



Systeme d'information




SEMIFIR

contact@semifir.com

13 Avenue du Président John F. Kennedy,
59000 Lille

Programme

- 
- Introduction / Définition
 - Le système d'information
 - La sécurité du système d'information

Systeme d'Information



Introduction

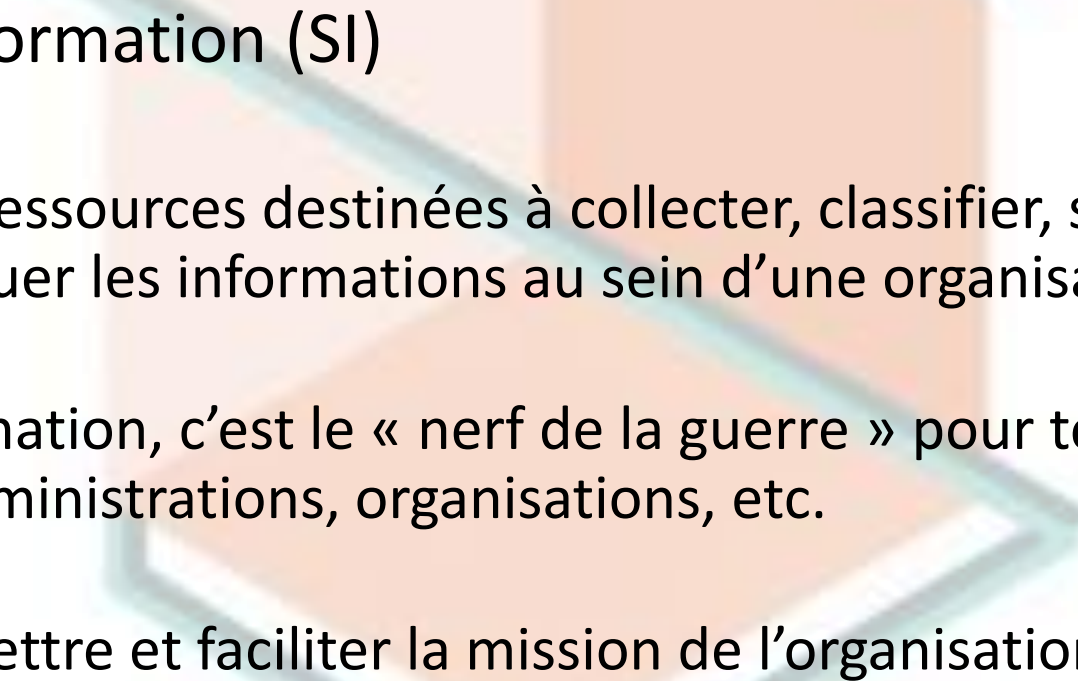
Introduction

- Toute organisation humaine (entreprise, l'Etat, ...) peut être perçue comme un système. Le système tient compte de son environnement et régule son fonctionnement en s'adaptant aux changements
- L'interaction entre le système et son environnement est possible grâce à des flux d'informations. La circulation de ces flux nous permet de comprendre le fonctionnement du système.

Introduction

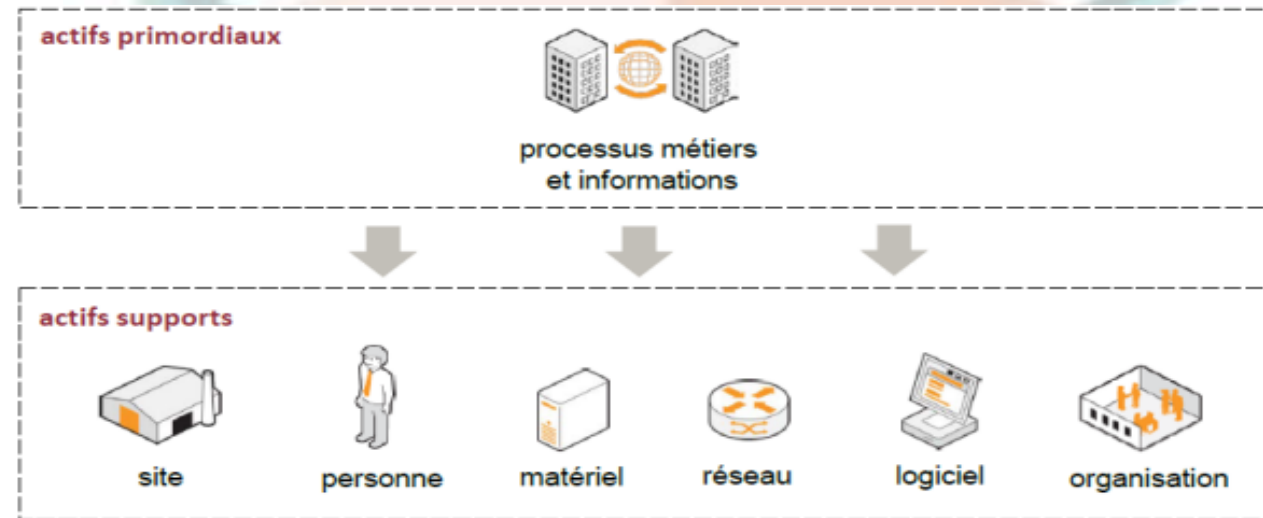
- Système
 - Ensemble d'éléments matériels ou immatériels en interaction dynamique, organisé en fonction d'un but bien défini (transformer des éléments d'entrée en éléments de sortie).
- Information
 - Les informations sont des données traitées ou transformées qui aident quelqu'un à prendre une décision ou à tirer des conclusions.
 - En informatique et en télécommunication, l'information est un élément de connaissance (donnée, voix, image) susceptible d'être conservé, traité ou transmis à l'aide d'un support et d'un mode de codification normalisé

