

PRA / PCA : assurer la continuité d'activité

Combien de temps votre entreprise peut-elle tenir sans informatique ? Construire un plan de reprise réaliste.

11 min de lecture · Niveau Avancé · cyberionis.fr/ressources/pr-pca

Le Plan de Reprise d'Activité (PRA) décrit comment redémarrer l'informatique après un sinistre ; le Plan de Continuité (PCA) comment continuer à travailler pendant. Pour une PME, il ne s'agit pas de produire un classeur de 200 pages, mais de répondre à quelques questions concrètes avant que l'incident ne les pose.

1. Les deux questions fondatrices

Deux chiffres, définis par le métier et non par la technique, dimensionnent tout le reste — fréquence des sauvegardes, redondance, budget :

- RTO (délai de reprise) : combien de temps pouvez-vous tenir sans chaque système ? Une heure ? Un jour ? Une semaine ?
- RPO (perte de données admissible) : combien de données pouvez-vous perdre ? Une heure de travail ? Une journée ?

2. Construire un plan proportionné

- Cartographier les systèmes critiques : sans quoi l'activité s'arrête vraiment ?
- Définir l'ordre de restauration (messagerie ? facturation ? production ?)
- Prévoir des solutions de contournement : travailler en 4G si le réseau tombe, basculer la téléphonie sur mobile
- Documenter les contacts, licences, mots de passe d'urgence — accessibles hors ligne
- Tester le plan par un exercice annuel, même modeste

3. Le bon niveau pour une TPE/PME

Un PRA de PME tient souvent en quelques pages : les scénarios majeurs (serveur mort, ransomware, incendie, coupure prolongée), et pour chacun qui fait quoi, avec quels moyens, en combien de temps. L'essentiel est qu'il existe, qu'il soit à jour et que quelqu'un d'autre que « la personne qui sait » puisse l'exécuter.

4. L'exercice annuel : le test qui révèle tout

Un plan jamais testé est une fiction rassurante. L'exercice n'a pas besoin d'être spectaculaire pour être utile :

- L'exercice sur table (2 heures) : autour d'un café, dérouler un scénario — « le serveur est chiffré, il est lundi 8 h » — et vérifier que chacun sait quoi faire ; noter tout ce qui coince
- Le test technique : restaurer réellement un système depuis les sauvegardes et chronométrer — le chiffre

obtenu EST votre RTO réel, souvent loin de celui espéré

- Le test d'absence : la personne clé est injoignable — quelqu'un d'autre peut-il exécuter le plan avec la seule documentation ?
- Après chaque exercice : mettre à jour le plan avec les leçons, et re-planifier le suivant

CAS CONCRET

Découverte classique lors d'un premier exercice sur table : les sauvegardes fonctionnent, mais la restauration complète du serveur prend 30 heures — pour un RTO métier fixé à 4 heures. Mieux vaut l'apprendre autour d'un café que devant un ransomware : ici, la réponse fut un serveur de secours à moins de 100 € par mois.

L'essentiel à retenir

- 01 Définir RTO et RPO pour chaque système critique
- 02 Écrire les scénarios de sinistre majeurs et les réponses associées
- 03 Conserver une version imprimée ou hors ligne du plan
- 04 Vérifier que les sauvegardes permettent réellement de tenir le RPO
- 05 Chronométrer une restauration réelle : c'est votre vrai RTO
- 06 Faire un exercice (au moins sur table) une fois par an

Questions fréquentes

PRA et PCA, faut-il vraiment les deux ?

Ce sont deux réponses à la même question, à des moments différents : le PCA fait tenir l'activité PENDANT l'incident (travailler en 4G, procédures manuelles, téléphonie de secours), le PRA remet l'informatique debout APRÈS. Une PME pragmatique les traite dans un même document de quelques pages — l'important est de couvrir les deux temps.

Quel budget pour un PRA de PME ?

L'écriture du plan coûte surtout du temps de réflexion. Les moyens techniques dépendent de vos RTO/RPO : des sauvegardes bien faites suffisent pour un RTO de 24-48 h ; un RTO de quelques heures demande de la réplication ou un serveur de secours (dizaines à centaines d'euros par mois en cloud). C'est précisément l'intérêt de fixer les RTO d'abord : ils dimensionnent le budget, pas l'inverse.

Nous sommes 100 % cloud (Microsoft 365, logiciels SaaS). Avons-nous encore besoin d'un PRA ?

Oui, mais différent : vos scénarios deviennent la perte d'accès (compte piraté, Internet coupé), la défaillance ou la fermeture d'un fournisseur SaaS, et la suppression de données (le cloud réplique vos erreurs). Le plan couvre alors : sauvegardes indépendantes des données SaaS critiques, connexion Internet de secours (4G), et procédure de récupération des comptes.

Qui doit porter le sujet dans l'entreprise ?

La direction — pas l'informatique. Les questions fondatrices (combien de temps peut-on tenir sans facturation ? quelle perte de données est acceptable ?) sont des décisions métier avec des implications budgétaires. Le prestataire IT traduit ensuite ces choix en solutions techniques.

Pour aller plus loin

Cybermalveillance.gouv.fr — plan de continuité pour les TPE/PME — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

ANSSI — maîtrise du risque numérique — cyber.gouv.fr/publications/maitrise-du-risque-numerique-latout-confiance

Vos sauvegardes tiendraient-elles le choc ?

Mise en place, tests de restauration, plan de reprise : nous rendons votre activité résiliente, à votre échelle.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr