

**Ministère de l'enseignement supérieur et de la recherche scientifique**

**Université de Batna 2**

**Institut d'hygiène et sécurité**

**Département Sécurité Industrielle**

**Enseignant : Mr Abdelouahab Makhloufi**

**Support de cours destiné aux étudiants de Licence L3 SIE**

## **Intitulé du cours : Sécurité de l'information**

**Semestre 2 - Année : 2019/2020**

### **Programme**

I : Généralités sur la notion de l'information

II : Différents supports de l'information

III : Systèmes d'information

IV : La Sécurité de l'information : (Qu'est-ce que la sécurité ? Menaces et Attaques, Les objectifs de la sécurité de l'information : Confidentialité, Intégrité, Disponibilité, Les mesures de sécurité)

# **I : Généralités sur les notions : Information et Communication, TIC, Multimédia.**

## **Information**

### **Qu'est-ce que l'information ?**

**Étymologie** : du latin *informare*, façonner, former.

l'étymologie latine du terme information

(du verbe *informare* : action de former, de façonner), ils mettent en valeur ses différents usages.

### **Plusieurs sens : dépend du contexte d'utilisation**

**Sens 1** : Une information est une nouvelle, un renseignement, une documentation sur quelque chose ou sur quelqu'un, portés à la connaissance de quelqu'un. Exemple : un bulletin d'informations.

**Sens 2** : L'information est l'**actualité**, les **nouvelles** diffusées par les médias : presse, radio, télévision, Internet. Familier : les infos.

**Sens 3** : En droit, une **information judiciaire** est une enquête judiciaire déclenchée par le procureur de la République dans les affaires complexes et confiée à un juge d'instruction, préalablement au jugement.

### **Référence :**

*Sylvie Leleu-Merviel, Philippe Useille. « Quelques révisions du concept d'information ». Hermès. Problématiques émergentes dans les sciences de l'information, Lavoisier, pp.25-56, 2008*

L'information est un **élément de connaissance**, qui peut être **collecté, traité, conservé, communiqué** au sein de l'organisation ou auprès de ses partenaires.

L'information est constituée de deux éléments :

- des **données**,
- un **sens** qui dépend de chaque individu.

### **Exemple :**

Enseignant : le cours dure 3h

Étudiant : c'est vraiment long

3h : représente une donnée

Long : représente le sens de l'information

## Autres définitions

- des données, traces matérielles stockées, depuis une stèle de pierre jusqu'à des cristaux de silicone dans un disque dur. Elles perpétuent des signes (mots, images, sons, bits électroniques). Les données perdurent.
- des messages, information en mouvement, destinée à un récepteur capable de l'interpréter et de la distinguer comme signifiante d'entre tous les signaux. Ils circulent à travers l'espace et s'adressent à quelqu'un.
- des savoirs, de l'information, interprétée et mise en relation avec d'autres informations, contextualisée et faisant sens. Les connaissances sont produites par un cerveau. – des programmes, depuis le code génétique jusqu'à un logiciel, qui contiennent des instructions destinées à un agent matériel. Les programmes « font » virtuellement quelque chose.

L'information est une différence qui engendre des différences ou une forme qui fait sens pour un interprétant. Pour être une information, et pas du bruit, elle doit :

1. Émerger d'un fond ou d'un bruit, se distinguer, créer un minimum de surprise
2. Susciter une réaction qualitative chez celui qui la reçoit et l'interprète, que ce soit la compréhension d'un énoncé ou un simple état émotif. Contenir un minimum d'intelligibilité

L'information comme catégorie générale est l'incessant processus de passage entre des données, des messages, des connaissances et des programmes.

Dans l'usage courant et suivant le contexte, le même mot, information, désigne :

— son contenu (ce en quoi elle renseigne et innove, ce qu'elle nous apprend que nous ne savions pas) : L'info vient de tomber : le numéro gagnant au loto est le 768080“

– son acquisition (le fait d'être au courant, de l'avoir ou pas) ; merci, j'avais déjà reçu l'information.

– son mode de circulation (les moyens par lesquels elle parvient) : J'ai regardé les informations à la télévision

— sa mesure : Mon disque dur contient 70 gigabits d'information

— et le résultat attendu (le fait de « mettre en forme », conformément à l'étymologie, de savoir) : Cette dernière information me permet de conclure : le coupable est X

Dans l'usage courant, les termes « donnée » et « information » sont souvent considérés comme des synonymes. Cependant, lorsqu'on recherche la précision, il apparaît que la donnée ne devient une information que lorsqu'elle est reçue par un être humain qui l'interprète. Une information est une donnée observée par un acteur.

