BTS Informatique de gestion
2e année

Anne-Marie Cazaurang – Frédérique Parisot

Gestion des entreprises et organisation des systèmes d'information

Cours

Directrice de publication : Valérie Brard-Trigo

Conseils généraux

Pourquoi GEOSI ?

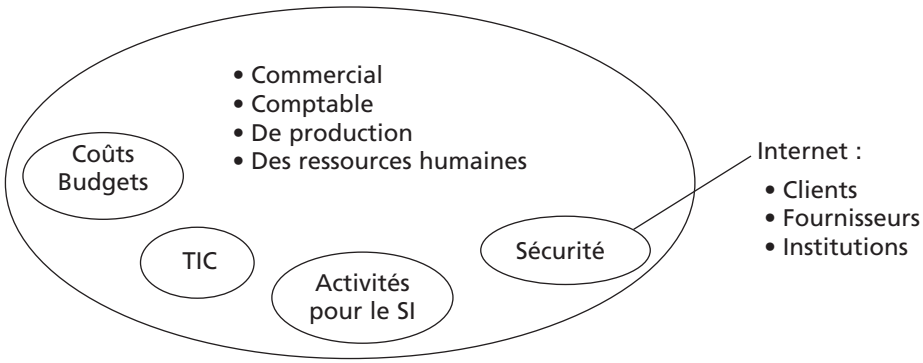
GEOSI : gestion des entreprises et organisation des systèmes d'information.
De par le nom de cette matière on pourrait s'attendre à un cours de gestion et un autre sur l'organisation des systèmes d'information (SI).
Or, dans l'optique du BTS Informatique de gestion, destiné à former des informaticiens de gestion, l'enseignement de GEOSI revêt plusieurs objectifs.

- Appréhender, concevoir et adapter le SI afin qu'il puisse servir au mieux pour la gestion quotidienne et future de l'entreprise.
- S'assurer que le SI répond aux besoins de l'entreprise sans être surdimensionné ou sous-dimensionné.
- Suggérer aux décideurs de l'entreprise de nouveaux indicateurs de gestion en fonction des informations internes ou externes, disponibles ou potentielles du SI.
- En tant qu'informaticien, proposer des évolutions du SI de l'entreprise en accord avec l'état des technologies et de l'environnement (veille technique et informationnelle).
- Participer à l'évolution de l'organisation de l'entreprise en étant le gérant de la complémentarité et de la compatibilité entre organisation et SI.
- Avoir des connaissances de base en gestion (et en économie d'entreprise) afin d'être un interlocuteur efficace vis-à-vis de vos futurs « clients »…

Ce n'est donc pas un cours qui prétend être une initiation à la gestion des entreprises, mais simplement un outil pour vous aider à comprendre les buts et éléments essentiels du SI vus sous l'angle d'une gestion efficace de l'entreprise.
La réalité économique, élément principal de l'environnement de l'entreprise, et l'évolution technique permanente, font que nous ne prétendons pas ici retracer les dernières évolutions possibles d'un SI.
De plus, il **n'y a pas un SI mais des SI**, avec des réalités bien différentes. Il vous appartiendra donc, dans votre vie professionnelle, vos stages, vos actions professionnelles ou même lors des exercices proposés, d'analyser chaque situation au plus juste. Au cours de toutes ces activités, vous délimiterez le pourtour du SI considéré par votre mission et ses interactions internes ou externes en fonction des moyens et objectifs de l'entreprise ou du domaine étudié.

Le cœur de ce cours est donc le SI
Vous l'avez défini dans le cours de 1re année et nous allons, cette année, détailler certains de ses aspects.

SI de l'entreprise



Ce cours abordera donc les divers points suivants :

Unité 1 : informations et SI de l'entreprise
Unité 2 : coûts et budgets
Unité 3 : gestion des systèmes d'information
Unité 4 : les TIC (Technologies de l'Information et de la Communication) au service du système d'information
Unité 5 : sécurité du SI

Ces grandes subdivisions feront l'objet des cinq parties que constituent ce fascicule.

Supports de formation

Pour cette matière, vous avez trois fascicules :

- un fascicule « cours » référencé 8 3936 TG PA 00 qui comporte le cours proprement dit et les exercices d'autoévaluation ;
- un fascicule « autocorrection » référencé 8 3936 TC PA 00 qui comporte les corrigés des exercices du fascicule « cours » ;
- un fascicule « devoirs » référencé 8 3936 DG PA 00 qui comporte deux devoirs d'évaluation à traiter et à envoyer à la correction. Reportez-vous à ce fascicule pour savoir à quel moment il faut traiter les devoirs.

GEOSI à l'examen

Nous aurions tendance à dire : « *il y a du GEOSI partout* ! ».
En effet, toutes les matières non générales du BTS peuvent faire appel à des questions de GEOSI.

- À l'étude de cas tout d'abord, où les interrogations de GEOSI sont disséminées sous forme de petites questions dans les divers dossiers, ou le plus souvent, font l'objet d'un dossier spécial, qui est en général le dernier dossier proposé. N'oubliez donc pas « d'aller chercher » ce dossier et d'en faire au moins les premières questions, pour « aller à la pêche aux points » (notation globale de l'étude de cas tout dossier confondu) au lieu de vous entêter sur un point technique des dossiers précédents sur lequel vous butez et qui risque de vous « manger tout votre temps ».
- Lors de la soutenance de votre projet (et bien entendu la rédaction de la note de synthèse) où des questions générales vous seront toujours posées pour vérifier que vous avez analysé le SI étudié et que vous avez pris le recul nécessaire par rapport à l'état actuel et à ses objectifs, ses moyens et ses performances futures.
- Lors des « pratiques des techniques informatiques » pour la même raison que ci-dessus ou parce que votre dossier traite d'un point particulier de GEOSI (sécurité, mise en place d'un outil de TIC…)

Sommaire

Unité 1

Informations et système d'information de l'entreprise

▶ *Contenu*

Séquence 1

Système d'information, compléments

Lors de la 1re année de préparation au BTS, vous avez vu ce qu'est un système d'information (SI) en GEOSI. De plus, n'oubliez pas que vos matières sont liées les unes aux autres, et donc l'analyse du SI que vous avez abordée en économie d'entreprise prend toute sa place ici.

Nous allons donc, dans cette séquence, revenir uniquement sur la différence entre SI et système informatique, avant d'aborder les points suivants : quels sont les liens entre le SI et l'organisation d'une entreprise et comment qualifier une « bonne » information ?

1. Système d'information / Système informatique

Le système d'information regroupe l'ensemble des moyens organisationnels, humains et technologiques qui permettent à une organisation d'acquérir, de créer, de stocker, de traiter, de mettre à jour et de communiquer les informations nécessaires à son activité.

Ceci ne se limite pas aux frontières de l'organisation, le système s'étend aux partenaires, et même au monde entier (informations diffusées sur Internet). Cette ouverture du SI de l'organisation vers l'extérieur doit être maîtrisée pour des raisons de sécurité et de confidentialité.

Pour que le SI soit un avantage concurrentiel pour l'organisation, il faut qu'il soit construit, organisé et géré avec une finalité commune. C'est donc un ensemble **finalisé** (avec un but) et **organisé**, qui, outre les moyens informatiques, a ses propres méthodes, règles et procédures.

Ses trois fonctions principales sont la production d'informations pour le système opérationnel (aide à la gestion quotidienne), le système d'aide à la décision et la circulation des informations.

Le système informatique quant à lui, ne représente que la partie technologique du SI, soit l'ensemble des moyens de traitement de l'information. On y retrouve donc principalement les matériels, logiciels et tout type de dispositif de communication numérique.

2. Système d'information et Organisation

Le mot « organisation » dans ce titre est vu sous deux angles :

- l'Organisation en tant qu'institution (une entreprise, une association…) ;
- l'organisation interne (structure organisationnelle), étendue aux partenaires : structure, unités de management, coordination entre les différentes unités…

⚠ **J'insiste ici sur la différence entre Organisation et organisation *(une majuscule, quelle différence !)* mais sachez que les divers documents ou sujets d'examen qui vous seront présentés ne feront pas toujours cette différence graphique. À vous d'analyser le contexte et de ne pas faire de contresens.**

2A. *Structure organisationnelle et SI*

La structure organisationnelle est l'ensemble des procédures et des moyens qui permettent à une organisation de coordonner ses activités et ses diverses unités ainsi que de gérer ses ressources humaines. Elle doit tenir compte et viser les objectifs généraux d'une entreprise.

La question principale qui se pose au niveau de la relation SI – organisation est : le SI doit-il s'adapter à la structure organisationnelle tout en favorisant son évolution, ou, au contraire, le SI doit-il pousser à l'évolution de la structure organisationnelle en lui exhibant ses nouveaux outils technologiques et en l'incitant à les mettre en œuvre pour pouvoir bénéficier des avantages concurrentiels qu'elle pourrait lui produire ? La réponse est (*les 2 !!!!)* difficile à trancher car l'organisation ne peut se plier à la technique, elle doit pouvoir rester créative sans se limiter aux restrictions technologiques, mais la technologie évoluant, l'organisation ne peut rester sans réagir sous peine d'être dépassée par la concurrence.

Voici deux exemples caricaturaux de cette ambivalence. Le système informatique (rappel *: qui fait partie du SI*) doit résoudre les problèmes techniques liés à la mise en place d'une certaine structure organisationnelle. Soit, dit autrement, l'informaticien doit chercher des solutions techniques, pour mettre en place une évolution de la structure voulue par les manageurs. D'un autre côté, la mise en place de TIC telles que celles favorisant le travail collaboratif, la messagerie électronique… impliquent obligatoirement une adaptation de l'organisation à ces nouveaux modes de communication.

2B. *Vers un pilotage des SI*

Le double problème que nous venons d'évoquer a conduit les entreprises à modifier leurs visions de l'apport du système d'information. On a évolué, dans la plupart des grandes entreprises d'un management de l'informatique à un management des systèmes d'information, en passant la plus souvent par la case « management de l'organisation et des systèmes informatiques ».

Que des mots, que des mots… simplement un changement de terme ou de titre (de « directeur informatique » à « directeur du SI ») … peut-être pour un collaborateur qui ne voit qu'une part du SI, mais au niveau du pilotage de l'entreprise, cette distinction tend à créer des effets positifs de synergie entre SI et organisation.

3. La fiabilité de l'information dans une organisation

L'information est devenue un élément clé pour le management d'une organisation, mais comment gérer l'immensité des informations que crée ou manipule une organisation ?

De plus, la réactivité d'une entreprise, ou d'une organisation en général, aux événements qui se passent dans son environnement économique et social est aussi un point clé de réussite. Il nous faut donc rajouter la variable « temps » dans la prise en compte de la fiabilité des informations.

Nous allons nous limiter à énumérer quelques principes simples de « qualité » de l'information.

- La fiabilité est le critère principal, il faut donc vérifier ses sources et analyser les prises de positions que peuvent contenir une information, ainsi que considérer les traitements précédents qui ont menés à cette information… De même, elle doit être précise ou annoncer clairement ses critères d'imprécisions.
- Le critère temps nous impose un deuxième élément fondamental : l'actualisation, ou mise à jour, d'une information. Cependant il faudra juger de la pertinence du délai de mise à jour. Prenons un exemple simple : les cours boursiers. Ces derniers doivent être connus en temps réel par les courtiers en Bourse qui fondent leur activité sur leurs réactions immédiates aux fluctuations des cours ; en revanche, cette information ne sera publiée qu'une fois par trimestre (ou par mois) aux petits porteurs qui ne sont pas sans cesse le nez sur leurs portefeuilles de titres.
- L'information doit être pertinente, c'est-à-dire répondre au besoin d'un utilisateur et être destinée uniquement aux utilisateurs intéressés (ne dit on pas « *trop d'informations tue l'information* » ?). De même, elle doit s'adapter à l'utilisateur. On ne va pas, par exemple, détailler les mêmes choses concernant une moto si on s'adresse à un acheteur, un réparateur ou un vendeur.
- La confidentialité d'une information et son accès relèvent de la sécurité du SI.

Rappel : la sécurité n'est que matérielle.

Séquence 2

Les divers systèmes d'information

Le système d'information (SI) de l'organisation est unique et global. Avec la notion d'entreprise étendue, il s'étend également vers les systèmes d'information des entreprises partenaires. Mais pour les besoins d'analyse et, en entreprise pour mieux cerner les domaines étudiés, on peut cependant regarder le SI sous un angle particulier ou pour un domaine fonctionnel spécifique. C'est ce que nous allons faire ici par l'analyse successive des divers SI d'une même organisation.

Dans tous les cas vous ne devez pas oublier que les ponts entre ces divers SI ne permettent pas leur cloisonnement. Chaque fonction va s'interfacer avec les autres.

Les progiciels de gestion intégrée, que nous verrons lors de la séquence 11, tentent de proposer des outils pour l'ensemble de ces SI. Ils les différencient cependant par modules (gestion commerciale, de production…).

1. Le SI commercial

Le SI commercial ne se limite pas à la gestion des clients. Il intègre celle des approvisionnements, et des stocks, il est donc lié au SI de gestion de production. De même au niveau de la facturation, ses liens avec la gestion comptable ne peuvent être ignorés.

Au niveau de la relation avec les partenaires, on peut distinguer plusieurs domaines sensibles pour le SI commercial.

- La gestion post-vente avec notamment les centres d'appels (call desk ou hot line) dont l'automatisation et les besoins en informations (qualité et quantité) sont de plus en plus importants et s'intègrent dans les points stratégiques de l'entreprise.
- La gestion des commerciaux, surtout ceux qui ne sont pas résidents dans l'entreprise, bénéficie des accès distants, pour lesquels la sécurité doit être maximale. L'informatique nomade (exemple : informations par téléphone portable) est intégrée au SI commercial de l'entreprise ainsi qu'à celle des partenariats (exemple : information en temps réel des partenaires technico-commerciaux).
- La veille concurrentielle est un facteur clé de succès pour l'entreprise. Elle ne se limite pas aux recherches Internet, même si ces dernières sont d'un apport précieux. Nous analyserons les systèmes de forage de données (data minima) qui permettent des analyses multidimensionnelles et prospectives de l'environnement de l'entreprise.
- L'individualisation de la relation avec certains clients (ou profilage) est un atout de certaines grandes entreprises. Tout client n'a pas besoin d'être « profilé » de la même façon, on va détailler plus ou moins son profil en fonction de son statut. Vous rencontrez facilement ce type de situation de profilage lorsque vous surfez sur Internet en tant que client, ou simplement prospect. Par exemple, les magasins virtuels de musique, livres, films… vous identifient lors de la connexion et vous proposent sur la page d'accueil des produits auxquels vous êtes personnellement sensibles en fonction de vos actions antérieures sur le site.

- La mise à jour constante des données et la réactivité : prix de ventes, nouveaux articles, nouvelles promotions, campagnes de communication proactive ou réactive… sont aujourd'hui un élément indispensable dans les relations concurrentielles.

Les logiciels de GRC (gestion de la relation client ou CRM customer relationship management) sont aujourd'hui très répandus. Ils tentent de prendre la place des PGI, avec une spécialisation sur l'ensemble des activités commerciales.

2. Le SI comptable et financier

Ce SI recouvre les domaines suivants de l'organisation : comptabilité, finances, contrôle de gestion, budgets, trésorerie.

Vous avez largement étudié ce SI dans le cours de 1re année, nous n'y reviendrons donc pas.

L'analyse des SI suivants est explicitement au programme des étudiants qui font l'option DA, mais il est conseillé de les lire, à titre de culture générale, pour le BTS par ceux de l'option ARLE.

3. Le SI de la gestion de production et de la logistique

Le rôle de la gestion de production est d'organiser l'ensemble des activités de production afin de répondre dans les meilleures conditions aux commandes des clients.

Les impératifs sont donc de :

- satisfaire les clients dans les délais et au niveau de qualité fixés ;
- ne pas avoir trop de stocks tout en s'assurant que les matières ou articles stockés soient disponibles au moment voulu ;
- disposer de moyens matériels et humains adéquats au moment où l'on veut produire.

Et tout cela, au moindre coût.
Pour cela la gestion de production s'oriente vers des objectifs différents selon l'échéance envisagée.

- À long terme, elle cherche à établir un plan de production et à définir les ressources nécessaires (moyens matériels et humains) à la réalisation de ce plan de production.
- À moyen terme, elle vise à optimiser les approvisionnements, à gérer les stocks et à calculer les charges découlant du programme de production pour les ajuster aux capacités de l'entreprise mesurées par ses effectifs, ses horaires, ses moyens de production et à déterminer éventuellement s'il faut faire appel à la sous-traitance.
- À court terme, elle se charge d'ordonnancer (planifier) les opérations sur les machines, de suivre l'état d'avancement de la fabrication, et de fournir des éléments au contrôle de gestion *(cf. Séquence 8, planification).*

En gestion de production, il est important que le SI permette :

- de décrire le processus complet de fabrication de chaque produit fini en distinguant les diverses pièces (composants) qui composent ce produit, leur mode de production ou d'approvisionnement et la façon dont ils vont ensuite être assemblés. Cette décomposition peut se faire à plusieurs niveaux. La nomenclature est le document qui va répertorier cette décomposition avec le détail des tâches à réaliser à chaque étape (ou pour chaque sous-produit) et les moyens matériels et humains nécessaires. *Cf. Exercice* ;

- d'évaluer les besoins dans le temps tout en gérant au mieux les stocks ;
- de planifier les diverses tâches à réaliser. Lors de la séquence 8, vous aborderez quelques techniques d'ordonnancement afin d'aboutir à des plannings concrets et réalistes ;
- de prévoir et d'adapter en fonction des besoins la logistique afférente à ces diverses tâches de production.

Ces dernières années, au niveau de la logistique, l'évolution du commerce électronique a fait considérablement avancer les méthodes ou les outils. De plus, c'est un domaine où la coopération entre partenaires (fournisseurs, entreposeurs, emballeurs, livreurs…) est forte, ce qui a obligé les entreprises à développer leur Extranet en maîtrisant cette ouverture de leur SI sur l'extérieur, y compris vers l'international aux régulations différentes des nôtres.

L'offre logicielle (progiciels) permettant de gérer la logistique est donc fort importante et diversifiée (large gamme de fonctionnalités disponibles, spécialisation par grands domaines d'activités, traçabilité…).

4. Le SI de la gestion des ressources humaines

Longtemps la gestion des ressources humaines (GRH) a été assimilée à la gestion (administrative) du personnel : élaboration des bulletins de salaires et des documents comptables et fiscaux afférents, tenues des registres du personnel…

Or la GRH recouvre aujourd'hui tous les points relatifs au salarié dans l'entreprise. On peut nommer par exemple :

- le recrutement : définition et description des postes actuels et prospectifs, animation et gestion de toute la procédure de recrutement ;
- la politique salariale : salaires, incitations financières diverses, épargne salariale, avantages divers… ;
- la formation et le suivi de carrière ;
- la communication interne ;
- la santé et le respect des conditions d'hygiène et de sécurité…

De plus, les cadres de la GRH interviennent dans de nombreux projets relatifs aux SI non liés directement à la GRH : confidentialité des données, installation d'un collecticiel, d'une base de connaissances, accès à Internet… *Vous analyserez ces outils lors des séquences 11 et 12.*
La paie avec ses nombreuses législations complexes et changeantes est la partie du SI qui est la plus souvent externalisée (surtout dans les petites et moyennes entreprises). En revanche, les autres domaines touchant à la GRH sont en général gérés en interne, vu qu'il s'agit d'un sujet « sensible » pour l'entreprise.
De nombreux progiciels de GRH existent sur le marché, lors d'une acquisition, outre leurs diverses fonctionnalités, les possibilités de paramétrage sont à étudier en détail afin de ne pas enfermer l'entreprise dans un mode de gestion qui ne lui conviendrait pas.
Nous avons parcouru l'analyse des principaux sous-SI de l'organisation, cependant n'oubliez pas que ce découpage du SI global de l'organisation en sous-systèmes n'est qu'un moyen pour appréhender les diverses facettes du SI et pour mieux le gérer. Les interactions entre ces divers sous-systèmes d'information sont constantes et le SI global de l'organisation ne fait qu'un.

Exercice 1

Exercice de calcul de besoins en gestion de la production

Une fabrique de montures de lunettes fabrique, entre autres, deux types de montures que nous appellerons M1 et M2. La monture M1 est composée de deux éléments : la partie faciale avec son système incorporé de fixation aux branches, que nous appellerons l'élément F1 et une paire de branches, que nous appellerons B1.
La monture M2 est composée d'une partie faciale F2 et de la même paire de branches que pour le modèle précédent, soit B1.

- Voici le nombre de commandes de montures à livrer pour les semaines à venir :

Semaine	1	2	3	4	5
M1	500	480	530	450	420
M2	220	240	260	250	240

- Voici le stock réel au début de la semaine 1 et le stock de sécurité (stock minimal désiré à tout moment) de chaque élément ainsi que le temps de montage de chaque élément.

Éléments	M1	M2	F1	F2	B1
Stock début semaine 1	160	70	160	70	200
Stock de sécurité	140	50	150	60	200
Temps montage unitaire	0,07 *	0,06	0,03	0,03	0,01

** 0,07 : pour monter une monture M1, il est nécessaire de passer 0,07 heure.*

1. **Décrire, sous forme d'arbre (de hiérarchie) la partie de la nomenclature des deux montures qui détaille simplement les produits finis et les éléments qui les composent.**
2. **Déterminer les besoins des divers éléments et le nombre d'heures de travail pour les semaines à venir.**

Il est conseillé de faire cette question à l'aide d'un tableur. Vous pourrez, pour cela réaliser un tableau de ce type :

Besoins nets	1	2	3	4	5
Montures M1					
Montures M2					
F1					
F2					
B1					
Temps de production					

On considère maintenant que le temps de production disponible pour le montage de M1 et de M2 n'est que de 75 heures par semaine, en tenant compte du temps de disponibilité des machines, de la préparation des diverses tâches et de la disponibilité de la main-d'œuvre.

3. **Quel est le problème qui se pose pour la production des montures M1 et M2 lors des cinq prochaines semaines ?**
4. **Donner des pistes générales pour remédier à ce problème (calculs inutiles).**

Séquence 3

Outils d'aide à la décision

Le vocable « outil d'aide à la décision » couvre un large champ, du simple petit tableau tenu à la main et qui a une durée de vie très courte, à d'importants sous-systèmes d'information qui font appel à des outils de génie logiciel complexes.

Mais ils ont tous un point commun, ils servent au décideur pour l'éclairer dans sa connaissance du domaine étudié et, lorsqu'il s'agit de prendre une décision, l'aider à évaluer les divers scénarios qui se présentent à lui ou qu'il crée.

Dans cette séquence nous nous limiterons aux tableaux de bord de gestion, même si leurs homologues scientifiques et techniques présentent les mêmes caractéristiques. Nous allons tout d'abord présenter les tableaux de bord avant d'analyser la place des outils d'aide à la décision dans le système d'information.

1. Les tableaux de bord

Un tableau de bord est un outil d'aide à la décision qui présente au décideur des éléments pour l'aider dans ses choix. Les éléments présentés concernent à la fois l'état de certains indicateurs importants pour la gestion de l'entreprise, et la comparaison de leur niveau avec un niveau prévu d'avancement en fonction des objectifs fixés.

Replaçons tout d'abord les tableaux de bord dans leur contexte avant de détailler leur mise en œuvre et leur utilisation.

1A. Management et décision

L'une des bases du management est de mettre en place des objectifs pour l'organisation, puis de déterminer les moyens et actions nécessaires pour les atteindre. On va ensuite prévoir leur mise en œuvre, puis tout au long de la phase de réalisation on va comparer les résultats obtenus à ceux escomptés. En fonction des écarts, et surtout de leur ampleur, qui se présenteront entre ces deux niveaux, le décideur pourra agir par des actions correctrices.

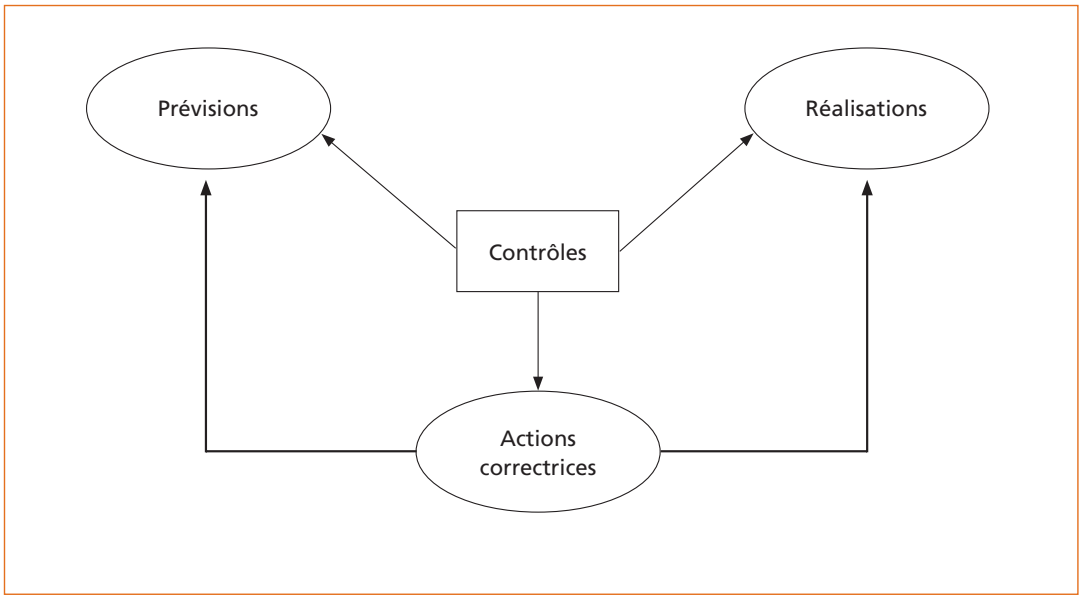
1B. Tableau de bord stratégique/opérationnel

Les tableaux de bord stratégiques concernent le pilotage à long terme de l'organisation. On y trouve des éléments mesurant la performance à long terme : les avantages concurrentiels, des outils qui aident à traduire la stratégie globale en objectifs concrets, des données sur le capital humain, les éléments immatériels, l'évolution des marchés… Beaucoup de ces éléments viennent de la cellule de veille informationnelle de l'organisation qui utilise pour cela des outils sophistiqués de recherche, agrégation et traitement approprié de l'information.

Les tableaux de bord opérationnels (ou « de gestion » ou « de pilotage opérationnel ») sont centrés sur des éléments plus ciblés de l'entreprise : un service, un projet, … Ils vont

directement avertir chaque responsable de la situation réelle par rapport à la situation prévue. Ces indicateurs vont présenter les écarts entre prévisions et réalisations et mettre en place des « systèmes d'alerte » en fonction de l'importance de ces écarts. Ces indicateurs sont souvent le fruit de l'agrégation de multiples données (recueil, sommation, regroupement...).

C'est essentiellement sur ce type de tableaux de bord que porte cette partie du cours.



1C. Mise en place du tableau de bord

À partir d'un objectif général fixé on va réfléchir sur les actions et moyens à mettre en œuvre. Pour chaque action on déterminera des critères de réussite, et pour chacun d'eux on se fixera des indicateurs qui permettent de le « mesurer ». On aura donc un ensemble de mesures qui contribueront à approcher l'avancement de ces objectifs, chacune d'elles pouvant être approchée par un ou plusieurs indicateurs. Tout ceci va conduire à la définition de prévisions.

On va ensuite réaliser l'action déterminée.

À chaque étape ou sous-étape on comparera (contrôle) alors les prévisions aux réalisations. S'il y a des écarts ente les deux on en cherchera les causes. Si besoin est, on apportera des actions correctrices au cours de la réalisation.

1D. Étapes dans la construction d'un tableau de bord

Tout tableau de bord présente un ensemble d'indicateurs.

Un indicateur peut se rapporter à un projet, une entité (service…) de l'organisation, un élément transversal… On ne peut donc vous présenter une « recette miracle » qui puisse satisfaire toutes les situations. On peut cependant dégager quelques critères.

La procédure générale vers la mise en place de tableaux de bord est la suivante :

- découpage d'un objectif principal en missions ;
- pour chaque mission déterminer le(les) facteur(s) à surveiller (élément de gestion, partie d'un projet…) qui doivent influer directement sur l'objectif de management visé ;
- définir les divers indicateurs qui serviront à apprécier ce facteur (indicateurs de résultat, de moyen ou de processus) et préciser pour chaque indicateur son niveau attendu ainsi que ses fourchettes d'acceptabilité (valeurs minimale et maximale « acceptables », valeurs minimale et maximale « critiques »…) ;
- identifier les destinataires de chaque indicateur.

1E. Exemples d'indicateurs

Production : nombre de produits fabriqués, nombre de produits semi-finis mis à disposition d'une autre entité de l'organisation…

Commercialisation : nombre de produits vendus, taux d'augmentation de l'image de marque, nombre de points de ventes, rentabilité d'un point de vente ramené à sa surface (par m^2), nombre de nouvelles cartes de fidélité…

Service client : taux de satisfaction client, nombre de cas traités, rapport des cas résolus sur les cas soumis…

Service financier : rentabilité des actifs placés, taux de rotation des actifs, évolution de la valeur ajoutée, valeurs empruntées/autofinancement…

GRH : nombre d'arrêts de travail, satisfaction générale des employés, nombre de propositions d'innovation, taux de participation aux activités péri professionnelles, taux de rotation, participation aux élections…

1F. Présentation du tableau de bord

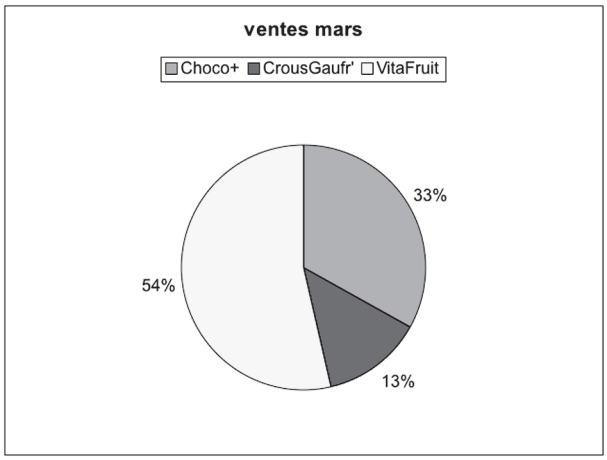
La lisibilité en suivant un axe allant du général au particulier doit guider la construction d'un tableau de bord.

Les présentations sous formes de graphiques, de tableaux à double entrée, de plannings, de liens hypertexte pour les détails ou les liens entre tableaux de bord sont à préférer pour leur lisibilité. Cependant des commentaires concis et précis ne peuvent qu'éclairer le lecteur.

Le concepteur du tableau de bord ne doit en aucun cas réaliser l'interprétation à la place du décideur. Il doit simplement le guider par une présentation adaptée au lecteur mais surtout à la situation traitée et son « degré de gravité ».

1G. Exemple

Le directeur commercial d'une petite entreprise de biscuits désire connaître, à la fin de chaque mois, la répartition mensuelle des ventes réalisées par type de biscuits. Un simple graphique de ce type permet de le renseigner. Cependant on peut lui proposer des graphiques comparatifs dans le temps s'il désire connaître l'évolution de cette répartition.



Le directeur commercial, destinataire de ce tableau de bord, voulait, en outre, en priorité, être averti trimestriellement des ventes qui n'obtiendraient pas 70 % des prévisions et de celles qui excéderaient d'au moins 30 % les prévisions.

Ventes	Choco+			CrousGaufr'			VitaFruit		
	P	R	% R/P	P	R	% R/P	P	R	% R/P
Janvier	32	35	109,38	22	20	90,91	45	45	100,00
Février	30	30	100,00	21	19	90,48	44	71	161,36
Mars	33	32	96,97	22	13	59,09	46	52	113,04
Trimestre	95	97	102,11	65	52	80,00	135	168	124,44

P = prévision, R = réalisation, % R/P= pourcentage de réalisation par rapport aux prévisions.

Ce tableau répond à ses attentes. En effet, il voit avant tout la faiblesse des ventes de CrousGaufr' en mars (environ 60 % des prévisions) et les ventes exceptionnelles de VitaFruit en février (161% des prévisions).

Mais ce tableau ne montre pas que ces deux chiffres importants.

La ligne **trimestre** nous permet de connaître les résultats, et leur performance par rapport aux objectifs fixés pour les trois mois. On peut, par exemple, en déduire que les Choco+ se vendent comme cela été prévu (total des réalisations par rapport aux prévisions proche de 100%) ; que les CrousGaufr' sont en baisse de 20% par rapport aux ventes espérées sans jamais les atteindre, alors que les VitaFruit se vendent mieux que prévu (ceci étant dû au chiffre exceptionnel de février).

Mais le directeur commercial ne peut se contenter de ces conclusions pour prendre ses décisions, il doit tenir compte d'autres éléments :

- possibilités de prévisions trop ambitieuses ou pessimistes ;
- campagnes de promotion non prises en compte ;
- problèmes provenant d'une attaque de la concurrence ;
- problème sanitaire ou de réglementation…

Comme nous l'avons montré dans cette première partie, un tableau de bord est avant tout un outil d'aide à la décision. Il informe le décideur sur la situation, l'aide à réaliser ses prévisions et surtout l'avertit lorsque certains indicateurs « passent au rouge », tout ceci afin de l'aider dans ses prises de décisions. En aucun cas (sauf rares cas d'automatisation

décidés par le responsable) le tableau de bord ne va pas prendre de décision à la place du responsable.

Outre ces tableaux de bord, le système d'information de l'entreprise est doté d'outils plus généraux d'aide à la décision que nous allons voir maintenant.

2. Place des outils d'aide à la décision dans le système d'information

Le sigle SIAD revêt diverses significations :

- système d'information d'aide à la décision ;
- système informatique d'aide à la décision ;
- système interactif d'aide à la décision.

La première proposition fait appel à la notion d'information et de système d'information. En effet, comme nous l'avons vu dans les tableaux de bord, les productions résultant d'un SIAD sont basées sur des données qui ont été agrégées, retraitées, triées… Ces données ne sont produites et n'ont de sens que dans un système d'information cohérent au service de l'organisation.

La deuxième proposition diffère de la précédente par le mot informatique, elle est donc axée vers la dimension « technique » et se réfère à tous les éléments matériels, organisationnels et humains qui permettent au système d'information (de décision) de fonctionner.

La dernière proposition est, quant à elle, plus axée vers les outils, outils logiciels principalement. Le vocable « interactif » replace le décideur face à la nécessaire rapidité d'analyse et d'action, élément stratégique de l'organisation d'aujourd'hui face à la réalité concurrentielle.

Concrètement, dans l'organisation actuelle, le SIAD englobe ces trois pôles.

Nous allons voir successivement quelles sont les informations qui vont alimenter le SIAD, puis nous présenterons l'intérêt des outils de simulation pour le décideur, avant d'ébaucher l'architecture générale d'outils de SIAD.

2A. Informations et SIAD

Comme nous l'avons vu toute information du système d'information ne va pas se retrouver dans le SIAD. En effet ces informations ont besoin d'être agrégées (recueillies, consolidées et éventuellement épurées) avant d'être présentes dans les données disponibles pour le décideur.

En revanche, des informations stratégiques et de pilotage vont venir compléter les données quotidiennes de l'organisation, ou tout au moins privilégier certains axes d'étude.

C'est pourquoi on parle de SIAD comme d'un sous-système d'information.

Ce sous système d'information va se nourrir sans cesse des informations opérationnelles « prélevées » sur le système d'information assurant la gestion quotidienne.

Pour assurer correctement et rapidement (n'oubliez pas le terme « interactif ») cette « remontée » des informations, des procédures organisationnelles spécifiques au SIAD vont être mises en place.

2B. SIAD et outils de simulation

Nous vous avons présenté les tableaux de bord comme des outils permettant de mettre en place des prévisions, de comparer ensuite ces dernières avec la réalité afin d'avertir le décideur de divergences importantes qui devraient l'amener à prendre des mesures correctrices.

Pour l'aider davantage dans cette dernière partie le SIAD va lui permettre de faire des prévisions.

Face à une décision à prendre, le décideur va pouvoir émettre des scénarii, scénarii qui peuvent être, en partie, proposés par le système de SIAD si ce dernier est correctement paramétré, conformément aux objectifs du décideur. La réalité va alors être modélisée en prenant en compte les mises à jour continuelles de la gestion quotidienne et de l'environnement. Le décideur, en fonction des scénarii entre lesquels il hésite, va pouvoir agir sur une ou quelques variables et évaluer les résultats probables de ses décisions.

2C. Outils du SIAD

Les outils, principalement logiciels, seront vus dans la séquence relative aux outils des technologies de l'information et de la communication.

On peut citer ici principalement les entrepôts de données (datawarehouse) et leurs outils

Exercice 1

Nous sommes dans un centre d'appel spécialisé dans l'assistance à l'utilisation d'imprimantes. Nos clients sont des sociétés et nos usagers (ceux qui nous appellent) sont des employés de ces sociétés. Ces derniers téléphonent pour tout problème d'installation, de paramétrage, d'utilisation en réseau ou de maintenance de plusieurs types d'imprimantes.

Le service commercial de notre entreprise envisage de modifier les contrats des clients en spécifiant que :

- tout problème de paramétrage ou d'installation sera traité en moins de dix minutes ;
- tout problème de maintenance devra être traité en moins de trois appels ;
- tout problème lié au réseau doit être traité en une journée maximum.

La direction commerciale de notre entreprise désire mettre en place un tableau de bord afin de mesurer cette activité et analyser si ces nouveaux types de contrats pourraient être honorés par nos services.

1. **Quel est l'objectif de la mise en place de ce tableau de bord ?**
2. **À quel type d'entité (service, projet…) s'intéresse t-il ?**
3. **Définir des critères de réussite.**
4. **Pour chaque critère retenu définir des indicateurs permettant de mesurer sa réalisation. Pour chaque indicateur donner sa valeur « attendue », ainsi que les valeurs extrêmes (faibles et fortes) qui devront être signalées de toute urgence au décideur.**

Exercice 2

Pour chacune des affirmations suivantes concernant les tableaux de bord, dire si elle est vraie ou fausse en argumentant votre réponse.

1. **Tout indicateur doit être mesurable en numéraire (euros, dollars…) ou en quantité (lot, unité…).**
2. **Le tableau de bord de l'entreprise est unique.**
3. **Grâce au tableau de bord le décideur peut mettre en place des actions correctrices.**
4. **C'est le décideur qui définit les niveaux d'acceptabilité de chaque indicateur du tableau de bord.**
5. **Toutes les variables qui jouent sur le résultat espéré doivent figurer sur un tableau de bord.**
6. **Si un niveau de « réalisation » est inférieur au niveau de « prévision » alors il faut immédiatement mettre en place une action corrective.**

Unité 2

Coûts et budgets

▶ *Contenu*

Séquence 4

Les coûts complets

1. Présentation de la comptabilité de gestion

1A. Comptabilité générale/comptabilité analytique

Comme vous l'avez vu l'an dernier, la comptabilité générale a deux buts :

- l'un interne : connaître à tout moment la situation financière de l'entreprise et pouvoir prendre des décisions de gestion pour améliorer la compétitivité de l'entreprise ou corriger les éventuels problèmes (aidé pour cela par l'analyse financière) ;
- l'autre externe : informer les banques, fournisseurs, État (administration fiscale...).

Pour atteindre ces buts, la comptabilité générale doit être normalisée et conçue de façon à représenter la situation patrimoniale de l'entreprise de manière standard c'est-à-dire d'une manière commune à toutes les organisations.

De son côté, la comptabilité de gestion va s'occuper de calculer des coûts, tels que le coût de revient d'un article ou d'un service produit par l'entreprise.

Le résultat du calcul du coût servira en tant que tel pour déterminer, par exemple, le prix de vente d'un article.

Le calcul des coûts va également permettre d'analyser la **structure de ces coûts**. On peut, par exemple, connaître l'ensemble des frais d'un service de l'entreprise et pouvoir ainsi apporter des actions correctrices sur la gestion de ce service.

On peut aussi utiliser la connaissance de ce que nous coûte un approvisionnement externe pour décider soit de continuer d'acheter cet approvisionnement à l'extérieur de l'entreprise soit de le produire en interne.

Ce dernier exemple nous montre que la comptabilité de gestion est bien un outil au service du décideur car elle **l'informe sur des indicateurs de gestion de l'activité**. C'est ensuite au décideur de choisir une ligne de conduite à suivre, indépendamment des résultats de la comptabilité de gestion.

Par exemple, dans le cas d'un approvisionnement externe qui lui coûte trop cher, il peut décider de continuer à l'acheter à l'extérieur car il n'a pas, et ne désire pas avoir, les compétences nécessaires pour le produire, ou parce qu'il désire développer un partenariat avec son fournisseur.

1B. Principes généraux de la détermination des coûts

1B1. Coût / prix

On appelle un **coût**, la somme des charges relatives à un élément défini par l'entreprise elle-même (exemple : un article fabriqué).
Ne pas le confondre avec un prix qui correspond à ce que le consommateur paye pour acheter quelque chose.

1B2. Approche du calcul et de la structure des coûts par un exemple

Pour vous, le prix d'achat de votre micro-ordinateur est représenté par le montant que vous payez au magasin dans lequel vous l'achetez.

Mais pour déterminer son coût d'achat il faudrait rajouter à ce prix d'achat le montant des diverses revues informatiques que vous avez éventuellement achetées pour vous informer, le montant de l'essence que vous avez consommée pour vous rendre au magasin, le montant du ticket de parking…

Ces premiers éléments sont faciles à déterminer, ils sont directement imputables à l'achat de l'ordinateur et leur montant est aisé à trouver.

Supposons maintenant que le jour de cet achat vous ayez garé votre voiture au parking puis que vous ayez fait diverses courses ou promenades avant d'acheter votre ordinateur. Vous ne pouvez raisonnablement pas considérer que la totalité du temps de parking facturé concerne votre ordinateur. Va-t-on considérer que le montant du parking qui concerne l'achat de l'ordinateur doit être proportionnel au temps passé à cet achat (par rapport au temps total de parking) ou proportionnel aux montants des achats du jour ?

Cet exemple, simpliste, peut vous paraître un peu exagéré. En effet, qui voudrait, à titre personnel, déterminer au centime près le coût de son ordinateur ?

Mais pour une entreprise, ces coûts annexes vont être d'une toute autre importance.

Au simple prix du ticket de parking peut se substituer, par exemple, tous les frais engagés par un service de maintenance du matériel. Ce service a du matériel (telles que des machines de plusieurs milliers d'euros), du personnel, des frais d'administration… Il va falloir tout d'abord rechercher et évaluer toutes les charges afférentes à ce service. Puis lorsqu'on aura le montant global (annuel ou mensuel) de ce qu'il coûte à l'entreprise, nous considérerons qu'il « refacture » ses prestations aux divers autres services de l'entreprise. Pour effectuer cette « refacturation » il faudra alors déterminer un critère de répartition. On pourra, par exemple, décider que l'ensemble des charges du service maintenance d'une entreprise sera refacturé à chacun des autres services en fonction des heures passées à réparer ou maintenir les équipements du service « client », c'est-à-dire celui qui bénéficie des prestations de maintenance.

Tout ceci devrait nous mener, étape par étape, à calculer le coût global pour l'entreprise d'avoir un certain service (exemple : le service de maintenance). Ce coût global sera ensuite ventilé selon les prestations que ce service offre aux autres services. Ceci va augmenter l'ensemble des charges afférentes aux services d'approvisionnement, de production ou de commercialisation et nous permettre enfin d'obtenir le coût de revient d'un article vendu par l'entreprise en ayant tenu compte de toutes les charges de l'organisation.

1B3. Calcul des coûts et décisions de gestion

Comme nous venons de le voir, le fait de « refacturer » en fonction des heures passées n'est pas neutre sur le montant total des charges du service qui reçoit la prestation. On aurait aussi pu choisir de « refacturer » sur la base d'un autre critère tel que le niveau de complexité de la réparation. Si on avait choisi de « refacturer » en fonction du niveau de délai d'intervention (désir d'un service plus ou moins rapide) choisi par le service consommateur, les résultats ne seraient pas les mêmes. En revanche, l'incitation à la rapidité ou le niveau d'exigence du service qui reçoit la prestation n'aurait pas été identique.

- **Le choix des divers indicateurs de gestion à prendre en compte dans le calcul des coûts va donc influer directement sur le montant de ces coûts ainsi que sur l'activité et le management de l'entreprise.**

De même, ces coûts vont, en aval, servir à revoir certaines activités, certains prix de vente, à modifier l'organisation de l'entreprise pour être plus compétitifs, abandonner certains produits ou s'orienter vers d'autres…

- **Le calcul des coûts est donc un instrument d'information pour le décideur et a pour objectif de l'aider non seulement à suivre la gestion quotidienne mais également à prendre des décisions stratégiques pour l'entreprise.**

De même, le **calcul des coûts peut être prévisionnel** pour servir à évaluer tous les coûts afférents à une nouvelle activité ou un futur produit.

- **Nous voyons ici que le choix des indicateurs de gestion influe sur le calcul des coûts qui, à leur tour, influencent sur les décisions de gestion.**

1B4. Divers niveaux de coûts

On distingue généralement, et dans cet ordre :

- les coûts d'achat (ou d'acquisition, ou d'approvisionnement) ;
- les coûts de production ;
- les coûts de revient (= **coûts complets** comprenant toutes les charges courantes) y compris les coûts de commercialisation.

Les coûts se calculent dans cet ordre car dans le coût de production, par exemple, on intégrera le coût d'achat des matières qui seront utilisées lors de la phase de production.

Certaines entreprises, qui ne font que revendre des produits qu'elles achètent peuvent ne pas avoir de coût de production.

Vous trouverez, dans certains manuels, le fait que l'on puisse passer par une phase intermédiaire entre le calcul du coût de production et celui de revient en calculant un coût de commercialisation (ou distribution). Ici, nous intégrerons ces frais au calcul du coût de revient.

1C. De la totalité des charges aux charges incorporables aux coûts

Pour déterminer un coût, on doit répertorier toutes les charges imputables à ce coût. Le principe, pour recenser toutes ces charges, est le même que dans l'exemple de l'achat de votre micro-ordinateur, où nous avions récupéré le ticket du parking et les autres éléments des frais afférents à cet achat.

On va, pour cela, se servir des charges de la comptabilité générale en y apportant quelques modifications.

