

# Plan de Reprise d'Activité

---

## Évaluation des risques :

- **Physiques :**

Nous n'avons pas de serveurs physiques, il est donc inutile de prendre en charge les risques physiques tels que les catastrophes naturelles (inondation, tsunami, tempête) ou les risques dus aux humains tels que les attentats, les erreurs de construction...

- **Informatique :**

Il faut prendre en compte les risques liés aux cyberattaques ou à un virus, mais aussi les erreurs de configuration des serveurs, routeurs, etc...

## Priorités selon les types d'incidents :

- **Liste du « matériel » (physique et virtuel) dont nous disposons :**

*Le matériel est trié selon un ordre décroissant des priorités de récupération.*

- 1. Différentes sauvegardes :**

- i. Fichiers de configuration du serveur HTTP
- ii. Site internet (moins important)

- 2. Serveur DNS et DHCP**

- 3. Serveur HTTP**

- 4. Serveur DNS esclave**

- 5. Site de supervision**

- 6. Postes clients (Windows 10)**

- 7. Site e-commerce (réalisé par une autre entreprise)**

## Conditions d'application du PRA :

Le plan de reprise d'activité nécessite des prérequis avant de pouvoir être appliqué dans un système.

Le prérequis le plus courant serait un incident limitant voire arrêtant l'activité du système.

Par exemple, des problèmes techniques (virus, cyberattaque...) ou encore des phénomènes naturels (inondations, tremblements de terre...) ou encore des problèmes liés à l'homme (incendie, attentats...)

## Stratégie de sauvegarde/récupération :

### - Mesures Préventives :

Pour ne pas perdre les sauvegardes des fichiers de configuration du serveur HTTP et du site internet, nous devons effectuer les sauvegardes en deux exemplaires et les stocker à des endroits différents pour plus de sécurité.

Les sauvegardes seront effectuées à l'aide de script permettant des sauvegardes ponctuelles et régulières toutes les semaines pour le site Internet et tous les mois pour les fichiers de configuration.

La configuration du réseau ne pourra être accessible seulement par un administrateur muni d'un code d'accès ce qui permet d'avoir une sécurité amplifiée et ainsi éviter des risques.

### - Mesures Défectives :

Pour éviter que des problèmes mineurs ne deviennent majeurs, il est nécessaire d'avoir identifier le problème le plus tôt possible afin qu'il soit résolu au plus vite.

Des problèmes liés à la connexion au site WEB peuvent survenir, donc pour l'identifier le plus rapidement possible, un script effectue un ping et des tests d'accès au site web toute les 5 minutes pour vérifier l'état de la connexion et le rentre dans un fichier au format CSV consultable continuellement par des techniciens.

Ils peuvent par la suite permettre une remise en état du système avec rapidité. Il faudrait aussi pouvoir être informé par les visiteurs du site s'ils remarquent un problème (bug ou tout autre problème pouvant être dérangeant).

Un service client serait donc un outil permettant de déceler les problèmes sur le site et être pris en charge par des techniciens avant qu'ils ne deviennent très important.

### - Mesures Correctives :

#### ○ Données nécessaires pour le nouveau système relais :

Le nouveau système aura besoin pour fonctionner des sauvegardes des configurations effectuées à l'aides des scripts qui permettent une sauvegarde des fichiers.

Ces fichiers seront sauvegardés dans les fichiers de sauvegardes correspondant à la date de sauvegarde. Exemple : Web\_Backup\_date

#### ○ Temps nécessaire pour la mise en place du nouveau système :

Pour la mise en place du nouveau système, nous avons besoin d'une durée allant de 20min à 25min pour effectuer le transfert des sauvegardes vers le nouveau système.

## Quantité de données maximale perdues lors du PRA :

En chargeant une ancienne sauvegarde, on perd des données. Ces données ne peuvent pas être récupérées pour une question de sécurité.

Nous devons donc savoir quelle serait la quantité maximale de données perdues dans l'application du PRA. Effectuer une sauvegarde toutes les semaines permettent d'avoir une perte éventuelle de données de maximum une semaine si les techniciens n'identifient pas assez vite le problème, ce qui peut paraître long pour les grosses entreprises.

## Procédures de test :

- Effectuer des sauvegardes
- « Arrivée théorique du problème »
- Identification de la sauvegarde voulu (la plus récente sans le problème rencontré)
- Création d'une nouvelle machine virtuelle
- Suivre la « Procédures d'installation et de configurations des serveurs » (documents dans les livrables), pour pouvoir remettre en état les serveurs (DNS « maître et esclave », http, DHCP).
- Remplacer les fichiers de configuration nouvellement installés par les fichiers de configurations sauvegardés tous les mois.
- Reprise des sauvegardes des données du site Internet de l'entreprises
- Reprise d'activité du système

## Test du PRA :

Dans un premier temps, pour effectuer le test il faut avoir des sauvegardes, nous en effectuons donc pour faire des tests. Puis dans la théorie un problème survient pour devoir effectuer le PRA.

Puis nous suivons la « Procédures d'installation et de configuration des serveurs » pour remettre fonctionnel les serveurs.

Nous commençons donc par chercher la sauvegarde que l'on veut charger. Elles se trouvent dans le dossier comprenant toutes les sauvegardes, et elles sont nommé par date.

Après avoir identifié la date de la sauvegarde voulue, il faut la charger pour remplacer les données actuelles par la sauvegarde sélectionné. Cela permet de résoudre des problèmes majeures et irrésolvables autrement, tel qu'une corruption des données ou encore une perte de données totale ou presque total.

Puis le système reprend son activité normale avec certes des données en moins mais est sécurisé.

Au total le plan de reprise d'activité à une durée d'environ 30min pour être exécuté dans son intégralité.