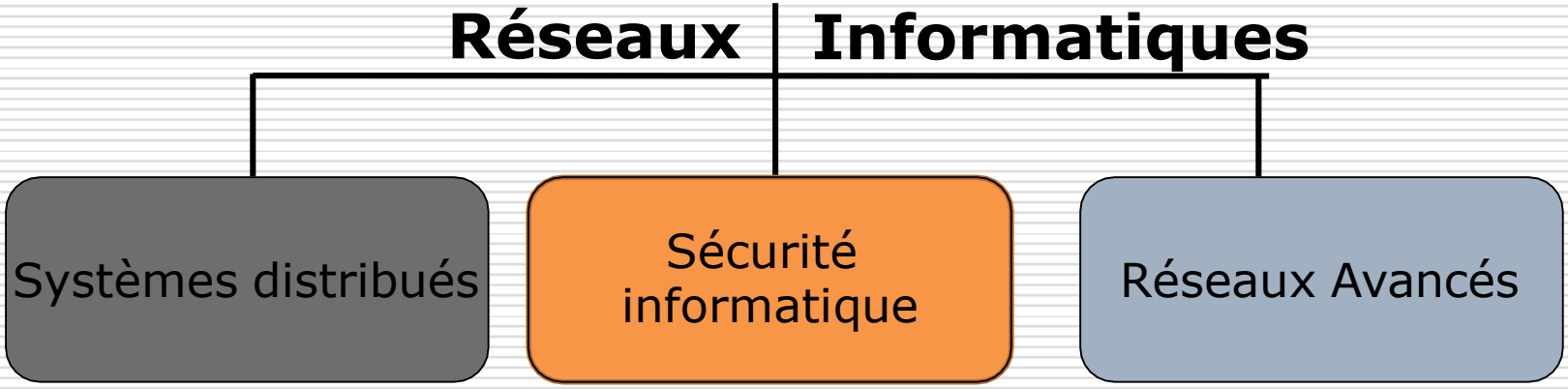
Université
De Boumerdes

Université
De Limoges

Introduction à la sécurité Informatique

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de Conférences classe A à l'université de Boumerdes

Prérequis Réseaux Informatiques



- Rappels TCP/IP
- Client serveur (FTP, Telnet, SSH,…)
- Socket
- NFS
- RPC, CORBA, RMI
- Algorithmes distribués

- Routage avancé
- Réseaux Dynamiques:
- Réseaux Ad Hoc
- Réseaux P2P

Programme

4 parties

I. Introduction à la sécurité informatique
II. Menaces (failles de sécurité, Attaques et vulnérabilités)
III. Protections
IV. Gestion de la sécurité

4 parties

I. Introduction à la sécurité informatique

II. Menaces (failles de sécurité, Attaques et vulnérabilités)

III. Protections

IV. Gestion de la sécurité

Introduction
à la sécurité informatique

- **Introduction** (généralités et historiques).
- **Exigences fondamentales** et **objectifs** de la sécurité.
- Etude des **risques**.
- L'établissement d'une **politique de sécurité**.
- **Eléments** d'une politique de sécurité.
- Principaux **défauts** de sécurité.
- Notion **d'audit**.

Cryptographie

- Cryptographie classique
- Cryptographie symétrique
- Cryptographie asymétrique
- Cryptage hybride
- Signature et Certificat numérique
- PKI (Public Key Infrastructure)
- Communications et applications sécurisées

4 parties

I. Introduction à la sécurité informatique

II. Menaces (failles de sécurité, Attaques et vulnérabilités)

III. Protections

IV. Gestion de la sécurité

Menaces
(failles de sécurité, Attaques et vulnérabilités)

- Introduction
- Les différents types de vulnérabilités
- Virus, vers, chevaux de Troie et autres
- Vulnérabilités applicatives
- Vulnérabilités des réseaux
- Espionnage

4 parties

I. Introduction à la sécurité informatique

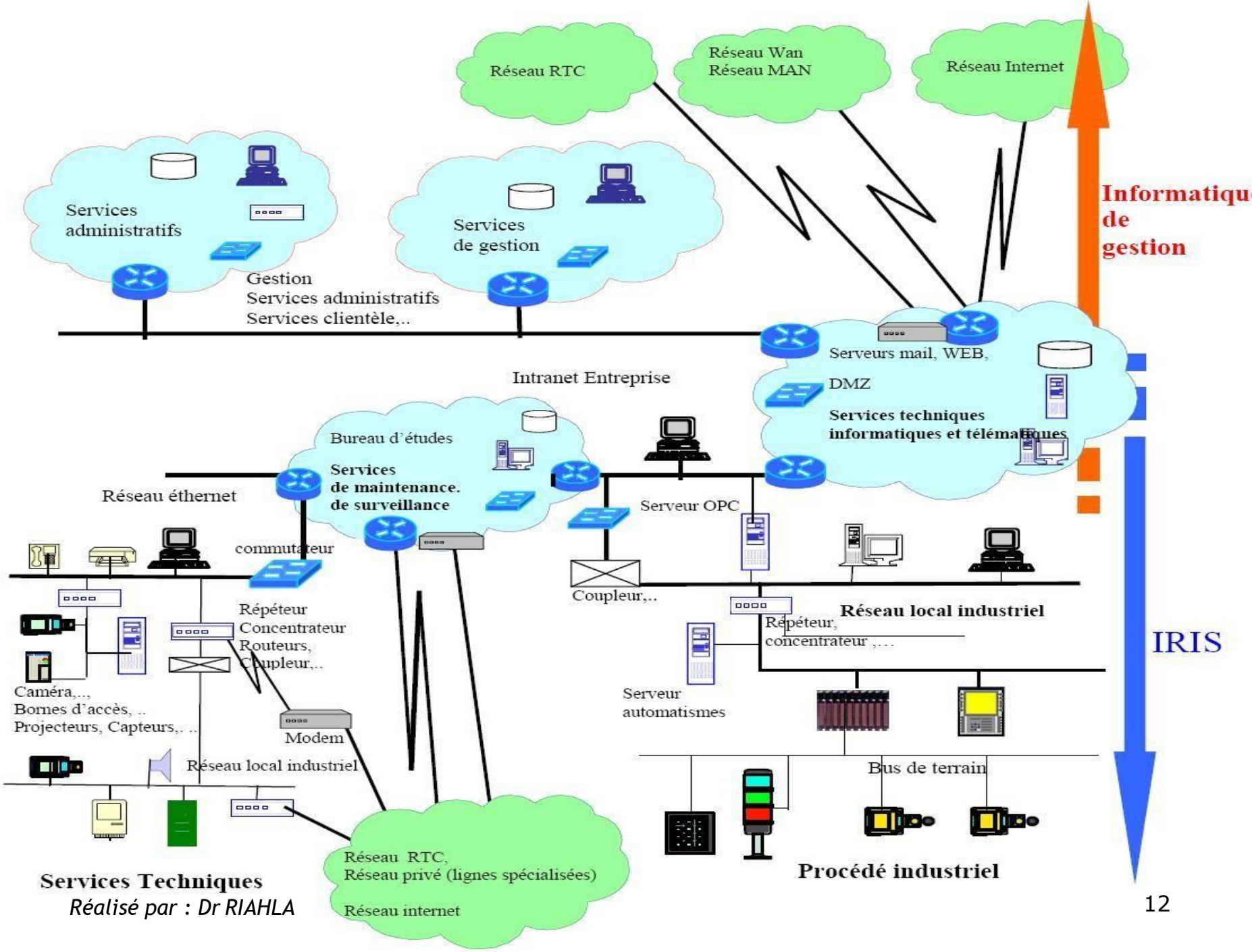
II. Menaces (failles de sécurité, Attaques et vulnérabilités)

