A.Définition d'information

1- Selon P.ROMAGNI & V.WILD, l'information est considérée comme « un renseignement qui améliore notre connaissance sur un sujet quelconque ».

2- Le dictionnaire le petit Larousse présente l'information comme : « un renseignement obtenu de quelqu'un ou sur quelque chose, ou une nouvelle communiquée par un agence de presse, un journal, la radio, la télévision »

B. Les sources de l'information

Les sources d'information pour l'entreprise peuvent être regroupées en 2 ensembles :

- Sources internes : données statistiques (ventes, ratios financiers, effectifs…) rapports et notes de services, documents comptables…
- Sources externes : médias (presse et internet), partenaires de l'entreprise (clients, fournisseurs, banque, bases de données des greffes…)

Pour être utile, l'information doit avoir plusieurs caractéristiques :

- Fiabilité (vérifiable)
- Pertinence (répondre à besoin précis)
- Disponibilité (pouvoir être obtenue rapidement et à un cout absorbable)

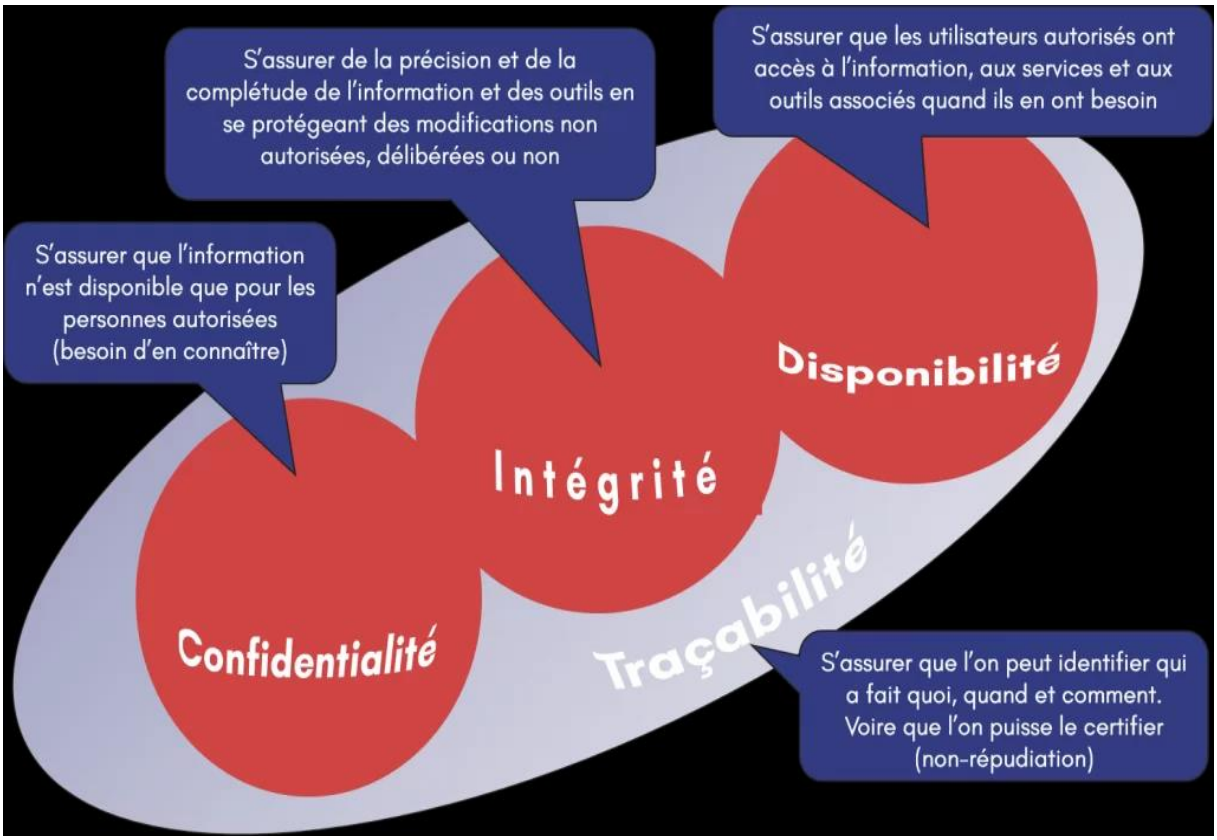
La maîtrise de l'information est devenue progressivement une source de compétitivité fondamentale. Une véritable question stratégique.