L'observation implique la comparaison à d'autres données pour qu'il y ait interprétation. Passer du rang de donnée à celui d'information suppose que la connaissance de la donnée contribue à l'action de celui qui l'observe. Les données (mots, nombres, images, sons, etc.) constituent donc la matière première de l'information par un processus d'interprétation qui leur attribue de la signification et du sens.

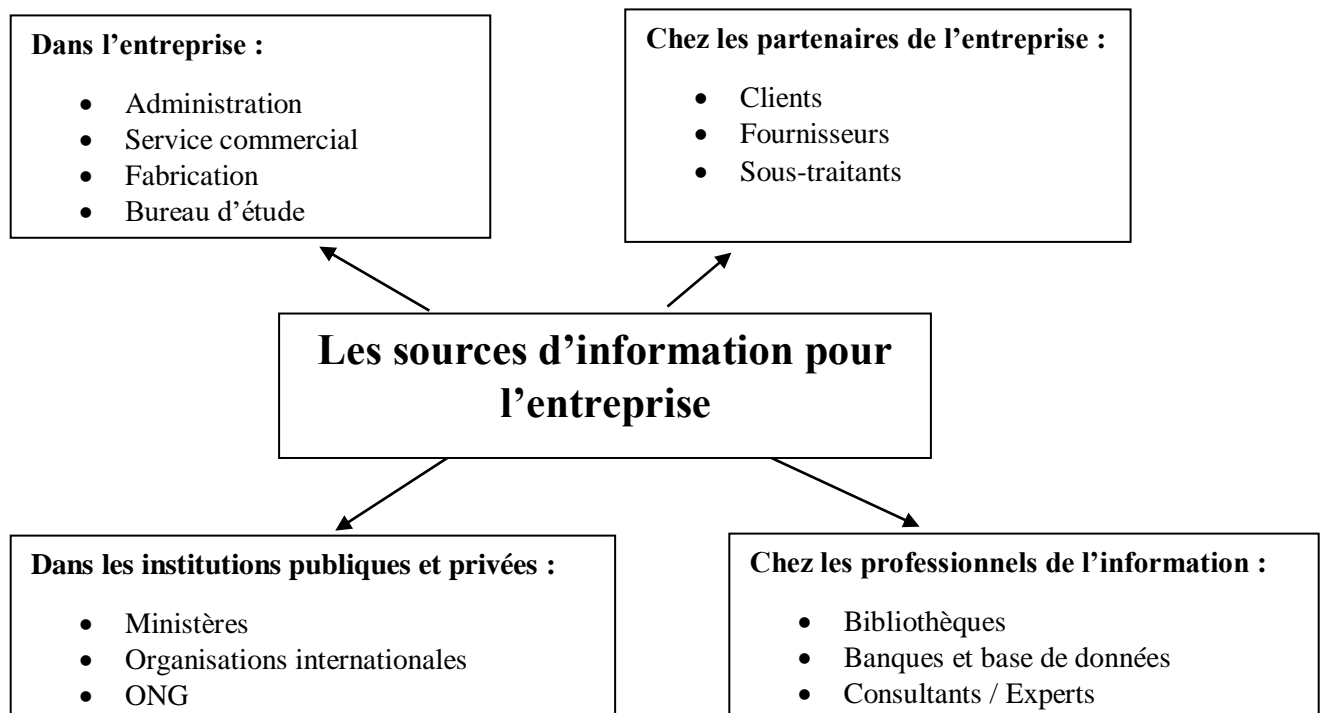
## Information comme outil de réduction d'incertitude

Pour March (1991), la principale incertitude dans la prise de décision est l'ignorance des informations détenues par les autres et leurs actions probables. La principale raison d'être de l'information est son rôle dans un processus de diminution de cette incertitude.

L'information a aussi une valeur, car elle permet de choisir, de prendre des décisions et d'agir. Sa valeur est ainsi liée à son emploi dans le contexte de prise de décisions. Ainsi pour March (1991), l'information donne son sens à une situation de décision et modifie donc à la fois la structure des options et les préférences recherchées.

Dans le même esprit, De Rosnay (1975) a proposé de définir l'information comme le contenu d'un message capable de déclencher une action. En effet, l'information n'aura de valeur, théoriquement du moins, que si elle a une influence sur les décisions à prendre ou les actions à mener. Comme le notent Amabile et Caron-Fasan (2002), l'attention se recentre sur les conditions qui lui permettent de prendre sens, et de fonder une interprétation utile pour l'action.

## Schéma : Sources d'information en entreprise



Source : schéma proposé par l'auteur

La source la plus importante d'informations sur une entreprise est naturellement l'entreprise elle-même. Les sources d'information peuvent être internes ou externes. En effet, les sources internes sont composées des fichiers propres à l'entreprise la renseignant sur l'activité de ses différents services et des statistiques qu'elle a pu faire pour analyser les fluctuations d'une période à l'autre (sur les ventes, sur les accidents du travail et les plannings). Les sources externes sont composées des renseignements et des données provenant des partenaires, des collaborateurs de l'entreprise, des institutions nationales et internationales ainsi que des professionnels de l'information à qui elle a pu en acheter.