III. Protections

IV. Gestion de la sécurité

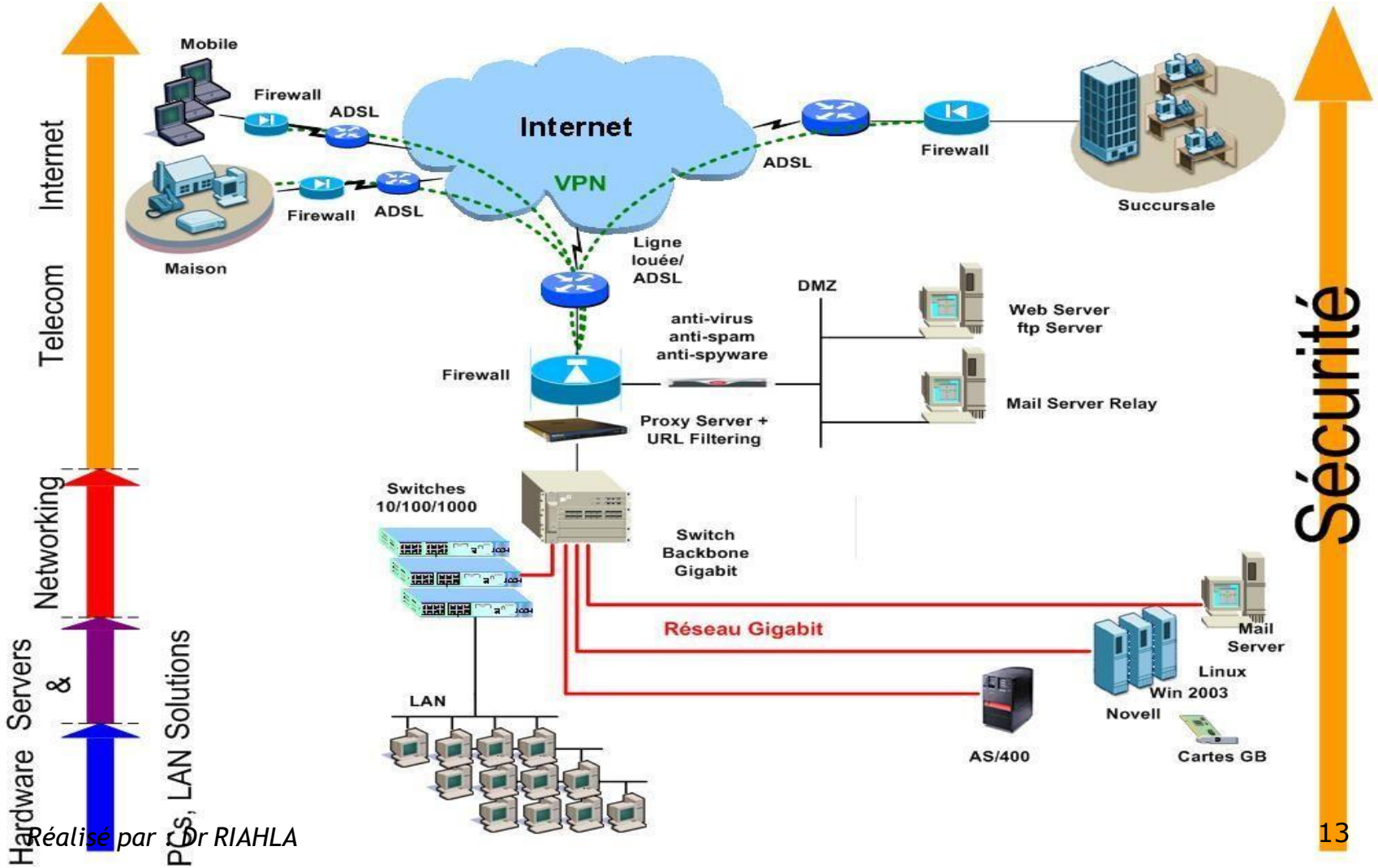
Protections

- Formation des utilisateurs
- Poste de travail
- Antivirus
- Authentification et cryptage
- Pare-feu (firewall) : translation, filtrage et proxies
- Détection d'intrusion
- Communications et applications sécurisées
- VPNs



Réalisé par : Dr RIAHLA

Protections



4 parties

I. Introduction à la sécurité informatique

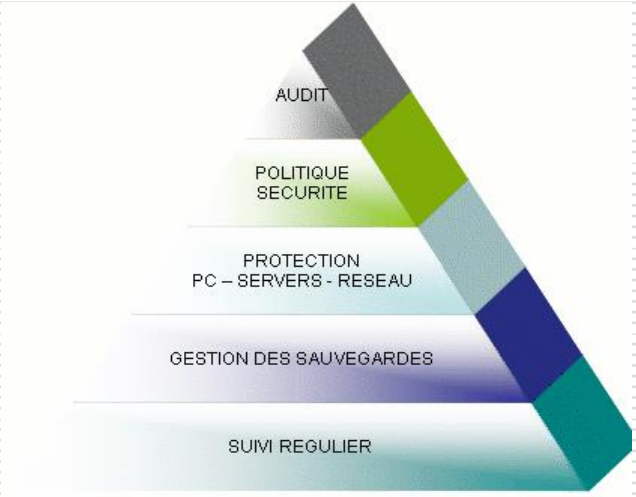
II. Menaces (failles de sécurité, Attaques et vulnérabilités)

III. Protections

IV. Gestion de la sécurité

Gestion de la sécurité

- Définition d'une politique de sécurité.
- Normes et standards de sécurité
- L'audit.
- **Certification ISO XX XXX**

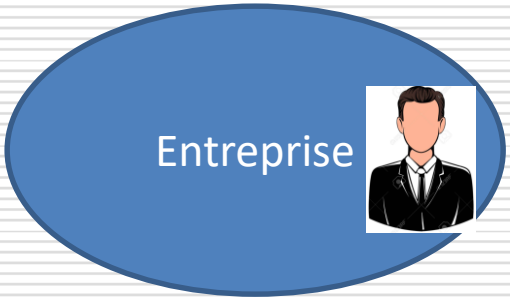


Objectif Principal

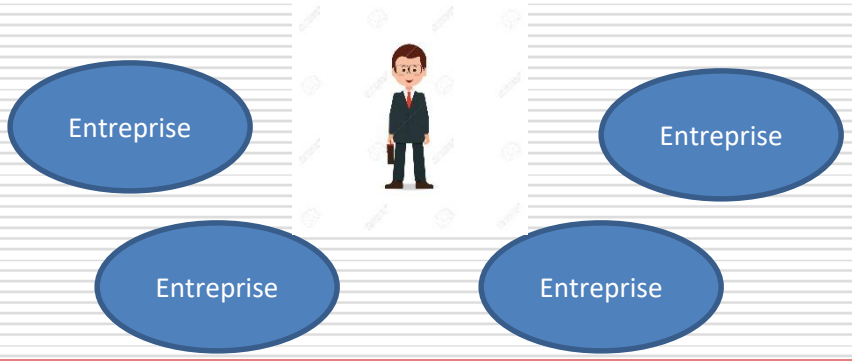
- **Connaissances générales** pour les non spécialistes
- **Une bonne base** pour les futurs spécialistes de la Sécurité.

Sécurité informatique Métier

- **Débutant en SSI**: 32 000 euros par an --- 3000 euros /mois
- **RSSI**: 70 000 euros par an --- 6000 euros/mois



- **Consultant expert**: 600 € la journée--- 18 000/mois ou plus !



I. Introduction à la sécurité informatique

Introduction (historique)

Historique (**Kevin mitnick**)

U.S. Department of Justice
United States Marshals Service

WANTED
BY U.S. MARSHALS

NOTICE TO ARRESTING AGENCY: Before arrest, validate warrant through National Crime Information Center (NCIC).

United States Marshals Service NCIC entry number: (NIC/ W721460921).

NAME: .....MITNICK, KEVIN DAVID

AKS (S): .....MITNIK, KEVIN DAVID
MERRILL, BRIAN ALLEN

DESCRIPTION:

Sex: .....MALE
Race: .....WHITE
Place of Birth: .....VAN NUYS, CALIFORNIA
Date(s) of Birth: 08/06/63; 10/18/70
Height: .....5'11"
Weight: 190
Eyes: .....BLUE
Hair: .....BROWN
Skintone: .....LIGHT
Scars, Marks, Tattoos: .....NONE KNOWN
Social Security Number (s): 550-39-5695
NCIC Fingerprint Classification: ...DOPM20PM13DIPM19PM09

ADDRESS AND LOCALE: KNOWN TO RESIDE IN THE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND LAS VEGAS, NEVADA

WANTED FOR: VIOLATION OF SUPERVISED RELEASE
ORIGINAL CHARGES: POSSESSION UNAUTHORIZED ACCESS DEVICE; COMPUTER FRAUD
Warrant Issued: CENTRAL DISTRICT OF CALIFORNIA
Warrant Number: 9312-1112-0154-C

DATE WARRANT ISSUED: NOVEMBER 10, 1992

MISCELLANEOUS INFORMATION: SUBJECT SUFFERS FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED WEIGHT GAIN OR WEIGHT LOSS
VEHICLE/TAG INFORMATION: NONE KNOWN OFTEN USES PUBLIC TRANSPORTATION

If arrested or whereabouts known, notify the local United States Marshals Office, (Telephone: 213-894-2485).

If no answer, call United States Marshals Service Communications Center in McLean Virginia.
Telephone (800)336-0102 (24 hour telephone contact) NLETS access code is VAUSM0000.

PRIOR EDITIONS ARE OBSOLETE AND NOT TO BE USED

Form USM -132
(Rev. 3/2/92)

November 1992

Historique (**Kevin mitnick**)

- Commencé à hacker des réseaux téléphoniques
- Il a attaqués les machines de **tsutomu shimomura** au centre du **supercomputing**

.

- Il a pénétré dans les serveurs du **WELL** et a accédé au courrier de **markoff** (un journaliste)

- Il a été arrêté avec l'aide d'annonce du **shimomura** et la société **WELL**

- A servi 5 années en prison et interdit d'utiliser des ordinateurs pour 2 années

Historique (**Kevin mitnick**)

- Il est maintenant depuis 2000 Consultant en sécurité informatique.
- il a publié un livre traitant de **l'ingénierie sociale, IDS,…**

Historique (**DDOS**)

Février 2000

- Plusieurs sites Web majeurs non accessibles (ebay, cnn, amazon, microsoft,....) pour quelques heures.
- Ils sont inondés par un flux énorme de traffic (jusqu'à 1 gbps), de plusieurs adresses.