Définissez ce qu'est un Système d'Information

- 
- Le système d'information (SI)
 - Ensemble des ressources destinées à collecter, classier, stocker, gérer/traiter, diffuser/distribuer les informations au sein d'une organisation.
 - Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.
 - Le SI doit permettre et faciliter la mission de l'organisation

Définissez le Système d'Information

- Le système d'information d'une organisation contient un ensemble d'actifs:



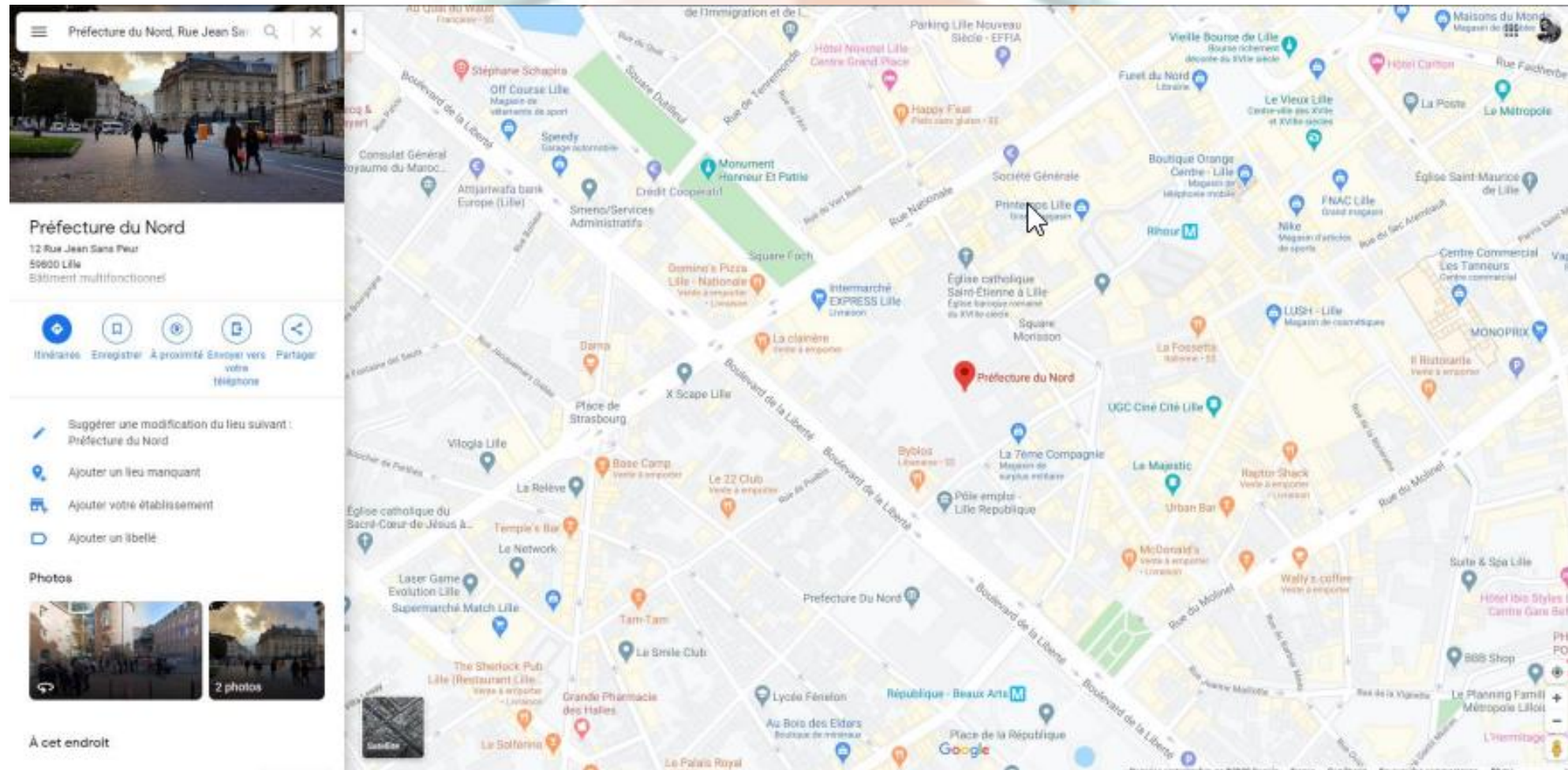
- La sécurité du SI consiste donc à assurer la sécurité de l'ensemble de ses biens

Définissez ce qu'est un Système d'Information

- 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

Définissez ce qu'est un Système d'Information

- Exemple avec le service de cartographie de Google appelé Google Maps.