## **La communication**

La communication est l'action de véhiculer un message, d'établir une relation avec autrui, de transmettre quelque chose à quelqu'un...etc

Elle peut aussi désigner l'ensemble des moyens et techniques permettant les diffusions d'un message auprès d'une audience plus ou moins vaste, ou l'action pour quelqu'un, ou une organisation d'informer et de promouvoir son activité auprès d'autrui.

Dans le cas d'une entreprise, la communication devient une action visant à informer et promouvoir l'activité de celle-ci auprès du public, d'entretenir son image à travers un procédé médiatique

C'est pourquoi, les entreprises se dotent d'une structure de communication qui tendra à faire connaître leurs prestations et leurs activités mais aussi à booster leurs notoriétés et image.

En résumé :

La communication est :

1 – une activité ...

De production, de transmission/diffusion, d'interprétation, de partage ...

2- de message (informations)

3 – entre personnes, groupes de personnes, institutions, etc

4 – via d'un ou de plusieurs médias et d'instruments (les canaux de transmission)

5 – au sujet d'un objet donné

6 – en fonction d'un objectif posé

7 – dans un contexte spécifique

8 – et en s'inscrivant dans une tradition (une culture)

La communication est également :

Une activité, une pratique sociale qui remplit 3 grandes fonctions dans la vie humaine :

**Fonction d'information** : = Production et circulation de messages, d'informations

**Fonction d'expression (ou de représentation)** : = « mise en scène » de l'identité des participants, de leur appartenance sociale et culturelle, ...

**Fonction relationnelle** : = création/maintien du « lien social », c.-à-d. des rapports sociaux (de domination, d'intérêts, ...)

## **Les formes de communication**

On distingue deux grandes formes de communication : la communication verbale et la communication non verbale.

### **La communication verbale**

Elle est constituée des signaux linguistiques ayant un sens comme les lettres, la ponctuation, les panneaux de signalisation qui appartiennent aussi à la communication non verbale (trois types de signes : indice, signal, symbole). Elle sert à évoquer une réalité. Les mots et le langage lui sont nécessaires, au travers de la parole. Le langage répond à une commande motrice volontaire. Les mots peuvent avoir un sens dénотatif (sens donné par le dictionnaire) et connotatif (sens qui dépend du contexte, et de la signification subjective de celui qui l'émet). Le soignant doit se détacher de cette subjectivité.

Dans de nombreuses pathologies, la communication verbale va être altérée, qualitativement ou quantitativement, voire devenir impossible. En effet, pour que la communication verbale puisse avoir lieu, plusieurs étapes sont nécessaires : élaboration d'un langage cohérent au niveau cérébral (aires du langage), production au niveau oral. Ainsi, les pathologies qui vont toucher soit les commandes motrices, les zones cérébrales du langage et le cortex frontal, soit l'appareil phonique, cordes vocales et oropharynx, vont entraver la possibilité du patient de communiquer.

Elle englobe la communication orale et la communication écrite

#### **-La communication orale :**

Il s'agit de l'émission et de la réception des messages, participation à des réunions, appels téléphoniques, entretiens, accueil des clients, débats, discussion...Mais la communication orale présente l'inconvénient de ne pas laisser de traces.

Dans le cadre de la communication orale, différents registres de langues doivent être utilisés selon les situations et les interlocuteurs :

- registre de langue soutenu : caractérisé par l'emploi d'un vocabulaire recherché, soigné et parfois maniéré. Utilisé surtout dans le cadre des conférences, des séminaires et des interventions en public.
- registre de langue courant : caractérisé par l'emploi d'un vocabulaire précis, simple et clair.
- registre de langue familier : langage relâché et non surveillé, comprend des mots d'argot et le style est souvent incorrect.

#### **- Communication écrite :**

Il s'agit des notes de service, d'instruction, du courrier, des convocations. Ce type de communication est fiable et peut être consulté autant qu'il est nécessaire. Sur le plan juridique il constitue de moyen de preuve en cas de conflits.

## La communication non verbale

C'est la transmission et le partage entre deux personnes d'éléments signifiants (ayant un sens) sans l'emploi de la parole. C'est le premier mode de communication dans l'instauration de la relation mère-bébé, au travers du toucher ou des gestes, du regard, des odeurs... Certaines formes de communication non verbale sont probablement biologiquement ou génétiquement déterminées et sont communes à de nombreuses cultures, restant temporellement tout à fait stables (par exemple, les expressions faciales).