Février 16h

Quelqu'un est suspecté pour avoir lancé les attaques

Avril15h

il est arrêté au canada, il a **15 ans**

Historique (**DDOS**)

Il a été condamné à 8 mois dans un centre de détention

Avec un programme automatique, il était capable de hacker 75 machines différentes dû à une vulnérabilité dans leurs serveurs ftp

il a installé un programme d'attaque distribué sur ces machines **DDOS**

Historique (**Autres**)

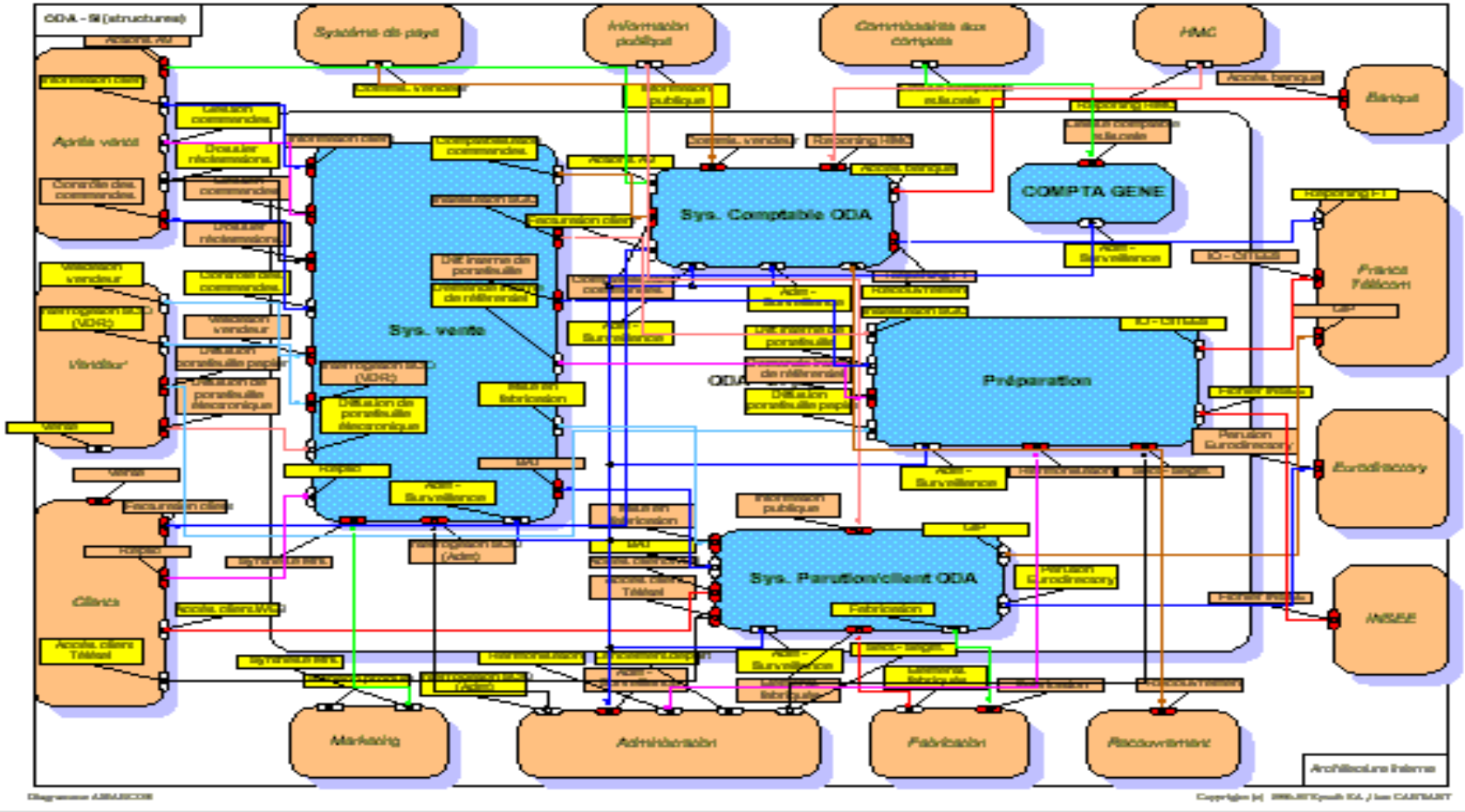
- MELLISA et autres bugs
- Programme de l'opération bancaire à distance.
- Virus, vers, spyware,…
- Attaques réseaux
- …etc

Systèmes d'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.

Systèmes d'information



Systèmes d'information

– Besoin de plus en plus d'informations

Systèmes d'information

- Grande diversitée dans la nature des informations:
  - données financières
  - données techniques
  - données médicales
  - …

Ces données constituent les biens des personnes et des entreprises et peuvent être très convoitées.

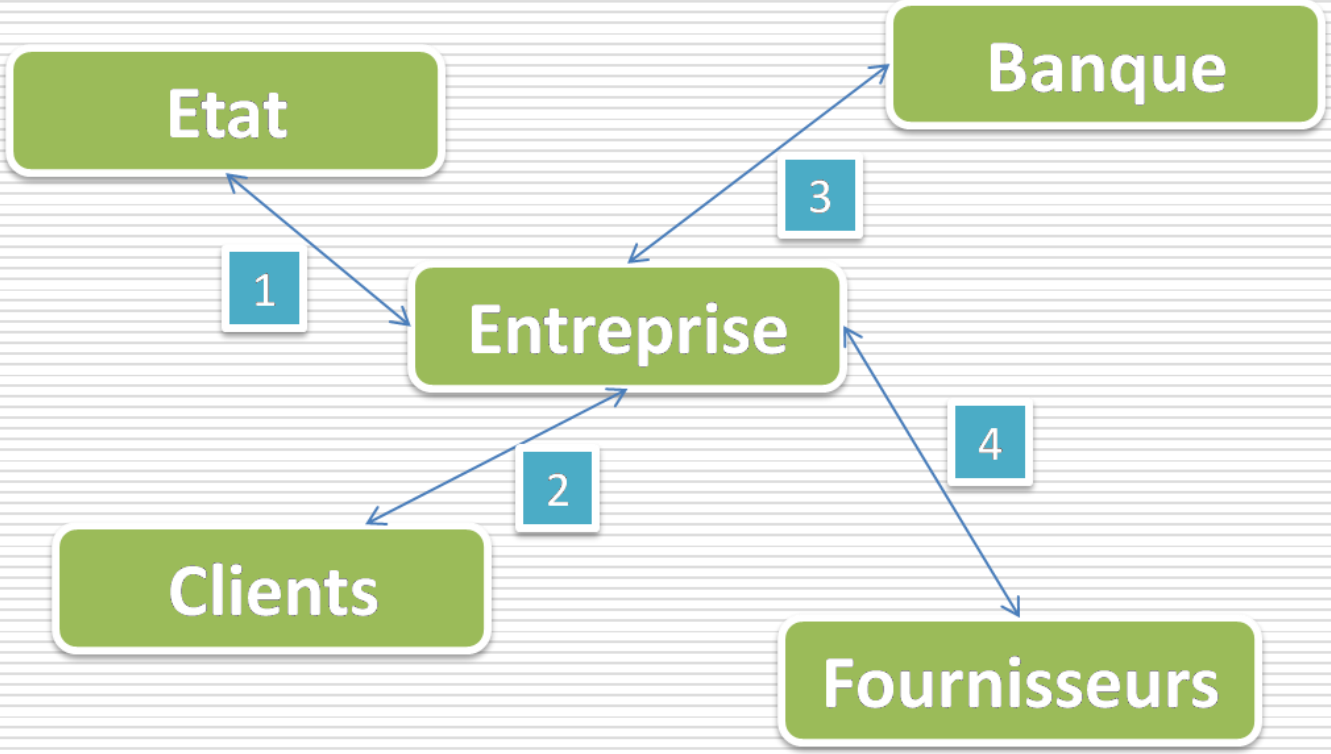
Systèmes Informatiques

- Un des moyens techniques pour faire fonctionner un système d'information est d'utiliser **un système informatique (coeur)**.

- **Les Systèmes informatiques sont devenus la cible de ceux qui convoitent l'information.**

Assurer la sécurité de l'information =➔ d'assurer la sécurité des systèmes informatiques.

Sécurité Informatique



Sécurité Informatique

- Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs **partenaires** ou leurs **fournisseurs**.

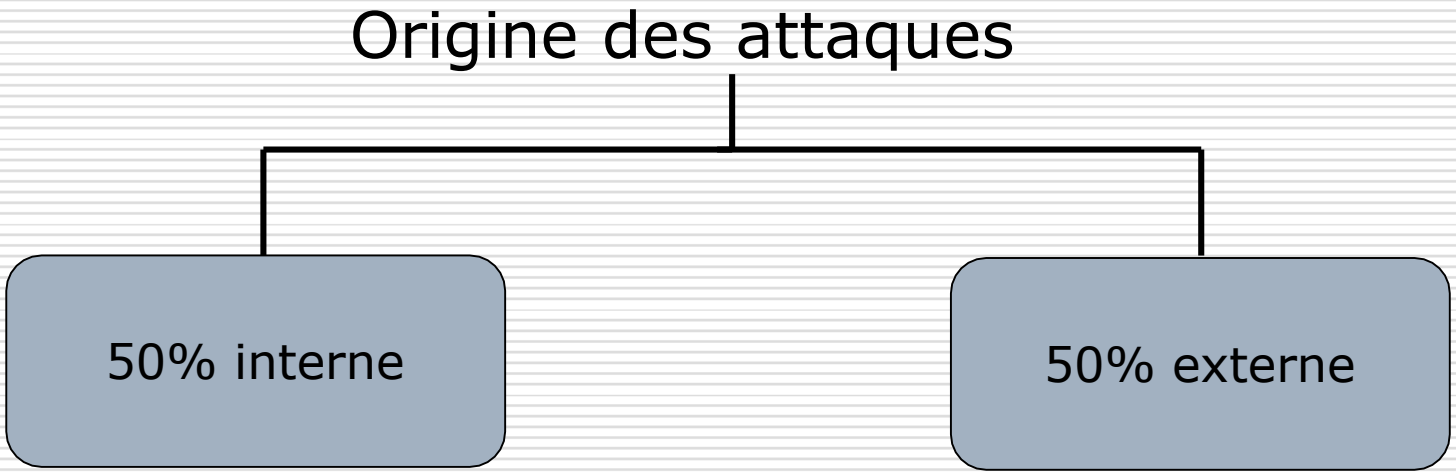
Il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information

Sécurité Informatique

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

Exigences fondamentales et objectifs

Exigences fondamentales et objectifs



Exemple :
•utilisateur malveillant, erreur involontaire,…

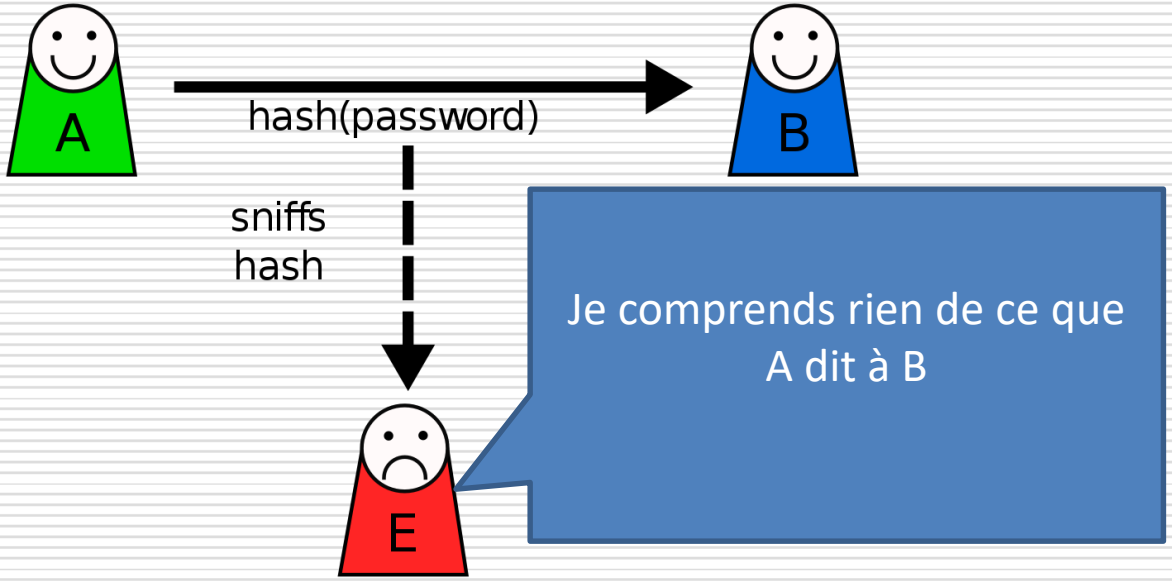
Exemple:
•Piratage, virus, intrusion…,..

Exigences fondamentales et objectifs

- Elles caractérisent ce à quoi s'attendent les utilisateurs du systèmes informatiques en regard de la sécurité.

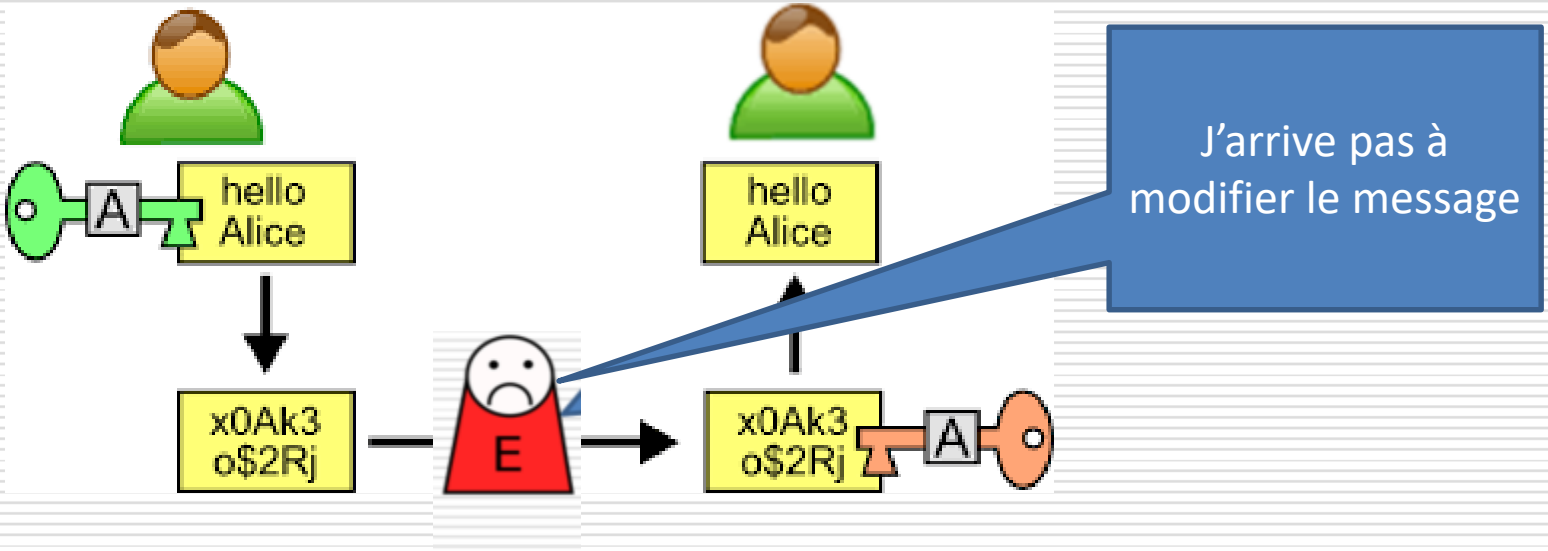
Exigences fondamentales et objectifs

➢**La confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.



Exigences fondamentales et objectifs

➢**L'intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être.



l'information n'a pas été modifiée entre sa création et son traitement (et transfert)

Exigences fondamentales et objectifs

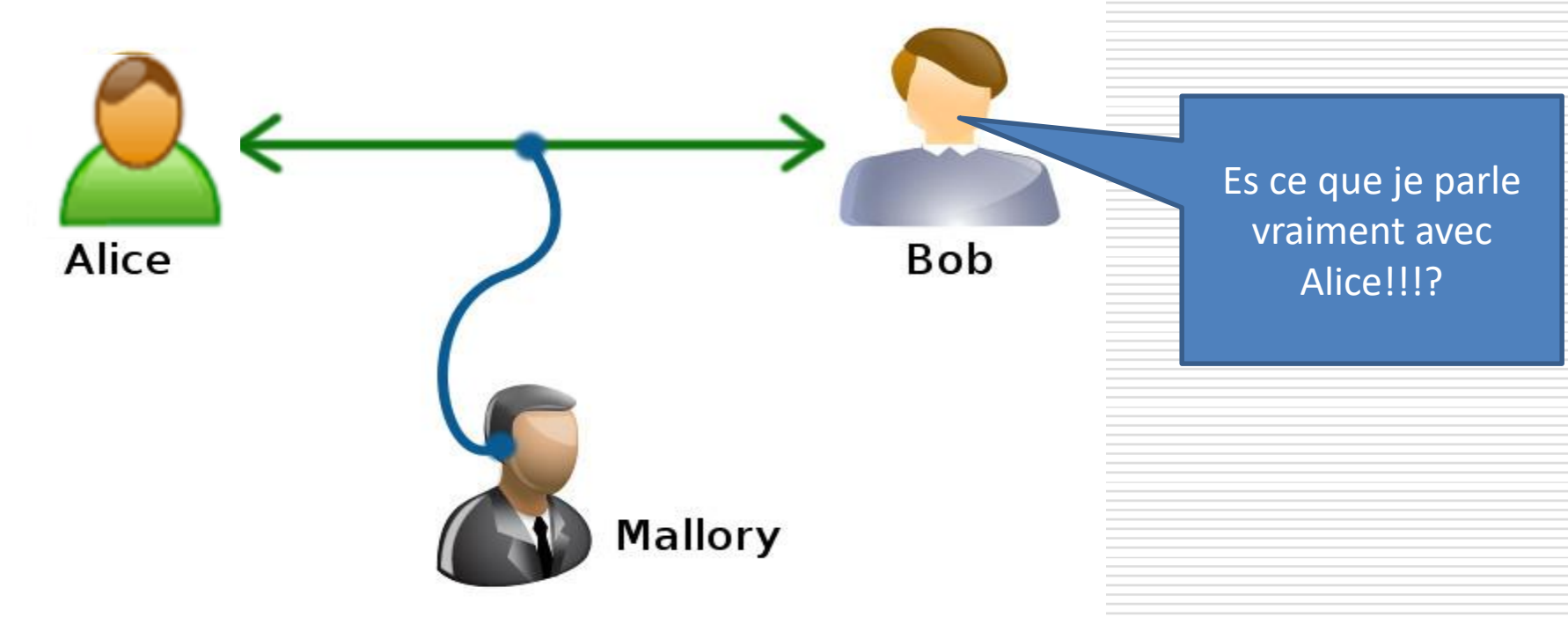
- **La disponibilité**, permettant de maintenir le bon fonctionnement du système d'information.

Exigences fondamentales et objectifs

La non répudiation, permettant de garantir qu'une transaction ne peut être niée.

Exigences fondamentales et objectifs

L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.