Définissez ce qu'est un Système d'Information

- Il permet de :
 - Collecter et stocker les données cartographiques prises par les satellites
 - Les traiter en les combinant à vos recherches sur le site
 - Et les distribuer, c'est-à-dire vous les afficher sur le site lors de vos recherches

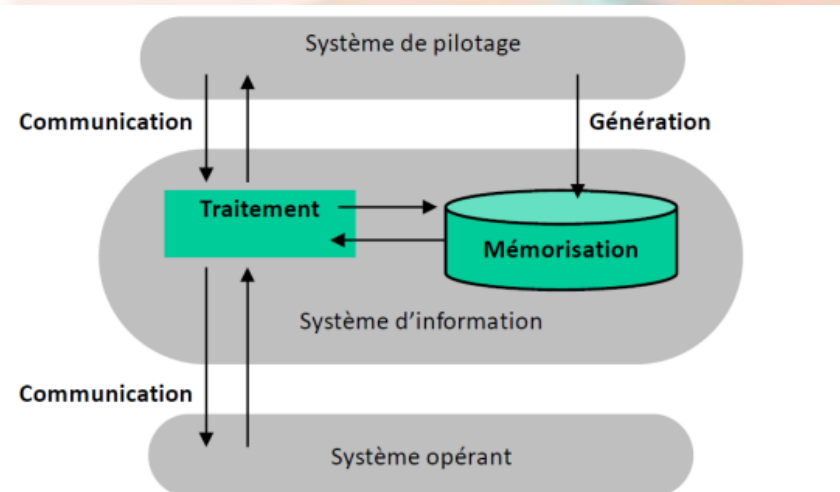


Définissez ce qu'est un Système d'Information

- C'est aussi un système d'information parce que Google Maps est un ensemble de :
 - Ressources humaines: c'est une équipe de développeurs, de cartographes, de géomètres, mais aussi les chauffeurs des voitures Google qui prennent les rues en photos.
 - Ressources matérielles: des ordinateurs, serveurs, caméras, satellites sont utilisés pour acquérir et stocker les données cartographiques.
 - Ressources immatérielles: Google Maps c'est aussi des photos satellites, des cartes, mais aussi des brevets créés et exploités par Google pour mettre en œuvre ce service.

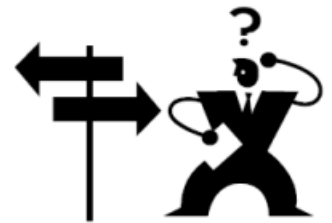
Définissez ce qu'est un Système d'Information

- L'entreprise en tant que système peut être décomposée en trois sous-systèmes:
 - Système de décision
 - Système d'information
 - Système opérant
- Chaque système apporte des services à l'autre



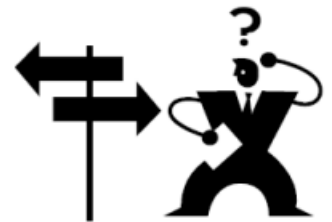
Définissez ce qu'est un Système d'Information

- Le système de pilotage ou 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 politiques de l'entreprise



Définissez ce qu'est un Système d'Information

- 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, ...



Définissez ce qu'est un Système d'Information

- Le système d'information
 - Pour organiser son fonctionnement, le système a besoin de mémoriser des informations
 - Pour comparer, prévoir, ...
 - Ce système a aussi la charge de :
 - Diffuser l'information
 - Réaliser tous les traitements
 - Nécessaires au fonctionnement du système