La communication non verbale vient compléter la communication orale de différentes manières :

- simple complément ;
- accentuation du discours ;
- régulation du langage oral ;
- contradiction du langage oral.

Dans une relation, la communication non verbale est légèrement prépondérante sur le langage oral.

Appelée aussi « paralangage » est tout ce qui traduit une information à part ou en complément du langage verbal.

- **Les expressions du visage** : le sourire, le regard, les signes d'attention, d'étonnement, d'impatience, de rejet... peuvent se lire sur le visage de celui qui écoute et peuvent constituer une grande part du feedback.
- **Les gestes** : au travers des gestes, des attitudes nous envoyons et recevons un grand nombre de messages.
- **Les postures** : elles jouent un grand rôle dans la relation qui s'établit lors de la communication. (Ex. : la façon dont une personne est assise sur la chaise peut donner une impression de timidité, d'arrogance...).
- **L'accoutrement ou l'aspect vestimentaire** : Les choix vestimentaires ont une signification sociale, culturelle et personnelle. Ils peuvent servir de base aux jugements des autres.

## **II : différents supports de l'information**

### **QU'EST-CE QU'UN SUPPORT D'INFORMATION ?**

La fonction première du support est la fixation d'une trace (contenu) sur un matériau qui lui garantira une certaine stabilité et une certaine durabilité, et ce, au moyen d'une technique particulière d'inscription ou d'enregistrement.

On attend donc du support qu'il rende possible toute opération de production, de duplication, de conservation, de transmission et de manipulation d'un document. Le support peut être envisagé sous deux aspects liés à ces fonctions :

- Il est un substrat matériel, nécessaire pour recevoir et pour conserver.
- Il constitue un moyen technique, indispensable pour inscrire, pour diffuser ou pour restituer.

Un support de l'information évolue en fonction de l'avancée technologique et culturelle. Les premiers documents étaient sur tablette de bois ou de cire. Désormais, les supports peuvent être choisis en fonction de la nature de l'information à communiquer : son, image ou texte seuls, voire les trois ensembles comme le permettent les supports électroniques, par exemple.

### **TYPOLOGIE DES SUPPORTS D'INFORMATION**

→ Support écrit ou imprimé

- Livres (ouvrages, monographies, œuvres littéraires)
- Périodiques
- Articles de presse
- Correspondance
- Cartes
- Partitions
- Affiches

→ Support magnétique

## **III : Système d'information**

L'information se présente sous trois formes : les données, les connaissances et les messages. On a l'habitude de désigner par « système d'information » l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information.

Un système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler.

Organisation des activités consistant à acquérir, stocker, transformer, diffuser, exploiter, gérer... les informations.



La notion de système d'information a donné lieu à différentes interprétations et sa définition est loin de faire l'unanimité. Parmi les nombreuses définitions retenons celle donnée par Reix (2004) : « *un système d'information est un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures [...] permettant d'acquérir, de traiter, de stocker des informations (sous forme de données, textes, images, sons, etc.) dans et entre des organisations* ».

Le système d'information de l'entreprise se caractérise donc par l'ensemble des moyens et procédures qu'il utilise (traitements manuels et/ou automatisés, traitements centralisés et/ou répartis, système éclaté ou intégré, etc.). Sa finalité est de restituer, au moment opportun, des informations sous forme directement utilisable, à ceux qui en ont besoin pour contrôler, coordonner ou prendre des décisions. De nos jours, les ordinateurs, les langages de programmation, les logiciels, les équipements de télécommunication, etc., sont très utilisés dans les systèmes d'information. Leur prépondérance actuelle est en partie due à la baisse continue des coûts des matériels, à l'amélioration des logiciels disponibles et au progrès de la formation des spécialistes comme de celle des utilisateurs (Haouet, 2008).

### **Objectifs d'un système d'information**

Pour acquérir la « culture » d'un Système d'Information, nous devons :

- Être capable d'analyser des solutions commerciales et de dialoguer avec des fournisseurs de solutions logicielles
- Intégrer un logiciel au sein d'un SI existant
- Savoir identifier des flux d'information
- Pouvoir collaborer à la mise en place d'un SI
- Appréhender un SI à haut niveau, dans sa globalité
- Avoir des connaissances techniques pour mieux comprendre les problèmes à plus bas niveau

### **L'information, vitale pour l'entreprise**

- Société de l'information : (ou société de la connaissance)
  - ✓ Société dans laquelle les technologies de l'information (TIC) jouent un rôle central
  - ✓ Dans la continuité de la société industrielle
  - ✓ Jamais humanité autant reliée les uns aux autres
  - ✓ Avant Internet, pas facile d'entrer en contact avec inconnus
  - ✓ Éclatement des frontières, échanges facilités
- Marché mondialisé hyperconcurrentiel
  - ✓ L'entreprise doit anticiper les changements et adapter son fonctionnement

### **Analogie avec systèmes biologiques**

- Le SI peut être comparé à une sorte de **système nerveux** primaire de l'organisation
  - ✓ Circulation rapide d'une information de qualité entre les différents « organes »
  - ✓ Délivrer la bonne information, au bon interlocuteur, au bon moment
    - Prise de décisions appropriées
    - Action de l'entreprise adaptée à la situation
  - ✓ Le SI contribue donc de manière évidente aux performances de l'organisation

## Analyse Systémique de l'Entreprise

Apparue dans les années 1970

Entreprise = **Système**

- ✓ « Ensemble d'éléments en interaction dynamique, organisé en fonction d'un but » Joël De Rosnay « Le microscope », éditions du seuil, 1975
- ✓ L'entreprise est alors considérée comme un ensemble d'éléments (des moyens humains, matériels, financiers et techniques) en **interrelations**
- ✓ Toute organisation humaine (l'État, une famille, ...) peut être perçue comme un système

Comme tout système, l'entreprise est un système :

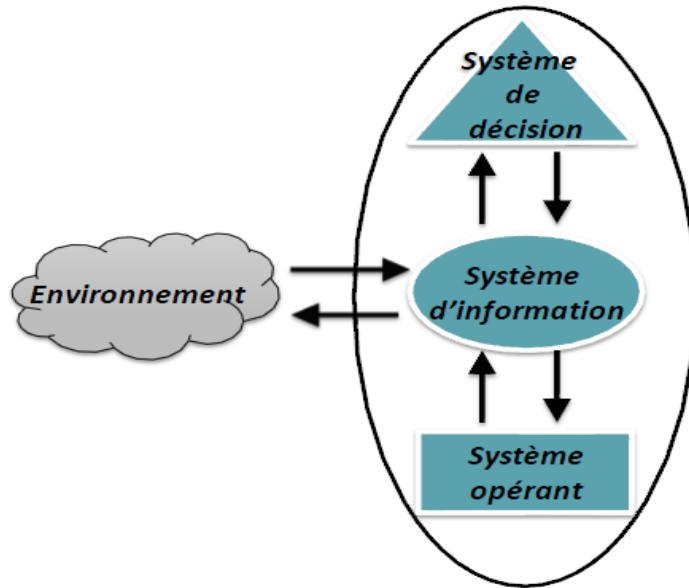
- ✓ Ouvert sur **l'environnement**
- ✓ Il est finalisé (**but = profit...**)
- ✓ Il est en constante **évolution**

Pour parvenir à son but, le système tient compte de son environnement et régule son fonctionnement en s'adaptant aux changements

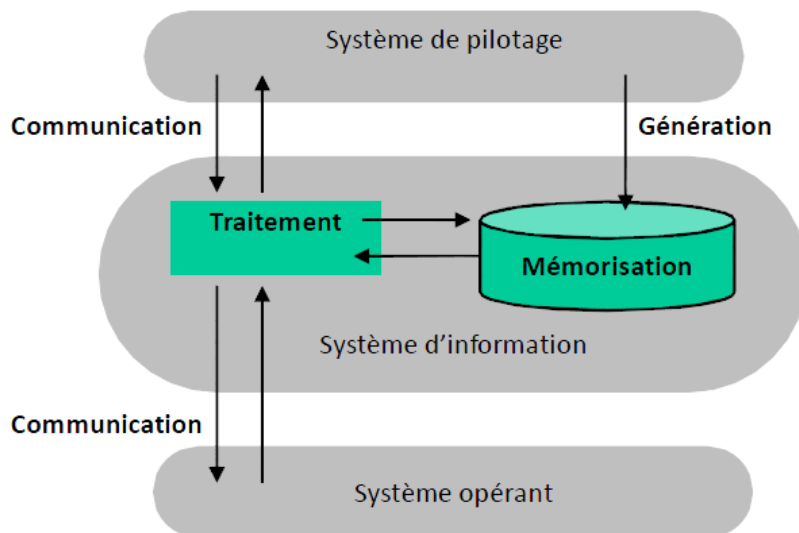
Les éléments du système sont eux-mêmes des systèmes (ou **sous-systèmes**)