Exigences fondamentales et objectifs

L'authentification

Exigences fondamentales et objectifs

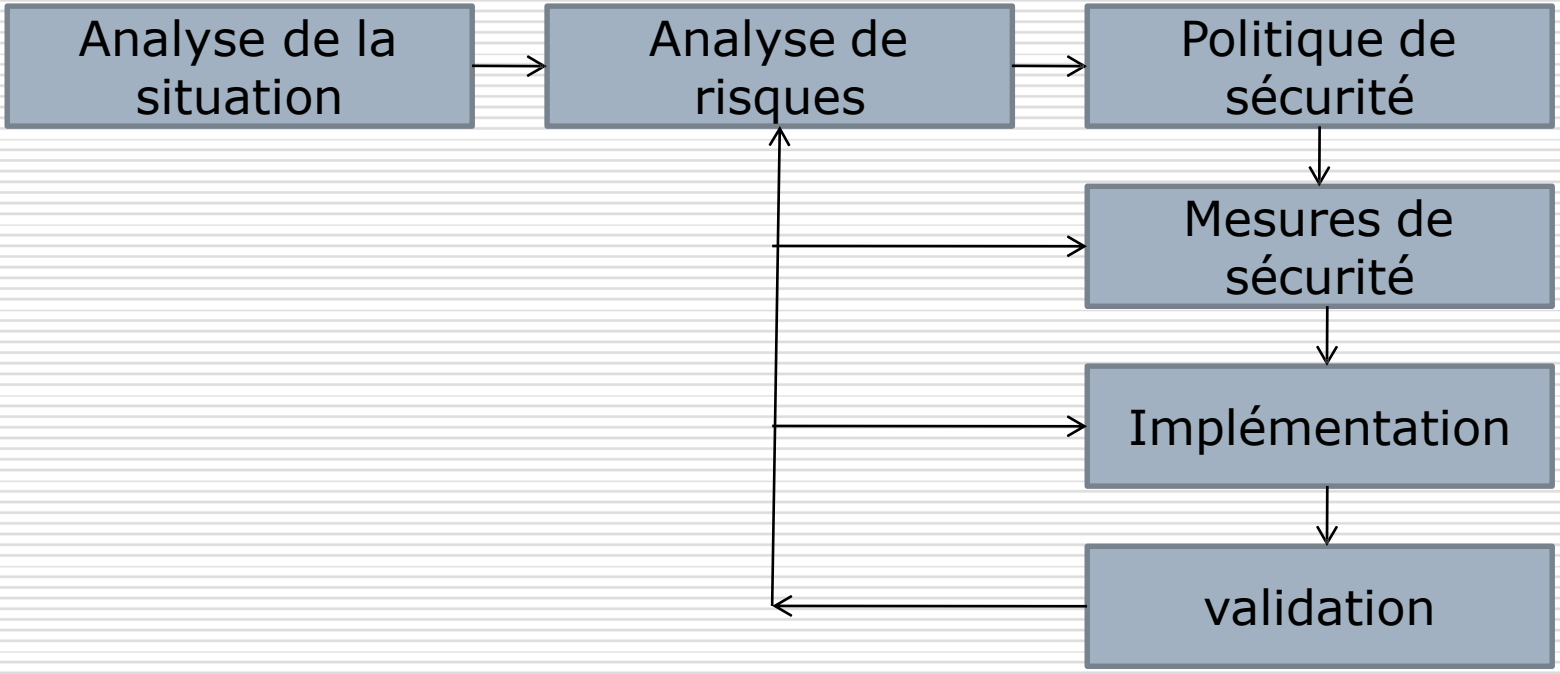
Respect de la vie privée (informatique et liberté).