Systeme d'Information

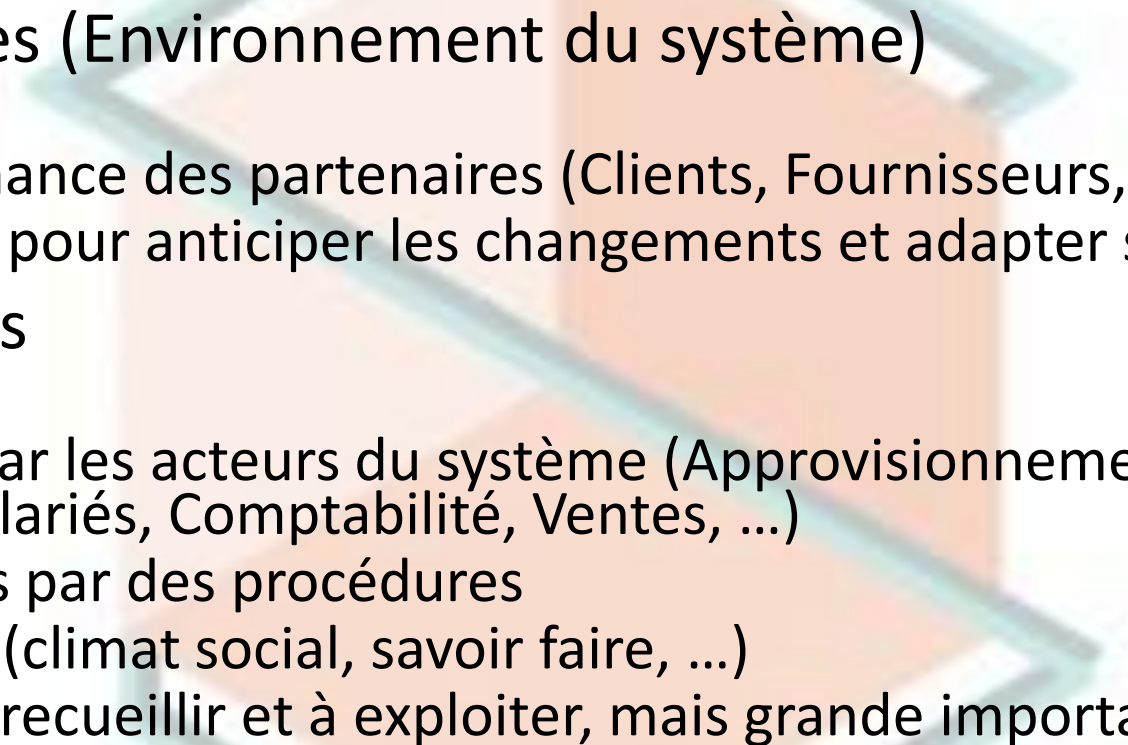


Le système d'information

Fonction du SI

- Le SI représente l'ensemble des ressources (humaines, matérielles, logicielles) organisées pour :
 - Collecter l'information : Enregistrer une information (support papier, informatique...) avant son traitement
 - Mémoriser l'information (stockage) : Conserver, archiver (utilisation ultérieure ou obligation légale)
 - Traiter l'information : effectuer des opérations (calcul, tri, classement, résumé, ...)
 - Diffuser : transmettre à la bonne personne (éditer, imprimer, afficher, ... une info après traitement)

La collecte de l'information

- 
- Sources externes (Environnement du système)
 - Flux en provenance des partenaires (Clients, Fournisseurs, Administration, ...)
 - Être à l'écoute pour anticiper les changements et adapter son fonctionnement
 - Sources internes
 - Flux générés par les acteurs du système (Approvisionnements, Production, Gestion des salariés, Comptabilité, Ventes, ...)
 - Flux formalisés par des procédures
 - Flux informels (climat social, savoir faire, ...)
 - Difficiles à recueillir et à exploiter, mais grande importance

La collecte de l'information

- Alimenter le SI
 - La saisie de l'information est généralement onéreuse
 - Nécessite souvent intervention humaine
 - Efforts pour automatiser le recueil d'information
 - Systèmes en temps réel
 - Lecture optique (questionnaires, ...)
 - Numérisation, Robots d'analyse de contenus, ...
 - L'info est précieuse, vitale pour l'entreprise
 - Mais elle a aussi un coût

La mémorisation de l'information

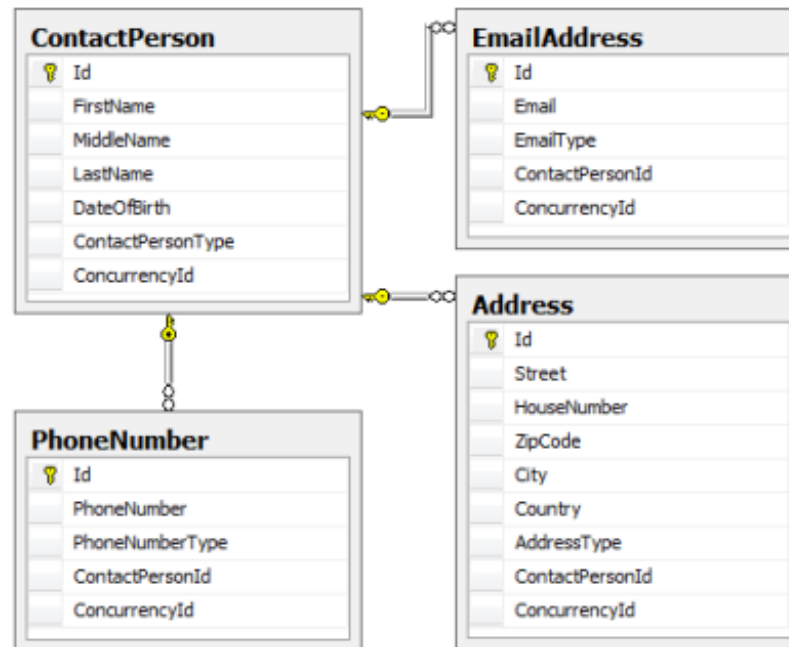
- Assurer la pérennité c'est garantir un stockage durable et fiable
 - Les supports privilégiés de l'information sont aujourd'hui les disques des ordinateurs
 - Fichiers sur Disque Dur, DVD, ...
 - Le SGBD est une composante fondamentale du SI
 - Cependant le papier reste un support très utilisé en entreprise
 - Conservation des archives papiers
 - Parfois par obligation légale
- Pour organiser le stockage de l'information, des moyens techniques et organisationnels sont mis en œuvre comme les méthodes d'archivage, des techniques de sauvegarde, de protection contre le piratage ou encore des méthodes pour prévenir la destruction de données.
Comme l'information est précieuse, il est impératif que les SI sécurisent bien ces informations.

