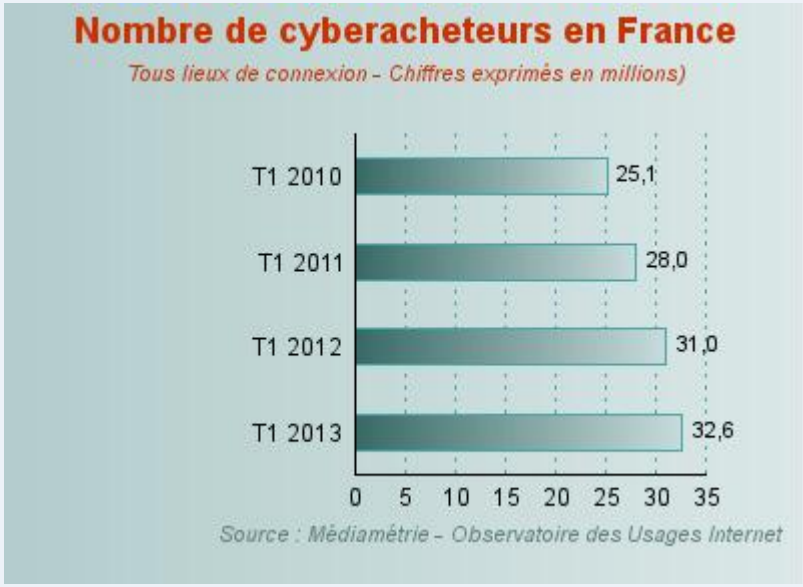
Généralités sur la sécurité

M2 Info, ULCO

Patrick Sondi

Quelques chiffres

Observation	2001	2006	2011
Nombre d'internautes en France (en millions)	11	26	40



- Coût de la cybercriminalité dans le monde : 500 milliards $ (MacAfee)
- Coût de la fraude fiscale dans le monde : 2500 milliards $ (Le point)

- Coût de la fraude fiscale en France: 80 milliards d'euros (Le monde)
Part de la drogue: 10%

La cybercriminalité dans le monde :
65% des utilisateurs d'internet ont été victimes d'une cyberattaque (virus, fraude à la carte de crédit en ligne, vol d'identité)
- Soit **1.5** millions de personnes par jour
- 8 victimes par seconde
75% des attaques sont financières
Dans les attaques de données : **92%** des agresseurs sont externes
Dans les intrusions réseau : **76%** des cas se font par vol ou déduction de code d'accès
Temps pour cracker un mot de passe :
- 10 minutes pour 6 lettres
- 3 ans pour 7 majuscules-minuscules
- 463 ans pour 8 lettres-chiffres-symboles

Sources : Mashable, Norton, Verizon 2013 Data Breach Investigations Report

Partie 1: Rappels et état des lieux en France

1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 1

***Sécurité**:*

- ***Safety** : protection contre les accidents dus à l'environnement ou aux défauts du système (lié aux domaines mettant en danger des vies humaines: transports, énergie, santé, etc)*
- ***security**: protection contre des actions malveillantes intentionnelles*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 2

Sécurité informatique *:*

« *ensemble des moyens mis en œuvre pour* ***minimiser la vulnérabilité*** *d'un système contre des menaces* ***accidentelles*** *ou* ***intentionnelles*** *»*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 3

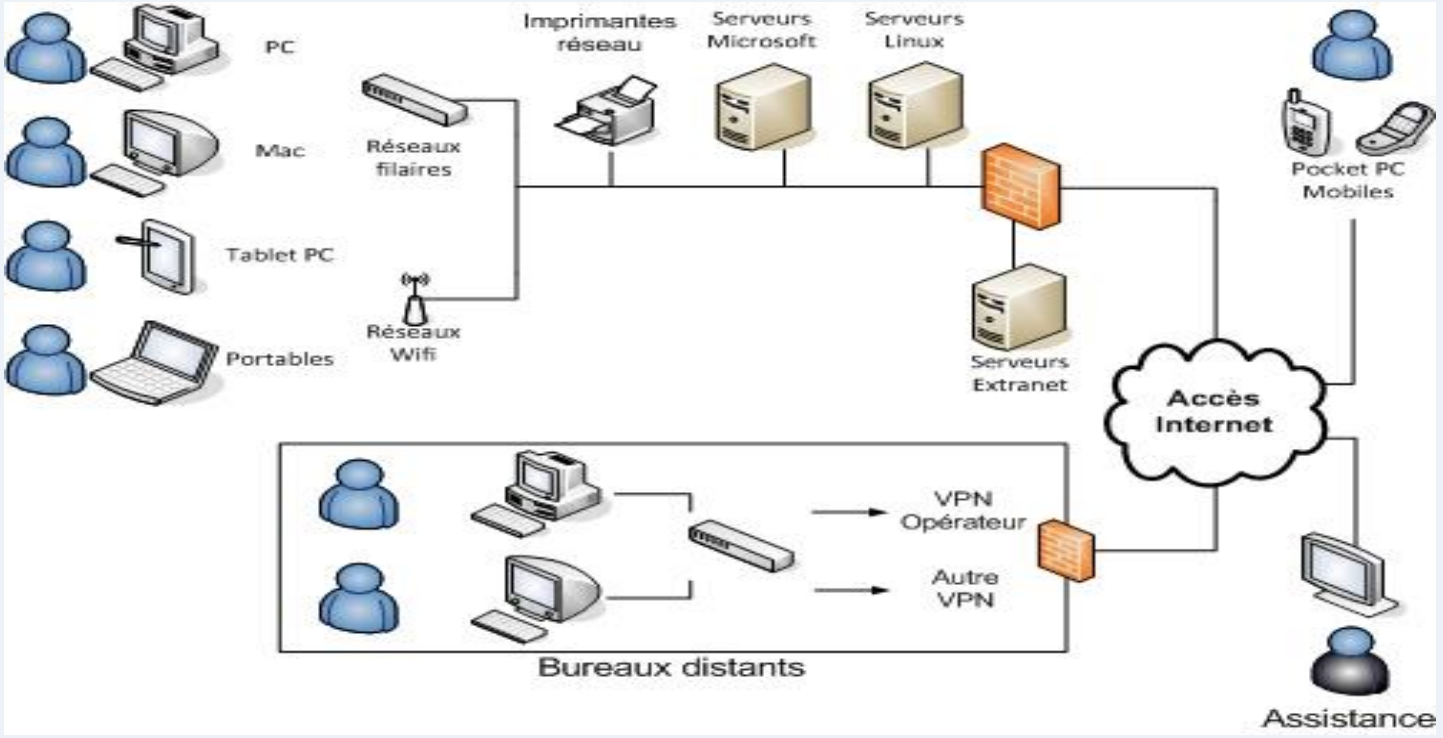
***Sécurité de système d'information**:*

*« ensemble de moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour **conserver**, **rétablir**, et **garantir** sa sécurité. »*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 4 ***Système informatique***



Source image : http://www.syrix.fr/activite/activite.htm

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 4

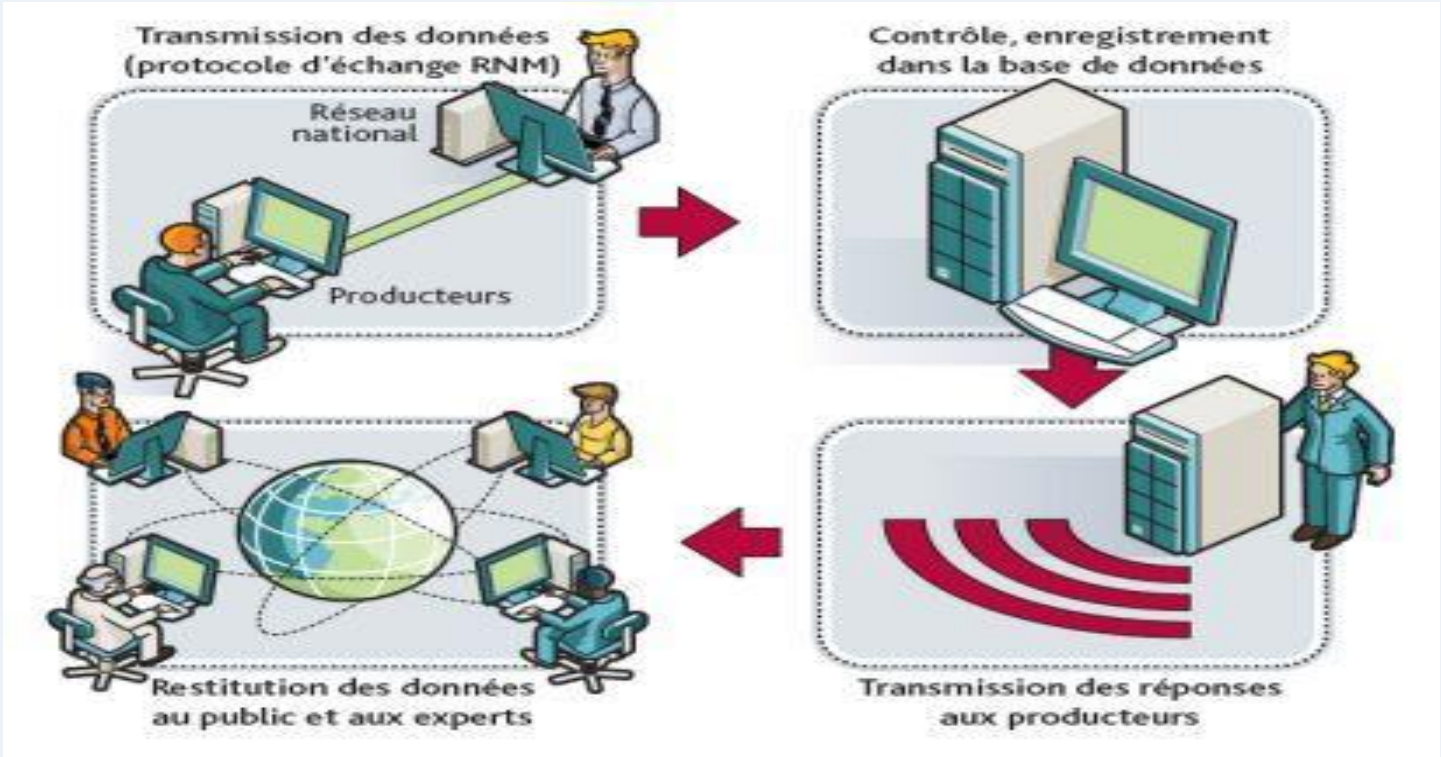
***Système informatique**:*

« ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est généralement constitué de serveurs, routeurs, imprimantes, médias (câbles, ondes), OS, applications, bases de données, etc.»

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

Définition 5 ***Système d'information***



Source image : http://www.mesure-radioactivite.fr/public/spip.php?rubrique93

Partie 1
1.1 Définitions et principes de la sécurité

1.1.1 Définitions

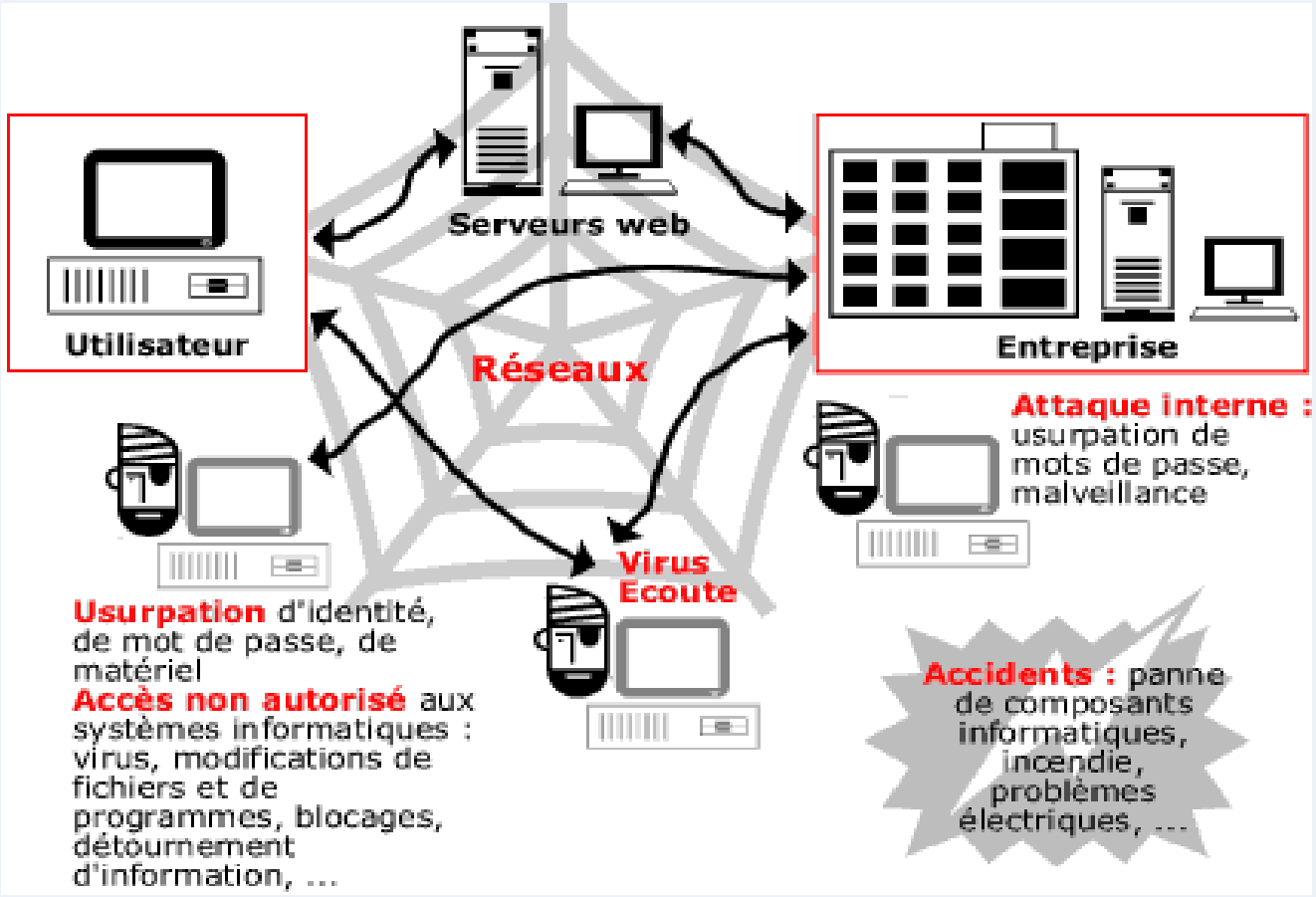
Définition 5

***Système d'information**:*

*« ensemble de moyens (**humains**, matériels, logiciels, etc.) organisés permettant d'élaborer, de traiter, de stocker et/ou de diffuser de l'information grâce aux processus ou services. Un système d'information est généralement délimité par un **périmètre** pouvant comprendre des sites, des locaux, des acteurs (partenaires, clients, employés, etc.), des équipements, des processus, des services, des applications et des bases de données.»*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces



Source image : http://www.awt.be/web/sec/index.aspx?page=sec,fr,fic,045,002

Partie 1

1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Quelques lois remarquables en France:

- Validité juridique des opérations informatiques
- Loi 78-17 (6/1/1978) : informatique et liberté

collecte et non-divulgation données privées

- Loi 85-660 (3/7/1985): contrefaçons/copyright

encadre la production de copies de sauvegarde

- Loi 88-19 (5/1/1988): fraude informatique

accès non autorisés, falsification, déni de service

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

La sécurité informatique se décline en domaine

- ***physique****: environnement du système*
- *de l'****exploitation****: fonctionnement, usages*
- ***logique****: architectures, protocoles et logiciels*
- ***applicatif****: écriture de codes, langages*
- ***réseaux****: canaux de communication sécurisés*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Sécurité physique (Normes et préventions)

- *Intempéries, accidents -> protection de site*
- *Vols, intrusions -> contrôle des accès*
- *Sabotages, pannes -> redondance physique*
- *Destruction des supports -> sauvegardes*
- *Pannes diverses -> Maintenances préventives*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Sécurité de l'exploitation (procédures qualité)

- *Pertes, écrasements -> plan de sauvegardes*
- *Erreurs d'utilisation -> formations, contrôles*
- *Dysfonctionnements logiciels -> plans de tests*
- *Dysfonctionnements matériels -> inventaires*
- *Dysfonctionnements services -> audits*
- *Perte d'expertise -> plan de départs/arrivées*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Sécurité logique (architectures et logiciels)

- *Usurpation -> contrôle d'accès (AAA)*
- *Ecoute -> cryptographie, isolement, leurres*
- *Altération de données -> contrôle d'intégrité*
- *Altération logiciels -> antivirus, code sécurisé*
- *Saturation ressources -> filtrage, suivi sessions*
- *Analyse et inférence -> données non corrélées*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Sécurité applicative (code et intégration sûrs)

- *Failles du langage -> langages sûrs & sécurisés*
- *Failles du logiciel -> développer avec méthode*
- *Obsolescence logiciel -> contrôles programmés*
- *Obsolescence système -> plan de migration*
- *Codes tiers occasionnels -> validation et audit*
- *Codes tiers de confiance-> assurance sécurité*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.2 Domaines de la sécurité et menaces

Sécurité du réseau (canal sûr de bout en bout)

- *Attaque sur hôtes -> pare-feu, contrôle d'accès*
- *Attaque du média -> isolement, cryptographie*
- *Déni de service média -> contrôle d'admission*
- *Déni de service équipements -> bannissement*
- *Failles des protocoles -> détection d'intrusions*
- *Attaques innovantes -> monitoring, évolution*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

Les principes qui guident la mise en œuvre et l'évaluation de la sécurité informatique sont:

- *La disponibilité*
- *L'intégrité*
- *La confidentialité*
- *L'authentification*
- *La non-répudiation*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

La disponibilité

garantit qu'une ressource reste accessible et qu'il réagit avec un temps de réponse conforme à la qualité de service annoncée

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

La disponibilité

Moyens de réalisation:

- *Dimensionnement approprié*
- *Gestion opérationnelle des ressources/services*

Garde-fous

- *Tests par montée en charge et observation*
- *Sauvegarde système et redondance services*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

L'intégrité

assure qu'une information n'est modifiée que dans des conditions prédéfinies, qu'elle n'a subi aucune altération accidentelle ou intentionnelle

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

L'intégrité

Moyens de réalisation:

- réaliser une empreinte des données

- reproduire l'empreinte à la réception

Garde-fous

- *recourir à des algorithmes réputés*
- *insérer des métadonnées personnels*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

Confidentialité

garantit que seuls des acteurs habilités dans des conditions prédéfinies auront accès aux données

Source image : http://www.dmgtechnologies.ca/Securite-Informatique.html

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

La confidentialité

Moyens de réalisation:

- *mécanismes de contrôle d'accès aux données*
- *chiffrer les données pour éviter la divulgation*

Garde-fous

- *Tests et preuves de l'inviolabilité des contrôles*
- *Recours à un chiffrement réputé inviolable*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

L'authentification

assure que seules les entités autorisées pour une composante du système y ont accès

Source image :
http://www.navi-mag.com/

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

L'authentification

Moyens de réalisation:

- *utiliser des points d'identification uniques*
- *assurer l'inviolabilité des références stockées*

Garde-fous

- *associer avec l'intégrité et la confidentialité*
- *recourir à des tiers de confiance spécialisés*

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

Non-répudiation

garantit que l'auteur de toute action dans le système ne puisse ni la dissimuler, ni la nier, et qu'il soit possible de prouver qu'elle lui incombe

Partie 1
1.1 Définitions et principes de la sécurité

1.1.3 Principes de la sécurité

La non-répudiation

Moyens de réalisation:

- *recourir à une authentification forte*
- *stocker l'origine et traces des actions critiques*

Garde-fous

- *rendre impossible la modification des traces*
- *veiller à la conformité avec les cadres légaux*

Partie 1
1.2 Politique de sécurité

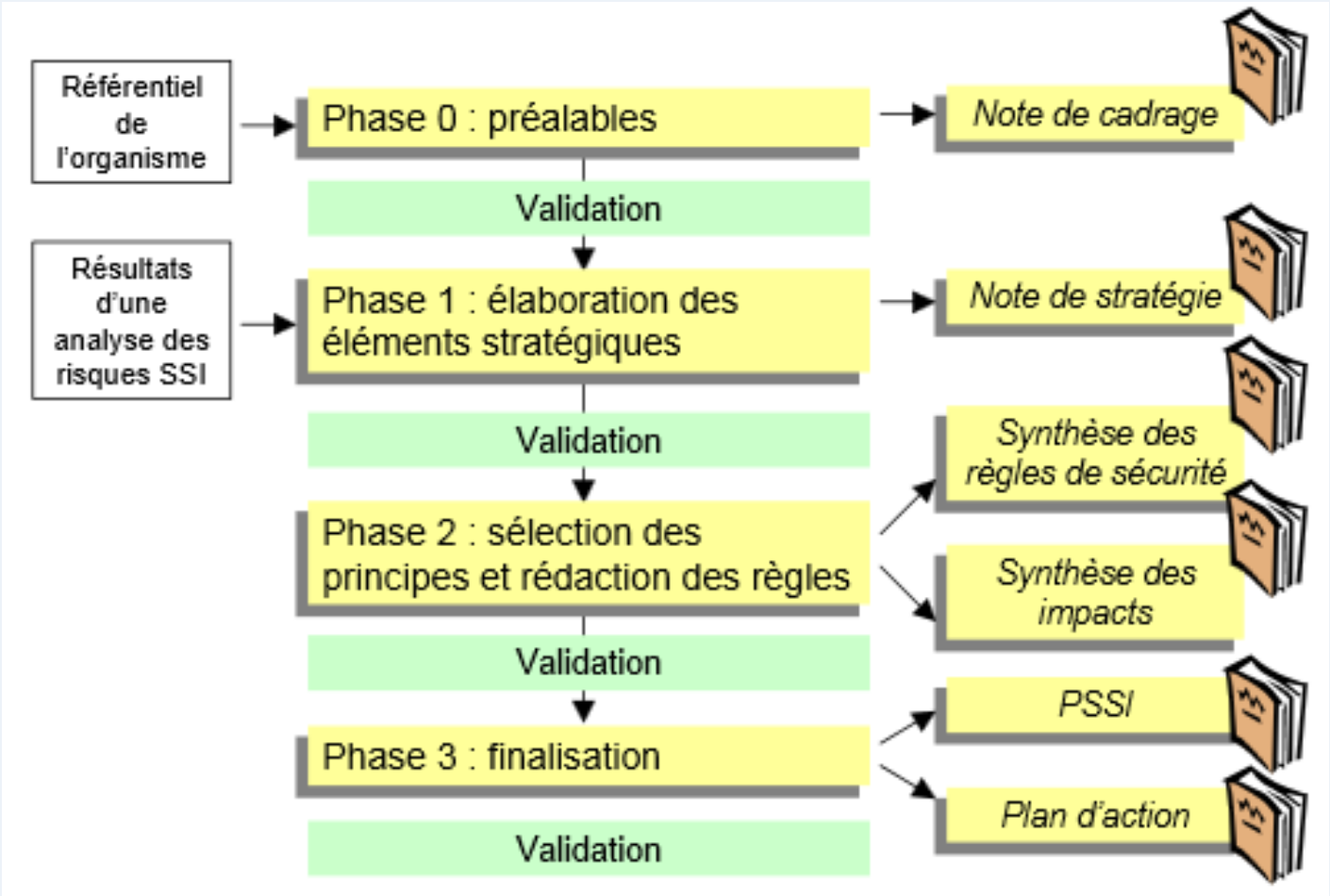
1.2.1 Définition et grandes étapes

Ensemble de règles qui fixent a priori les actions autorisées ou interdites dans le système. Sa mise en place suit les grandes étapes suivantes:

- *identification et analyse des vulnérabilités*
- *considérations normatives et juridiques*
- *mise en place d'une architecture de sécurité*
- *formation des utilisateurs*