Et autres…

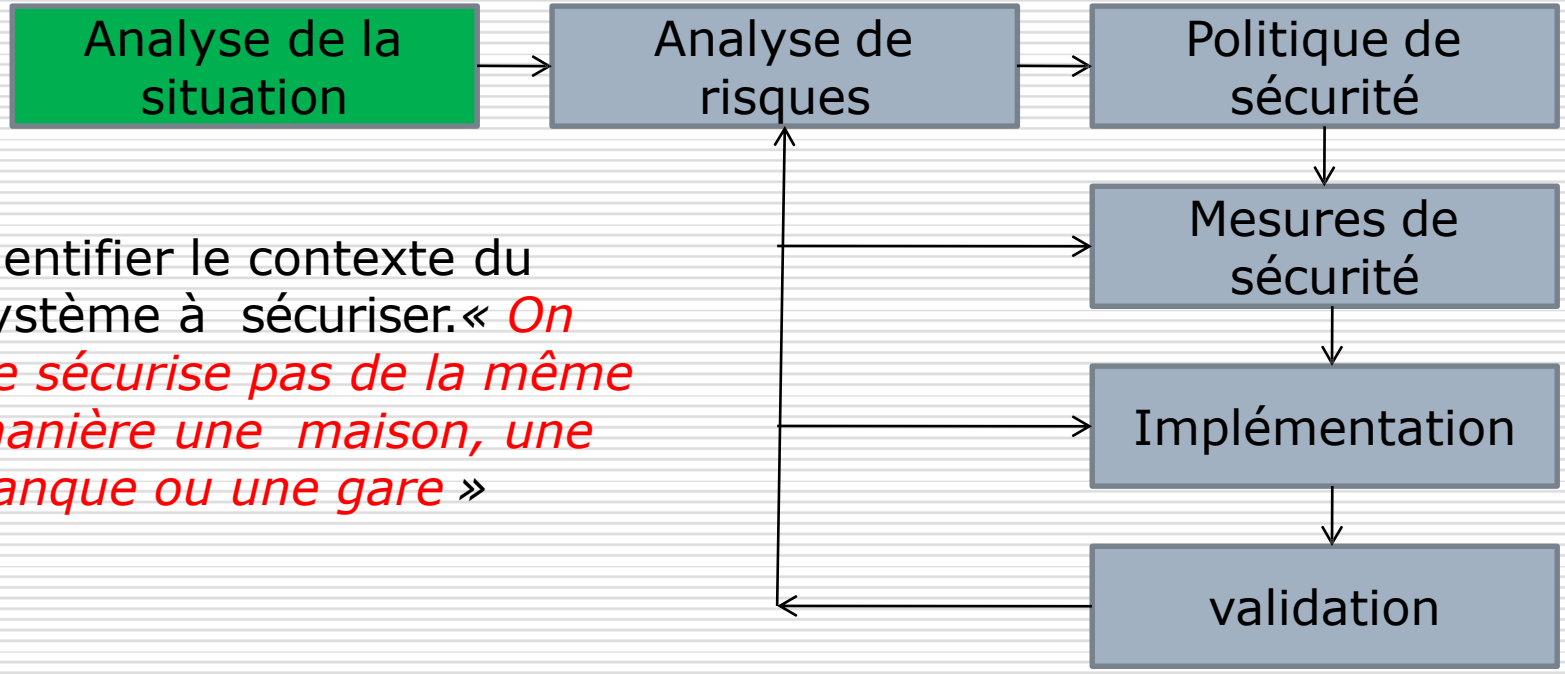
- Admissibilité
- Utilité
- …

Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau

Démarche (Méthodologie ?) pour sécuriser un système d'information dans un réseau

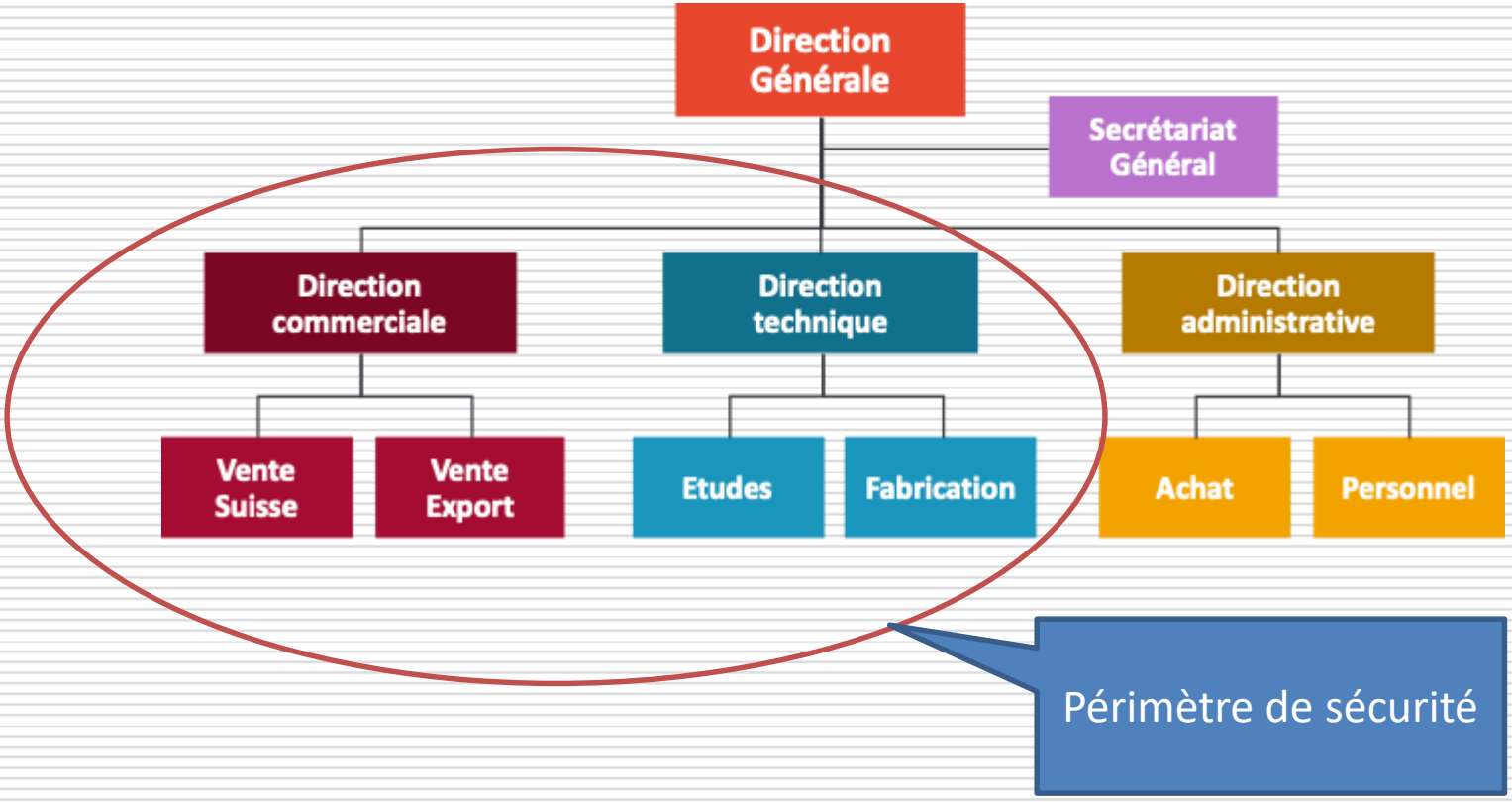


Démarche pour sécuriser un SI
Analyse de la situation



identifier le contexte du système à sécuriser.« *On ne sécurise pas de la même manière une maison, une banque ou une gare* »

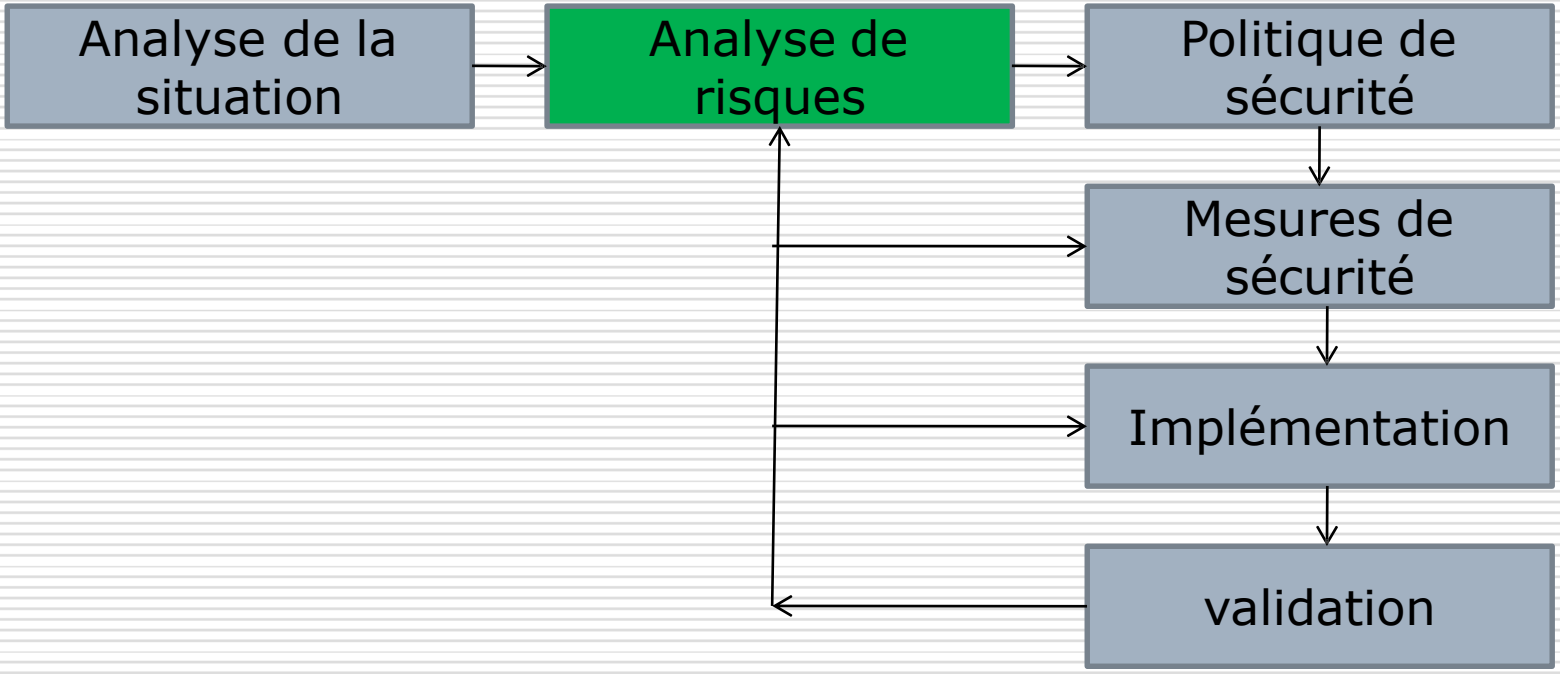
Démarche pour sécuriser un SI
Analyse de la situation : périmètre de sécurité



Démarche pour sécuriser un SI
Analyse de la situation : périmètre de sécurité

Étude (analyse) des risques

Démarche pour sécuriser un SI
Analyse de risque



Démarche pour sécuriser un SI
Analyse de risque

- 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.

Démarche pour sécuriser un SI
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

Démarche pour sécuriser un SI
Analyse de risque

- 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 (programmes d'analyse des paquets, logs…).
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ?

Démarche pour sécuriser un SI
Analyse de risque

Il faut cependant prendre conscience que les principaux risques restent :

- « câble arraché »,
- « coupure secteur »,
- « crash disque »,
- « mauvais profil utilisateur », …

Étude (analyse) des risques
Ce qu'il faut retenir

1. Inventaire des éléments du système à protéger
2. Inventaire des **menaces** (incidents) possibles sur ces éléments
3. Estimation de la **probabilité** que ces menaces se réalisent
4. Estimation du cout relatif à chaque incident

Étude (analyse) des risques
Ce qu'il faut retenir

	Cout cher	Cout faible
Incidents fréquent	Incident Incident Incident …	Incident Incident Incident …
Incidents rare	Incident Incident Incident …	Incident Incident Incident …

Étude (analyse) des risques
Ce qu'il faut retenir

	Cout cher	Cout faible
Incidents fréquent	• **Mettre en place des mécanismes de sécurité** • **Recruter** • **Former** • **…**	
Incidents rare		

Étude (analyse) des risques
Ce qu'il faut retenir

	Cout cher	Cout faible
Incidents fréquent	• **Mettre en place des mécanismes de sécurité** • **Recruter** • **Former** • **…**	Assurer la disponibilité (serveurs miroirs. etc)
Incidents rare		

Étude (analyse) des risques
Ce qu'il faut retenir

	Cout cher	Cout faible
Incidents fréquent	• **Mettre en place des mécanismes de sécurité** • **Recruter** • **Former** • **…**	Assurer la disponibilité (serveurs miroirs. etc)
Incidents rare	S'assurer	

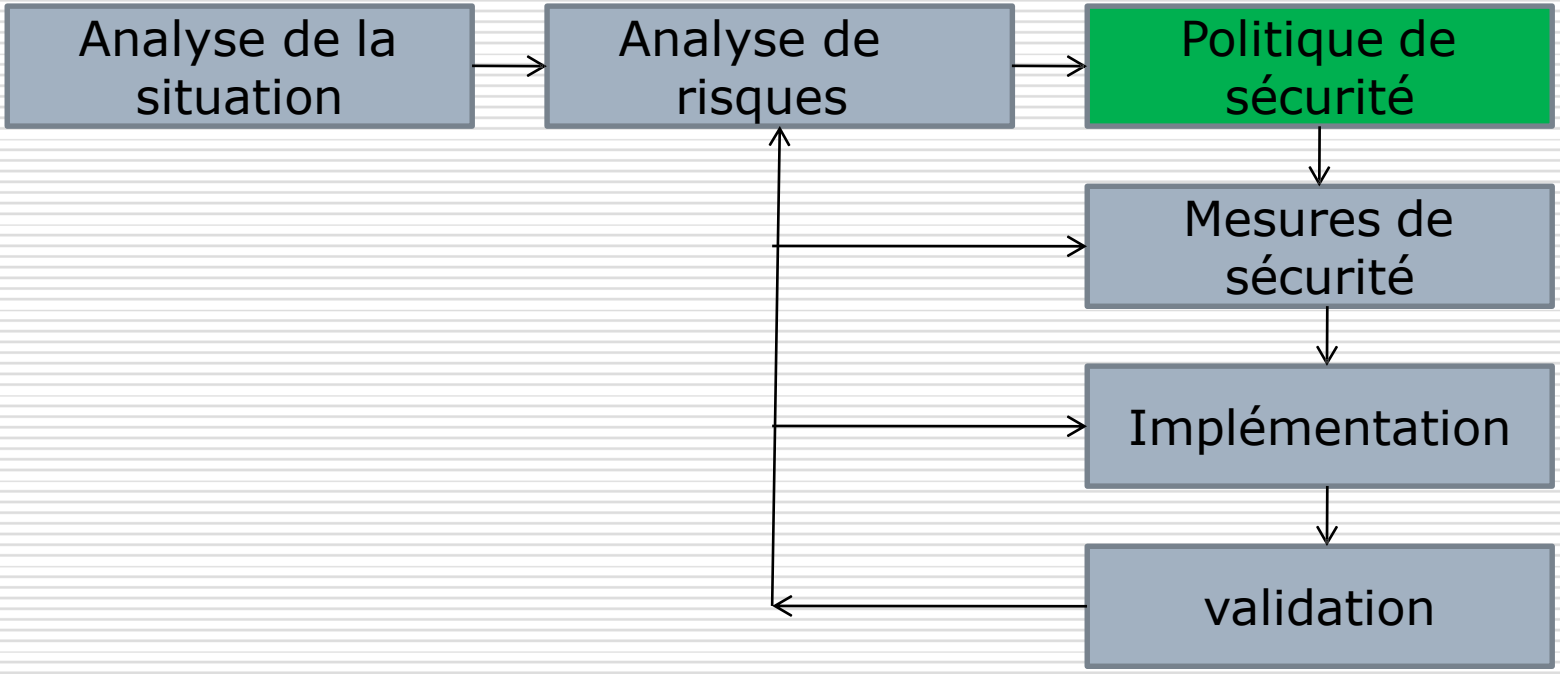
Étude (analyse) des risques
Ce qu'il faut retenir

	Cout cher	Cout faible
Incidents fréquent	• **Mettre en place des mécanismes de sécurité** • **Recruter** • **Former** • **…**	Assurer la disponibilité (serveurs miroirs. etc)
Incidents rare	S'assurer	Accepter

Le risque « **zéro** » n'existe pas, il faut définir le risque résiduel que l'on est prêt à accepter.

