Plan de reprise d'activité (PRA)

Le PRA, parfois appelé Disaster recovery plan (DRP) en anglais, est un document stratégique et opérationnel qui définit comment une organisation peut redémarrer son activité après un incident majeur (cyberattaque, panne, incendie, inondation, coupure réseau, 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)

2. Activités critiques et ressources essentielles

2.1. Activités prioritaires à relancer

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

2.2. Ressources nécessaires

- Logiciels métiers
- Accès internet sécurisé.

3. Objectifs de reprise

3.1. RTO (Recovery Time Objective)

ERP 2 heures

Email 4 heures

Réseau interne 1 heure

Outils de production 2 heures.

3.2. RPO (Recovery Point Objective)

Données clients 1 heure

Documents internes 4 heures

Données financières 24 heures

4. Mesures préventives mises en place

Utilisation d'outils cloud compatibles avec le présent PRA.

Sauvegardes automatiques quotidiennes (redondance cloud).

Formation des équipes à la cybersécurité.

5. Scenarii et procédures de reprise

5.1. Cas 1 : Panne d'un site Internet client en production

1. Informer les équipes via le canal de communication interne
2. Redéployer une instance
3. Déployer l'application sur la nouvelle instance

4. Reconfigurer les accès distants si nécessaire

5. Information du client

5.2. Cas 2 : Cyberattaque (ransomware) sur un site Internet client en production

1. Isoler immédiatement le système infecté

2. Alerter l'équipe sécurité et le DPO

3. Redéployer une instance fraîche

4. Déployer l'application sur la nouvelle instance

5. Restaurer les données à partir des sauvegardes validées

6. Reconfigurer les accès distants si nécessaire

7. Information du client

8. Information des autorités si nécessaire (CNIL, ANSSI)

6. Documentation et communication

Plan diffusé à toute l'équipe ; Plan accessible publiquement sur le site https://gouvernance.noesya.coop ; Communication de crise préparée (emails type).

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 de l'équipe.

8. Révisions

1.0 Date of change: 25/08/2025 - Responsible: Technical team - Summary of Change: Initial release