La mémorisation de l'information

- L'organisation du stockage
 - Les informations sont donc collectées et rangées soit dans des fichiers soit dans ce qu'on appelle une base de données (ou BDD).
 - Le fichier est une collection, un ensemble de données réunies sous un même nom.
Techniquement c'est une information numérique constituée d'une séquence d'octets, c'est-à-dire d'une séquence de nombre.
 - La base de données (BDD) est une structure de rangement d'informations qui prend un peu la forme de grands tableaux, comme un peu un tableau Excel. Chaque colonne sert à tirer un type de données et chaque ligne représente un enregistrement.

La mémorisation de l'information

- Exemple d'un carnet de contacts téléphoniques. On peut retrouver en colonne le numéro du contact, son nom, son prénom, sa fonction et son numéro de téléphone. Chaque ligne représente un enregistrement



Traitement de l'information

- Le traitement de l'information peut prendre 4 formes différentes. On peut :
 - Consulter l'information : il s'agit du traitement le plus simple puisqu'il consiste à accéder à l'information telle qu'elle a été enregistrée.
 - Organiser l'information : ce traitement consiste à structurer l'information selon des critères spécifiques. Cela peut-être par exemple regrouper l'information par client, par zones géographiques, par activités et bien d'autres encore.
 - Mettre à jour l'information : Ce traitement va consister à reprendre une information précédemment enregistrée et à l'actualiser.
 - Produire des nouvelles informations : à partir d'information(s) existante(s), ce traitement va permettre la création de nouvelles informations.
- Ces traitements peuvent être :
 - Manuels (de moins en moins souvent)
 - Automatiques (réalisés par des ordinateurs)

Diffusion de l'information

- Pour être exploitée, l'information doit parvenir dans les meilleurs délais à son destinataire
 - Forme orale
 - Support papier (courrier, note interne, ...)
 - Support numérique (de plus en plus)
 - Vitesse optimale
 - Large diffusion
 - Internet (web, email, mobiles)
 - Interconnexion des SI

Construisez vos infrastructures

- Un SI repose sur un ou plusieurs systèmes informatiques eux-mêmes composés de différents éléments comme :
 - Les équipements réseau
 - Les commutateurs réseaux, les routeurs
 - Réseaux de différentes tailles
 - LAN (Local Area Network) échelle d'un bâtiment
 - MAN (Metropolitan Area Network) échelle d'une ville
 - WAN (Wide Area Network) échelle mondiale
 - Les capteurs
 - Les serveurs
 - Les terminaux bancaires
 - Les boîtiers de stockage en réseau
 - Les robots
 - Les automates industriels

Construisez vos infrastructures

- Plusieurs types de déploiements sont possibles
 - Centralisée : quand les utilisateurs, les traitements et les données sont situés sur le même ordinateur.
 - Répartie : permet de distribuer les différentes briques fonctionnelles (application utilisateur, traitements et données sur des ordinateurs différents).

Type	Description	Exemple
Centralisée	Un ordinateur unique héberge le traitement, les données et donne accès aux utilisateurs.	Un PC qui n'est pas en réseau.
Maitre / Esclave	Plusieurs terminaux passifs sont reliés à un ordinateur central.	Distributeur automatique de billets
Client-serveur	Un ensemble de stations clientes consomme les ressources d'un serveur.	Sites web
Peer to peer	Chaque ordinateur du réseau est un client et un serveur.	Emule / Napster

Construisez vos infrastructures

- La virtualisation permet de faire cohabiter sur un même serveur physique des systèmes d'exploitation différents.
- La virtualisation offre de nombreux avantages :
 - Comme pour les voitures : on optimise l'espace, la consommation, la puissance !
 - L'administration des serveurs virtualisés est centralisée et permet de gérer des parcs de machines virtuelles pouvant aller jusqu'à plusieurs milliers d'unités.
 - La disponibilité des plateformes virtualisées est souvent plus importante que celle de serveurs physiques équivalents, car ils sont sujets aux pannes.
 - La répartition de la charge de travail entre machines virtualisées est gérée de manière automatique.
 - Les infrastructures virtualisées sont beaucoup moins gourmandes en électricité et en climatisation qu'un ensemble de serveurs physiques.