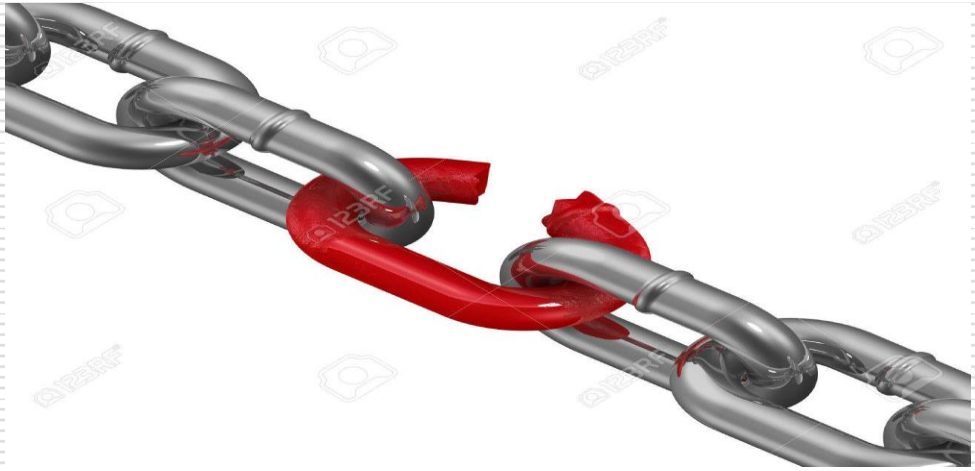
Établissement d'une politique de sécurité

Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité



Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité

- Il ne faut pas perdre de vue que la sécurité est comme une chaîne, guère plus solide que son maillon le plus faible



Une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Démarche pour sécuriser un SI
Etablissement 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

Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité

- Identifier les risques et leurs conséquences.

•Elaborer des règles et des procédures à mettre en oeuvre 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.

Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité

- Quels furent les coûts des incidents informatiques passés ?
- Quel degré de confiance pouvez-vous avoir envers vous utilisateurs interne ?
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quel sera l'impact sur la clientèle si la sécurité est insuffisante, ou tellement forte qu'elle devient contraignante ?

Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité

- Y a-t-il des informations importantes sur des ordinateurs en réseaux ? Sont-ils accessible de l'externe ?

- Quelle est la configuration du réseau et y a-t-il des services accessibles de l'extérieur ?

- Quelles sont les règles juridiques applicables à votre entreprise concernant la sécurité et la confidentialité des informations ?

Démarche pour sécuriser un SI
Etablissement d'une Politique de sécurité

Mise en œuvre

- Audit
- Tests d'intrusion
- Détection d'incidents
- Réactions
- Restauration

Éléments d'une politique de sécurité

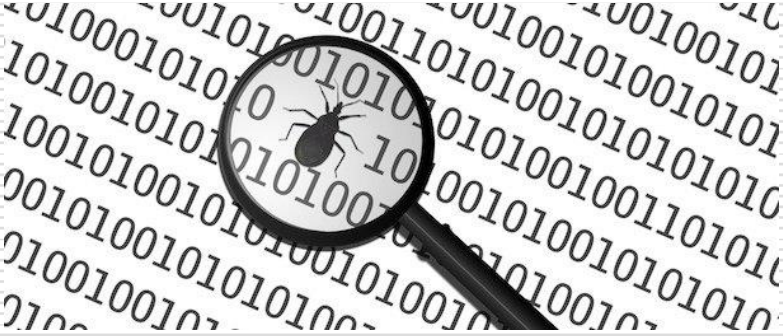
Démarche pour sécuriser un SI
Eléments d'une Politique de sécurité

- En plus de la formation et de la **sensibilisation permanente des utilisateurs**, la politique de sécurité peut être découpée en plusieurs parties :

Démarche pour sécuriser un SI
Eléments d'une Politique de sécurité

- **Défaillance matérielle**

  (vieillissement, défaut…)



Défaillance logicielle
(bugs, MAJ…)

Démarche pour sécuriser un SI
Eléments d'une Politique de sécurité

- **Accidents**

(pannes, incendies, inondations…)

Erreur humaine
(Formation)