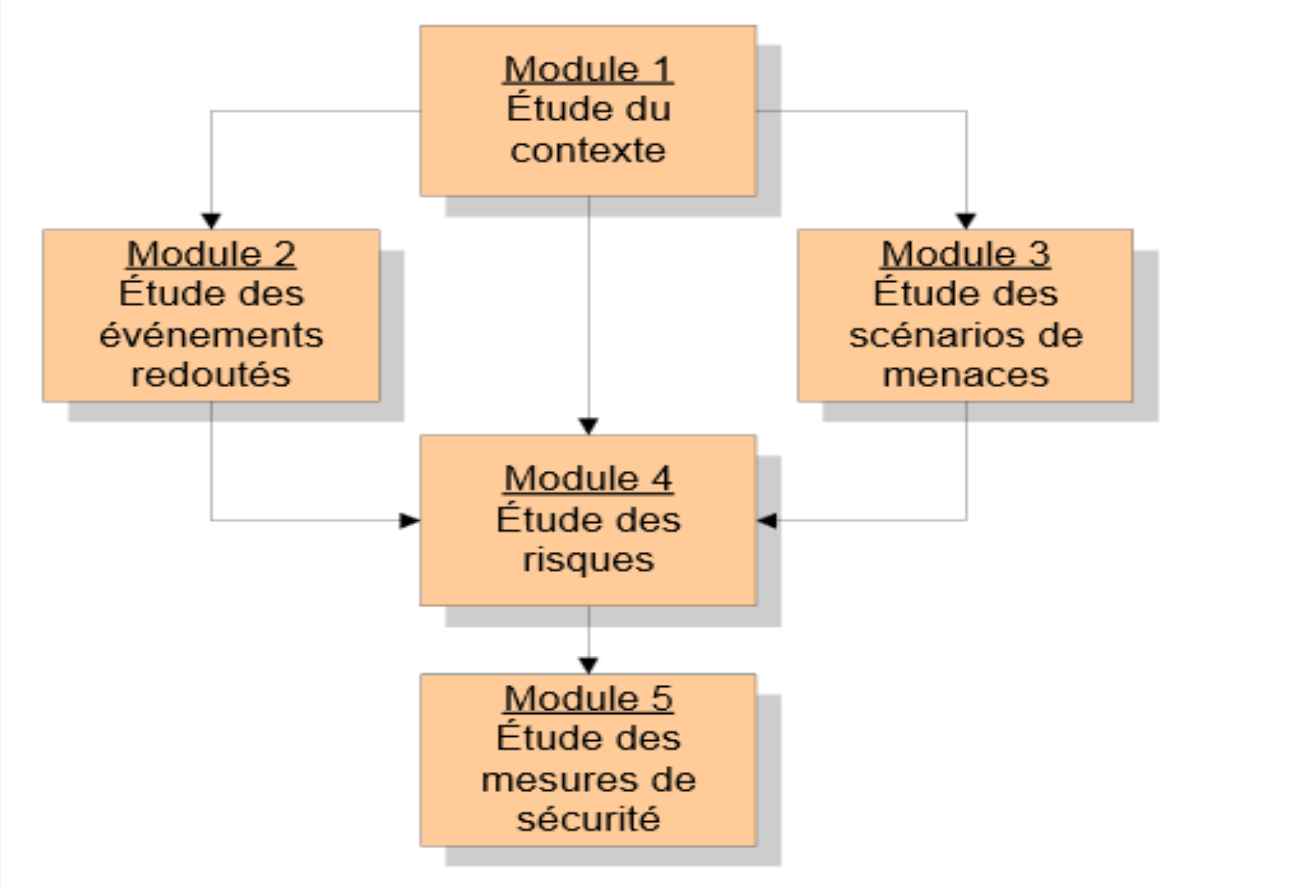
Partie 1
1.2 Politique de sécurité

1.2.2 Exemple 1 : le PSSI de l'ANSSI



Partie 1
1.2 Politique de sécurité

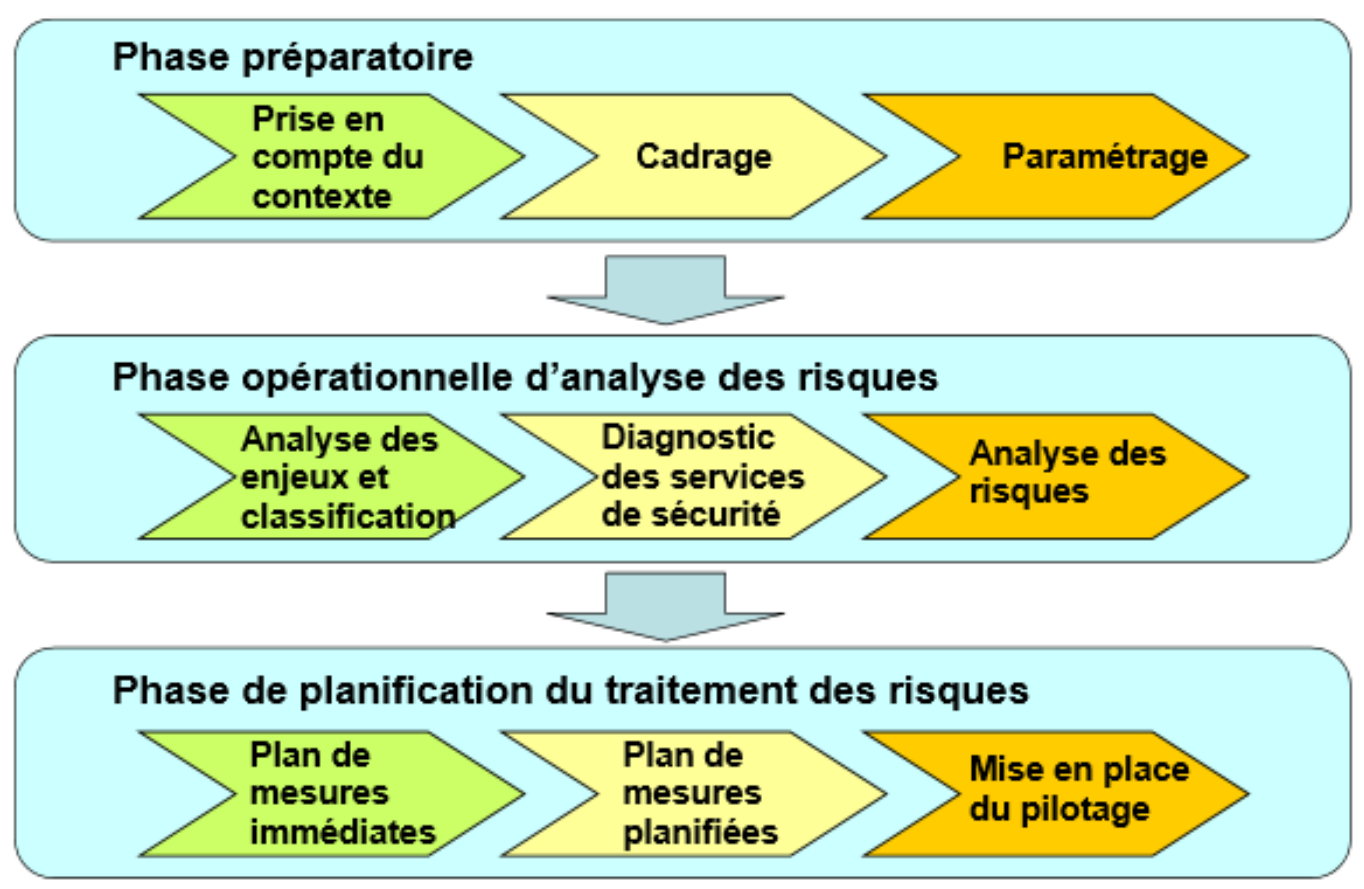
1.2.2 Exemple 2 : la méthode EBIOS de l'ANSSI



http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html *(consulter étude de cas Archimed pour le TD)*