1C1. Les charges incorporables aux coûts

Charges non incorporables

Toutes les charges de la comptabilité générale (classe 6) n'entrent pas forcément dans le calcul des coûts. Certaines ont un caractère exceptionnel ou anormal, comme, par exemple, les frais relatifs à la reconstruction suite à un incendie.

Il est naturel de prendre en compte ces charges exceptionnelles dans la comptabilité générale de l'entreprise afin de respecter le principe comptable « d'image fidèle » et parce que ces frais ont grevé la santé financière de l'entreprise.

Mais ces charges, exceptionnelles, ne vont pas rentrer dans le calcul global des coûts afin de ne pas gonfler artificiellement le coût de revient unitaire d'un produit, ce qui pourrait influencer négativement les décisions de gestion futures.

Charges incorporables après vérification de la période
De même, la périodicité de calcul des coûts (le mois, le trimestre ou le semestre) est en général plus courte que la durée de l'exercice comptable, qui lui est généralement d'une année.

Certaines charges enregistrées globalement en comptabilité générale au moment de leur survenance, ne sont pas toutes « consommées » pour le même but et leur « utilisation » varie au cours du temps.

Dans le calcul des coûts, il ne faudra imputer que la partie réellement consommée pendant la période considérée et pour l'activité considérée.

Certaines charges annuelles, comme la dotation aux amortissements, ne sont calculées qu'une seule fois par exercice comptable (ici généralement en fin d'année civile, le 31 décembre). Or, pour le calcul des coûts, nous aurons besoin de connaître leur montant avant cette date, soit avant qu'elles n'entrent en comptabilité générale.

Exemple 1 : *si la dotation annuelle aux amortissements (calculée en fin d'exercice comptable) est de 3 000 €, on va répartir cette charge sur chaque mois (3 000/12 = 250 €/mois). En comptabilité de gestion on va intégrer cette somme mensuelle dès le calcul du 1er mois de l'année, alors qu'en comptabilité générale le montant total ne sera calculé et pris en compte qu'en fin d'année.*

Exemple 2 : *une entreprise paie au début de chaque trimestre un loyer de 600 €, cette somme est donc comprise dans les charges en comptabilité générale dès les premiers jours du trimestre. Si on calcule des coûts pour un mois en début de trimestre, on ne prendra en compte que 200 € alors que les 600 ont déjà été enregistrés en comptabilité générale.*

- **Ne pas oublier que toute charge est enregistrée dans sa totalité en comptabilité générale au moment où on dispose de la pièce comptable correspondante. Alors qu'en comptabilité de gestion, elle n'est prise en compte qu'à la période correspondant à sa consommation réelle.**

1C2. Les charges non enregistrées en comptabilité générale

La comptabilité de gestion prend en considération des charges qui ne figurent pas dans la comptabilité générale en classe 6 : les « charges supplétives ».

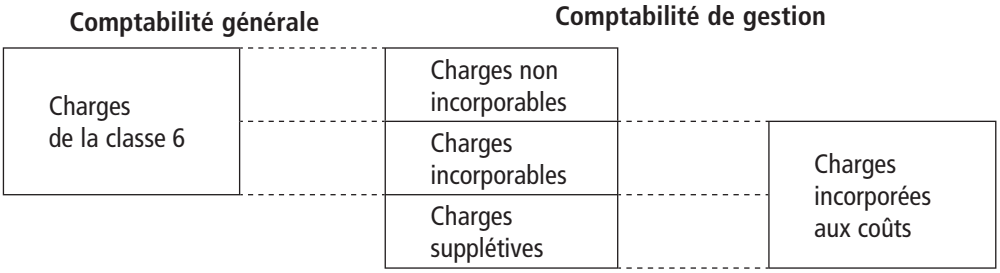
Ces charges permettent d'obtenir des coûts qui ne dépendent ni du statut juridique de l'entreprise ni du mode de financement.

Exemple 1 : *la rémunération du travail (salaire) du chef d'entreprise individuel n'est pas considérée comme une charge car ce dernier est rémunéré par ses prélèvements sur les bénéfices, et non par un salaire. Cependant, lors du calcul des coûts, l'incorporation de cette rémunération facilite la comparaison avec les coûts des entreprises dont les dirigeants ont un statut de salarié.*

Exemple 2 : *la rémunération théorique des capitaux propres (comme si on les avait placés pour qu'ils rapportent) permet d'obtenir des coûts comparables à ceux d'une entreprise financée par des emprunts.*

En général on ne trouve que ces deux seuls types de charges supplétives.

1C3. Quelles charges retenir ?



Application

Les charges recensées par l'entreprise « InfoCned » s'élèvent à 313 800 € pour l'année N (dont 1 230 € d'exceptionnelles). Le responsable considère que les charges exceptionnelles ne doivent pas être retenues pour le calcul des coûts, mais il estime devoir tenir compte d'une rémunération de 4% l'an du capital qui s'élève à 43 000 €.

Déterminer les charges incorporables
Ici, on considère (par défaut) qu'on calcule les coûts sur la même période que celle de constatation des charges, l'année N.

Total des charges	313 800
Charges non incorporables (charges exceptionnelles)	– 1 230
Charges supplétives (rémunération du capital à 4%)	+ 1 720
Charges à prendre en compte pour le calcul des coûts	314 290

1D. Charges directes et indirectes

Reprenons l'exemple de l'achat de votre micro-ordinateur. Si vous n'achetez que cela au magasin d'informatique ce jour là, le prix figurant sur la facture sera **directement** imputable au coût de revient de votre ordinateur.

En revanche, nous avons vu que si vous avez fait diverses courses ou que vous vous êtes promenés avant d'acheter votre ordinateur, la totalité du temps de parking facturé ne pourra concerner votre ordinateur. Le prix du parking ne peut directement être incorporé au coût d'achat du micro-ordinateur. Il va falloir déterminer à quelles activités l'imputer (achat de l'ordinateur, ballade, courses diverses…) puis réaffecter à l'achat de l'ordinateur la partie le concernant. Le parking est donc ici une **charge indirecte.**

1D1. Les charges directes

Elles sont affectées directement au coût calculé. C'est-à-dire qu'**on sait directement à quel type de coût elles se rapportent** (coût d'achat d'une matière particulière...)

Exemples :

- *les matières et fournitures qui entrent dans la composition des produits finis ;*
- *les frais de personnel concernant les travaux effectués sur un seul produit : la main-d'œuvre directe ;*
- *les dotations aux amortissements des machines qui contribuent à la production d'un produit bien précis.*

1D2. Les charges indirectes

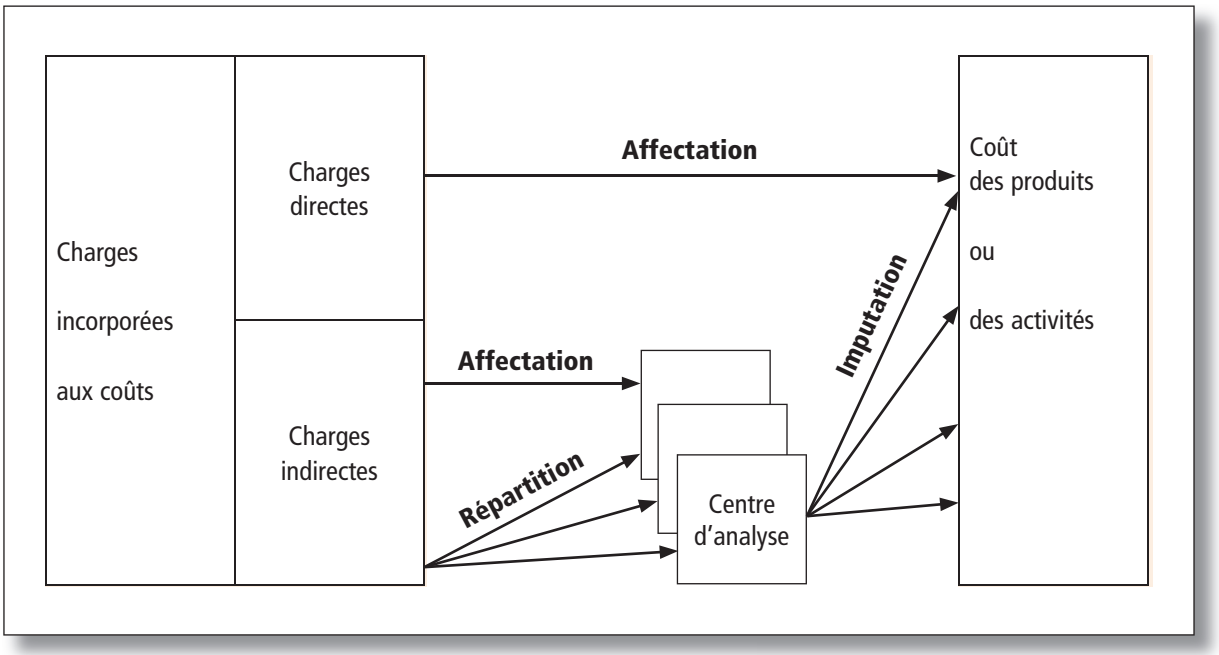
Elles concernent simultanément plusieurs coûts. Il n'est pas possible de les affecter directement à un seul coût, elles doivent d'abord être analysées pour être ensuite réparties.

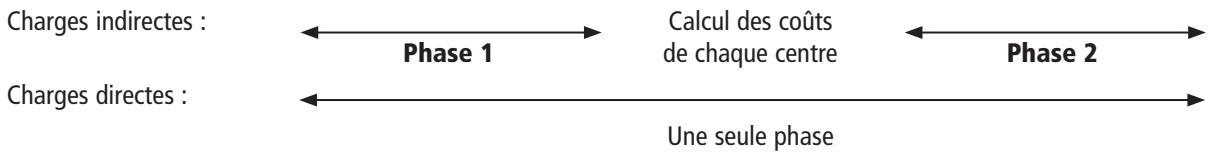
La répartition des charges indirectes se base sur les **centres d'analyse**, qui sont des divisions réelles (le service maintenance) ou fictives (l'achat d'une certaine matière nécessaire à plusieurs produits finis) de l'entreprise.

Alors que les charges directes vont être directement (!) affectées aux coûts ; pour les charges indirectes, on va passer tout d'abord par une affectation dans un ou plusieurs centres d'analyse, puis lorsqu'on aura déterminé le total des charges qui concernent chaque centre d'analyse, ces charges seront imputées aux divers coûts.

1D3. Détermination et imputation de ces charges

Retenez le schéma page suivante, le point suivant vous aidera à mieux le comprendre, n'hésitez pas y revenir.





2. Les centres d'analyse

Un centre d'analyse correspond à une division de l'entreprise où sont analysés des éléments de charges indirectes avant leur imputation aux coûts des produits ou activités concernés.

Exemples : *le service informatique, le service transport...*

2A. *Les principaux centres d'analyse*

Le découpage en centres d'analyse dépend de l'organisation, du secteur d'activité de l'entreprise et du management.

On peut cependant en citer quelques uns en les répartissant en deux catégories.

- **Les centres opérationnels principaux** : ceux dont la destination des charges est facile à déterminer. C'est-à-dire qu'on sait facilement pour quel type de produit, de service, … ils travaillent.

Exemples :

– centres d'approvisionnement : service achats, magasinage…

– centres de production : atelier de fabrication d'un certain produit…

– centres de distribution : vente, conditionnement...

- **Les centres auxiliaires et de structure** : ceux qui globalement travaillent pour un autre centre et qui ne participent pas directement à l'approvisionnement, la production ou la distribution. Leurs charges seront transférées dans d'autres centres, en général des centres principaux.

Exemples :

– gestion du personnel : paie, recrutement, formation...

– services généraux : courrier, entretien des locaux…

– autres centres financiers, de mercatique…

2B. *Les unités d'œuvre*

Une fois que l'on aura calculé les coûts des divers centres (phase 1 du schéma) il faudra affecter ces charges aux coûts des produits ou activités. Nous sommes donc au niveau de la phase 2 du schéma précédent.

Par exemple, les charges du centre « publicité » seront affectées à chaque type de produit en fonction du nombre d'articles publicitaires pour ce type de produit.

2B1. Détermination de l'unité d'œuvre

Toute activité d'un centre d'analyse est mesurée en **unités d'œuvre** qui sont en général des unités physiques pour ce qui concerne les centres opérationnels.

L'unité d'œuvre est une **unité de mesure de la productivité du service**.

Exemples : *pour un service de production qui manipule essentiellement une certaine matière première, son unité d'œuvre pourra être le kilogramme de matière traitée.*

Pour le centre « recrutement », ce peut être le nombre d'embauches réalisées.

Ceci suppose que le centre soit suffisamment homogène pour que son activité puisse être mesurée par une seule et même unité d'œuvre.

Le choix de l'unité d'œuvre va conditionner la pertinence du calcul des charges du centre à imputer aux autres services ou produits.

2B2. Calcul du coût unitaire de l'unité d'œuvre

Une fois que l'on connaît le total des charges d'un service (fin de la phase 1) et que l'on connaît le nombre d'unités d'œuvre, il est aisé de calculer le coût unitaire de l'unité d'œuvre.
Par exemple, si le centre « recrutement » a un total de charges annuelles de 302 400 € (à l'issue de la phase 1 de répartition des charges dans son centre d'analyse) et qu'il a recruté 180 personnes dans l'année, un recrutement coûte à l'entreprise en moyenne 1 680 €.

2B3. Imputation des charges indirectes au coût des activités ou produits.

Muni de ce coût unitaire de l'unité d'œuvre, il nous suffît de connaître le nombre d'unités d'œuvre « consommées » par chaque activité ou produit pour lui imputer une partie des charges du centre d'analyse.

Exemple : *supposons un centre auxiliaire de « recrutement » qui a comme unité d'œuvre le nombre de personnes recrutées. Pour une certaine année, le total de ses charges divisé par le nombre total de recrutements réalisés donne 1 500 €. Cette somme représente le coût d'une unité d'œuvre pour ce centre. Si, par ailleurs, une activité de recherche a nécessité le recrutement de trois personnes qui travaillent uniquement pour ce projet de recherche, ce projet va se voir imputer 4 500 € de charges provenant du centre « recrutement ».*

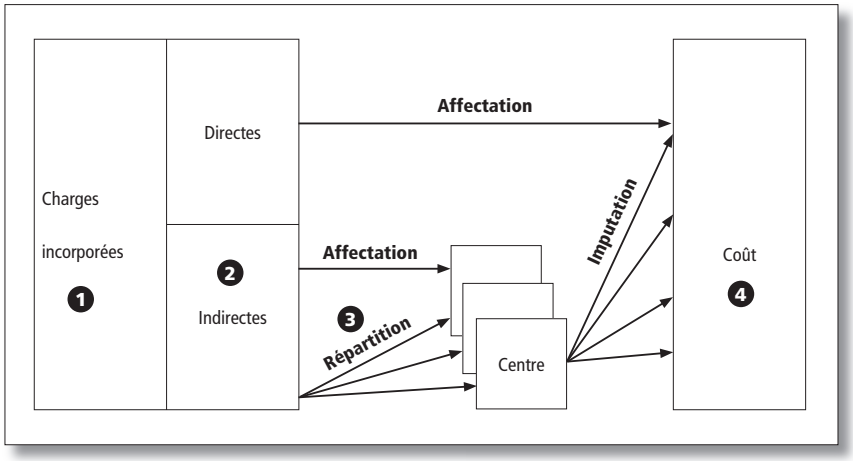
3. Le calcul du coût complet

Voyons tout d'abord les diverses étapes de calcul du coût, avant de nous attarder sur celles qui nécessitent plus de détails.

3A. Les diverses étapes

Comme le montre le schéma concernant le calcul et l'imputation des charges, le calcul du coût complet d'une activité ou d'un produit se réalise selon les étapes suivantes :

- détermination des charges à incorporer aux coûts ;
- parmi ces charges, détermination des charges indirectes ;
- pour les charges indirectes, affectation dans un seul centre ou répartition dans plusieurs centres ;
- calcul du coût par affectation des changes directes et imputation des charges indirectes.



Seule la 3e phase (3) présente une technicité particulière, c'est donc la seule que nous détaillerons. Les autres phases demandent seulement une recherche des données en entreprise ou une bonne lecture du texte de vos exercices. Vous rencontrerez ces phases lors des exercices.

3B. *La répartition des charges indirectes*

Lors de la phase 3 on distingue trois sous-phases :

- la répartition des charges indirectes dans les centres d'analyse : **répartition primaire** ;
- la cession des charges des centres auxiliaires aux centres d'analyse principaux : **répartition secondaire** ;
- la détermination des coûts unitaires des unités d'œuvre.

3B1. La répartition primaire

On répartit tout d'abord les charges dans les divers centres. Pour cela on doit déterminer la part de consommation de chaque centre pour la charge considérée. Dans les exercices, cette dernière vous est souvent donnée sous forme de pourcentage ou proportion.

Exemple : *pour les charges d'électricité qui s'élèvent à 10 000 €, on vous donne la répartition selon les trois centres d'analyse qui consomment de l'électricité, à vous de calculer le montant d'électricité de chaque centre.*

Charges	Montants	Centres d'analyse		
		Entretien	Production	Administration
Électricité	10 000	35%	60%	5%
Répartition primaire	10 000	3 500	6 000	500

Dans la colonne « Montant » toujours vérifier que le total des montants calculés correspond à la charge globale.

La répartition primaire se limite donc à répartir les 10 000 € de frais d'électricité dans les trois centres en fonction des critères de répartition (ici les pourcentages) donnés.

3B2. La répartition secondaire

Elle correspond à la cession de prestations entre centres d'analyse. On va affecter aux centres principaux les charges des autres centres qui ont « travaillé » pour eux. En effet, comme nous l'avons vu lors des définitions, les centres non principaux peuvent être considérés comme des prestataires qui vont alors « refacturer » leurs diverses prestations aux centres principaux.

À l'issue de la répartition secondaire, les centres auxiliaires n'ont plus de charges. Elles sont toutes regroupées dans les centres principaux.

Cette répartition secondaire peut être plus ou moins simple selon que les divers centres assurent des prestations mutuelles ou croisées les uns pour les autres. Par exemple, le centre « gestion du personnel » va s'occuper des employés du centre « services généraux » qui lui, à son tour, assurera le nettoyage et les prestations courrier du centre « gestion du personnel ».

Dans le cas de prestations entre centres non principaux, il faudra en premier répartir les charges d'un centre sur les autres, ce qui viendra gonfler le total des charges de ces derniers, ce n'est qu'ensuite que l'on pourra répartir leurs (« nouveaux ») montants de charges globales.

Répartition simple

Au cours du mois de mars la répartition dans les centres d'analyse après répartition primaire nous donne (extrait du tableau de répartition primaire) :

Centres prestataires	Totaux	Centres d'analyse destinataires de prestations			
		Entretien	Approv.	Production	Distribution
Entretien	3569			3/4	1/4
Approvisionnement	8565	10 %		80 %	10 %

Le centre entretien fournit ses prestations aux ¾ au service production et au service distribution pour le quart restant.

Le centre approvisionnement fournit des prestations à tous les autres services, dont le service entretien. Ce dernier n'a donc pas uniquement 3 569 € de charges, il a également des charges d'approvisionnement qui s'élèvent à 856,50 € (10 % de 8 565).

Pour la répartition secondaire on va donc répartir en premier les charges du centre approvisionnement, puis celles du centre entretien.

Centres prestataires	Totaux	Centres d'analyse destinataires de prestations			
		Entretien	Approv.	Production	Distribution
Entretien	0	(3 569 + 856,50) – 4 425,5		3 319,12	1 106,38
Approvisionnement	0	856,50	– 8 565,00	6 852,00	856,50

Vous constatez qu'à la fin de cette répartition secondaire, les totaux de charges des centres auxiliaires approvisionnement et entretien sont à zéro.

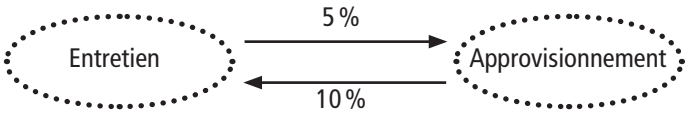
Le total de charges réparties pour le centre entretien correspond aux charges déjà affectées lors de la répartition primaire (3 569 €) auquel on a ajouté les charges provenant de la répartition secondaire d'un autre centre (856,50 € d'approvisionnement).

Prestations réciproques

Supposons maintenant que ces deux centres assurent des prestations réciproques l'un pour l'autre, et qu'à l'issue de la répartition primaire on ait :

Centres prestataires	Totaux	Centres d'analyse destinataires de prestations			
		Entretien	Approv.	Production	Distribution
Entretien	3 569		5 %	70 %	25 %
Approvisionnement	8 565	10 %		80 %	10 %

Les deux centres ont leurs totaux de charges liés puisque chacun vient augmenter le total de charges de l'autre.



Nous ne pouvons plus, comme dans l'exemple précédent, commencer les calculs par un centre plutôt que par l'autre. Il faut mener les calculs relatifs aux deux centres en parallèle, en posant un système d'équations à deux inconnues.

Les inconnues du système d'équations sont :

x : le total du centre « entretien »
y : le total du centre « approvisionnement »

Pour le centre « entretien » : **x = 3 569 + 0,10 y**

(charges calculées antérieurement plus celles d'approvisionnement)

Pour le centre « approvisionnement » : **y = 8 565 + 0,05 x**

(charges calculées antérieurement plus celles d'entretien)

Soit le système d'équations :

$$\begin{cases} x = 3569 + 0{,}10\ y \\ y = 8565 + 0{,}05\ x \end{cases}$$

Qui nous donne après résolution :

x = 4 447,74 €
y = 8 787,39 €

Il nous suffit donc de réaliser la répartition secondaire à partir de ces deux nouveaux montants de charges et des coefficients de répartition entre les centres.

Centres	Totaux	Centres d'analyse destinataires de prestations			
		Entretien	Approv.	Production	Distribution
Total répartition primaire	39 040,00	3 569,00	8 565,00	24 852,00	2 054,00
Répartition « entretien »	0	– 4 447,74	*222,39	**3 113,42	1 111,94
Répartition « approvisionnement »	0	878,74	– 8 787,39	7 029,91	878,74
Total	39 040,00	0	0	34 995,33	4 044,67

*222,39 = 4 447,74 x 5 %

**3 113,42 = 4 447,74 x 70 %

Remarquez que le total des charges globales obtenu après la répartition primaire n'a pas été modifié et que les deux centres auxiliaires (entretien et approvisionnement) n'ont plus de charges, vu qu'ils ont été « refacturées » aux centres principaux.

3B3. Le calcul du coût des unités d'œuvre

Selon ce que nous avons vu sur la détermination et le calcul des unités d'œuvre, nous devons rajouter au bas du tableau de répartition des charges, les trois lignes suivantes :

- la nature de l'unité d'œuvre de chaque centre principal ;
- le nombre d'unités d'œuvre produites par le centre ;
- le coût unitaire de l'unité d'œuvre.

Si, dans l'exemple précédent on suppose que les unités d'œuvre sont les suivantes :

- centre production : le nombre d'articles fabriqués, ce nombre s'élève à 2300 pour le mois de mars ;
- centre distribution : le nombre d'articles vendus, ce nombre s'élève à 2610 pour le mois de mars.

Le tableau de répartition secondaire se résume donc à :

Centres	Totaux	Production	Distribution
Total après répartition secondaire	39 040,00	34 995,33	4 044,67
Unité d'œuvre (u-o)		Nombre d'articles fabriqués	Nombre d'articles vendus
Nombre d'u-p		2 300	2 610
Coût de l'u-o		15,2153609	1,54968199

Remarque

En général on n'arrondit pas ces coûts unitaires puisqu'ils vont ensuite être remultipliés par des valeurs importantes lorsqu'ils serviront au calcul des coûts.