C- la sécurité de l'information

- Définition : Sécurité des SI=
  - Protéger les biens et informations les plus précieuses pour l'entreprise.

La sécurité de l'information se caractérise par :

1- La protection de la confidentialité,
2- L'intégrité et de la disponibilité de l'information.
3- La sensibilité » de l'information
4- La traçabilité de l'information



Représentation des 4 axes définissent la sécurité de l'information

- Critères d'évaluation de la sécurité de l'information :

La sécurité peut s'évaluer suivant plusieurs critères :

Disponibilité : garantie que ces éléments considérés sont accessibles au moment voulu par les personnes autorisées.

Intégrité : garantie que les éléments considérés sont exacts et complets.

Confidentialité : garantie que seules les personnes autorisées ont accès aux éléments considérés.

Traçabilité (ou « **Preuve** ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

D-Les Risques

- Mesurés par la combinaison d'une menace et des pertes qu'elles pourraient engendrées
- Plusieurs éléments :
  - Méthode d'attaque
  - Éléments menaçants
  - Vulnérabilités des entités
- Attaque passive
- Attaque active
- Usurpation
- Répudiation.
- Intrusion

- **Exemple de risque décomposé:**
- Méthode d'attaque = piégeage du logiciel (introduction d'un ver)
- Élément menaçant = un pirate expérimenté engagé par un concurrent
- Entité = reseau WIFI
- Vulnérabilité = possibilité d'administrer le réseau à distance
- Opportunité jugée = Moyenne
- Atteinte des éléments essentiels = atteinte à la confidentialité (vol d'informations)
- Impact sur l'organisme = perte d'avantages concurrentiels

E- Sécurité de l'information de Protection

Protéger les données stockées ou en transit sur le réseau contre :

- Modification (destruction) non autorisée
- Utilisation frauduleuse
- Divulgation non autorisée
- **Sécuriser** l'accès aux systèmes, services et données par :
- Vérification de l'identité déclinée par le requérant
- Gestion des droits d'accès et des autorisations

1. Cryptographie

- Ensemble des techniques permettant de crypter / décrypter des messages
- Crypter : brouiller l'information, la rendre "incompréhensible"
- Décrypter : rendre le message compréhensible

Ill existe de types de cryptographie

1-1 Cryptographie : Clé Symétrique

Même clé pour chiffrer et déchiffrer

Avantages :

Facile à implémenter
Rapide

1-2 Cryptographie : Clé Asymétrique

Chaque communicant possède une paire de clés associées : clé publique **Kpb** et clé privée **Kpv**
Un message chiffré par l'une des clés
Ne peut pas être déchiffré par cette même clé
Mais peut être déchiffré par l'autre clé de la paire

- La clé privée doit être conservée par son propriétaire
  - Rien n'impose de la dévoiler à qui que ce soit
  - La clé publique est diffusée sans restriction

- Idéalement avec un niveau de diffusion comparable à l'annuaire téléphonique
- Aucun moyen pratique de déduire l'une des clés de la connaissance de l'autre clé

Avantages de la Cryptographie

- Message chiffré avec la clé publique
  - Seul le propriétaire de la clé privée correspondante peut en prendre connaissance : **confidentialité**
    - Le receveur n'a aucune idée de l'expéditeur puisque la clé publique est accessible à tous

- Message chiffré avec la clé privée
  - Altération frauduleuse impossible car nécessite la connaissance de la clé privée : **intégrité**
    - Pas de confidentialité : la clé publique peut être utilisée par tous pour lire
  - La clé privée dévoile **l'identité** de l'expéditeur
    - Propriétaire de la clé privée

Inconvénients de la Cryptographie

- Algorithmes complexes et difficiles à implémenter
- Peu performant : long et gourmand en CPU
  - ≈ 1000 plus lents que les algorithmes à clés symétriques
- Moins sûrs contre les attaques de « force brute »
  - Nécessite des clés plus longues que les algorithmes symétriques

Calcule un « condensé significatif » de taille fixe, quelque soit la taille d'origine

- Irréversible : transformation inverse impossible
- Déterministe : le même message produit le même résumé

effets imprévisibles

L'intégrité du résumé significatif est une garantie de l'intégrité du document d'origine

C'est une « empreinte digitale » du document.