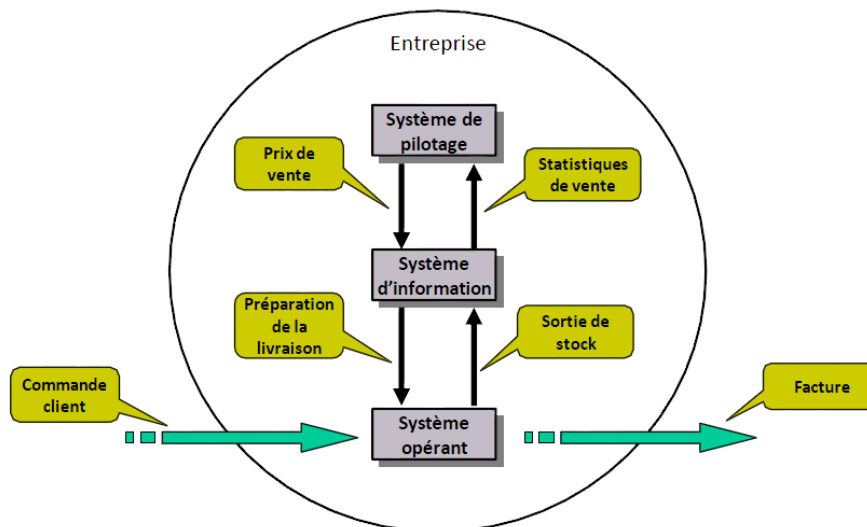
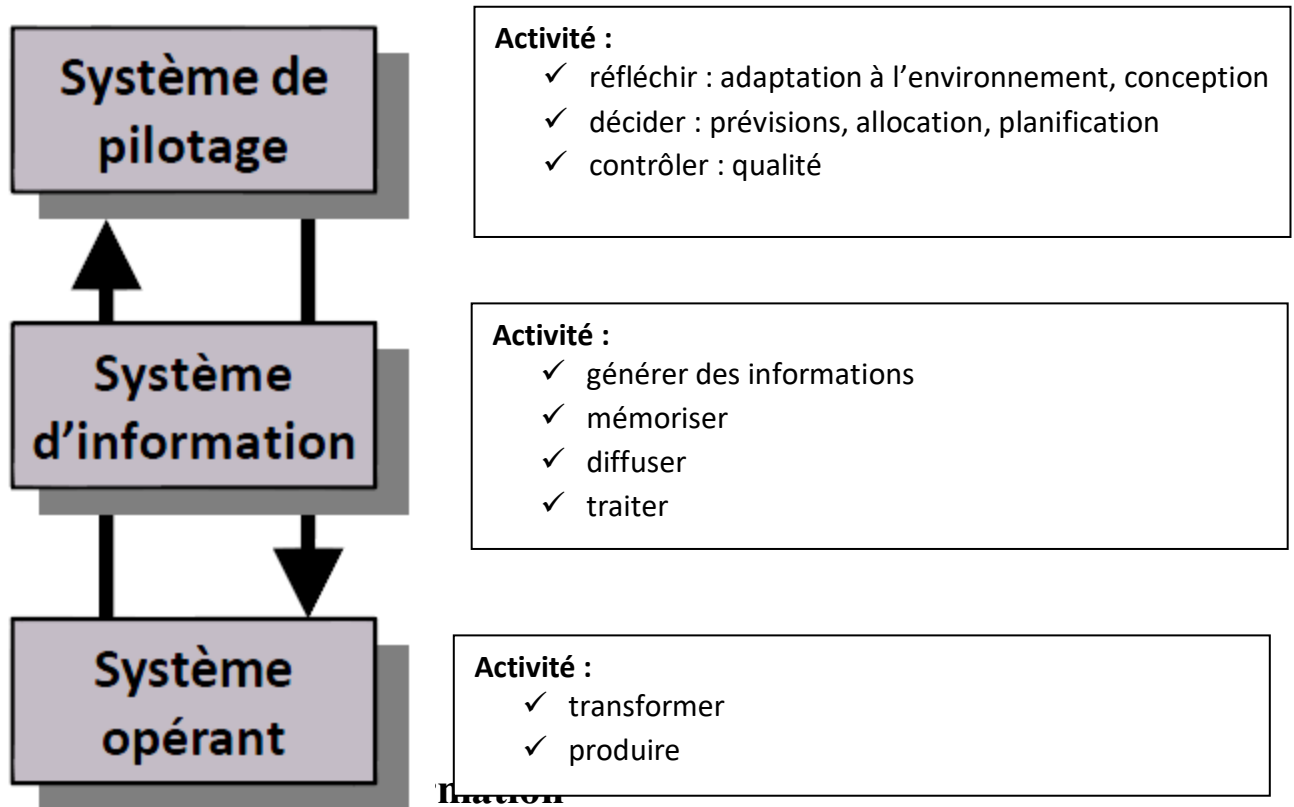
L'entreprise peut se décomposer en 3 sous-systèmes :

- Le système de décision
- Le système d'information
- Le système opérant



Chaque système apporte des services à l'autre





## Le système de pilotage

- Le système de pilotage : (appelé également système de décision)
  - Exploite les informations qui circulent
  - Organise le fonctionnement du système
  - Décide des actions à conduire sur le système opérant
  - Raisonne en fonction des objectifs et des politiques de l'entreprise

## **Le système opérant**

•Le système opérant :

–Reçoit les informations émises par le système de pilotage

–Se charge de réaliser les tâches qui lui sont confiées

–Génère à son tour des informations en direction du système de pilotage

    Qui peut ainsi contrôler les écarts et agir en conséquence

–Il englobe toutes les fonctions liées à l'activité propre de l'entreprise :

    Facturer les clients, régler les salaires, gérer les stocks, ...

