Modèle de plan de reprise d'activité PRA

Ce document constitue un **modèle de plan de reprise d'activité (PRA)** à destination des entreprises.

Son objectif ? Vous aider à structurer votre réponse en cas d'incident majeur affectant vos **systèmes d'information** ou votre **infrastructure informatique**.

Il vous revient de l'adapter selon les spécificités de votre structure : secteur d'activité, taille d'équipe, criticité des ressources, architecture IT, etc.

Informations générales

- **Nom de l'entreprise** : [Nom de votre société]
- **Responsable du PRA** : [Nom, fonction, contact]
- **Date de dernière mise à jour** : [JJ/MM/AAAA]
- **Version** : [X.X]
- **Périmètre couvert** : [ex. Systèmes d'information, applications métiers, données clients, etc.]

---

1. Analyse des risques

Risques identifiés :

- Cyberattaque (ransomware, intrusion, vol de données)
- Panne matérielle (serveur, disques, onduleur)
- Sinistre naturel (inondation, incendie, tempête)
- Erreur humaine (suppression accidentelle, mauvaise manipulation)
- Coupure électrique ou réseau prolongée

---

2. Activités critiques et ressources essentielles

Activités prioritaires à relancer :

- Accès aux outils de production
- ERP (gestion des commandes, facturation)
- Service client (emails, téléphone, chat)
- Accès aux bases de données internes

Ressources nécessaires :

- Serveurs cloud / locaux
- Logiciels métiers
- Accès internet sécurisé
- Équipes IT, prestataires externes, responsables métiers

---

3. Objectifs de reprise

- **RTO (Recovery Time Objective)** :
    - ERP : 2 heures
    - Email : 4 heures
    - Réseau interne : 1 heure
    - Site web : 12 heures
- **RPO (Recovery Point Objective)** :
    - Données clients : 1 heure
    - Documents internes : 4 heures
    - Données financières : 24 heures

---

4. Mesures préventives mises en place

- Sauvegardes automatiques quotidiennes (cloud + local)
- Redondance des serveurs critiques

- Double alimentation électrique (onduleur)
- Formation des équipes à la cybersécurité
- Supervision 24/7 du système d'information

---

5. Scenarii et procédures de reprise

Cas 1 : Panne serveur principal

- Basculer sur le serveur de secours hébergé à [lieu]
- Informer les équipes via le canal de communication interne
- Relancer l'accès aux applications critiques

Cas 2 : Cyberattaque (ransomware)

- Isoler immédiatement le système infecté
- Alerter l'équipe sécurité et le DPO
- Restaurer les données à partir des sauvegardes validées
- Informer les autorités si nécessaire (CNIL, ANSSI)

Cas 3 : Inondation du site principal

- Activation du site de repli à [adresse]
- Reconfiguration des accès distants
- Communication externe vers les clients/partenaires

---

6. Documentation et communication

- Plan diffusé à : équipe IT, direction générale, responsables d'activité
- Version imprimée disponible dans le local sécurisé
- Fiche contact d'urgence en annexe

- Communication de crise préparée (email type, message vocal, bannière web)

---

7. Tests et maintenance

- Test PRA technique : tous les 6 mois
- Test PRA organisationnel : 1 fois par an
- Mise à jour du plan après chaque incident significatif
- Revue annuelle avec l'ensemble des responsables métiers

📎 Annexes

- Annexe A : Liste des contacts d'urgence
- Annexe B : Check-list post-sinistre
- Annexe C : Architecture du système d'information
- Annexe D : Procédure de restauration des données
- Annexe E : Plan de communication