Construisez vos infrastructures

- La tendance majeure des dernières années consiste à distribuer les différents composants d'un système informatique comme le Cloud.
- Le Cloud Computing (informatique « dans les nuages ») est le résultat d'une évolution générale de l'informatique qui peut se caractériser par les éléments suivants :
 - Les ressources de calcul et de stockage des données nécessaires au fonctionnement des applications sont situées dans des Datacenters accessibles dans un nuage
 - L'accès aux services peut se faire, la plupart du temps, via un navigateur Web
 - La facturation des ressources, généralement mensuelle, se fait soit au forfait, soit à la consommation

Construisez vos infrastructures

- On peut classer les services proposés par le Cloud Computing en trois couches :
 - Software-as-a-service (SaaS) : Le SaaS rend le service à l'utilisateur. Il remplit une fonction, la messagerie par exemple. On ne se soucie pas de la façon dont il est opéré, seul le service rendu compte. Office 365 ou Dynamics CRM Online sont les offres de Microsoft qui répondent à cette définition.
 - Platform-as-a-service (PaaS) : Le PaaS a pour fonction de proposer un environnement d'exécution d'applications, ainsi que des composants facilitant leur développement. Il est composé de plusieurs briques logicielles assurant la prise en charge des applications développées dans différents langages. Il assure l'isolation des applications et de nombreuses autres fonctions sur lesquelles nous reviendrons.
 - Infrastructure-as-a-service (IaaS) : Le IaaS propose une couche d'exécution bas niveau, généralement destinée à exécuter des machines virtuelles.

Systeme d'Information



La sécurité du système d'information

Introduction

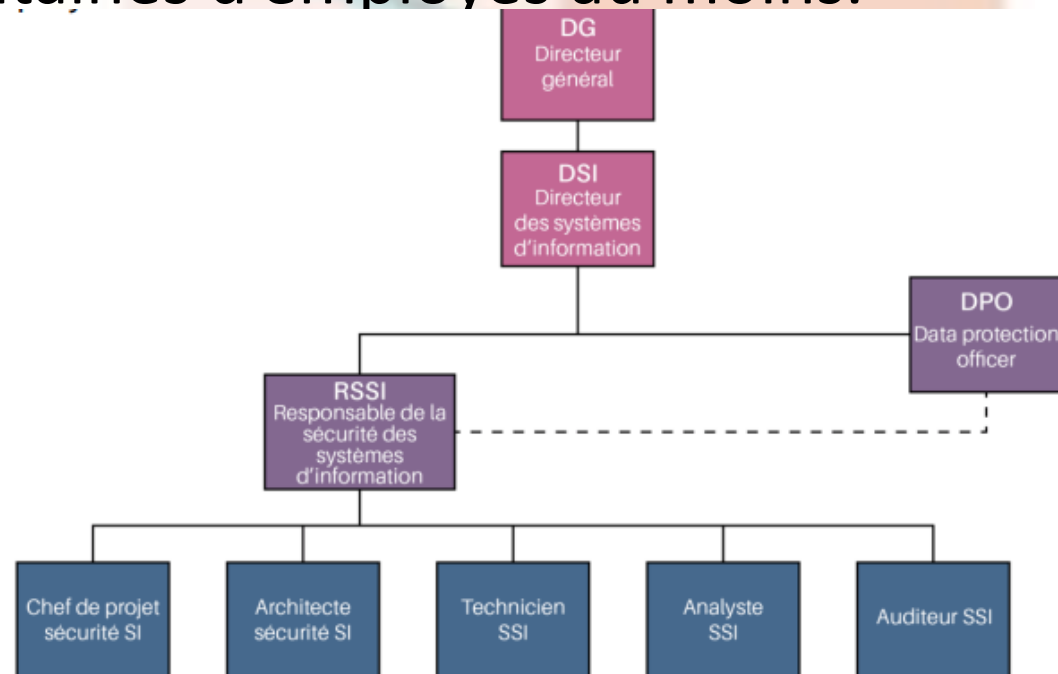
- La sécurité des systèmes d'information (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher : l'utilisation non-autorisée, le mauvais usage, la modification, ou le détournement du système d'information.
- Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients. Sur le court terme, l'objectif est que chacun ait accès à l'informations.

Budget

- On estime le budget des entreprises en matière de cybersécurité à 96 milliards de dollars dans le monde. Ce budget est actuellement en forte croissance étant donné la recrudescence des cyberattaques.
- Mais concrètement, quels sont les métiers derrière ? Que font les experts en cybersécurité ? Y a-t-il des spécialisations ?

Organigramme

- Ce schéma ne représente pas toutes les entreprises ! Il s'agit d'une organisation théorique, qui correspond en moyenne à une entreprise de plusieurs centaines d'employés au moins.



- L'Agence National de la Sécurité des Systèmes d'Information (ANSSI), répertorie les métiers suivant comme acteur de la cybersécurité :
 - [Agence nationale de la sécurité des systèmes d'information \(ssi.gouv.fr\)](https://ssi.gouv.fr)

- Rechercher des opportunités aux métiers présentés.
- Rechercher un métier dans lequel vous voudriez travailler.
 - Compétences
 - Opportunités
 - Diplômes
 - Salaires
 - ...