Donc, pour chaque article fabriqué, les charges indirectes à rajouter sont de 15,21 € et elles sont de 1,54 € pour tout article vendu.

Ne pas oublier qu'il faudra rajouter les charges directes.

Après avoir vu comment on affecte puis impute les charges indirectes (*la partie la plus délicate de ce cours !!!*) nous avons maintenant tous les éléments pour calculer les coûts complets des activités, biens ou services réalisés par l'entreprise.

Nous vous rappelons que nous calculons le coût d'achat, puis de production et enfin de revient.

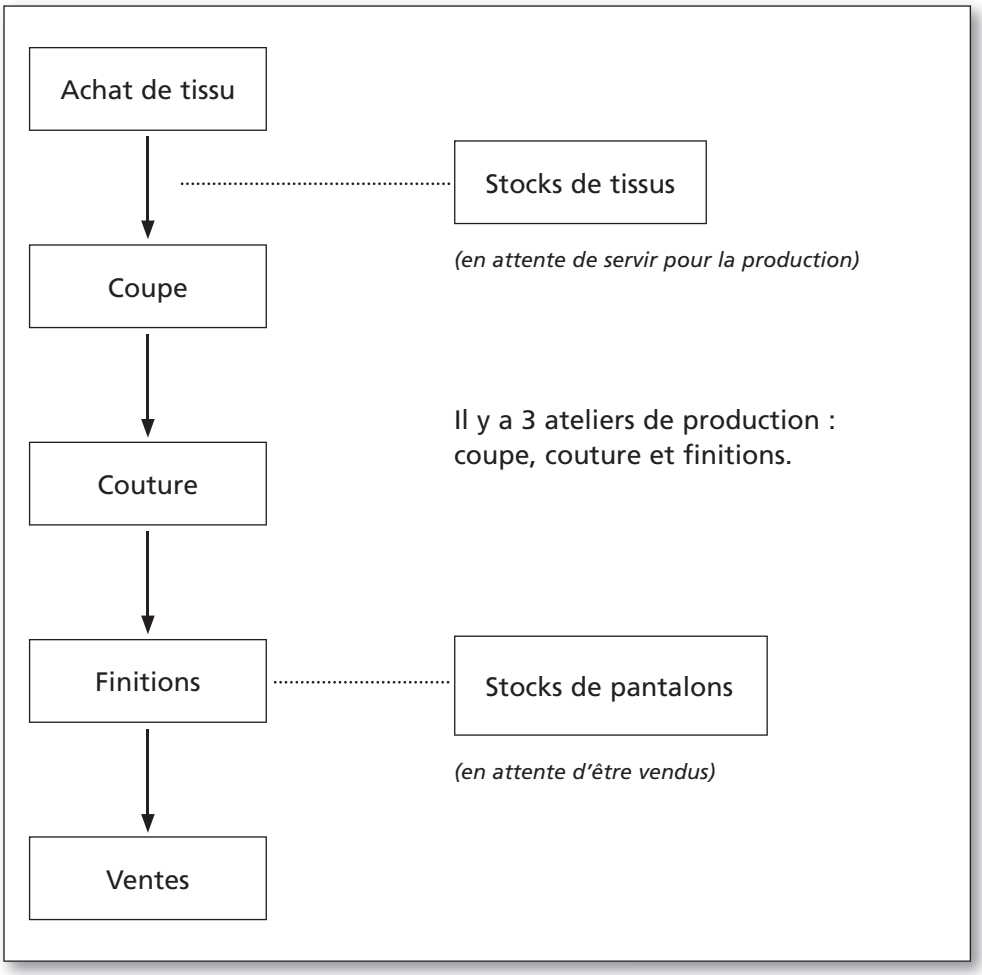
4. Coût d'achat, stocks de marchandises et d'approvisionnements

Toute la suite du cours sera appréhendée en partant du même exemple, celui de l'entreprise TouTex qui fabrique des pantalons et les revend au commerce de détail.

Pour simplifier le cas, on supposera :

- qu'il n'y a qu'une seule matière utilisée pour la production : du tissu d'un seul type ;
- qu'il n'y a qu'un seul modèle de pantalon fabriqué et commercialisé.

L'entreprise TouTex fonctionne selon le schéma général suivant :



L'analyse des charges indirectes de TouTex pour le mois de mars 2006 a donné le tableau suivant :

Charges	TOTAUX	Centres d'analyse				
		Approvisionnement	Coupe	Couture	Finition	Distribution
TOTAL après répartition secondaire	45 870	10 860	10 800	6 080	6 130	12 000
Unité d'œuvre (u-o)		montant des achats (en € H.T.)	m de tissu	h machine	h de travail	Ventes (en € H.T.)
Nombre d'u-o		54 000	10 000	5 400	1 750	165 000
Coût de l'u-o		0,2011	1,0800	1,1259	3,5029	0,0727

Un schéma général récapitulant la chronologie des opérations à réaliser pour calculer les coûts complets se trouve en fin de ce cours, vous pouvez vous y référez si vous désirez, dès maintenant, avoir une vision d'ensemble.

Cependant, pour une première approche, nous vous conseillons une lecture linéaire de la fin du cours.

4A. Coût d'achat

Un coût d'achat (ou d'acquisition) est calculé pour toute matière ou fourniture qui entre dans l'entreprise, il comprend :

- le **prix d'achat** de la marchandise ou la fourniture achetée ;
- les **charges directes** affectées à l'achat :
  - montant de l'achat figurant sur la facture d'achat (hors taxe),
  - frais directs affectés à l'achat (le montant de la facture du transporteur qui a livré le bien considéré, le salaire des acheteurs…) ;
- les **charges indirectes** d'approvisionnement imputées au coût d'achat, proportionnellement aux unités d'œuvre d'approvisionnement employées pour réaliser l'achat considéré.

Au cours du mois mars 2006, l'entreprise TouTex a acheté 20 000 mètres de tissu pour un montant de 54 000 € H.T. Comme seules charges directes d'achat TouTex retient le salaire brut et les charges patronales sur le salaire de l'acheteur qui s'élèvent à 2 250 € (travail à temps partiel) et des frais postaux de 148 €.

Coût d'achat du tissu acheté en mars 2006

Charges	Quantité	Coût unitaire	Montant
Charges directes :			
– tissu acheté	20 000	2,70	54 000
– frais de personnel	1		2 250
– frais postaux			148
Charges indirectes :			
– approvisionnement	54 000	0,2011	10 860
TOTAL	**20 000**	**3,3629**	**67 258**

Au niveau des charges indirectes nous n'avons que les charges du centre approvisionnement à prendre en compte. Le coût unitaire de ce centre a été évalué à 0,2011 € (voir tableau précédent), l'unité d'œuvre est le nombre d'euros H.T. de marchandise achetée, donc ici 54 000 €. Ce qui nous donne un montant global de 10 860 €.

Ici, nous sommes face à un cas particulier car nous n'achetons qu'une seule chose, du tissu. Ce passage par les unités d'œuvre est donc superflu car toutes les charges du centre approvisionnement ne concernent que le coût d'achat du tissu. Nous aurions donc pu nous dispenser de passer par les unités d'œuvre et reporter les charges globales du centre approvisionnement (10 860 €) dans la colonne « montant ». S'il y avait eu une autre marchandise achetée, le calcul tel que nous l'avions fait était indispensable.

Ne pas oublier le prix d'achat de la marchandise (ici « Tissu acheté ») dans le calcul du coût d'achat.

Le coût unitaire du mètre de tissu acheté en mars 2006 est donc de 3,36 € hors taxes. Pour le déterminer on calcule le montant total en faisant la somme des diverses charges,

puis on inscrit la quantité achetée, ici en mètre, et enfin on obtient le coût unitaire en divisant le montant par la quantité.

Vous noterez que la colonne « quantité » ne contient pas des données homogènes, ce qui est normal par définition de ce qu'est une unité d'œuvre. 20 000 représente le nombre de mètres de tissus achetés, un le nombre de salarié affecté uniquement à l'achat et 54 000 le nombre d'unité d'œuvre du centre Approvisionnement. Faites attention de ne pas additionner ces diverses quantités au bas de la colonne « TOTAL », qui elle contient le nombre d'articles (ici les mètres de tissu) achetés.

4B. Stock de marchandises et approvisionnements

Nous venons de calculer le coût d'achat du tissu acheté en mars 2006, mais la totalité de ce tissu n'est pas utilisée pour la production du mois de mars. De même, si dans une période antérieure le tissu était à un prix inférieur (et donc un coût d'achat inférieur si les autres charges n'étaient pas identiques) et qu'il nous reste de ce tissu « ancien », il ne serait pas correct de prendre en compte ce nouveau coût d'achat pour déterminer le coût de production alors que nous allons utiliser du tissu « ancien ».

Pour cela nous allons tenir un **compte de stock de marchandises**. Plusieurs techniques existent pour tenir un tel compte, nous utiliserons celle du **coût moyen pondéré en fin de période**.

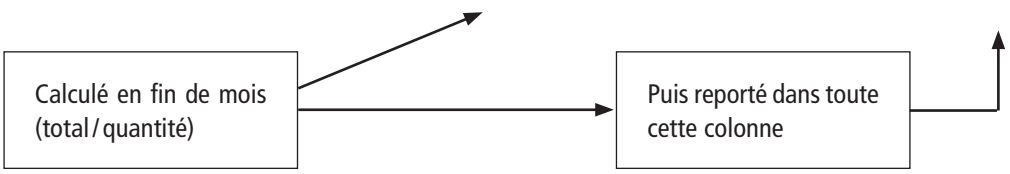
Nous allons donc tenir un compte de stock pour le tissu en y enregistrant les entrées et les sorties.

Les entrées sont valorisées au coût d'achat (que l'on vient de calculer). En fin de mois (qui correspond ici à la période de calcul des coûts), on calculera le coût unitaire moyen pondéré (CUMP) du mois, et ensuite on valorisera toutes les sorties à ce coût.

Le stock au 1er mars 2006 était de 5 000 m pour 15 500 € et on a utilisé 10 000 m de tissu pour la fabrication de pantalons en mars 2006.

Stock de tissu

		Entrées			Sorties		
Date	Mouvement	Quantité	C.U.	Total	Quantité	C.U.	Total
01/03	Stock initial	5000	3,1000	15500,00			
?/03	Achat	20000	3,3629	67258,00			
?/03	Sorties				10000	3,3103	33103,20
31/03	Stock final				15000	3,3103	49654,80
	TOTAUX	**25000**	**3,3103**	**82758,00**	**25000**	**3,3103**	**82758,00**



N.B. : Dans ce tableau, « c.u » signifie coût unitaire.

Donc le tissu **utilisé** pour la production de mars 2006 sera **valorisé à 3,3103 € le mètre** qui correspond à la valeur moyenne du tissu en stock (« ancien » et acheté en mars), et non à 3,3629 € qui correspond au coût d'achat du tissu uniquement acheté en mars.

Remarque

Le stock initial au 1er avril (= stock final fin mars) sera de 15 000 m, valorisé à 3,3103 € le mètre.

5. Coût de production et stocks de produits

On va calculer un coût de production pour chaque produit (bien ou service) créé dans l'entreprise.

Le coût de production comprend :

- la valorisation au **CUMP des matières premières utilisées** pour la fabrication du produit ;
- des autres **charges directes** de production (main-d'œuvre, fournitures…) ;
- des **charges indirectes** concernant la production.

Comme charges directes de production, on retient le coût salarial (salaire brut et charges patronales) des cinq ouvriers (2 956 € chacun) qui travaillent dans les divers ateliers de production. De même on a utilisé 854 € (HT) de fournitures diverses non stockées. Les quantités d'unités d'œuvre et leur coût se trouvent en bas du tableau de répartition secondaire des charges indirectes.

La production du mois s'est élevée à 8 500 pièces.

Coût de production des pantalons en mars 2006

Charges	Quantité	Coût unitaire	Montant
Charges directes :			
– tissu utilisé	10 000	3,3103	33 103,20
– frais de personnel	5	2 956,00	14 780,00
– fournitures			854,00
Charges indirectes :			
– coupe	10 000	1,0800	10 800,00
– couture	5 400	1,1259	6 080,00
– finition	1 750	3,5029	6 130,00
TOTAL	**8 500**	**8,4408**	**71 747,20**

En mars 2006, la fabrication a donc dégagé un coût de production de 8,44 € par pantalon.

Dans cet exercice (cas particulier), la totalité des unités d'œuvre des divers centres d'analyse sont attribuées à ces pantalons, puisque que nous avons une production unique. Si nous fabriquions plusieurs produits finis, il faudrait, pour chacun, rechercher le nombre d'unité d'œuvre le concernant.

Intéressons-nous maintenant au stock de produits finis.

De même que pour le tissu, toute la production de pantalons du mois n'est pas vendue. On va donc tenir un compte de stock des pantalons afin de déterminer le coût unitaire moyen pondéré (CUMP) en fin de mois des pantalons en stock, et valoriser toutes les sorties du mois à ce CUMP.

Durant le mois de mars 2006, on a vendu 11 000 pantalons. Et le stock initial était de 10 000 pièces valorisées à 8,10 € la pièce.

Stock de pantalons

		Entrées			Sorties		
Date	Mouvement	Quantité	C.U.	Total	Quantité	C.U.	Total
01/03	Stock initial	10000	8,1000	81000,00			
?/03	Entrées	8500	8,4408	71747,20			
?/03	Sorties				11000	8,2566	90822,66
31/03	Stock final				7500	8,2566	61924,54
	TOTAUX	18500	8,2566	152747,20	18500	8,2566	152747,20

On estime donc à 8,2566 € le coût de revient unitaire des pantalons qui seront vendus.

6. Coût de revient des produits vendus

On détermine un coût de revient pour chaque **produit vendu** par l'entreprise, chaque activité ou chaque commande client. En effet les charges de commercialisation, entre autres, ne s'appliquent qu'aux produits vendus et non à ceux fabriqués.

Dans une entreprise produisant des biens ou services, le coût de revient comprend :

- le coût de production des produits finis vendus (évalué à la sortie du stock de produits finis) ;
- le coût de distribution des produits finis vendus ;
- une quote-part des charges communes des centres de structure (administration générale, finance).

Chez TouTex une personne travaille uniquement aux expéditions, son salaire (salaire brut plus charges patronales) est de 1 998 € par mois. Au cours du mois de mars 2006 on a dépensé pour 705 € de frais d'expédition, et on a vendu 11 000 pantalons au prix de vente de 15 € l'unité. Déterminons maintenant le coût de revient des pantalons vendus.

Les seules charges indirectes sont celles de distribution. Se reporter au tableau de répartition secondaire pour les trouver : l'unité d'œuvre est le montant HT des ventes, soit ici 11 000 x 15 € l'unité, et le coût unitaire trouvé était de 0,0727 €.

Les pantalons vendus ont donc coûtés 9,59 € pièce à l'entreprise.

Coût de revient des pantalons vendus en mars 2006

Charges	Quantité	Coût unitaire	Montant
Charges directes :			
– pantalons vendus	11000	8,2566	90822,66
– frais de personnel	1	1998,00	1998,00
– frais d'expédition			705,00
Charges indirectes :			
– distribution	165000	0,0727	12000,00
TOTAL	**11000**	**9,5932**	**105525,66**

7. Résultat analytique

Le résultat analytique va permettre à l'entreprise de connaître le bénéfice ou la perte réalisé sur les produits vendus.

Le résultat analytique est la différence entre le chiffre d'affaires et le coût de revient des produits vendus.

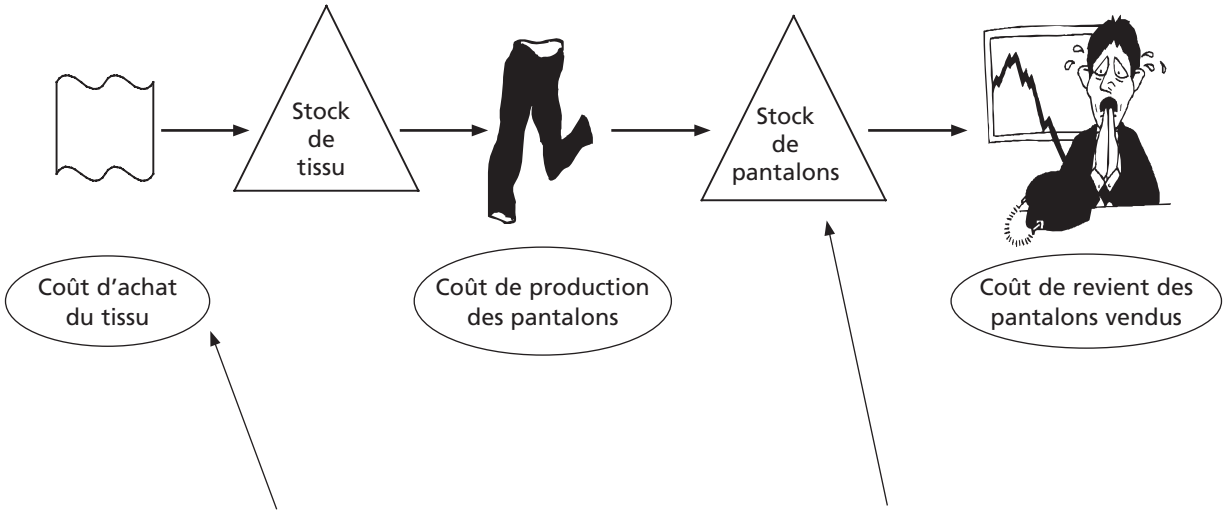
Résultat analytique des pantalons vendus en mars 2006

	Quantité	Coût unitaire	Montant
Ventes	11 000	15	165 000,00
Coût de revient des pantalons vendus	11 000	9,5932	105 525,66
TOTAL	**11 000**	**5,40676**	**59 474,34**

L'entreprise a donc gagné 59 474,34 € sur ses ventes de mars 2006, ce qui se traduit par un gain de 5,41 € sur chaque pantalon vendu.

8. Résumé du calcul des coûts complets

Pour l'entreprise TouTex, de l'achat de la matière première au calcul du résultat sur les ventes, notre démarche a été celle-ci :

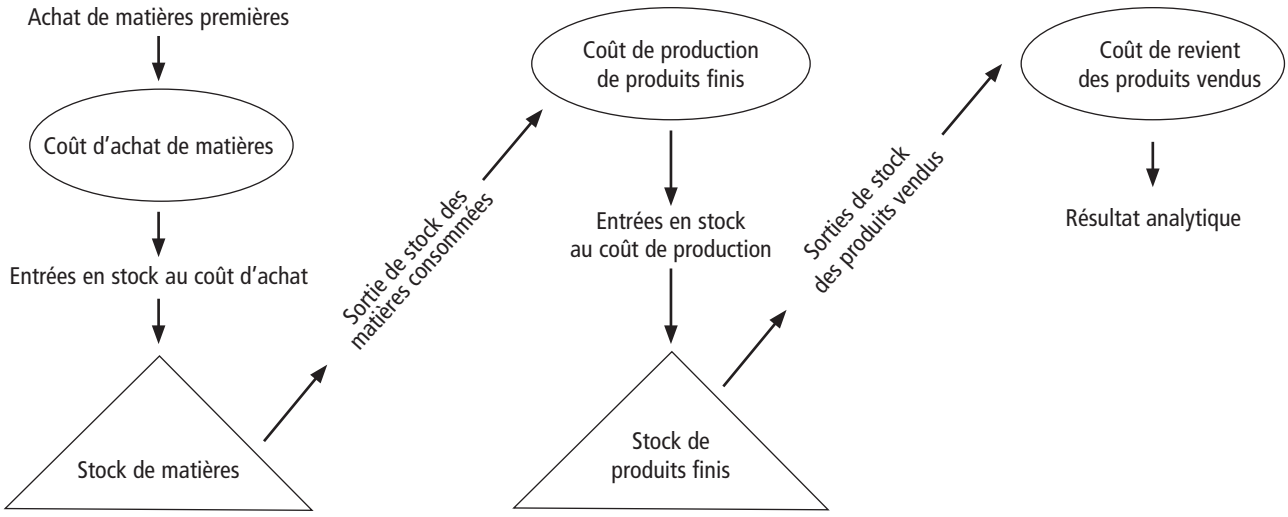


À partir de ce cas simplifié on peut en déduire le schéma général suivant.

Calcul des coûts complets

Les **ovales** correspondent à des **coûts à calculer**, alors que les **triangles** correspondent à des **comptes de stock à tenir**.

De plus, on rappelle que les entreprises purement commerciales (qui ne font qu'acheter pour revendre) n'ont pas de stock de matières premières, ni de coût de production à calculer. À l'issue du calcul du coût d'achat, on réalise le stock de produits finis (dont les entrées sont alors valorisées au coût d'achat).



Exercices autocorrectifs

Exercice 1

Une entreprise est spécialisée dans la fabrication de « SUPERDAN » des crèmes desserts au chocolat de qualité supérieure. Ces crèmes sont réalisées à l'aide de deux matières principales, le lait et le sucre. Ces crèmes sont vendues dans des pots représentant des portions individuelles (125 g) et sont regroupées, et vendues, par paquet de 6 pots dans un emballage en carton. Les clients de l'entreprise sont des épiceries fines.

1. Quels centres d'analyse liés à la production proposeriez-vous ?

2. N'y a-t-il que des centres d'analyse liés à la production ?

L'entreprise a choisi de se limiter aux centres suivants : approvisionnement, fabrication et mise en pot, emballage et commercialisation. Elle vous donne le tableau des charges pour le mois de mai 2006.

Répartition des charges

Centres	TOTAUX	Approvisionnement	Fabrication	Emballage	Commercialisation
TOTAL après répartition secondaire	17 870	1 250	10 800	3 860	1 960
Unité d'œuvre (u-o)		Éléments achetés*	Pots fabriqués	Paquets fabriqués	Paquets vendus
Nombre d'u-o		8 706	196 000	32 500	32 400
Coût de l'u-o		0,1436	0,0551	0,1188	0,0605

** Ici les « éléments achetés » représentent les quantités achetées. Elles sont exprimées dans les unités différentes (kg, l, unités) mais sont toutes cumulées car on suppose que les charges indirectes sont identiques pour un kg de sucre, un litre de lait, un pot ou un emballage.*

De plus, elle vous donne les informations suivantes concernant le mois de mai 2006 :

Éléments	Lait (en l)	Sucre (en kg)	Pots vides	Emballages
Stocks au 01/05/06	14 000	7 000	200 000	36 000
Valeur en € au 01/05/06	2 400	700	1 240	2 600
Achats	45 000	8 000	32 000	22 000
Valeurs achats en €	6 540	560	154	1 452
Consommation	35 000	2 060	196 000	32 500

Autres informations :

- on ne gère pas de stock de pots pleins, on suppose qu'ils sont immédiatement emballés par paquets de six dès leur production ;
- au 01/05/2006 il n'y a aucun stock de paquets ;
- en plus des deux ingrédients principaux, SUPERDAN nécessite des « consommables » pour la fabrication qui s'est élevée à 1 235 € en mai 2006 ;
- on suppose (*cas rare !! mais pour simplification ici*) qu'il n'y a pas de charge directe de personnel d'approvisionnement ;
- la fabrication nécessite du personnel dont le salaire horaire tout compris (charges salariales, patronales et frais divers de personnel compris) est de 21,20 € pour la fabrication et 17,85 € pour l'emballage. Pour le mois de mai 2006 la production a nécessité 300 heures de fabrication et 110 heures d'emballage ;

- globalement l'entreprise a eu pour 705 € de frais de livraison à ses clients ;
- elle a employé un technicien spécialisé à mi-temps, dont le salaire mensuel à temps plein tout compris (salaire brut et charges patronales), est de 2 156 € ;
- les paquets sont vendus 2,05 € l'unité.

