

Fiche pratique pour la mise en oeuvre de votre plan d'actions cyber dans votre collectivité.

### Description rapide de l'objectif visé :

Une fois par an une vérification du bon fonctionnement des sauvegardes et un test de restauration technique sont réalisés.

### Coût estimé :

0 €



### Niveau de difficulté de l'action :

Moyen



### Ressources nécessaires :

Ordinateur, support de sauvegarde, un fichier issu d'une sauvegarde



### Niveau d'accompagnement :

Elevé



### Temps estimé :

1 jour



### Public visé pour l'action :

Responsable informatique  
Personne en charge de l'informatique



### Organisation conseillée pour la mise en œuvre dans votre collectivité :

#### 1. Qui fait quoi ? Définir les rôles et responsabilités.

Qui a la responsabilité des supports de sauvegarde ?  
Qui réalise le test de restauration de sauvegarde ?  
Qui s'assure de l'intégrité de l'élément restauré ?

#### 2. Pourquoi ?

Communiquer pour expliquer la démarche à vos collaborateurs. Un test de restauration de sauvegarde permet de vérifier l'intégrité de la donnée restaurée et donc de tester le bon état des sauvegardes.

#### 3. Comment ?

Un fichier devra être restauré à partir d'une sauvegarde. Sollicitez un ou des utilisateurs pour le vérifier le résultat du test de restauration. Restaurez un fichier exploité par l'utilisateur qui pourra ainsi attester de son intégrité. Une fois le test achevé, un procès-verbal doit être signé par l'utilisateur et le référent informatique.

#### 4. Combien ?

Un test de restauration par an.

#### 5. Quand ?

Une fois par an.

## Livrable de l'action terminée :

Procès-verbal signé et contre-signé.

Procès-verbal suite à un test de restauration

Matrice Restauration de fichiers				
Date de l'action	Fichier concerné (chemin complet)	Opération (modification ou suppression)	Résultat Restauration Succès (oui/non)	Signature du membre du groupe de travail concerné

## Description étape par étape pour la mise en œuvre :

1. Vérifier la bonne configuration des sauvegardes
2. L'utilisateur choisit un fichier à restaurer.  
Conseil : Restaurez un fichier exploité régulièrement afin de tester sa bonne restauration en cas d'incident.
3. La personne en charge des sauvegardes restaure le fichier choisi dans un dossier de test qu'il aura préalablement créé après avoir attendu qu'une sauvegarde du dossier soit réalisé.
4. Une fois l'élément restauré, l'utilisateur est invité à en vérifier la conformité et l'intégrité.
5. Une fois le test achevé, que le résultat de la restauration soit concluant ou non, un procès-verbal est contre-signé par l'utilisateur et le référent informatique.
6. Conserver soigneusement le procès-verbal.

## Pour aller plus loin :

ANSSI :  
- [Guide des bonnes pratiques de l'ANSSI](#)

Cybermalveillance :  
- [Fiche sauvegarde](#)