## **IV : Sécurité de l'information (*Qu'est-ce que la sécurité ? Menaces et Attaques*)**

Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et d'outils chargés de protéger les ressources d'un système d'information afin d'assurer :

♣ La disponibilité des services : les services (ordinateurs, réseaux, périphériques, applications...) et les informations (données, fichiers...) doivent être accessibles aux personnes autorisées quand elles en ont besoin ;

♣ La confidentialité des informations : les informations n'appartiennent pas à tout le monde ; seuls peuvent y accéder ceux qui en ont le droit ;

♣ L'intégrité des systèmes : les services et les informations (fichiers, messages...) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires...).

La « politique de sécurité » d'une entité (société, organisme public, unité d'enseignement ou de recherche, ...) est l'expression de ces objectifs. Elle doit indiquer l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place, afin :

♣ D'empêcher (ou tout au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;

♣ De détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;

♣ D'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit

On ne protège bien que ce à quoi on tient, c'est-à-dire ce à quoi on associe « une valeur ». La trilogie confidentialité, intégrité, disponibilité, détermine la valeur d'une information. La sécurité des systèmes d'information (SSI) a pour but de garantir la valeur des informations qu'on utilise.

Si cette garantie n'est plus assurée, on dira que le système d'information a été altéré. Une altération n'est pas uniquement le fait de malveillances. Il est plus souvent encore, la conséquence de pannes, de maladresses, d'accidents ou d'erreurs humaines dont les plus fréquentes sont les erreurs de conception.

Ces phénomènes relèvent de la « sûreté de fonctionnement » qui est une autre manière d'appréhender la sécurité globale. Les sauvegardes, le fonctionnement en mode de repli, la redondance, etc. font aussi partie de la trousse à outils traditionnelle de la sécurité prise dans son sens général. Avec le développement de l'informatisation des échanges (courriers officiels, transactions financières, commerciales...), la simple affirmation de la valeur de l'information n'est plus suffisante.

Il est nécessaire d'y adjoindre des propriétés nouvelles comme l'authentification (garantie de l'origine d'un message, de l'auteur d'un document), la paternité (l'information ne peut pas être répudiée par son auteur), la traçabilité (on connaît le circuit qu'a suivi une information), etc. La préservation et la garantie de ces propriétés relèvent également de la fonction « sécurité ».

## **LES SYSTÈMES D'INFORMATION : UN OUTIL VULNÉRABLE**

Les sources de dysfonctionnement des systèmes d'information sont diverses et variées. Elles ont le plus souvent des causes d'origine « humaines » :

- ♣ Les sauvegardes sont mal faites ou mal gérées et rendent le système sensible aux pannes, aux maladresses et aux sinistres ;
- ♣ L'absence d'une vision globale de la sécurité, traitée par petits morceaux, au cas par cas débouche inmanquablement sur un manque d'organisation (qui fait quoi dans quelle structure ?) et plus spécialement sur de mauvaises architectures réseaux ;
- ♣ Le manque de consignes claires qui permettraient à chacun de savoir ce qu'il a à faire, ce qu'il peut faire et ce qu'il n'a pas le droit de faire ;
- ♣ La divulgation malencontreuse d'informations due à une imprudence ou un manque de vigilance ou une non-sensibilisation aux risques, ceci se traduisant par le non-respect de règles parfois élémentaires ou simplement d'un manque de conscience.

L'importance de l'information dans notre société s'est accrue dans les dernières décennies, en même temps que les moyens utilisables pour la création et l'échange d'information et en même temps, aussi, que les vulnérabilités des systèmes associés. Ce qui était compliqué est

devenu complexe. Quand les échanges étaient limités à des moyens de télécoms restreints, les risques étaient faibles tout comme le volume des informations que l'on pouvait échanger. Avec l'ouverture des réseaux et le nouvel environnement créé par l'Internet, des millions d'individus aux motivations très différentes sont mis en relation de manière voulue ou non.