Tous les montants vous sont donnés en HT (hors taxe).

3. ***Retrouvez (par le calcul) la somme de 8 706 € qui se trouve dans le tableau de répartition au niveau des frais du centre approvisionnement.***
4. ***En mai 2006 on a fabriqué 196 000 pots et 32 500 paquets. Est-ce logique ? Donnez une explication à ce problème.***
5. ***Calculez les coûts d'achat nécessaires, puis donnez le coût unitaire actuel des diverses matières pour l'entreprise.***
6. ***Calculez le coût de production des SUPERDAN pour mai 2006.***
7. ***Quel est le coût unitaire de production d'un paquet pour l'entreprise ? Pourquoi est-ce inutile ici de dresser le compte de stock de paquets de SUPERDAN ?***
8. ***Calculez le coût de revient et dire combien l'entreprise a gagné (ou perdu) sur les ventes de SUPERDAN en mai 2006.***

Exercice 2

Comme dernier exercice nous allons nous occuper de la répartition des charges indirectes. Le but de cet exercice va être de compléter le tableau ci-dessous en effectuant la répartition primaire puis secondaire des charges indirectes :

Charges	Totaux	Centres auxiliaires		Centres principaux			
		Personnel	Entretien	Atelier 1	Atelier 2	Distribution	Administration
Charges de personnel	10 000	9%	8%	31%	17%	18%	17%
Impôts et taxes	3500		50%		10%	30%	10%
Charges diverses	11000	10%	17%	25%	25%	13%	10%
Charges supplétives	400						100%
Total après répartition primaire							
Répartition centre Personnel			10%	27%	31%	17%	15%
Répartition centre Entretien		7%		41%	52%		
Total après répartition secondaire							
Unité d'œuvre				Nombre de produits coupés	Nombre de produits fabriqués	Nombre de produits vendus	Ventes en centaines d'euros
Nombre total d'u-o				11 250	8 100	7 500	82 000
Coût de l'u-o							

1. ***Pourquoi, dans ce tableau, y a-t-il des charges de personnel (1re ligne) à répartir ainsi qu'un centre auxiliaire « personnel » ?***
2. ***Effectuez la répartition primaire des charges indirectes.***
3. ***Que veut dire « charges supplétives » et pourquoi sont-elles toutes affectées au centre administration ?***
4. ***Quel est le montant total des charges du centre entretien ?***
5. ***Déterminez les totaux de charges de ces deux centres.***
6. ***Réalisez la répartition secondaire des charges indirectes.***
7. ***Calculez le coût unitaire des unités d'œuvre de chaque centre.***

Séquence 5

Les coûts variables

1. Distinction coûts variables/coûts complets

Dans l'exercice qui nous a servi de modèle pour le cours sur les coûts complets, nous avions montré que l'entreprise TouTex gagnait 5,41 € sur chaque pantalon vendu lors du mois de mars 2006. Supposons maintenant que son volume d'activité subisse une chute considérable et qu'elle passe de 11 000 pantalons vendus en mars 2006 à seulement 8 000 pantalons vendus le mois suivant, le prix de vente restant inchangé.

Le calcul des coûts variables va nous aider à montrer que le bénéfice unitaire sur chaque pantalon va, lui aussi, baisser, car le prix de vente restant identique, c'est le coût de revient unitaire des pantalons qui va augmenter.

Pourquoi cela ? La quantité (et le prix) de tissu incorporée dans chaque pantalon va être la même, donc, le coût du tissu pour chaque pantalon reste inchangé.

Mais les charges générales de l'entreprise telles que le loyer, les primes d'assurance, les salaires des administratifs… vont être identiques par rapport au mois précédent et donc leur montant global se répartira sur moins de pantalons vendus. La partie de ces charges « fixes » qui va être incorporée dans chaque pantalon va donc augmenter, c'est pourquoi le coût de revient unitaire d'un pantalon va augmenter. En effet, lors du mois où une baisse d'activité importante est survenue, l'entreprise n'a pu réagir immédiatement au niveau de ses engagements généraux et donc, ses frais fixes sont identiques à ceux du mois précédent.

De même, il se peut que les ventes d'un certain produit augmentent considérablement sans pour cela que les charges fixes de l'entreprise ne subissent une hausse importante. Le coût de revient de chaque pantalon va donc diminuer car les charges fixes vont être supportées par un plus grand nombre d'articles (les autres articles que peut fabriquer TouTex).

L'analyse par les coûts complets nous permettait de dégager le coût de revient de chaque produit vendu, mais pas de déterminer quelle est la partie de ce coût qui est due à la variation de l'activité. L'analyse des coûts variables va donc être complémentaire à celle des coûts complets et permettre d'isoler la partie correspondant aux charges variables (celles qui évoluent en fonction de l'activité) et la partie correspondant aux charges fixes.

- Les **coûts complets** font la distinction entre charges directes et indirectes et mettent l'accent sur le **produit ou service**.
- Les **coûts variables** font la distinction entre charges variables et fixes et mettent l'accent sur **l'activité** de l'entreprise.

2. Les charges et leur évolution

Pour le calcul des coûts complets, nous avions au préalable fait la distinction entre charges fixes et variables, nous allons ici distinguer les charges variables (celles proportionnelles à l'activité) des fixes.

2A. Les charges fixes et variables

2A1. Les charges variables

Ce sont des charges qui varient en fonction du volume d'activité. On admet que ces charges sont proportionnelles aux quantités produites, et donc vendues. Ces charges sont croissantes et proportionnelles au niveau global, mais restent constantes au niveau unitaire.

***Exemple** : on a toujours besoin de 5 kg d'une certaine matière et de 0,20 heure de main-d'œuvre pour fabriquer une unité d'un certain produit fini. **Le coût variable global va donc être proportionnel au nombre d'unités produites** (plus on produit, plus on a besoin de matière et de travail). Mais le coût variable unitaire de matière et de main-d'œuvre **reste constant** (si les prix des matières ne changent pas) quel que soit le niveau de la production.*

2A2. Les charges fixes

Les charges fixes (ou charges de structure) sont indépendantes du niveau d'activité de l'entreprise, elles **sont constantes pour une structure donnée** (niveau de production, d'achat ou de vente) de l'entreprise.

Elles sont **constantes au niveau global** mais **décroissent unitairement** avec l'augmentation du volume de l'activité (économie d'échelle due à la productivité), car leur montant est fixe mais **le nombre d'éléments sur lesquels il faudra les répartir est plus important** (on divise le total des charges par un nombre supérieur d'unités achetées, produites ou vendues, on obtient donc un résultat unitaire inférieur).

Lors d'un changement de structure, l'entreprise va investir pour se développer (acquisition de matériel, location d'un nouvel entrepôt, embauche de personnel...), ceci va augmenter les coûts. Les charges fixes vont donc **évoluer par paliers**.

***Exemple :** si le loyer d'un entrepôt, dans lequel nous pouvons stocker au maximum 100 000 articles, est de 980 € par mois, et que nous puissions en louer un second au même prix en cas de surstock, quel sera le coût unitaire du loyer à appliquer aux articles stockés dans les cas suivants ?*

Nombre d'articles	Nombre d'entrepôts	Coût total de stockage	Coût unitaire du loyer par article
85 000	1	980	(85000/980) 0,0115
99 500	1	980	0,0098
105 000	2	(980*2) 1960	0,0187
170 000	2	1960	0,0115
190 000	2	1960	0,0103

Nous avons ici deux structures de l'entreprise : la première avec un seul entrepôt (coût fixe 980 €, capacité de stockage 100 000 unités) et la seconde avec deux entrepôts (coût fixe 1 960 €, capacité de stockage 200 000 unités). Tant que nous restons avec un seul entrepôt, le coût fixe unitaire de stockage décroît avec le nombre d'articles stockés.

Dès que nous passons à deux entrepôts, avec une nécessité de stockage supplémentaire de seulement 5 000 unités (passage à 105 000, avec une capacité maximale de 100 000 par entrepôt), le coût fixe unitaire va augmenter, puis décroître à nouveau au fur et à mesure que nous « rentabilisons » la location du second entrepôt.

2A3. Les charges semi-variables

Ce sont des charges qui varient en fonction de l'activité mais pas de manière proportionnelle. Elles sont composées d'une partie de charges variables et d'une partie de charges fixes. Vous devrez décomposer ces charges en deux parties (charges variables et charges fixes) dans vos calculs.

Exemple : *le salaire d'un commercial rémunéré par un fixe de 1 000 € (charge fixe) et une commission de 5% sur les ventes (charge variable).*

2B. Le calcul des charges

Les charges totales de l'entreprise s'obtiennent par la somme des charges variables et des charges fixes.

Les charges variables vont être calculées unitairement. Les charges fixes, quant à elles, vont s'exprimer par un montant global « fixe ».

2B1. Les charges totales

Exemple : *si on suppose que pour produire un certain article les charges variables sont de 3,10 € par unité, et que l'entreprise doit faire face à 19 500 € de charges fixes, alors le mois où elle produit 10 000 articles, ses charges totales vont s'exprimer sous la forme :*

3,10 X 10 000 + 19 500 = 50 500

a x + b = y

avec a = 3,10 (coût variable unitaire), x = 10 000 (quantités produites) et y représentant le coût total.

Charges totales = charges variables unitaires X quantité + charges fixes

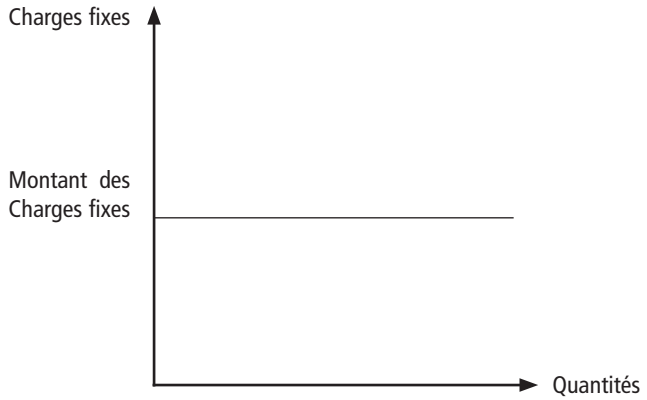
Cette équation restera toujours valable, quelle que soit la manière dont sont calculées les diverses charges.

2B2. Représentation graphique

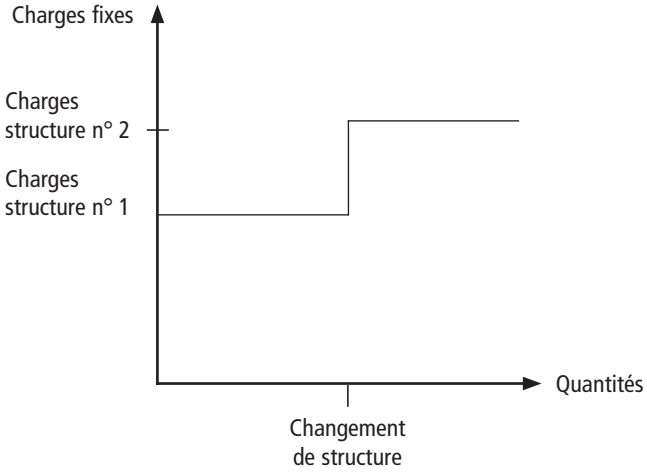
La représentation graphique permet de visualiser l'évolution des charges et de déterminer certains seuils importants.

En général, on représente les quantités en abscisse et les charges en ordonnée. Nous verrons que nous pouvons, sur le même graphique, rajouter deux autres axes des abscisses : le temps et le chiffre d'affaires.

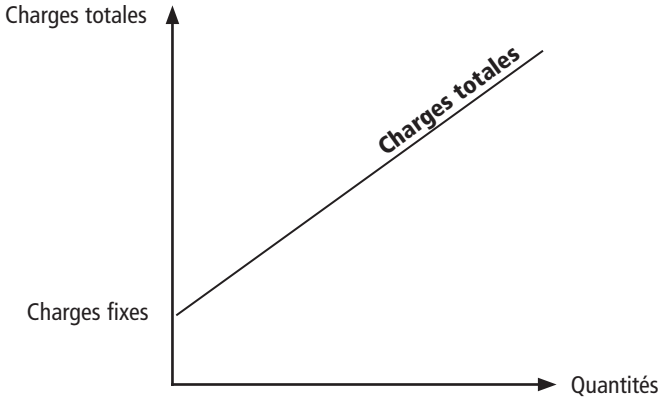
Les charges fixes ne varient pas en fonction de l'activité, elles ont toujours le même montant, elles seront donc représentées par une droite (parallèle à l'axe des abscisses, soit « horizontale »).



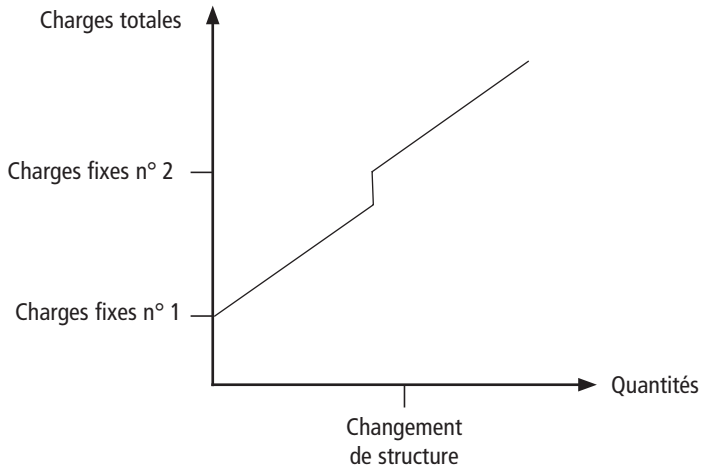
Si on change de structure (on fait de nouveaux investissements par exemple), on aura un palier :



Les charges variables, quant à elles, évoluent en fonction de l'activité et donc des quantités (achetées, stockées ou vendues). Nous aurons donc une droite proportionnelle aux quantités (partant du point zéro). Le coût variable unitaire sera le coefficient directeur de cette droite.
Les charges globales vont donc se déterminer par la droite $y = ax + b$, comme nous l'avons présenté en début de ce chapitre (y : coût total, a : coût variable unitaire, x : quantités, b : coût fixe) :



Dans le cas où il aurait un changement de structure, la représentation graphique serait alors :



Par exemple si l'entreprise loue un local qui devient trop petit, elle va subitement augmenter ses charges fixes en louant un local supplémentaire, or les quantités qu'elle va pouvoir produire (stocker ou vendre) ne vont pas augmenter aussi rapidement. Le nouveau niveau des charges fixes va donc, au moins au début, porter sur une quantité quasi identique à celle que nous produisions (stockions ou vendions) avec l'ancienne structure. Les charges unitaires vont donc augmenter subitement pour ensuite suivre une progression linéaire.

3. L'analyse des marges

Cette analyse permet de dégager des marges en reposant sur la distinction entre charges variables et fixes.

3A. La marge sur coût variable

- Une marge est toujours la différence entre un chiffre d'affaires et un coût.
- Un coût est un ensemble de charges.
- La marge sur coût variable (MCV) est la différence entre le chiffre d'affaires et le coût variable (ensemble des charges variables).

Marge sur coût variable = Chiffre d'affaires - Coût Variable

3B. Le taux de marge sur coût variable

Le taux de marge sur coût variable est le rapport de la marge sur coût variable sur le chiffre d'affaires.

$$\textbf{Taux de marge sur coût variable} = \frac{\textbf{marge sur coût variable}}{\textbf{chiffre d'affaires}}$$

Ce taux est utile lorsqu'on ne peut calculer la MCV unitairement (trop grande quantité de produits distincts…) ou qu'on veut l'exprimer sous forme de pourcentage.

4. Le seuil de rentabilité

4A. *Définition*

Le seuil de rentabilité (SR) (ou chiffre d'affaires critique) d'une entreprise est le **chiffre d'affaires** pour lequel l'entreprise couvre la totalité de ses charges **sans dégager ni gain ni perte**.

C'est donc le **chiffre d'affaires qui correspond à un bénéfice nul**. Si on n'arrive pas à atteindre ce chiffre, on ne couvre pas toutes les charges, l'entreprise fait alors des pertes.

Donc on a : **Seuil de rentabilité – charges totales = 0**

ou **Seuil de rentabilité = charges totales**

↓

Seuil de rentabilité = Charges variables + Charges fixes

*Soit au **seuil de rentabilité** :* **MCV = Charges Fixes**

Comme c'est un chiffre d'affaires, on l'exprime en euros, mais on peut l'exprimer en quantité d'articles à produire ou à vendre en disant « seuil de rentabilité en quantité ».

Cette égalité, valable uniquement au seuil de rentabilité, provient de la définition de ce dernier. En effet, c'est le point où l'entreprise ne gagne ni ne perd rien. Son bénéfice en ce point est donc nul, soit :

	Bénéfice	=	**0**
Soit :	**Chiffre d'affaires – coût total**	=	**0**
	Chiffre d'affaires	=	**coût total**
	Chiffre d'affaires	=	**charges fixes + charges variables**
	Chiffre d'affaires – charges variables	=	**charges fixes**
Et donc :	**MCV**	=	**charges fixes**
Cette égalité équivaut à :	**SR X Taux MCV**	=	**Charges Fixes**

4B. Détermination du seuil de rentabilité

On peut déterminer ce seuil par le calcul ou à l'aide d'une représentation graphique.

4B1. Calcul arithmétique

On peut se servir de n'importe quelle équation que nous avons vue. Le plus souvent on se sert de la plus simple soit :

Chiffres d'affaires = Coût total

Qui peut aussi s'écrire sous la forme : **Ventes = Coût variable + Coût fixe**

4C. Représentation graphique

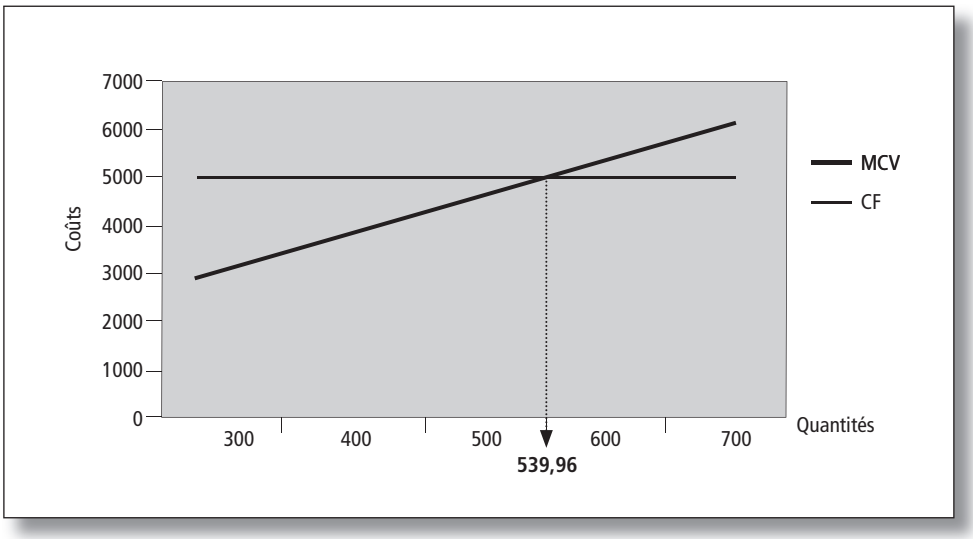
Soit une entreprise dont les charges fixes sont de 5 000 € par mois et les charges variables unitaires de 0,74 € pour le seul produit qu'elle fabrique. Elle vend son produit 10 € l'unité. Déterminons tout d'abord graphiquement son seuil de rentabilité puis retrouvons-le par le calcul.

Par le graphique

On se sert de : ***marge sur coûts variables = charges fixes.***

L'équation de M.C.V. est : ***MCV = 10 x – 0,74 x, soit MCV = 9,26 x*** avec *x : quantités vendues.*

L'équation des charges fixes est : ***CF = 5 000***



On représente ces deux équations, puis on regarde pour quelle quantité vendue les deux droites se coupent.

Si on vend 539,96 produits, le bénéfice sera nul. Au-delà de cette limite (ventes > 536,96), on fera des bénéfices, et en deçà (ventes < 539,96), on sera en perte.

Par le calcul

Seuil de rentabilité = charges variables + charges fixes
10 x = 0,74 x + 5 000
9,26 x = 5 000
x = 539,96

Il faut donc vendre 540 unités pour couvrir la totalité des charges. Le seuil de rentabilité en quantité est de 540, et il est de 5 400 € en valeur.

Remarque

Selon le type de produit que nous manipulons (ici le texte de l'exercice ne vous donne pas de précision) il est probable qu'il faille arrondir ce montant. S'il s'agit d'un produit dont le conditionnement se fait au litre, par exemple, on peut laisser 539,96 l ; en revanche on doit l'arrondir à 540 s'il s'agit d'objets.

4D. Temps et seuil de rentabilité

Indépendamment de la valeur du seuil de rentabilité, les entreprises peuvent être intéressées par la date à laquelle il sera atteint, ou, plus exactement, le délai nécessaire à la couverture de tous les frais.

Deux cas sont possibles, selon que l'on réalise une production (ou achat ou vente) régulière ou une production irrégulière au cours du temps. En effet, une modification du rythme de production a des conséquences sur la date à laquelle on va atteindre le seuil de rentabilité, mais pas sur sa valeur.

4D1. Cas de ventes régulières

On considère que les ventes (et la production) sont réparties de façon linéaire et continue au cours de l'année. C'est-à-dire qu'on réalise le chiffre d'affaires annuel de 15 000 € sur les 360 jours que constituent une année comptable. On a calculé par ailleurs que le seuil de rentabilité était atteint à 5 400 €. Quand sera-t-il atteint ?

Le chiffre d'affaires journalier est donc de *15 000/360* et on atteindra le seuil de rentabilité au bout de : *(5 400 X 360) / 15 000 = 129,6 jours*, soit au cours du 130e jour de l'année : le 10 mai.

Avant le 10 mai, toutes les ventes de l'entreprise ne serviront qu'à compenser les charges engagées, mais à partir de cette date, on réalisera un bénéfice.

4D2. Cas de ventes saisonnières

Si le chiffre d'affaires n'est pas régulier, on va faire le cumul des chiffres d'affaires mensuels pour déterminer à quel mois dans l'année sera atteint le seuil de rentabilité. Ensuite pour connaître le jour, au niveau du mois trouvé, si aucune précision ne nous est donnée, on supposera que les ventes sont régulières tout au long du mois.

Mois	Janvier	Février	Mars	Avril	Mai	Juin	Juillet	...
CA	853	820	1087	1195	1210	1208	1186	…
CA cumulé	853	1673	2760	3955	5165	6373	7559	

Le seuil de rentabilité de 5 400 € sera atteint au cours du mois de juin (5 165 < 5 400 < 6 373). Maintenant il faut déterminer quel jour.

Le seuil de rentabilité sera atteint, lorsqu'au cours du mois de juin, on aura fait 235 € de ventes (5 400 – 5 165 = total fin de mois – seuil de rentabilité). Si en juin les ventes sont régulières, ce chiffre d'affaires sera réalisé au bout de (30 X 235) / 1 208 ≈ 5,84 jours, soit le 6e jour du mois de juin, le 6 juin. On utilise ici les mois comptables de 30 jours.

- **Si on ne vous dit rien dans les exercices, on supposera toujours que les ventes sont régulières au cours d'un même mois ainsi que d'une même année.**

5. Le compte de résultat différentiel et la prise de décision

5A. *Le compte de résultat différentiel*

Le compte de résultat différentiel se présente en montants mais aussi en pourcentages par rapport au chiffre d'affaires.

Exemple : *gardons le même exemple avec un chiffre d'affaires annuel de 15 000 € (1 500 unités à 10 €), un coût variable unitaire de 0,74 € et des charges fixes de 5 000 € annuelles.*

	Quantité	Prix unitaire	Montants	% du CA
Chiffre d'affaires	1500	10	15 000,00	100,00%
Charges variables	1500	0,74	1 110,00	7,40%
Marge sur coût variable			13 890,00	92,60%
Charges fixes			5 000,00	
Résultat	1500	5,9267	8 890,00	59,27%

Remarque

Les pourcentages de MCV et de charges variables se complètent toujours à 100 % (car par définition : MCV + charges variables = chiffre d'affaires).

5B. *Coûts variables et prise de décision*

Ce compte de résultat différentiel n'a pas pour seul but de nous donner le résultat global. Il permet de mettre en évidence des dysfonctionnements dans la gestion et de donner au décideur des éléments pour l'aider dans sa prise de décision.

5B1. Structure des coûts

Le compte de résultat différentiel met en évidence comment se composent le coût et le résultat dégagé, notamment en terme de répartition entre charges variables et fixes.

Cette analyse va permettre de mettre en place éventuellement des actions correctrices de gestion et de faire des comparaisons avec les concurrents ou entre produits.

Dans notre exemple, on remarque que les charges fixes représentent un tiers du montant des ventes, ce qui est un montant assez élevé pour certains secteurs d'activité, alors qu'il peut être « correct » pour d'autres. C'est au décideur d'apprécier s'il y a lieu de mettre en œuvre des améliorations de gestion ou non.

De même, le résultat (ici un bénéfice) représente 59,27 % du chiffre d'affaires total, ce qui est un montant très élevé. Ceci peut être la conséquence du fait que c'est un produit

nouveau et que nous sommes leader sur le marché tout en ayant déjà une structure de production qui nous assure des coûts assez bas et une image commerciale qui nous permet de vendre relativement cher. Il est clair que ce haut niveau de résultat ne va pas se maintenir sans que l'entreprise n'agisse par une politique de différenciation commerciale, par des actions auprès de la concurrence…

5B2. Indicateur et simulateur d'aide à la décision

Ce compte de résultat va nous aider à faire des simulations pour prendre des décisions quant à la quantité à vendre ou au prix de vente. On peut réaliser ce tableau à l'aide d'un tableur et modifier ensuite, manuellement ou à l'aide d'outils de simulation, la quantité ou le prix de vente jusqu'à obtenir un résultat qui nous convienne.

Si vous possédez le tableur EXCEL, regardez à ce sujet l'outil « valeur cible » ou celui des scénarii.

- Fixation du prix de vente : en fonction d'une quantité de ventes espérée, on détermine le prix de vente, de sorte que le chiffre d'affaires total ne soit pas inférieur au seuil de rentabilité et que l'on dégage un certain bénéfice.
- Fixation des quantités à vendre : on se fixe un prix de vente désiré et on détermine ensuite les quantités par le même procédé (seuil de rentabilité + bénéfice).

Il est difficile de faire varier ces deux paramètres en même temps, même si certains outils peuvent nous y aider (cf. gestionnaire de scénarios). Dans la réalité on pratique par fourchettes.

En fonction d'une fourchette de prix de vente commercialement possible, on va déterminer les quantités à vendre (minimum et maximum) pour atteindre le seuil de rentabilité, ces quantités seront à leur tour ajustées en fonction de la réalité commerciale du marché et de notre structure productive, ce qui va nous permettre de revoir alors le prix de vente. Nous pourrions avoir le même raisonnement en partant des quantités que l'entreprise peut produire et vendre.

5B3. Prise de décision et paramètres non financiers

La comptabilité de gestion par les coûts variables est donc un bon indicateur pour le gestionnaire et va le guider dans sa prise de décision. Mais n'oubliez pas (surtout dans les exercices !!!!) de prendre en compte le fait que le décideur ne se base pas uniquement sur des critères financiers pour prendre ses décisions. On peut, par exemple, engager l'entreprise dans un nouveau secteur ou produit, simplement pour ne pas être à la traîne par rapport à ses concurrents, même si à court terme il est difficile d'atteindre le seuil de rentabilité.

Vos connaissances en « économie d'entreprise » sont une nouvelle fois un atout à mobiliser dans le cadre de vos réflexions sur la comptabilité de gestion.

Exercices autocorrectifs

Exercice 1

Vous pouvez effectuer cet exercice sur tableur. Mais n'oubliez pas que le jour de l'examen ce sera sur feuille, donc… entraînez-vous.

L'entreprise TOUROLL fabrique un seul modèle de rollers spécialisé dans les revêtements « tout terrain ». Elle vous fournit l'analyse des charges de l'exercice comptable précédent en fonction de leur variabilité.

- Charges purement fixes :
  – impôts et taxes : 2 350 € ;
  – charges financières : 28 400 € ;
  – dotations aux amortissements et provisions : 55 000 € .
- Charge purement variable : 61 480 € d'achats de matières premières pour la production.
- Charges semi-variables :
  – services externes : 62 000 € dont 70% de fixes ;
  – frais de personnel : 95 000 dont 20% de variables.

Lors de l'exercice comptable en question, TouRoll a vendu 10 200 paires de rollers à 65 € la paire.

1. ***Dresser un tableau des charges en faisant ressortir les fixes et les variables.***
2. ***Définir ce qu'est une charge semi-variable et expliquez pourquoi les deux charges semi-variables de cet exercice le sont.***
3. ***Déterminer graphiquement le seuil de rentabilité puis le retrouver par le calcul.***
4. ***Si on réussit à faire baisser le coût unitaire variable à 9 € et qu'on porte le prix de vente à 69 €, quel sera le nouveau seuil de rentabilité ?***

Exercice 2

La société MODTOU se demande s'il est réellement intéressant pour elle de continuer, dans les conditions actuelles, de commercialiser un certain type de sac de luxe, le « Marlyn ». Ce sac est acheté 25 € pièce et revendu 79 €. On constate que les charges fixes pour l'année N sont de 45 200 € et que les charges variables (hors coût d'achat des sacs) sont de 105 475 €. On a vendu 3 100 sacs au cours de l'année N. L'entreprise travaille 6 jours par semaine toute l'année et est fermée 4 semaines au mois d'août.

1. ***Dresser le tableau de calcul de la marge sur coût variable et du résultat. Comment s'appelle ce tableau ?***
2. ***Le résultat que vous venez de trouver n'est pas un résultat net, que manque-t-il comme type de « coût » ?***
3. ***Quel est le seuil de rentabilité ?***
4. ***Si on ne veut pas modifier le prix de vente, combien de sacs doit-on prévoir de vendre pour assurer le seuil de rentabilité ?***
5. ***Si on suppose que les ventes sont régulières tout au long de l'année, quand sera atteint ce seuil de rentabilité ?***
6. ***Que deviendrait le seuil de rentabilité si on devait augmenter les charges fixes pour les amener à 63 225 € ?***
7. ***Si on veut toujours maintenir à 79 € le prix de vente unitaire, combien doit-on vendre de sacs pour assurer ce nouveau seuil de rentabilité ?***
8. ***Pensez-vous que cette dernière hypothèse (question 7) soit possible ?***

Séquence 6

Budgets et analyse de la performance

1. Introduction, principaux concepts

Toute organisation, quelle que soit sa taille ou son importance, ne peut se passer de management pour organiser ses activités et prendre les décisions quant à ses orientations futures.

Pour une entreprise, par exemple, la stratégie peut être de faire évoluer le personnel vers plus de polyvalence et d'autonomie. Elle mettra en œuvre pour cela des objectifs concernant les procédés de recrutement ou le type de formation.

Pour une association, par exemple, l'objectif stratégique de se faire connaître au sein de sa commune peut passer par l'organisation d'une fête avec démonstration de ses activités. Pour réaliser une telle manifestation, outre le programme des festivités, l'association devra se préoccuper de toute la logistique nécessaire et de son financement (sonorisations, buvette, publicité…).

Ce financement va devoir être prévu à l'avance, afin de connaître les ressources financières dont elle disposera avant le début de la manifestation et qui lui serviront à régler les dépenses d'organisation, ainsi qu'au cours ou après la manifestation. Ces dernières seront des prévisions, car avant le jour précis de la manifestation, il est difficile pour l'association de connaître le nombre exact de billets qu'elle vendra ou la recette de la buvette.

Cette planification financière va donc se baser à la fois sur des ressources que l'organisation aura de manière sûre et certaine (l'utilisation d'un certain fonds ou l'obtention d'une subvention) et sur des prévisions budgétaires (ventes...).

De manière générale, les orientations stratégiques d'une organisation sont déclinées en de multiples objectifs et sous-objectifs, jusqu'au niveau opérationnel le plus élémentaire. Pour cela, on va définir des programmes d'actions à plus ou moins long terme et des budgets qui correspondent à des prévisions financières de tous les éléments correspondant à un programme d'action.

Nous voyons donc qu'ici plusieurs niveaux de décision de l'organisation interviennent et touchent à la fois à la stratégie, aux objectifs et à la budgétisation.

La notion de **temps** est omniprésente et guide, ou contraint, chacun de ces niveaux, de même que celle d'**incertitude**. Pour compenser cette incertitude, l'organisation va faire des prévisions en fonction des informations dont elle dispose (études de marché, environnement économique,…).

Les **budgets** vont servir à l'organisation pour clarifier ses objectifs mais également pour éviter tout problème de **trésorerie**. En effet, sans prévisions chiffrées et planifiées dans le temps, des découverts bancaires peuvent subvenir ou des surplus de trésorerie qui pourraient être investis par ailleurs ou utilisés pour d'autres étapes du projet.

En comptabilité générale, vous enregistrez un mouvement au moment de la survenance d'un évènement. Par exemple, une facture d'un client est enregistrée le jour de

sa création (créance client et TVA collectée entre autres). Au niveau des budgets, vous allez raisonner en **encaissements** et **décaissements**, comme avec votre propre porte-monnaie, si vous payiez et receviez tout votre argent en liquide. Pour la facture client, l'encaissement sera pris en compte au moment où le client règle effectivement. La TVA (Taxe sur la Valeur Ajoutée) collectée se retrouvera alors dans le calcul de fin de mois de TVA de l'entreprise.

L'établissement des budgets ne représente aucune difficulté technique particulière, mais soyez attentifs à bien rechercher les informations (même dans les exercices !) et à prendre en compte le temps : date réelle du décaissement ou de l'encaissement. N'oubliez pas qu'en terme de trésorerie, pour une certaine somme, l'échéance est tout aussi importante que le montant.

2. Comment budgétiser ?

Les deux exemples ci-dessus, revoir les politiques de recrutement et de formation d'une entreprise, ou organiser une fête communale, nous montrent que mettre en œuvre des budgets peut être très différent selon le programme d'action considéré. La notion de temps ne joue pas de la même manière et les zones d'incertitude ne se situent pas à la même échelle.

On peut néanmoins dégager une démarche commune à toute organisation, même si certains budgets ou critères n'auront pas la même importance (voire seront totalement inexistants) pour certains programmes d'action.

On va tout d'abord partir des recettes espérées par l'organisation, puis on en déduira un budget de production, d'approvisionnement et éventuellement un budget des investissements à réaliser. Ces ventes et divers achats vont nous permettre de mettre en évidence les liquidités financières dont nous devrons disposer. Les frais impliquent des décaissements au cours du déroulement du programme d'action (les charges elles-mêmes ainsi que la TVA associée). De plus, on va dresser le budget des charges hors production (des charges fixes pour la plupart). À l'issue de ces divers budgets, nous dresserons le budget global de synthèse qui nous donnera les sommes à décaisser et à encaisser au cours du temps. C'est ce que nous appellerons le **budget de trésorerie**.

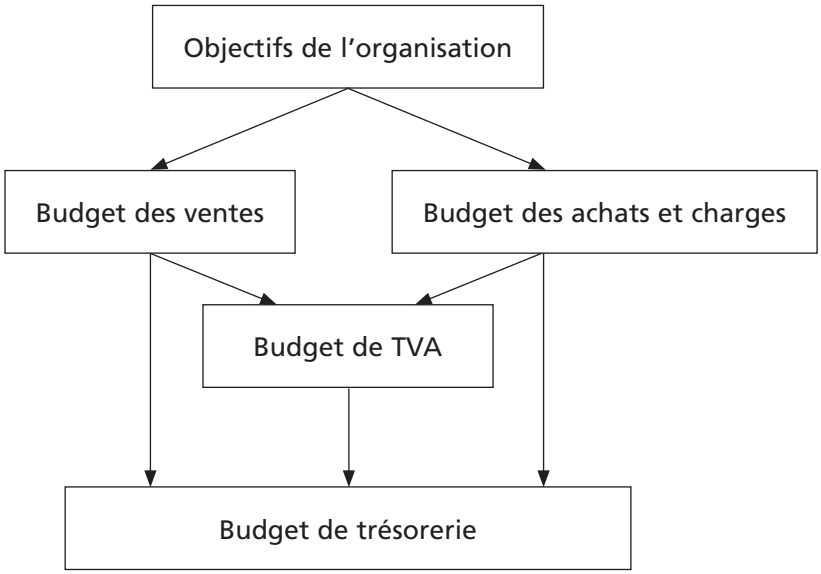
Ce schéma présente la version la plus simple de tous les budgets, nous verrons que certains d'entre eux peuvent faire l'objet de sous budgets. Par exemple, le budget des achats peut se subdiviser en budget des investissements, des approvisionnements, des charges hors production… Cela dépendra de l'organisation étudiée et de l'ensemble des données manipulées.

Lorsque le programme d'action sera terminé, ou lorsque certaines étapes seront achevées, ces divers budgets serviront à comparer les réalisations avec les prévisions afin d'apporter des actions correctrices si nécessaire.

Vous pouvez aussi trouver comme distinction :

- **budget des encaissements** : budget des ventes et de toutes les « rentrées d'argent » ;
- **budget des décaissements** : budget des achats, des charges et de la TVA ;

• **budget de trésorerie** : encaissements – décaissements.



3. Les divers budgets

Nous allons dresser chacun de ces budgets au travers d'un exemple, celui de la société ARTIBRICO qui vend du petit outillage et des articles de quincaillerie à des artisans. Elle est assujettie à la TVA au taux de 19,60 %.

Fin août de l'année N, le bilan provisoire fait ressortir les éléments suivants :

		Échéances de paiement		
	Total	Septembre	Octobre	Novembre
Créances clients	20 210	20 000	210	
Disponibilités	2 500			
Dettes d'approvisionnements	15 875	3 540	9 080	3 255
Dettes fiscales (impôts)	2 287	800	1 487	

Les prévisions d'activités et de charges sont les suivantes :

	Échéances		
	Septembre	Octobre	Novembre
Ventes (HT)	22 000	23 000	19 500
Approvisionnements (HT)	11 200	13 800	9 100
Autres charges	10 000	6 500	6 500
Dotations aux amortissements	950	950	950

Les ventes sont réglées à 40% comptant et 60% le mois suivant. Les approvisionnements sont réglés à 20% comptant et 80% le mois suivant.

Parmi les « autres charges », 4 000 € mensuels (les salaires) ne sont pas soumis à la TVA et le reste est donné en HT.

La TVA à payer se calcule toujours en fin de mois mais cette taxe n'est réglée à l'administration fiscale que le 22 du mois suivant. Fin août la TVA à décaisser a été calculée à 6 800 €.

3A. Budget des ventes

Le budget des ventes présente les prévisions de ventes. Il est basé sur les ventes passées, les nouveaux projets mercatiques, l'analyse des flux saisonniers passés…

De manière générale, le **budget des encaissements**, présente tous les encaissements prévus : ventes et remboursements financiers en tout genre dont l'entreprise est destinataire.

À partir du montant hors taxes (HT) prévu des ventes, on va rajouter la TVA. Ceci est dû au fait que toute prévision et tout enregistrement comptable des ventes se fait sur des montants hors taxes car l'entreprise ne supporte pas la totalité du coût de la TVA (cf. cours de 1re année). Cette TVA collectée va se retrouver ensuite dans le budget de TVA, c'est pourquoi nous allons la calculer ici alors qu'elle n'est pas indispensable à ce niveau : tout pourrait être en TTC (toutes taxes comprises) vu que les règlements de clients se font en TTC.

S'il s'agit d'une organisation non soumise à la TVA (comme certaines associations), on présentera les budgets directement en TTC.

Vous avez vu en première année l'enregistrement comptable des ventes et l'établissement du bilan et du compte de résultat. Je vous rappelle que dans ces deux documents, les éléments de ventes et d'achats, sont enregistrés en HT et que la TVA s'enregistre dans des comptes de dettes fiscales.

Pour l'entreprise ARTIBRICO, les prévisions de ventes pour chacun des trois prochains mois sont respectivement de 22 000 €, 23 000 € et 19 500 €. Son budget des ventes se présente donc ainsi :

Budget des ventes

				Échéances		
	HT	TVA collectée	TTC	Septembre	Octobre	Novembre
Créances clients antérieures (1)			20 210,00	20 000,00	210,00	
Ventes septembre (2)	22 000,00	4 312,00	26 312,00	10 524,80	15 787,20	
Ventes octobre	23 000,00	4 508,00	27 508,00		11 003,20	16 504,80
Ventes novembre	19 500,00	3 822,00	23 322,00			9 328,80
TOTAL des encaissements relatifs aux ventes				30 524,80 (3)	27 000,40	25 833,60

(1) Cf. le 1er tableau : échéances de paiement des créances clients au bilan.

(2) Les ventes prévues en septembre s'élèvent à 22 000 € HT, mais les règlements des clients se font en TTC, il faut donc tout d'abord transformer les sommes en TTC mais étaler les règlements pour 40 % le mois de la vente et 60 % le mois suivant.

(3) Ce chiffre représente le montant des règlements clients que l'on doit recevoir en septembre. Il provient (pour 20 000 €) des anciennes créances clients trouvées au bilan et de l'encaissement d'une partie (40 %) des ventes de septembre. En aucun cas il ne s'agit donc des ventes de septembre.

Les trois montants totaux seront reportés au niveau des encaissements du budget général de trésorerie.

3B. Budget des achats et autres charges

Ce budget recouvre toutes les dépenses auxquelles doit faire face l'organisation. De manière générale, il présente tous les décaissements prévus, on l'appelle aussi le **budget des décaissements**.

De même que pour les achats soumis à la TVA, on va faire apparaître la TVA déductible afin de pouvoir construire ensuite le budget de la TVA. Nous vous rappelons qu'en comptabilité générale, les achats sont enregistrés en HT dans les comptes de charges et que leur TVA est enregistrée dans les comptes de « TVA déductible ».

Budget des achats et autres charges

				Échéances		
	HT	TVA déductible	TTC	Septembre	Octobre	Novembre
Dettes fournisseurs antérieures			15 875,00	3 540,00	9 080,00	3 255,00
Achats septembre (1)	11 200,00	2 195,20	13 395,20	2 679,04	10 716,16	
Achats octobre	13 800,00	2 704,80	16 504,80		3 300,96	13 203,84
Achats novembre	9 100,00	1 783,60	10 883,60			2 176,72
Total achats				6 219,04	23 097,12	18 635,56
Dettes fiscales du bilan			2 287,00	800,00	1 487,00	
Autres charges sans TVA (2)			12 000,00	4 000,00	4 000,00	4 000,00
Autres charges avec TVA (3)	11 000,00	2 156,00	13 156,00	7 176,00	2 990,00	2 990,00
TOTAL des décaissements				18 195,04	31 574,12	25 625,56

(1) Comme pour les ventes on doit tout d'abord transcrire le budget en TTC, vu que l'entreprise va payer les montants TTC à ses fournisseurs. Puis ensuite on répartit ces décaissements de charges à raison de 20% le mois de leur survenance et 80% le mois suivant.

(2) Il s'agit des 4 000 € mensuels de salaires.

(3) Il s'agit des « autres charges » auxquelles on soustrait les 4 000 € mensuels de salaires. Elles doivent être traduites en TTC Pour ces charges, il n'y a pas de décalage de paiement (on règle immédiatement) précisé dans le texte de l'exercice. En septembre cela donne 6 000 € d'autres charges soumises à la TVA (10 000 – 4 000), soit en TTC 7 176 € (6 000 x 1,196).

Ce budget, appelé budget des achats et autres charges, contient tous les frais pour lesquels on va faire un règlement. C'est donc le budget des décaissements. On peut le subdiviser en :

– budget des investissements ;
– budget des approvisionnements ;
– budget de production ;
– budget hors production ;
– budget de commercialisation.

3B1. Budget des investissements

Le budget des investissements, comme pour tout budget, peut être réalisé au niveau général de l'entreprise ou pour un projet particulier. Dans ce dernier cas, on ne mentionnera les conséquences financières que de l'investissement considéré. Le choix du type de financement va avoir une grande importance sur le budget.

Le paragraphe suivant concerne essentiellement les étudiants de l'option ARLE mais peut se trouver dans tout exercice lorsqu'on vous fournit des données chiffrées concernant un emprunt.

Si vous avez un exercice sur un plan de financement (voir séquence 7), n'oubliez pas de reporter dans le budget des investissements les sommes réellement décaissées suite à l'obtention d'un emprunt, en ne négligeant pas la notion de temps. Par exemple, le jour où vous obtenez le montant prêté peut être différent du jour où vous réglez le montant correspondant à l'achat de votre investissement, de même, périodiquement, vous aurez les remboursements (capital + intérêts) à décaisser.

Par exemple, si une entreprise obtient un prêt d'un particulier de 3 000 € au mois de janvier, à rembourser en trois fois, à raison de 1 000 €, en commençant deux mois après la remise des fonds ; et que ce prêt est destiné à financer un investissement de 2 850 € à régler en février, le budget des investissements concernant cette opération se traduira par :

	Février	Mars	Avril	Mai
Décaissements	2 850	1 000	1 000	1 000

Ne pas oublier qu'au niveau des encaissements il y aura 3 000 € à rajouter pour le mois de janvier concernant l'encaissement de la somme prêtée.

3B2. Budget de production

Suite aux prévisions et au planning de production, on va déterminer un budget pour les approvisionnements et les charges de production.

3B3. Budget hors production

Il s'agit de toutes les charges générales ne concernant pas directement la production : charges d'administration, de personnel…

3B4. Budget de commercialisation

On va répertorier tous les frais de promotion et de distribution.

3C. *Budget de la TVA*

Comme vous l'avez vu en première année, la TVA à reverser à l'administration est calculée en fin de mois par soustraction de la TVA déductible sur les achats et autres frais, de la TVA collectée sur les ventes. Si la somme due est négative on parle de crédit de TVA qui viendra s'imputer (en négatif) sur le calcul de la TVA du mois suivant.