SOC

- Pour se protéger, les entreprises ont de plus en plus souvent recours à un SOC, il s'agit d'un centre opérationnel de sécurité.
- C'est l'environnement où sont supervisés les systèmes d'information pour assurer la détection, le confinement et la remédiation des incidents de sécurité.
- Il existe 2 types de SOC :



- Définir Qu'est-ce qu'un SOC ?
- Chercher l'ensemble des missions effectuée au sein d'un soc



Les critères DIC

- L' ANSSI définit la cybersécurité comme l'état recherché pour un SI lui permettant de résister à des événements issus du cyberspace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Bien à
protéger



Disponibilité

Propriété d'**accessibilité au moment voulu** des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité

Propriété d'**exactitude et de complétude** des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité

Propriété des biens de **n'être accessibles qu'aux personnes autorisées**

Les critères DIC

- 1 critère complémentaire est souvent associé au D.I.C.

Bien à
protéger



Preuve

Propriété d'un bien permettant de retrouver, avec une **confiance suffisante**, les circonstances dans lesquelles ce bien évolue. Cette propriété englobe Notamment :

La **traçabilité** des actions menées

L'**authentification** des utilisateurs

L'**imputabilité** du responsable de l'action effectuée

Différences entre sûreté et sécurité

- « Sûreté » et « Sécurité » ont des significations différentes en fonction du contexte. L'interprétation de ces expressions peuvent varier en fonction de la sensibilité de chacun.

- Sûreté

- Protection contre les dysfonctionnements et accidents involontaires
- Exemple de risque : saturation d'un point d'accès, panne d'un disque, erreur d'exécution, etc.
- Quantifiable statistiquement (ex. : la durée de vie moyenne d'un disque est de X milliers d'heures)
- Parades : sauvegarde, dimensionnement, redondance des équipements...

- Sécurité

- Protection contre les actions malveillantes volontaires
- Exemple de risque : blocage d'un service, modification d'informations, vol d'information
- Non quantifiable statistiquement, mais il est possible d'évaluer en amont le niveau du risque et les impacts
- Parades : contrôle d'accès, veille sécurité, correctifs, configuration renforcée, filtrage...*

Différences entre sûreté et sécurité

- Sûreté : ensemble de mécanismes mis en place pour assurer la continuité de fonctionnement du système dans les conditions requises.
- Sécurité : ensemble de mécanismes destinés à protéger l'information des utilisateurs ou processus n'ayant pas l'autorisation de la manipuler et d'assurer les accès autorisés.

Exemple d'évaluation DICP

- Ainsi, pour évaluer si un bien est correctement sécurisé, il faut auditer son niveau de Disponibilité, Intégrité, Confidentialité et de Preuve. L'évaluation de ces critères sur une échelle permet de déterminer si ce bien est correctement sécurisé.
- L'expression du besoin attendu peut-être d'origine :
 - Interne : inhérente au métier de l'entreprise
 - Externe : issue des contraintes légales qui pèsent sur les biens de l'entreprise.
- Exemple des résultats d'un audit sur un bien sur une échelle (Faible, Moyen, Fort, Très fort) :



Niveau de Disponibilité du bien	Très fort
Niveau d'Intégrité du bien	Moyen
Niveau de Confidentialité du bien	Très fort
Niveau de Preuve du bien	Faible



Le bien bénéficie d'un niveau de sécurité adéquat

Exemple d'évaluation DICP

- Tous les biens d'un S.I. n'ont pas nécessairement besoin d'atteindre les mêmes niveaux de DICP.
- Exemple avec un site simple (statique) d'une entreprise qui souhaite promouvoir ses services sur internet :

Disponibilité = Très fort ✓

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaître ses services au public

Intégrité = Très fort ✓

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)



Serveur
web

Confidentialité = Faible ✓

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = Faible ✓

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

Exemple d'évaluation DICP

- Un Système d'Information a besoin de mécanismes de sécurité qui ont pour objectif d'assurer de garantir les propriétés DICP sur les biens de ce S.I. Voici quelques exemples de mécanismes de sécurité participant à cette garantie

		D	I	C	P
Anti-virus	Mécanisme technique permettant de détecter toute attaque virale qui a déjà été identifiée par la communauté sécurité	✓	✓	✓	
Cryptographie	Mécanisme permettant d'implémenter du chiffrement et des signatures électroniques		✓	✓	✓
Pare-feu	Équipement permettant d'isoler des zones réseaux entre-elles et de n'autoriser le passage que de certains flux seulement	✓		✓	
Contrôles d'accès logiques	Mécanismes permettant de restreindre l'accès en lecture/écriture/suppression aux ressources aux seules personnes dûment habilitées		✓	✓	✓
Sécurité physique des équipements et locaux	Mécanismes de protection destinés à protéger l'intégrité physique du matériel et des bâtiments/bureaux.	✓	✓	✓	

Exemple d'évaluation DICP

Capacité d'audit

Mécanismes organisationnels destinés à s'assurer de l'efficacité et de la pertinence des mesures mises en œuvre. Participe à l'amélioration continue de la sécurité du S.I.

D I C P

✓ ✓ ✓ ✓

Clauses contractuelles avec les partenaires

Mécanismes organisationnels destinés à s'assurer que les partenaires et prestataires mettent en œuvre les mesures nécessaires pour ne pas impacter la sécurité des S.I. de leurs clients

✓ ✓ ✓ ✓

Formation et sensibilisation

Mécanismes organisationnels dont l'objectif est d'expliquer aux utilisateurs, administrateurs, techniciens, PDG, clients, grand public, etc. en quoi leurs actions affectent la sécurité des S.I.
Diffusion des bonnes pratiques de sécurité.
Le cours actuel en est une illustration !