Démarche pour sécuriser un SI
Eléments d'une Politique de sécurité

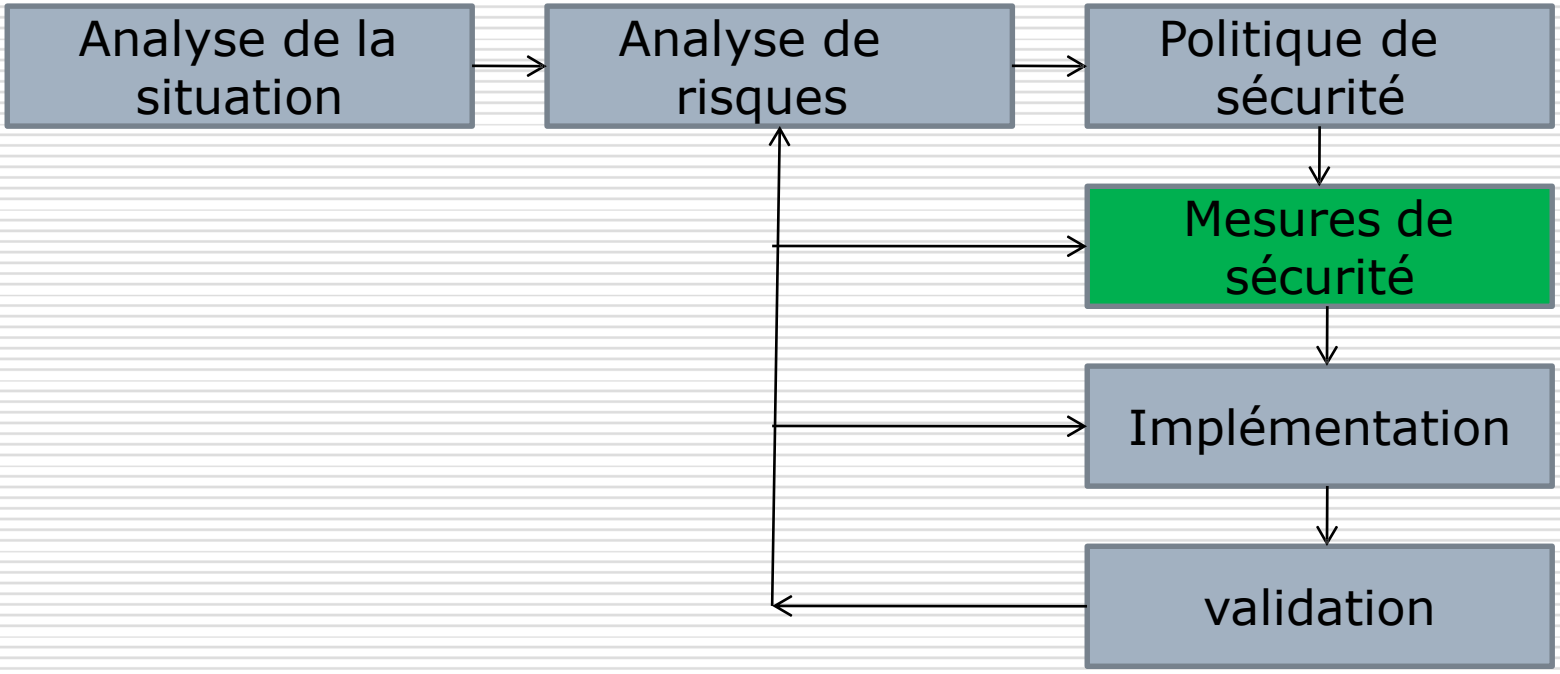
- **Vol via des dispositifs physique**

Disques,
Contrôler l'accès aux équipements

Virus provenant de disques

- **Piratage et virus réseau (plus complexe)**

Démarche pour sécuriser un SI
Mesures de sécurité



Démarche pour sécuriser un SI
Mesures de sécurité

Mesures techniques

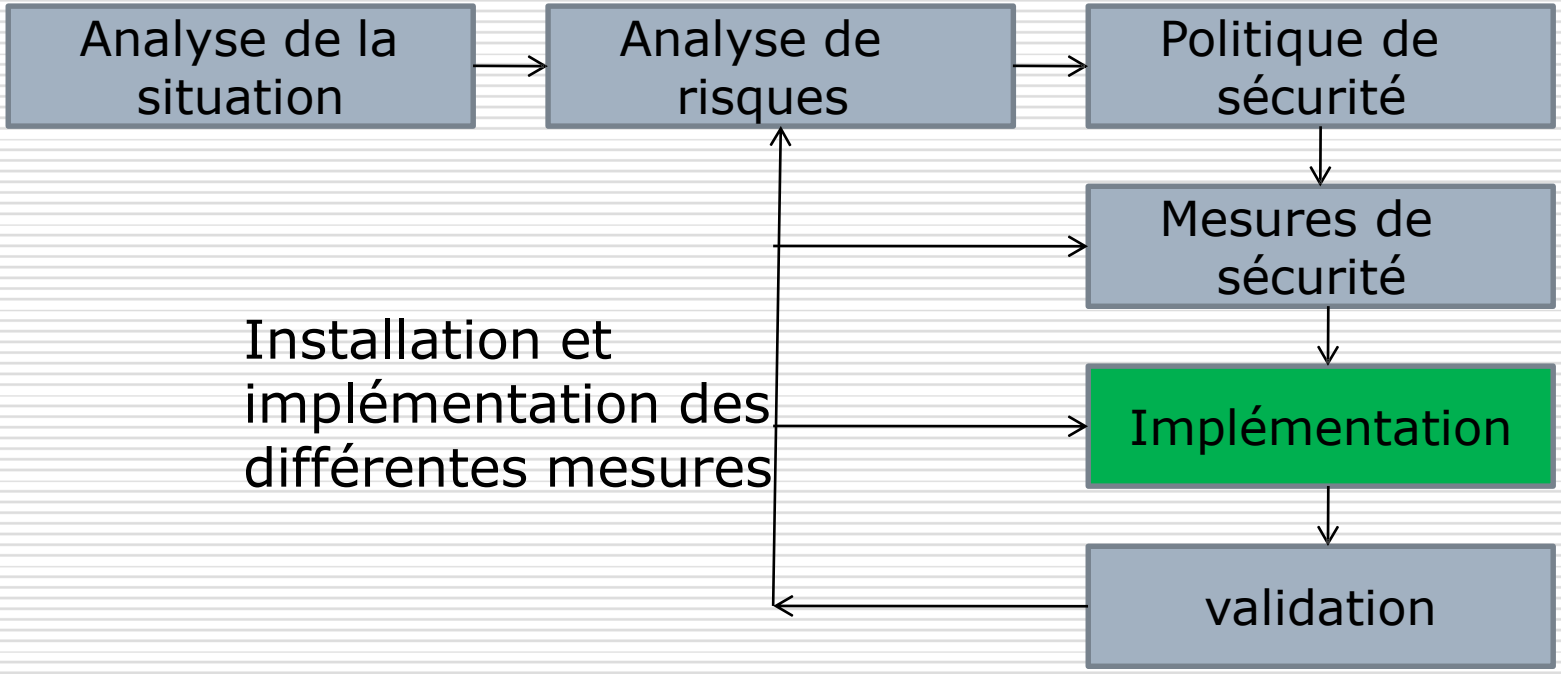
- FireWall,
- Antivirus,
- IDS,
- …)

Organisationnelles

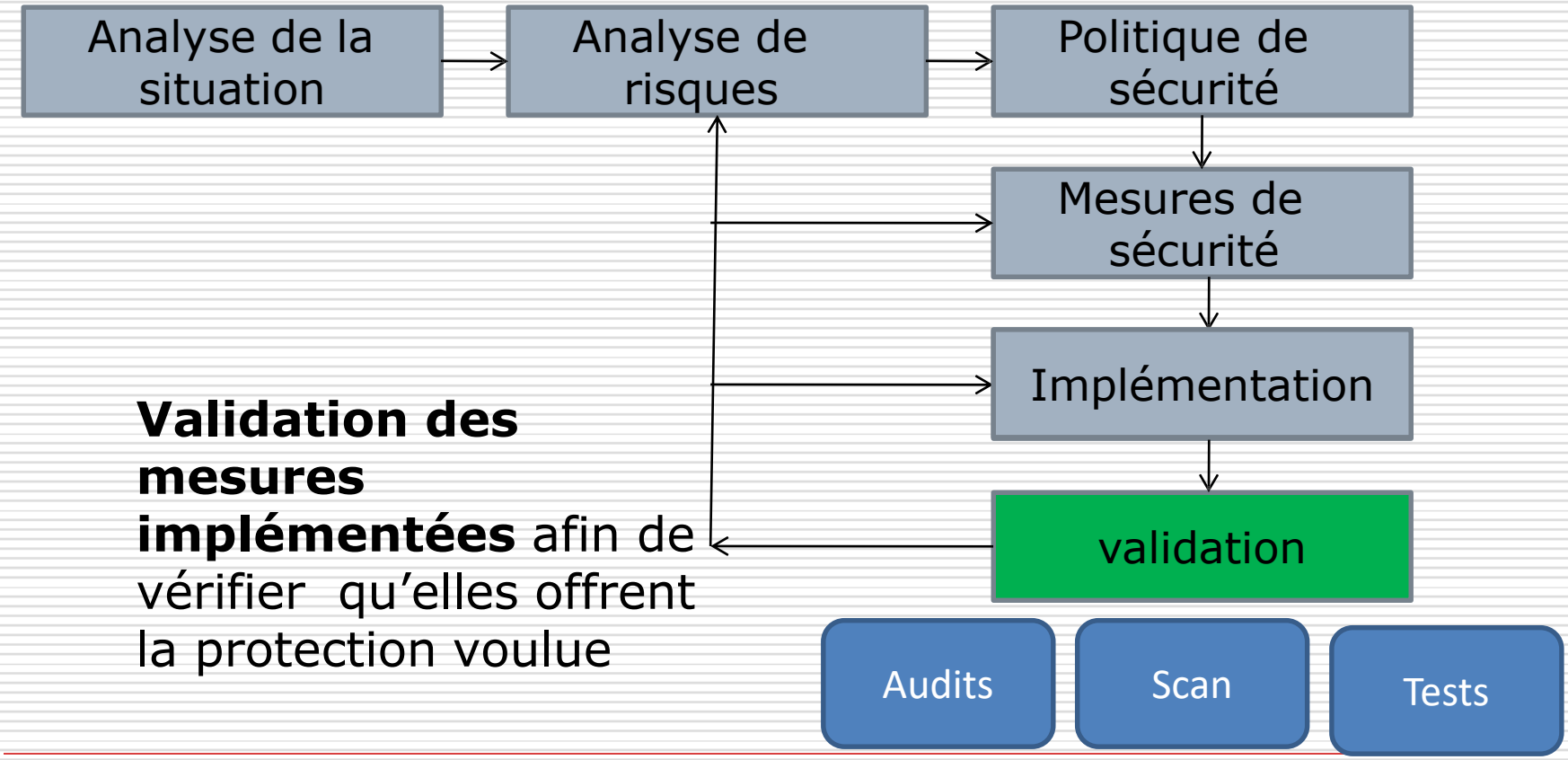
- Procédure de secours,
- nomination
- responsable sécurité,
- …)

<u>Pour permettre d'appliquer la politique de sécurité</u>

Démarche pour sécuriser un SI
Implémentation des Mesures de sécurité



Démarche pour sécuriser un SI
Validation de la politique de sécurité



Validation des mesures implémentées afin de vérifier qu'elles offrent la protection voulue

Démarche pour sécuriser un SI
Résumé

Analyse de la situation : identifier le contexte du système à sécuriser.« *On ne sécurise pas de la même manière une maison, une banque ou une gare* »

Analyse des risques : Diminuer le risque global auquel le système est exposé

Politique de sécurité :
Sert à décrire de quelle manière le risque global sera **diminué** (avec risque résiduel):

Démarche pour sécuriser un SI
Résumé

Mesures de sécurité :
Ensemble de mesures techniques ou **organisationnelles** qui vont permettre d'appliquer la politique de sécurité

Implémentation
Installation et implémentation des différentes mesures

Validation
Validation des mesures implémentées afin de vérifier qu'elles offrent la protection voulue (Audits, scans de vulnérabilité, tests d'intrusion, etc…)

Principaux défauts de sécurité

Principaux défauts de sécurité

- Installation des logiciels et matériels par défaut.

- Mises à jours non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (Netbios…).
- Traces inexploitées.

Principaux défauts de sécurité

- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Télémaintenance sans contrôle fort.
- Procédures de sécurité obsolètes (périmés).
- Authentification faible.

Principaux défauts de sécurité

- **L'état actif d'insécurité**:

L'utilisateur ne connait pas les fonctionnalités du système, dont certainnes pas nécessaires

Ex: le fait de ne pas désactiver des services réseaux non nécessaires

- **l'état passif d'insécurité**:

L'utilisateur ne connait pas ses moyens de sécurité

Ex: Lorsque l'administrateur ne connaît pas les dispositifs de sécurité dont il dispose.

Notion d'audit

Notion d'audit

- Un audit de sécurité consiste à s'appuyer sur un tiers de confiance (généralement une société spécialisée en sécurité informatique) afin de valider les moyens de protection mis en œuvre, au regard de la politique de sécurité.

- **L'objectif de l'audit est ainsi de vérifier que chaque règle de la politique de sécurité est correctement appliquée et que l'ensemble des dispositions prises forme un tout cohérent.**

Notion d'audit

Un audit de sécurité permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sûres.

Merci