Du temps où l'informatique était centralisé, les menaces « physiques » (pénétration dans des locaux informatiques sans autorisation, vol, vandalisme...) représentaient les menaces majeures. Nous citons quelques exemples de tout ce qui porte atteinte à l'intégrité du système

- le piégeage de systèmes (bombes logiques, chevaux de Troie, ...) afin de nuire à l'entité ou de se donner les moyens de revenir plus tard.,
- la modification des informations afin de porter atteinte à l'image de l'entité (exemple : modification de ses pages web),
- l'utilisation des ressources du site visé,
- une intrusion en vue « d'attaques par rebond », c'est-à-dire qu'une autre cible est visée, votre système servant seulement de point de passage. L'entité est alors complice involontaire du piratage.

Tout ce qui porte atteinte à la confidentialité des informations :

- la récupération d'informations sensibles (mots de passe, informations avant publication officielle, données personnelles, etc.),
- la fouille des messages, des données, des répertoires, des ressources réseaux...
- l'usurpation d'identité. ♣ Tout ce qui porte atteinte à la disponibilité des services :
- la paralysie du système (considérée ensuite comme un exploit par les pirates qui l'ont réalisée),
- la saturation d'une ressource (serveur, imprimante...),
- les virus et vers informatiques.

## **Qu'est-ce que la sécurité ?**

La sécurité de l'information est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

### **Les menaces**

Le système d'information doit être sécurisé par rapport à des menaces potentielles ou avérées. Le SI d'une entreprise ou d'une organisation est plus ou moins sensible à des menaces potentielles.

C'est le degré de sensibilité aux menaces potentielles. On parle alors d'une entreprise comme étant une cible potentielle compte tenu des enjeux qu'elle représente comme une banque ou une entreprise de haute technologie par exemple. Le SI d'une entreprise est plus ou moins exposé à des menaces avérées. C'est le degré d'exposition aux menaces avérées. Exemple de menaces :

- L'intrusion
- Le vol d'informations
- La falsification d'informations
- La destruction d'informations
- La mise hors service de ressources
- etc.

## **Les attaques**

Une attaque correspond à la réalisation d'une menace. Une attaque est réalisée par un ou des agresseurs.

Une attaque se définit par :

Son origine (qui ou quoi)

Son commanditaire

Sa cible (qui ou quoi)

Son objectif (pourquoi)

Ses moyens (techniques, humains, organisationnels, financiers, temporels)

Son type (attaque par IP, par ingénierie sociale...)

Son mobile ou sa motivation (pourquoi)

Sa justification (politique, économique, philosophique, culturelle, religieuse, etc.)

## **Les objectifs de la sécurité de l'information**

Les principaux objectifs à garantir :

- Intégrité
- Confidentialité
- Disponibilité



## Confidentialité

Seuls les utilisateurs habilités (autorisés) ont accès l'information  
Qui peut "voir" quoi ?

## Intégrité

- Une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).
- Les contraintes d'intégrité : l'ensemble des règles (des assertions) qui définissent la cohérence d'un système d'information. Ex: toute règle de cohérence d'une base de données.
- L'intégrité veut dire : exactitude, précision, modifications autorisées seulement, cohérence.

## Disponibilité et fiabilité (pérennité)

- Terminologie du milieu de la sécurité pour caractériser le bon fonctionnement d'un système informatique.
- Un système informatique doit être disponible à ses utilisateurs autorisés selon les conditions prédéfinies.
- Présence sous forme utilisable (besoins et spécifications) satisfaisant des contraintes de temps, performance et qualité
- La fiabilité est l'aptitude d'un système informatique à fonctionner d'une manière continue pendant une période donnée (sa durée de vie).  
Un système informatique ne doit pas avoir de bugs liés à des problèmes techniques de conception ou de programmation.

## Etude et analyse des risques

Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.

L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque.

On obtient ainsi la liste de ce qui doit être protégé.

Quelle est la valeur des équipements, des logiciels et surtout des informations ?

Quel est le coût et le délai de remplacement ?

Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau

Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Il faut cependant prendre conscience que les principaux risques restent :

- « Câble arraché »,
- « Coupure secteur »,
- « Crash disque »,
- « Mauvais profil utilisateur », ...
- Inventaire des éléments du système à protéger
- Inventaire des menaces possibles sur ces éléments
- Estimation de la probabilité que ces menaces se réalisent

### **Evolution des risques**

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

### **Établissement d'une politique de sécurité**

Suite à l'étude des risques et avant de mettre en place des mécanismes de protection, il faut préparer une politique à l'égard de la sécurité.

Une politique de sécurité vise à définir les moyens de protection à mettre en œuvre

- Identifier les risques et leurs conséquences.
- Elaborer des règles et des procédures à mettre en œuvre pour les risques identifiés.
- Surveillance et veille technologique sur les vulnérabilités découvertes.
- Actions à entreprendre et personnes à contacter en cas de détection d'un problème.