Partie 1
1.2 Politique de sécurité

1.2.2 Exemple 3 : la méthode MEHARI du CLUSIF



http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase préparatoire:

Prise en compte du contexte stratégique:

- positionnement: position sur le marché, criticité, concurrence, médiatisation des incidents

- contraintes: légales, réglementaires, normatives

- politique de sécurité: objectifs de sécurité, rôle de l'analyse, donneur d'ordre, décideur

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase préparatoire:

Prise en compte du contexte technique:

- architecture du SI: cartographie, architecture des réseaux et systèmes, architecture applicative

- plans & risques d'évolutions techniques: plan d'évolutions, pérennité des solutions opérationnelles

- fournisseurs externes: opérationnels (accès,réseaux), de logiciels, occasionnels (maintenance, assistance)

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase préparatoire:

Prise en compte du contexte organisationnel:

- organigramme complet: rattachements hiérarchiques, liens et rattachements fonctionnels, etc

- répartition des responsabilités sur la sécurité: notes sur les fonctions et répartition des responsabilités entre responsables de site, d'activités, le DSI et le RSSI

- Structures de pilotage: processus d'élaboration et validation de plans d'action, fonctionnement du pilotage

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase préparatoire:

Cadrage de la mission d'analyse:

- périmètre technique: géographique (sites, pays), SI (global?, exclusion processus industriels?, exclusion conception assistée?), types de supports (médias,etc)

- périmètre organisationnel: activités (filiales, services), types de risques concernés (divulgation, fraude, etc)

- structure de pilotage: structure et fonctionnement (membre, fréquence réunion), modes de validation

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase préparatoire:

Fixation des paramètres techniques:

- grille d'acceptabilité des risques: détermine si un scénario de risque est acceptable ou non

- grille des expositions naturelles: formaliser la grille pour décrire les scénarios des risques connus

- grille d'impacts résiduels: formaliser la grille permettant d'apprécier les impacts résiduels et les facteurs de réduction de risques des scénarios connus

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase opérationnelle d'analyse des risques:

Analyse des enjeux et classification des actifs:

- échelle de valeur des dysfonctionnements: formaliser les enjeux de l'activité qui aideront à classifier les actifs

- classification des actifs: déterminer la sensibilité de chaque classe d'actifs sous forme d'une classification

- tableau d'impact intrinsèque: utile pour apprécier les risques connus, à remplir par les automatismes MEHARI

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase opérationnelle d'analyse des risques:

Diagnostic de la qualité de services de sécurité:

- établissement du schéma d'audit: identifier les variantes des services nécessitant un diagnostic différencié

- diagnostic de la QoS des services de sécurité : faire un état de la qualité de chaque variante de service sécurité qui servira à évaluer les facteurs de réduction de risques

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase opérationnelle d'analyse des risques:

Analyse des risques:

- sélection des risques: sélectionner parmi les scénarios connus pour analyser ceux qui sont critiques

- estimation des risques: dresser un bilan de la gravité des scénarios de risques sélectionnés, en fonction des facteurs de réduction de risque découlant de l'état de services de sécurité

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase de planification et de traitement des risques:

Planification des actions immédiates:

- sélection des risques à traiter en priorité absolue: en dehors du cycle de décision habituel (en urgence)

- choix des mesures à mise en œuvre immédiate : proposer des actions immédiates pour réduire les risques considérés comme intolérables

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase de planification et de traitement des risques:

Planification des actions dans le cadre courant:

- stratégie de traitement et priorités: choisir parmi les stratégies de traitement possible et définir des critères pour fixer des priorités

- choix des mesures et planification: proposer des plans d'action pour réduire ou éviter les risques considérés comme inadmissibles

Partie 1
1.2 Politique de sécurité

1.2.3 Démarche de la méthode MEHARI

Phase de planification et de traitement des risques:

Placement du pilotage du traitement des risques:

- organisation du pilotage: mettre en place l'organisation de suivi et de pilotage du traitement des risques (membres, fréquence réunion, missions)

- choix des indicateurs et du tableau de bord: proposer au comité de pilotage des indicateurs pour vérifier le déploiement des mesures, l'évolution des niveaux de risques et décider des actions correctrices