**Mission2**

**10-méthode efficace pour s’assurer que les données ne seront pas lues ou modifiées**

1. Adopter une politique de mot de passe rigoureuse

### Concevoir une procédure de création et de suppression des comptes utilisateurs

### Sécuriser les postes de travail

### Identifier précisément qui peut avoir accès aux fichiers

### Veiller à la confidentialité des données vis-à-vis des prestataires

### Sécuriser le réseau local

### Sécuriser l’accès physique aux locaux

### Anticiper le risque de perte ou de divulgation des données

### Anticiper et formaliser une politique de sécurité du système d’information

### Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

**Définition :**

Confidentialité : (Maintien du secret d’informations) c’est le fait de s'assurer que l'information n'est accessible qu'à ceux dont l'accès est autorisé.

Intégrité : c’est l'exactitude, l'exhaustivité et la cohérence globales des données. L'intégrité désigne également la sûreté des données concernant la conformité à la réglementation (ex : la conformité au RGPD, la sécurité)

Disponibilité : c’est la capacité d'accomplir la fonction donnée dans le temps imparti et dans des conditions d'exploitation considérées comme normales.

La non-répudiation : c’est l’impossibilité, pour une personne ou pour toute autre entité engagée dans une communication par voie informatique, de nier avoir reçu ou émis un message.

L’authentification : c’est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).

Certificat : c’est une information que l'on ajoute à une donnée du problème pour certifier qu'elle est (ou n'est pas) solution.

Tiers de confiance : c’est une personne physique ou morale mettant en œuvre des services de confiance (ex : les signatures électroniques).