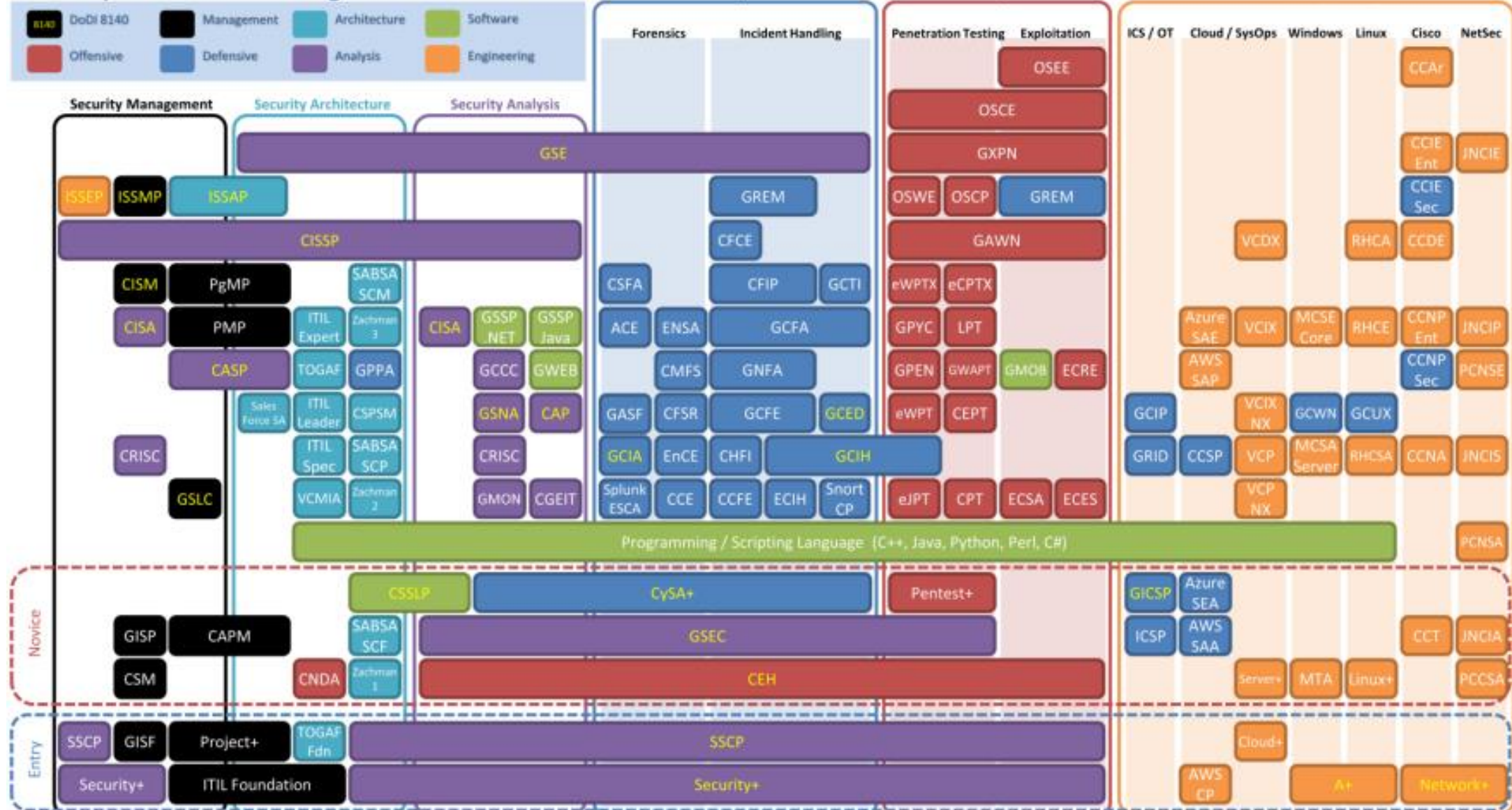
✓ ✓ ✓ ✓

Identifiez les contraintes de sécurité

- Déployer un SI en utilisant des composants Cloud tel que le IaaS, le PaaS ou le SaaS amène obligatoirement des questions sur la sécurité des données et des infrastructures Cloud
- Les données collectées et stockées sont soumises à des juridictions plus ou moins contraignantes. En Europe, le RGPD (Règlement général sur la Protection des Données) ou le CLOUD Act aux États-Unis permet d'encadrer et de mieux protéger les données
- L'émergence de l'IoT s'accompagne de défi de sécurité qui est aujourd'hui sous-estimée
- La vaste majorité des incidents de sécurité est due à des interventions humaines
 - externes avec les hackers
 - internes à l'entreprise avec ses utilisateurs.

Les certifications

Security Certification Progression Chart 2020



Merci pour votre attention !