Pour établir le budget de TVA, il suffit de reprendre les montants dégagés dans les deux budgets précédents.

Ne pas oublier, que le texte du sujet vous informe que la TVA à payer se calcule toujours en fin de mois mais qu'elle n'est réglée que le 22 du mois suivant. Il y a donc un décalage d'un mois entre le calcul et le règlement.

Budget de la TVA

	Échéances		
	Septembre	Octobre	Novembre
TVA collectée (1)		4 312,00	4 508,00
– TVA sur achats (2)		2 195,20	2 704,80
– TVA sur autres charges (3)		1 176,00	490,00
TVA à décaisser	**6 800,00 (4)**	**941,00**	**1 313,20**

(1) Cf. budget des ventes.

(2) Cf. budget des achats.

(3) Pour la « TVA sur autres charges », il faut retrouver le montant de la TVA à partir des montants HT pour les divers mois. Par exemple pour septembre, le montant HT des « autres charges » soumises à la TVA est de 6 000 € (10 000 € de « autres charges » HT, auxquelles on soustrait 4 000 € de salaires). La TVA est donc de 1176 € (6 000 X 19,60%).

(4) Le texte spécifie que « Fin août la TVA à décaisser a été calculée à 6 800 €. ».

3D. Budget de trésorerie

Le budget de trésorerie fait la synthèse de tous les budgets précédents. Il donne les flux nets de trésorerie de chaque mois (total des encaissements - total des décaissements) qui représentent l'ensemble des liquidités nécessaires et disponibles.

Á partir du montant des liquidités initiales (ici celles trouvées au bilan de fin août), on va calculer le solde net de trésorerie prévu en fin de mois. Si celui-ci est négatif, ou inférieur à un certain « niveau de sécurité », il faudra que l'entreprise recourt au crédit bancaire, à l'escompte, renégocie ses délais de règlements fournisseurs ou clients, …

Budget de trésorerie

	Échéances		
	Septembre	Octobre	Novembre
Encaissements	**30 524,80**	**27 000,40**	**25 833,60**
Achats et autres charges	18 195,04	31 574,12	25 625,56
TVA à décaisser	6 800,00	941,00	1 313,20
Décaissements	**24 995,04**	**32 515,12**	**26 938,76**
Flux net de trésorerie	**5 529,76**	**–5 514,72**	**–1 105,16**
Trésorerie début de mois	2 500,00	8 029,76	2 515,04
Trésorerie fin de mois	**8 029,76**	**2 515,04**	**1 409,88**

On constate que les flux nets de trésorerie d'octobre sont négatifs (l'entreprise doit « sortir » plus d'argent qu'elle « n'en rentre »). Globalement, vu que l'entreprise avait une trésorerie importante fin septembre, cela permet de compenser ce problème. En revanche, si cela se reproduit dans le futur, les gestionnaires devront agir pour corriger le problème : augmenter les encaissements, diminuer les décaissements, utiliser des réserves financières (rendre liquides des placements), obtenir un crédit, renégocier les échéances de règlement client ou fournisseur…

Remarque

Vous noterez que dans le tableau initial des charges il est mentionné des amortissements (950 € par mois), et qu'ils n'ont jamais été pris en compte dans les budgets. Ceci est normal car les amortissements sont bien une charge pour l'entreprise mais elle est « non-décaissée ».

4. L'analyse des budgets et de leur réalisation

L'analyse des écarts entre la réalisation concrète et les sommes prévues aux budgets est une phase importante qui permet :

- de savoir à tout moment où nous en sommes financièrement par rapport à nos prévisions ;
- de prendre des actions correctrices en cas de dérives justifiées ou injustifiées ;
- de réajuster nos prévisions en fonction des premières réalisations.

Ce processus va permettre à l'entreprise « d'apprendre » et de réaliser de meilleures prévisions, des budgets plus réalistes et de corriger les dérives.

La budgétisation donne une idée plus précise de l'application des objectifs généraux de l'organisation. Elle permet de dégager la trésorerie prévisionnelle, mais aussi d'analyser l'implication et les conséquences des diverses décisions de gestion envisagées sur l'état financier de l'organisation. En effet, tous ces budgets peuvent être informatisés et servir ainsi de base pour des simulations concernant les diverses options qui se présentent aux décideurs.

Nous vous rappelons que ces budgets peuvent être réalisés au niveau global de l'organisation ou au niveau d'une fonction ou d'un projet. De même, ils peuvent concerner soit la gestion quotidienne, soit des activités ou projets totalement nouveaux. Dans ce dernier cas, les budgets manipuleront essentiellement des prévisions comme données chiffrées.

Ces budgets permettent à l'organisation d'évaluer :

- l'équilibre global de la trésorerie ;
- l'équilibre financier (bilan prévisionnel) ;
- l'équilibre dans la formation du résultat (compte de résultat prévisionnel) ;
- les divers scénarios et la faisabilité d'un projet.

Les budgets servent donc à constater les réalisations du passé, et le plus souvent, à planifier les données financières des projets futurs. En général, les nouveaux budgets sont faits en tenant compte des budgets anciens et de leur comparaison à la réalité.

Lors du déroulement d'un projet l'analyse de la différence entre les budgets prévus et la réalisation concrète peut amener le gestionnaire à décider des actions correctrices.

Exercices autocorrectifs

Exercice 1

L'entreprise de bâtiment TouBati a fait ses prévisions en terme d'objectifs pour le 1er trimestre de l'année N, elle vous demande de l'aider à mettre en place une gestion prévisionnelle.

Elle vous présente tout d'abord l'état de certains de ses comptes au 01/01/N :

N° de compte	Intitulé	Solde (D = débit, C = crédit)	Échéances prévues
401000	Fournisseurs	C = 10 200	Tout en janvier
411000	Clients	D = 35 460	70% en janvier, 20% en février et le reste en mars
430000	Organismes sociaux	C = 6 200	Tout en janvier
445510	TVA à décaisser	C = 7 100	Tout en janvier
512000	Banque	D = 55 500	

Elle a également chiffré le niveau de ses recettes et dépenses :

Type	Janvier	Février	Mars	Échéances prévues
Achats divers (HT)	12 500	11 800	10 400	Tous les paiements se font à 30 jours
Ventes (HT)	32 000	31 000	32 000	2/3 réglés au comptant et le reste à 60 jours
Salaires nets	11 250	11 250	11 250	Charges salariales et patronales en sus : 80 % à payer le mois suivant
Impôts	0	2 500	0	
Achat d'une bétonnière (HT)			10 000	Paiement comptant

Toutes les TVA sont au taux normal de 19,60 %. Le solde de TVA calculé en fin de mois se règle le mois suivant.

1. ***Pourquoi dans le tableau ci-dessus, avoir séparé les « achats divers » de l'« achat d'une bétonnière » ?***
2. ***Établir le budget prévisionnel des achats en distinguant les montants HT, de la TVA et des montants TTC.***
3. ***Établir le budget prévisionnel de trésorerie concernant les achats.***
4. ***Établir le budget prévisionnel des décaissements concernant la TVA.***
5. ***Établir le budget des décaissements.***
6. ***Établir le budget des encaissements.***
7. ***Établir le budget de trésorerie. Que pensez-vous du résultat obtenu et que conseillez-vous à l'entreprise ?***
8. ***Supposons que le meilleur et principal client qui règle environ 15 000 € par mois ne puisse plus honorer ses dettes et que la trésorerie de l'entreprise n'était que de 30 000 € début janvier. Établir le nouveau budget de trésorerie. Que conseillez-vous à l'entreprise ?***

Exercice 2

Soit une section d'un club sportif (géré sous forme d'association) qui tient un budget prévisionnel pour les prochains mois. Le budget de la section est le suivant : **Budget de trésorerie.**

	Échéances		
Mois	M	M+1	M+2
Encaissements	1 800,00	2 000,00	1 900,00
Décaissements	1 600,00	2 100,00	2 000,00
Trésorerie début de mois	100,00	300,00	200,00
Trésorerie fin de mois	300,00	200,00	100,00

1. ***Pourquoi ne fait-on pas référence à la TVA dans ce budget ?***
2. ***Que pensez-vous de ce budget ?***
3. ***À la fin du mois M, la section fait le point sur son budget et constate que les encaissements sont conformes à ceux prévus, mais que ses frais ont été supérieurs de 10 % à ceux budgétés. Refaire le budget de trésorerie.***
4. ***Analyser ce nouveau budget et proposer des alternatives de gestion.***

Séquence 7

Rentabilité et financement d'un investissement

Cette séquence est explicitement au programme de ceux qui font l'option ARLE mais il est conseillé de le lire à titre de culture générale pour le BTS par les étudiants de l'option DA.

Avant d'engager un investissement dans un nouveau bien de production, de communication, ou dans tout nouveau projet, on évalue l'opportunité de ce dernier au regard de critères techniques, commerciaux ou économiques. En effet, investir implique de l'énergie et des flux financiers importants : une dépense importante au moment de l'acquisition du bien, et des recettes futures, souvent étalées dans le temps, engendrées par la valeur ajoutée générée par ce nouveau bien ou projet.

Nous allons dans ce chapitre aborder les méthodes de calcul qui permettent d'évaluer les implications financières d'un projet d'investissement.

L'exemple suivant va nous servir à illustrer le cours.

Un dirigeant hésite entre l'acquisition de deux matériels (projet 1 ou projet 2) qui peuvent être réalisés dès ce jour. Chacun permet d'investir dans une immobilisation (matériel de production) différente.

Éléments	Projet 1	Projet 2
Coût d'achat	30 500	37 000
Durée de vie	5 ans	5 ans
Augmentation annuelle prévue du chiffre d'affaires grâce au projet	23 000	25 000
Charges décaissables annuelles prévues dues au projet (matières premières et main-d'œuvre)	12 000	13 000

Dans les deux cas, le matériel sera amorti selon le système linéaire. On suppose que le taux d'imposition de l'entreprise est de 33 1/3 % (33,33 %). De même, on suppose que les charges et l'augmentation du chiffre d'affaires sont constantes (identiques) pendant toute la durée de vie de chacun des projets.

1. Flux nets de trésorerie

Pour savoir si un investissement est financièrement rentable, il faut comparer d'une part, les décaissements lors de l'achat (ou le coût du crédit à rembourser au cours du temps) et de l'exploitation du bien, et d'autre part, les encaissements futurs prévus grâce au nouvel investissement.

Nous allons donc calculer et comparer des flux nets de trésorerie qui se rapportent à l'investissement.

1A. Calcul des flux nets de trésorerie

Les flux nets de trésorerie représentent **le solde net des flux de trésorerie engagés par l'investissement**. Ils sont composés de produits encaissables (les « recettes » produites par l'investissement) et de charges décaissables (les dépenses).

Les recettes se concrétisent, dans notre exemple, par de nouvelles ventes que pourra réaliser l'entreprise grâce à l'investissement. Elles se mesurent donc par l'augmentation supplémentaire du chiffre d'affaire.

Parmi les dépenses on trouve :

- L'achat initial (au « coût d'achat » = prix d'achat + frais annexes d'achat). Dans un premier temps, on va supposer qu'on débourse la totalité du coût d'achat le jour de l'acquisition du bien. Mais dans la réalité on peut faire un emprunt, c'est ce que nous verrons dans une autre séquence de ce cours.
- Les dépenses supplémentaires d'exploitation : matières premières, main-d'œuvre…

Remarque

L'amortissement de la nouvelle immobilisation n'est pas une charge décaissée, elle ne figurera donc pas dans les charges.

- L'impôt supplémentaire sur les bénéfices engendré par l'investissement. Il ne faut pas oublier que l'amortissement, qui n'est pas une charge décaissée, participe à la formation du résultat comptable, résultat dont dépend le calcul de l'impôt. Il faudra donc prendre en compte l'amortissement, puis le soustraire des charges décaissées.

Remarque

Les flux net de trésorerie sont aussi appelés capacité d'autofinancement (CAF).

Application à notre exemple

Pour connaître le montant de l'impôt supplémentaire engendré par chaque projet, on passe par le calcul du résultat net comptable. À partir de ce dernier, on calcule l'impôt, qui viendra diminuer le résultat, puis, ensuite, on réintègre l'amortissement vu que ce n'est pas un décaissement (pas un flux de trésorerie), pour déterminer, enfin, le résultat réel.

Éléments	Projet 1	Projet 2
Recettes supplémentaires :	23 000,00	25 000,00
Charges supplémentaires :		
Main-d'œuvre et matière première	12 000,00	13 000,00
Amortissement (ex : 30500/5)	6 100,00	7 400,00
Résultat avant impôts	4 900,00	4 600,00
Charge supplémentaire : impôt sur les bénéfices (ex : 4900*33,33%)	1 633,33	1 533,33
Résultat net	3 266,67	3 066,67
Charge non décaissable à réintégrer : amortissement	6 100,00	7 400,00
FLUX NET DE TRESORERIE annuel	9 366,67	10 466,67

Ce tableau présente les flux nets de trésorerie annuels pour une année, car dans l'exemple, on a supposé que toutes les recettes et dépenses étaient constantes au cours des cinq ans de la vie des deux projets. Si ce n'était pas le cas il faudrait faire un calcul des flux nets de trésorerie pour chacune des années de la durée de vie du projet.

2. Valeur actuelle nette et choix d'investissement

Si quelqu'un vous propose de vous donner 2 000 € euros et vous donne le choix entre vous les donner aujourd'hui ou dans 10 ans ; vous préférerez sûrement les recevoir aujourd'hui, même si vous n'en avez pas l'utilité immédiate. Ceci parce que compte tenu de l'augmentation générale des prix, des intérêts bancaires que vous pouvez retirer de leur placement… 2 000 € aujourd'hui ne valent pas la même chose que dans 10 ans. Ceci fonctionne exactement sur le même principe pour les flux nets de trésorerie.

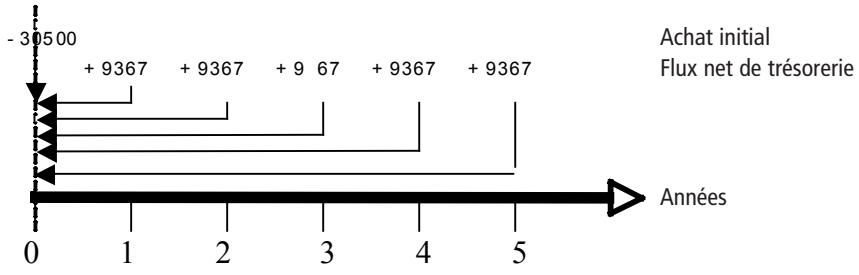
En effet, le projet numéro 1 rapporte 9 367 € la première année, de même que les quatre années suivantes. Cette somme, que dégagera l'entreprise la 5e année qui suit l'investissement, ne vaut pas à ses yeux celle dont elle va bénéficier la 1re année. En effet, si au moment de l'acquisition de l'investissement (année 0), l'entreprise disposait de la somme produite lors de la dernière année du projet, elle pourrait placer cette somme, ou l'investir dans un autre projet ayant une rentabilité plus rapide ou supérieure. De plus, ce raisonnement ne tient pas compte de l'incertitude qui augmente avec le temps, ou des désirs de l'entreprise qui peuvent varier.

C'est pourquoi nous allons tenir compte des décalages dans le temps et actualiser ces gains.

2A. *La notion d'actualisation*

Pour en revenir à notre investissement, nous avons vu qu'en général la dépense (achat du bien) se fait au temps 0 alors que les recettes sont étalées dans le temps. Pour plus d'homogénéité, on compare donc les recettes et les dépenses à une même période : le jour d'acquisition du bien (ou plus tard). C'est-à-dire que toutes les dépenses et recettes futures vont être « ramenées » au jour d'acquisition de l'investissement. On va les estimer au moment de leur survenance, puis les « ramener » au temps 0.

Dans notre exemple, pour le projet n° 1, les retombées financières (flux nets de trésorerie) sont de 9 367 € à l'issu de chacune des cinq années. On a donc le schéma suivant :



Le phénomène qui consiste à tout « ramener » à une même date s'appelle **l'actualisation.**

2B. *Actualisation des flux nets de trésorerie*

On va se placer à l'époque 0, le jour où on acquiert le bien, et ramener tous les flux nets de trésorerie à cette date en tenant compte d'un taux d'actualisation. Ce taux correspond à la rémunération des capitaux souhaitée par les actionnaires de l'entreprise ou les autres prêteurs.

FNi = Flux Net de Trésorerie de l'époque i (en fin de période)
n = périodes (années, mois ...), la durée de vie du projet
t = taux d'actualisation

FN cumulés actualisés = $FN_1(1+t)^{-1} + FN_2(1+t)^{-2} + FN_3(1+t)^{-3} + ... + FN_n(1+t)^{-n}$

Cas particulier (que l'on trouve souvent dans les exercices !) : **si** chaque année les **flux nets de trésorerie sont identiques** (FN1 = FN2 = FN3...) alors la formule devient :

FN cumulés actualisés = FN1 (1 – (1+t)-n)/t

Ceci est le cas dans notre exemple où tous les flux sont identiques au cours des cinq années.

2C. Calcul de la VAN

La valeur actuelle nette représente le surplus de trésorerie (ou le déficit, si elle est négative) dégagé à l'époque 0 par le projet d'investissement.

Donc :

VAN = FN cumulés actualisés – investissement initial

Remarquez qu'ici il n'y a rien à actualiser car les flux nets de trésorerie sont déjà actualisés à cette « date 0 », qui est également la date à laquelle on réalise l'investissement.

Soit I l'investissement initial :

$VAN = FN1(1+t)^{-1} + FN2(1+t)^{-2} + FN3(1+t)^{-3} + ... + FNn(1+t)^{-n} - I$

Soit **dans le cas des flux identiques** à chaque période :

$VAN = FN1\ (1 - (1+t)^{-n})\ /t - I$

Exemple : *si le taux du coût moyen pondéré du capital désiré par l'entreprise (taux d'actualisation) est de 10 %, calculons les VAN des deux projets :*

Projet 1 : VAN = FN (1 - $(1+t)^{-n}$)/t - I = 9 366,67 (1-$(1+0,1)^{-5}$)/0,1 – 30 500 = 5 007,04 €

Projet 2 : VAN = FN (1 - $(1+t)^{-n}$)/t - I = 10 466,67 (1-$(1+0,1)^{-5}$)/0,1 – 37 000 = 2 676,90 €

2D. Choix d'un investissement

Si on a le choix entre plusieurs investissements et que **l'on ne s'occupe que de l'aspect financier**, on écartera tous ceux dont la VAN est négative, car le montant de l'investissement ne pourra jamais être « récupéré ». De plus, on prendra l'investissement qui a la VAN la plus élevée car il nous donne un meilleur gain.

Dans les exercices, n'oubliez pas de spécifier que ces dernières conclusions... sont basées **uniquement sur l'aspect financier**. En effet, dans la réalité, il se peut qu'un décideur choisisse un projet ayant une VAN un peu moins importante qu'une autre si, par ailleurs, le projet lui rapporte un avantage concurrentiel profitable pour le futur (avantage technique, innovant ou commercial, qualité et réutilisabilité du bien acquis, capacité de l'entreprise à s'en servir efficacement, intérêt commercial de la production supplémentaire...).

Dans notre exemple

La VAN du premier projet (5 007,04 €) est supérieure à celle du second (2 676,90 €), leurs durées de vie sont identiques, donc, en ne tenant compte que de l'aspect financier, on choisira le projet numéro 1.

2E. *Délai de récupération du capital investi*

Dans la décision d'investir dans tel ou tel projet ou immobilisation, on peut aussi faire jouer le délai de récupération de la somme initialement investie. On optera pour le projet qui va nous permettre de récupérer le plus rapidement la somme investie dans le coût d'acquisition.

Cependant, ce critère ne peut être pris en compte qu'en complément de celui de la VAN.

La question est de se demander au bout de combien de temps l'entreprise va récupérer son investissement initial. On va donc calculer le nombre de périodes nécessaires au recouvrement de la mise initiale. Dans le cas de flux nets de trésorerie constants on aura :

Délai de récupération = Investissement/Flux nets de trésorerie

Dans tous les cas, ce délai doit être inférieur à la durée de vie du projet, sinon celui-ci sera considéré comme non rentable. En effet, si ce délai est supérieur à la durée de vie du projet cela revient à dire que le coût d'achat initial ne pourra jamais être « récupéré ».

Exemple :

Projet 1 : délai de récupération du capital investi = 30 500/9 366,67 = 3,26 ans

Projet 2 : délai de récupération du capital investi = 37 000/10 466,67 = 3,53 ans

Le projet 1 paraît donc moins risqué car on récupère l'investissement initial un peu plus rapidement.

Avez-vous remarqué qu'ici on parle de flux nets de trésorerie mais qu'on ne les actualise pas ?

En effet, le critère du délai de récupération étant approximatif, on se contente de cumuler les flux sans tenir compte du fait qu'ils sont prévus à des époques différentes.

Une autre manière de calculer ce délai, surtout lorsque les flux nets ne sont pas identiques, est de cumuler ces flux pour voir à quel moment ce cumul atteint (puis dépasse) la somme initialement investie.

Nous avons donc vu comment choisir entre deux ou plusieurs projets d'investissement, en tenant compte uniquement de l'aspect financier.

Jusqu'ici on a toujours supposé que le coût d'achat de l'investissement était payé directement par l'acquéreur le jour de l'acquisition. Or, peu d'entreprises ont suffisamment de liquidités disponibles pour pouvoir intégralement débourser le coût de l'investissement le jour de son acquisition. Nous allons donc maintenant nous intéresser aux divers modes de financement d'un investissement.

3. Modes de financement d'un investissement

Plusieurs possibilités de financement s'offrent à une organisation pour financer son investissement. Ces modes de financement peuvent se combiner. Il n'est pas rare, par exemple, de financer l'acquisition d'un nouveau matériel en partie sur fonds propres (autofinancement) et en partie à crédit (emprunt).

3A. *L'autofinancement*

C'est une source de financement interne : l'entreprise va se servir de ses propres ressources qu'elle a mis en réserve auparavant.

3B. *L'augmentation de capital*

Elle se réalise par appel public à l'épargne (pour les sociétés importantes), ou simplement auprès des actionnaires actuels. Ce mode de financement est réservé aux investissements lourds.

3C. *L'emprunt*

Les sociétés qui peuvent faire appel public à l'épargne peuvent émettre des obligations. L'emprunt obligataire sera alors réalisé auprès de toutes les personnes qui vont souscrire des obligations.

Les établissements de crédit, principalement les banques, octroient des prêts que l'on appelle indivis (car il n'y a qu'un seul prêteur). Nous allons détailler ce mode de financement dans la prochaine partie.

3D. *Le crédit-bail*

C'est une location (on paye chaque mois un loyer qui rentre dans nos charges) avec une option d'achat à la fin du contrat de location, option qui est prévue dans le contrat initial (prix d'achat déterminé).

Le bien loué ne fait pas partie du patrimoine (immobilisations) de l'entreprise, contrairement aux autres modes de financement.

3E. *La subvention d'investissement*

Dans certains domaines spécifiques ou innovants, l'organisation peut recevoir une subvention lorsqu'elle investit. Cette subvention peut s'assimiler à un don ou prendre la forme d'un prêt sans intérêt (taux 0).

4. Financement par emprunt

Le plan de financement présente le détail de la couverture des besoins de financement liés à l'investissement.

On va étudier uniquement les emprunts indivis dont le remboursement se réalise en général sur plusieurs années.

