infrastructure.

3. **Choix des solutions de sauvegarde**
   Nous comparons les solutions techniques envisageables : NAS internes et externes, serveurs dédiés, solutions Cloud souveraines ou hybrides.
   Nous analysons également les logiciels compatibles, comme Veeam ou Acronis, en considérant leurs avantages et limites.
   Les scripts PowerShell actuels montrent leurs limites, notamment sur la fiabilité, le chiffrement et l’absence de SLA.
   La souveraineté des données et les engagements contractuels des fournisseurs Cloud sont intégrés aux critères d’évaluation.
4. **Planification des sauvegardes**
   Nous définissons ensuite la fréquence des sauvegardes en tenant compte de la criticité des données, de la charge réseau et du temps de restauration attendu.
   Les créneaux horaires sont choisis pour minimiser l’impact sur la production.
   Nous prévoyons également une stratégie de tests réguliers de restauration afin de valider l’intégrité et la disponibilité des sauvegardes.
5. **Rédaction du plan final**
   La dernière étape consiste à formaliser la stratégie retenue : RPO et RTO par niveau de criticité, calendrier des sauvegardes, technologies choisies, architecture 3-2-1, exigences de sécurité, conformité réglementaire, et critères de sélection des fournisseurs Cloud.
   Ce plan constitue la base opérationnelle du futur dispositif de résilience.

# Réalisation

1. **Identification des données critiques**
   Nous avons analysé la classification fournie : 2 To de données critiques (clients, finances, projets), environ 500 Go de données importantes (RH, accompagnées d’un volume non précisé d’emails professionnels), et 1 To de données moins critiques (documents généraux).
   Les données critiques sont indispensables au fonctionnement de l’entreprise et doivent être restaurées prioritairement.
   Les données importantes comportent des obligations légales de conservation, alors que les moins critiques tolèrent une restauration différée ou partielle.
2. **Définition des nouveaux objectifs RPO/RTO**
   Les objectifs actuels de 24 h se révèlent insuffisants au regard de l’activité et des risques.

Nous avons fixé des objectifs réalistes : un RPO de 6 h et un RTO de 12 h pour les données critiques, un RPO de 12 h et un RTO de 24 h pour les données importantes, et un RPO de 24 h et un RTO de 48 h pour les données moins critiques.

Ces objectifs sont atteignables en tenant compte des performances des NAS RAID 6, de la bande passante disponible et de la capacité à exécuter plusieurs types de sauvegardes.

3. **Choix des types de sauvegarde**

   Nous avons défini une stratégie adaptée à chaque type de données.

   Pour les données critiques, une sauvegarde complète tous les deux jours accompagnée de sauvegardes incrémentielles toutes les six heures permet d'atteindre un RPO de 6 h tout en limitant la longueur de la chaîne de restauration. Ce compromis réduit considérablement le temps de reprise et évite les faiblesses d'une longue chaîne incrémentielle, particulièrement vulnérable face aux risques de corruption et aux attaques par rançongiciel.

   Pour les données importantes, une sauvegarde complète hebdomadaire complétée par une sauvegarde différentielle quotidienne simplifie la restauration tout en respectant les contraintes légales et un RTO de 24 h.

   Pour les données moins critiques, une sauvegarde complète hebdomadaire associée à une sauvegarde incrémentielle quotidienne est suffisante, compte tenu de leur faible impact métier.

4. **Choix du RAID pour les NAS**

   Les NAS de Berria utilisent un RAID 6. Ce choix est pertinent car il offre une forte tolérance aux pannes (perte de deux disques possible sans interruption), une capacité utile plus élevée qu'un RAID 10, et de très bonnes performances en lecture, particulièrement utiles lors des restaurations d'urgence.

   Le RAID 10, bien que supérieur en écriture, réduirait la capacité disponible et serait moins adapté à des sauvegardes volumineuses et majoritairement séquentielles.

   Le RAID 6 représente donc le meilleur compromis entre sécurité, capacité et performance pour une infrastructure de sauvegarde.

5. **Synthèse du plan final**

   Nous avons consolidé l'ensemble des décisions dans un plan structuré intégrant les RPO et RTO révisés, les méthodes de sauvegarde retenues pour chaque niveau de criticité, les solutions techniques locales et Cloud, l'utilisation d'une architecture 3-2-1, ainsi que les exigences en matière de sécurité, de conformité réglementaire et de disponibilité.

   Ce plan constitue un socle opérationnel permettant à Berria d'améliorer nettement sa résilience face aux incidents majeurs, notamment les rançongiciels.