Principes fondamentaux de la sécurité de l'information.

1. **Intégrité des données:** Ce principe concerne la garantie que les données restent exactes, complètes et non altérées. L'intégrité des données vise à prévenir toute modification non autorisée, corruption ou altération des informations.
2. **Confidentialité des données:** La confidentialité concerne la protection des données contre tout accès ou divulgation non autorisé. Cela garantit que seules les personnes ou entités autorisées ont accès à des informations sensibles, préservant ainsi la confidentialité.
3. **Disponibilité:** La disponibilité se concentre sur la garantie que les données et les ressources informatiques sont accessibles et utilisables lorsque nécessaire. Cela inclut la prévention des interruptions de service, des pannes, et d'autres problèmes qui pourraient empêcher l'accès aux données.
4. **Non répudiation:** Ce principe vise à empêcher une partie de nier l'authenticité ou l'origine de certaines actions, communications ou transactions. La non-répudiation assure qu'une entité ne peut pas renier sa participation à une activité spécifique.
5. **Authentification:** L'authentification est le processus de vérification de l'identité d'une personne, d'un système ou d'un processus. Cela garantit que seules les entités autorisées ont accès aux ressources ou aux informations, renforçant ainsi la sécurité en empêchant l'accès non autorisé.