Un emprunt est caractérisé par :

- un montant (ex : 50 000 €) ;
- un taux (ex : 3 %) ;
- une durée (ex : 5 ans) ;

- une date d'échéance (ex : le 01/06/N) et une date de paiement de la première annuité ;
- une périodicité de remboursement (ex : l'année, le mois, le trimestre...) ;
- une modalité de remboursement soit :
  - par remboursement *in fine,*
  - par amortissement constant,
  - par annuité constante.

Dans tous les cas, le montant à payer chaque période, le plus souvent l'année (ce que l'on appelle une « annuité ») est constitué d'une partie de remboursement du capital et d'une partie du paiement d'intérêts.

Annuité = amortissement + intérêts

De même, dans tous les cas, les intérêts sont calculés sur le capital restant dû en début de période :

Intérêts = capital dû en début de période X taux d'intérêt

Pour la suite du cours on va travailler sur un exemple.

Montant de l'emprunt : 50 000 €
Taux annuel : 4 %
Date d'emprunt : 01/07/N-1
Date de première échéance : 01/07/N
Durée : 5 ans

4A. Remboursement in fine

L'emprunt est remboursé en fin de contrat. À chaque échéance, on ne paye que le montant des intérêts, qui sont calculés par mois entier.

Date de remboursement	Capital restant dû	Intérêts	Amortissement	Annuité	Capital dû en fin de période
01/07/N	50 000	2 000	0	2 000	50 000
01/07/N+1	50 000	2 000	0	2 000	50 000
01/07/N+2	50 000	2 000	0	2 000	50 000
01/07/N+3	50 000	2 000	0	2 000	50 000
01/07/N+4	50 000	2 000	50000	52 000	0

Si on avait emprunté le 20/04/N et que les échéances se font en fin d'année civile (ici le 31/12/N), les intérêts de la première année auraient été calculés pour neuf mois entiers, soit : 50 000 X 4% X 9/12.

On aurait également eu une ligne pour l'année N+5 avec un montant correspondant au trois mois restants.

4B. Remboursement par amortissements constants

Les amortissements sont constants, les intérêts varient car la somme restant due le 01/07 de chaque année va diminuer au cours des années.

On procède dans l'ordre.

1. Calcul de l'amortissement
2. Calcul des intérêts
3. Calcul du capital restant dû en fin de période

L'amortissement est de 50 000/5 soit 10 000 € annuel.

Date de remboursement	Capital restant dû	Intérêts	Amortissement	Annuité	Capital dû en fin de période
01/07/N	50 000	2 000	10 000	12 000	40 000
01/07/N+1	40 000	1 600	10 000	11 600	30 000
01/07/N+2	30 000	1 200	10 000	11 200	20 000
01/07/N+3	20 000	800	10 000	10 800	10 000
01/07/N+4	10 000	400	10 000	10 400	0

4C. *Remboursement par annuités constantes*

L'emprunteur remboursera toujours la même somme.

Notons :

→ V : montant de l'emprunt
→ i : taux
→ n : durée de l'emprunt
→ a : montant de l'annuité constante

On a :

$$a = \frac{V \times i}{1-(1+i)^{-n}}$$

C'est la seule formule à retenir ! (sauf si vous pouvez la retrouver)

Méthode (à faire dans l'ordre)

1. Calculer l'annuité constante et la reporter dans tout le tableau.
2. Pour chaque période, calculer le montant de l'intérêt sur le capital restant dû en début de période.
3. Pour chaque période, calculer l'amortissement (= annuité - intérêt). Pour la dernière annuité, arrondir de quelques centimes si nécessaire.

Pour le dernier amortissement, il peut être nécessaire de l'arrondir de quelques centimes (pour que la somme totale des amortissements corresponde bien à la somme empruntée).

Exemple :

$$a = \frac{V \times i}{1-(1+i)^{-n}} = \frac{50000 \times 4\%}{1-1{,}04^{-5}} = 11231{,}3557$$

montant qui sera arrondi à 11 231,36 €

Les intérêts de la première année sont donc toujours de 2 000 € (50 000 X 4%), donc l'amortissement est de 9 231,36 €. On peut maintenant dresser le tableau en tenant compte de la méthode ci-dessus.

Date de remboursement	Capital restant dû	Intérêts	Amortissement	Annuité	Capital dû en fin de période
01/07/N	50 000,00	2 000,00	9 231,36	11 231,36	40 768,64
01/07/N+1	40 768,64	1 630,75	9 600,61	11 231,36	31 168,03
01/07/N+2	31 168,03	1 246,72	9 984,64	11 231,36	21 183,39
01/07/N+3	21 183,39	847,34	10 384,02	11 231,36	1 0799,36
01/07/N+4	10 799,36	431,97	10 799,37	11 231,36	0,00

5. Plan de financement d'un investissement

Le plan de financement présente le détail de la couverture des besoins de financement liés à l'investissement.

On doit donc calculer la VAN en y incluant l'option de financement choisie.

Dans le cas du crédit-bail, les redevances viendront s'ajouter aux charges à décaisser lors du paiement de chaque redevance, alors que le prix d'acquisition, si c'est le cas, sera à décaisser en une seule fois (sauf si on fait un emprunt pour le régler).

Dans le cas d'un emprunt, les annuités feront partie des charges à décaisser.

6. Rentabilité d'un projet avec financement externe

Si on reprend l'exemple qui nous a servi au début de cette séquence pour le calcul de la VAN :

Éléments	Projet 1
Coût d'achat	30 500
Durée de vie	5 ans
Amortissement du matériel	Linéaire sur 5 ans
Augmentation annuelle prévue du chiffre d'affaires grâce au projet	23 000
Charges décaissables annuelles prévues dues au projet (matières premières et main-d'œuvre)	12 000

On suppose que l'entreprise peut investir directement 10 000 € et qu'elle emprunte la différence (20 500 €). Cet emprunt se fait sur cinq ans au taux de 3,5 %, avec des remboursements à amortissement constant. La première échéance de remboursement est prévue le 01/03/N, un an après l'acquisition du matériel. Le tableau de remboursement de l'emprunt sera donc le suivant :

Date de remboursement	Capital restant dû	Intérêts	Amortissement	Annuité	Capital dû en fin de période
01/03/N	20 500	717,50	4 100	4 817,50	16 400
01/03/N+1	16 400	574,00	4 100	4 674,00	12 300
01/03/N+2	12 300	430,50	4 100	4 530,50	8 200
01/03/N+3	8 200	287,00	4 100	4 387,00	4 100
01/03/N+4	4 100	143,50	4 100	4 243,50	0

Le calcul des flux nets de trésorerie (FNT) va être modifié car on va prendre en compte une charge financière supplémentaire liée au projet : l'annuité de remboursement de l'emprunt. De plus, contrairement à notre situation initiale les FNT de chaque année ne vont plus être identiques. Il va donc falloir actualiser chacun d'eux à la date d'acquisition de l'immobilisation, soit le 01/03/N-1. Si on suppose que le taux d'actualisation est de 6 %, chaque flux va être actualisé grâce à la formule :

$$FN_{n,01/03/N-1} = FN_n\ (1+0,06)^{-n}$$

Les flux de trésorerie seront donc de :

Éléments	01/03/N	01/03/N+1	01/03/N+2	01/03/N+3	01/03/N+4
Recettes supplémentaires :	23 000,00	23 000,00	23 000,00	23 000,00	23 000,00
Charges supplémentaires : Main-d'œuvre et matière première	12 000,00	12 000,00	12 000,00	12 000,00	12 000,00
Amortissement matériel	6 100,00	6 100,00	6 100,00	6 100,00	6 100,00
Emprunt : annuité	4 817,50	4 674,00	4 530,50	4 387,00	4 243,50
Résultat avant impôts	82,50	226,00	369,50	513,00	656,50
Charge supplémentaire : impôts sur les bénéfices	27,50	75,33	123,17	171,00	218,83
Résultat net	55,00	150,67	246,33	342,00	437,67
Amortissement à réintégrer	6 100,00	6 100,00	6 100,00	6 100,00	6 100,00
Flux nets de trésorerie	6 155,00	6 250,67	6 346,33	6 442,00	6 537,67
Flux nets de trésorerie actualisés au 01/03/N-1	**5 806,60**	**5 563,07**	**5 328,50**	**5 102,67**	**4 885,32**
Flux nets de trésorerie actualisés cumulés	**26 686,17**				

Ces 26 286,17 € représentent donc le gain net du « projet 1 » que nous aurions le 01/03/N-1.

Pour calculer la VAN au 01/03/N-1, il nous suffit donc de prendre en compte que l'organisme de crédit nous prête 20 500 € ce jour, et que nous déboursons 30 500 € pour régler le matériel correspondant au projet 1.

$$VAN_{01/03/N-1} = 26\,686,17 + 20\,500 - 30\,500 = 16\,686,17\ €$$

Cette VAN est positive, donc le projet n° 1 financé avec le crédit ci-dessus reste toujours rentable.

Mais, nous ne savons pas ce qu'il en est de sa comparaison avec le projet n° 2, surtout si ce dernier doit aussi être financé en partie par un crédit… c'est donc ce que vous allez déterminer dans le premier exercice de cette séquence.

Exercices autocorrectifs

Exercice 1

Au début de cette séquence nous avions vu que le dirigeant d'une entreprise hésitait entre deux projets : le projet 1 et le projet 2. Ses réserves financières ne lui permettent pas d'autofinancer son investissement, il doit avoir recours au crédit. Au dernier point de cette séquence nous avons examiné la rentabilité du premier projet.

Á vous d'analyser celle du deuxième projet et de décider du choix entre les deux.

Le projet 2 avait les caractéristiques suivantes :

	Projet 2
Coût d'achat	37 000
Durée de vie	5 ans
Amortissement du matériel	Linéaire sur 5 ans
Augmentation annuelle prévue du chiffre d'affaires grâce au projet	25 000
Charges décaissables annuelles prévues dues au projet (matières premières et main-d'œuvre)	13 000

De plus, on suppose que l'entreprise peut investir directement 17 000 € et qu'elle emprunte la différence (20 000 €). Pour cet emprunt, elle a obtenu exactement les mêmes conditions auprès de sa banque que pour le projet n°1 : durée 5 ans, taux de 3,5 %, remboursements par amortissements constants. La première échéance de remboursement est aussi prévue le 01/03/N, un an après l'acquisition du matériel.

De même, pour l'actualisation on utilisera un taux de 6% qui est la rentabilité désirée du capital de l'entreprise par les actionnaires.

1. Présenter le tableau de remboursement de l'emprunt.

2. Calculer la Valeur Actuelle Nette de ce projet au 01/03/N-1.

3. D'un point de vue uniquement financier, choisiriez-vous le projet n°1 ou le projet n°2 ?

Exercice 2

Une entreprise veut acquérir un nouveau matériel de production. Elle estime qu'elle pourra l'exploiter pendant six ans. Les quatre premières années le chiffre d'affaires supplémentaire résultant de l'exploitation de ce matériel devrait produire 50 000 € de recettes supplémentaires, et 35 000 € les années suivantes. Les frais supplémentaires relatifs à cette acquisition (hors amortissement du matériel) devraient être constants, de 15 000 € par an.
Le matériel est amorti en linéaire sur 4 ans et a un coût d'acquisition de 120 000 €.
L'entreprise paie l'impôt sur les sociétés au taux de 33,1/3 %.

1. Calculer les flux nets de trésorerie annuels générés par l'investissement prévu.

2. Calculer le délai de récupération du montant investi.

3. Calculer la Valeur Actuelle Nette de ce projet, en sachant que le taux d'actualisation est de 7%.

4. Qu'en concluez-vous ?

Unité 3

Gestion des systèmes d'information

▶ *Contenu*

Séquence 8

Conduite d'un projet informatique

Dès que vous entendez parler un informaticien, vous êtes quasiment sûr d'entendre le mot « projet » : chef de projet, travailler sur le projet X, s'inscrire dans le projet X, avoir des interactions avec le projet X… Comme en DAIGL (développement d'applications informatiques et génie logiciel) ou dans les réseaux, où vous pouvez conclure que tout est « objet », au niveau organisationnel, dans la construction d'un système d' information, on peut dire que tout est « projet ».

1. Qu'est-ce qu'un projet informatique ?

Mais alors qu'est-ce qu'un projet ?

C'est un ensemble cohérent d'activités développées pour atteindre un objectif défini dans un certain domaine de l'organisation.

Il est placé sous la responsabilité d'une personne disposant de moyens définis (humains, matériels, financiers et organisationnels) et de contraintes (délais, budgets, autres éléments prédéfinis).

Exemples de projets :
– gestion des horaires flexibles et des repos compensateurs (domaine ressources humaines) ;
– profilage et suivi des clients (domaine commercial) ;
– refonte de la comptabilité pour qu'elle soit homogène avec celle d'un grand groupe financier (domaine comptable) ;
– sécurisation d'un Intranet (domaine sécurité des systèmes d'information).

Tout service ou société informatique fonctionne par projets.

1A. Pourquoi définir un projet ?

Il n'est pas possible de réaliser des évolutions du système d'information de l'entreprise au cas par cas sans se préoccuper de leurs interactions avec le système d'information en place. On va gérer l'ensemble de travaux à mener comme un tout, en constituant un projet de développement. Il est nécessaire de centraliser et coordonner ces diverses modifications et évolutions pour :

– analyser leurs interactions ;
– définir des priorités entre les projets par rapport aux objectifs globaux de l'organisation ;
– regrouper certains projets car ils représentent un même type d'intervention sur le système d'information ;
– assurer la rentabilité de la maintenance et l'évolution du système d'information ;
– organiser la gestion du personnel travaillant sur des projets liés au système d'information.

1B. Exemple de caractéristiques d'un projet

Pour définir un projet, on va spécifier quelques paramètres :

– son objectif ;
– son domaine fonctionnel ;
– le résultat attendu ;
– les contraintes ;
– les moyens ;
– les délais ;
– les critères spécifiques au projet.

Exemple : *pour un projet relatif au développement du commerce électronique d'une entreprise, on peut retenir les éléments suivants :*

– *son objectif : augmenter nos ventes et les diversifier ;*
– *son domaine fonctionnel : gestion commerciale ;*
– *le résultat attendu : se faire connaître par d'autres clients, modifier notre image de marque… ;*
– *les contraintes : contraintes juridiques sur les ventes sur Internet, pas de personnel de l'entreprise suffisamment compétent pour développer le logiciel désiré ;*
– *les moyens : trois développeurs, outils de développement de sites de e-commerce, outils de sécurisation ;*
– *le délai : un mois.*

1C. Qu'est-ce qu'un projet réussi ?

On peut déterminer quelques caractéristiques de la réussite d'un projet.

- Satisfaction des besoins des utilisateurs en maîtrisant les phases de développement, la réalisation et la mise en œuvre. La réponse aux besoins des utilisateurs est l'élément primordial de tout projet informatique.
- Apports positifs pour l'organisation : bénéfice, retour sur investissement, amélioration de l'organisation générale, avantage (ou rattrapage) concurrentiel.
- Coûts et délais maîtrisés.
- Maîtrise du projet tout au long de son déroulement : anticipation des risques et mise en place de mesures préventives, connaissance quasi-instantanée des dérives et prises de décisions adéquates.

Voici quelques problèmes qui peuvent exister lors de la durée de vie d'un projet et des exemples de réactions appropriées :

Risques	Causes	Réactions
Retard Glissement de budget	• Mauvaise estimation de la charge globale du projet • Mauvais suivi de projet • Mauvaise répartition des tâches • Facteurs humains (inexpérience, mauvaise entente entre personnes, mauvaise affectation,...)	• Méthodes d'évaluation appropriées • Utilisation de tableaux de bord et d'outils normalisés (cf. séquence suivante) • Choix et suivi des ressources humaines et techniques • Planification à surveiller et à adapter • Formation
Mauvaise qualité Non satisfaction des besoins	• Mauvaises spécifications • Mauvaises réalisations • Centrage exclusivement sur la technique	• Associer étroitement les utilisateurs tout au long du projet et leur faire valider les étapes • Identifier les fonctions métier essentielles • Méthodes de tests et de recette • Limiter les innovations au sein d'un même projet
Abandon du projet *(n'est pas obligatoirement une mauvaise décision)*	• Peu de valeur ajoutée du projet • Aléas fonctionnels (modification des règles de gestion,...) • Aléas techniques (défaillance, retard) • Changement d'avis ou mauvaise description des besoins des utilisateurs • Coûts trop élevés	• Ne jamais hésiter à abandonner un projet non rentable • Capitaliser l'expérience • Miser sur la réutilisation (modules logiciels par exemple) • Utiliser un progiciel à la place d'en développer un nouveau.

2. Les étapes de la gestion de projet

L'important dans un projet est de définir des étapes intermédiaires, qui sont un guide pour les divers acteurs comme une occasion de faire le point entre eux sur l'opportunité de continuer le projet. Chaque fin d'étape (ou de sous-étape) est un moment pour se mettre d'accord sur les actions correctrices qu'il est nécessaire de mener.

Ce découpage permet de dresser la liste des travaux à exécuter et des résultats attendus pour chaque étape, cela va aider le chef de projet à y voir plus clair, à faire des plannings et à évaluer les ressources et budgets nécessaires tout au long de la vie du projet.

Les diverses étapes dépendent du type de projet, des volumes (budgets et personnel) traités… Cependant, nous allons vous présenter deux types de découpages préconisés par des outils que vous avez dû voir en DAIGL : la méthode Merise et le langage de modélisation UML (unified modeling language).

2A. Étapes de la gestion de projet, méthode Merise

2A1. Le schéma directeur

Il fait l'état des lieux global du système d'information et fixe ses grandes orientations pour le futur.

2A2. L'étude préalable

Cette phase se limite à une partie particulière du système d'information, telle que la refonte ou la création d'une application.
Elle aboutit à une synthèse des scénarii retenus et à leurs estimations en termes de délais et de budgets.

2A3. L'étude détaillée

L'étude détaillée se consacre à un projet, tout en ne négligeant pas ses interactions avec le reste du système d'information. Elle décrit la solution retenue en la détaillant.
Le rapport de cette phase doit donner une vision externe du système (interface homme-machine, description des traitements réalisés…).

2A4. L'étude technique

C'est à partir de cette phase que les informaticiens vont devenir les acteurs principaux, sans négliger pour autant les diverses phases de validation par les utilisateurs.
Elle produit le document de base du développement de l'application : descriptions précises des structures de données et des traitements, normes techniques, indications de réutilisation…

2A5. La réalisation

Dans cette phase on va produire le logiciel en diverses étapes, allant de programmes séparés et testés individuellement, qui vont peu à peu s'inter-relier pour produire le logiciel global. Les premiers tests sont réalisés par les informaticiens alors que les suivants (et notamment lors de la phase de « recette ») nécessitent d'être réalisés par les utilisateurs sur la base de documents réels.
Lors de la recette, les informaticiens guident les utilisateurs, ce qui sert souvent de premier niveau de formation au logiciel.

2A6. La mise en œuvre

Il s'agit de l'installation et de l'intégration du logiciel dans le système d'information de l'entreprise. Elle concerne le paramétrage, la reprise ou l'alimentation des données et la modification d'interfaces.

2A7. La qualification et la livraison

C'est la dernière phase de la recette. Les tests seront réalisés dans l'environnement opérationnel (de production) de l'entreprise sans que ce dernier ne serve réellement d'environnement de production à ce moment. On va rédiger un bilan du projet selon divers critères de qualité.
La signature de ce rapport final par les représentants des utilisateurs (maître d'œuvre, responsable du domaine concerné ou personnes détachées pour la recette) signifiera que le projet a été « livré ». Il peut alors rentrer en exploitation et le « client » atteste qu'il est conforme aux besoins qu'il était censé combler.

La mise en exploitation d'un projet ne signifie pas la disparition complète des informaticiens. Ils participeront ensuite à la formation et veilleront à sa maintenance (corrective ou évolutive).

2B. Étapes de la gestion de projet, langage de conception UML

UML se base sur un processus nommé itératif et incrémental, impliquant l'utilisateur, centré sur l'architecture technique et piloté par les risques. Il débute par des analyses séparées du niveau fonctionnel et du niveau technique qui se rejoignent ensuite.

2B1. Itérativité

Basé sur le même principe que le RAD (rapid application developpement) UML préconise un processus en spirale où une maquette, ou une petite partie du projet final, est développée à chaque stade. Le projet évolue en détaillant et complétant le résultat de la précédente production.

On peut ainsi présenter et faire valider une partie du produit fini aux utilisateurs à chaque étape.

De plus, la production d'une partie (prototype ou maquette) à chaque itération oblige les développeurs à intégrer l'environnement technique. Une maquette sert à montrer à l'utilisateur une partie importante du logiciel pour qu'il ait une vue d'ensemble et puisse prendre conscience des liens entre les diverses fonctionnalités. Un prototype, quant à lui n'a aucun objectif d'exhaustivité, il sert à expérimenter des cas précis, à se mettre d'accord sur des procédures et points de détails importants.

2B2. Orienté selon deux types d'utilisateurs

UML considère deux types d'acteurs parmi les utilisateurs.
L'utilisateur au sens classique, qui se servira des résultats du projet pour remplir le rôle qu'il a à tenir dans l'organisation. Il permettra de valider l'adéquation aux besoins.

L'utilisateur exploitant le système, correspondant à un rôle plus technique et opérationnel commun à la plupart des systèmes informatiques.

2B3. Piloté par les risques

Ce développement incrémental et la participation des utilisateurs au projet permettent d'éviter le risque majeur de non adéquation des besoins.
De plus, la prise en compte au plus tôt de l'architecture technique permet d'éviter les « études » trop théoriques, les développeurs étant directement confrontés à l'environnement de développement.

2B4. Basé sur un système en Y : la méthode TTUP

Le processus de développement est représenté sous forme de Y car on part tout d'abord sur deux branches séparées (le modèle fonctionnel et l'architecture technique) qui vont ensuite se rejoindre pour la réalisation ultime.

Le modèle fonctionnel permet de se focaliser sur le métier des utilisateurs. Cette partie de l'analyse définit les besoins réels du système en termes de métier.

L'étude de l'architecture technique recense toutes les contraintes techniques liées à l'existant et construit les bases de l'architecture technique intégrée dans le système d'information global. Lors de cette phase on réalise souvent un prototype.
Lorsque les deux branches ci-dessus se rejoignent on passe ensuite par des phases assez traditionnelles, à savoir :

- l'étude préliminaire qui conforte l'adéquation et l'interaction des deux branches ci-dessus ;
- l'étude détaillée, similaire à celle de la méthode Merise, mais sur la base de spécificités techniques plus détaillées ;
- le codage et les premiers tests faits par les informaticiens ;
- la recette.

3. La planification de projet

Pour faire un planning, la première chose est de faire la liste des tâches relatives à un projet donné en évaluant le temps nécessaire à la réalisation de chacune et leur enchaînement (telle tâche nécessite que telle autre soit terminée pour pouvoir commencer, la fin de telle tâche implique qu'une ou plusieurs autres peuvent commencer…).

3A. *Exemple de planning*

Commençons par un exemple simple de planning : comment se préparer le matin. Supposons que le matin, avant de partir de chez vous vous ne fassiez que trois choses :

– vous préparer (se lever, se laver, s'habiller…) qui prend 20 minutes ;
– préparer votre café : 15 minutes ;
– prendre le petit déjeuner (céréales froides puis café) : 10 minutes.

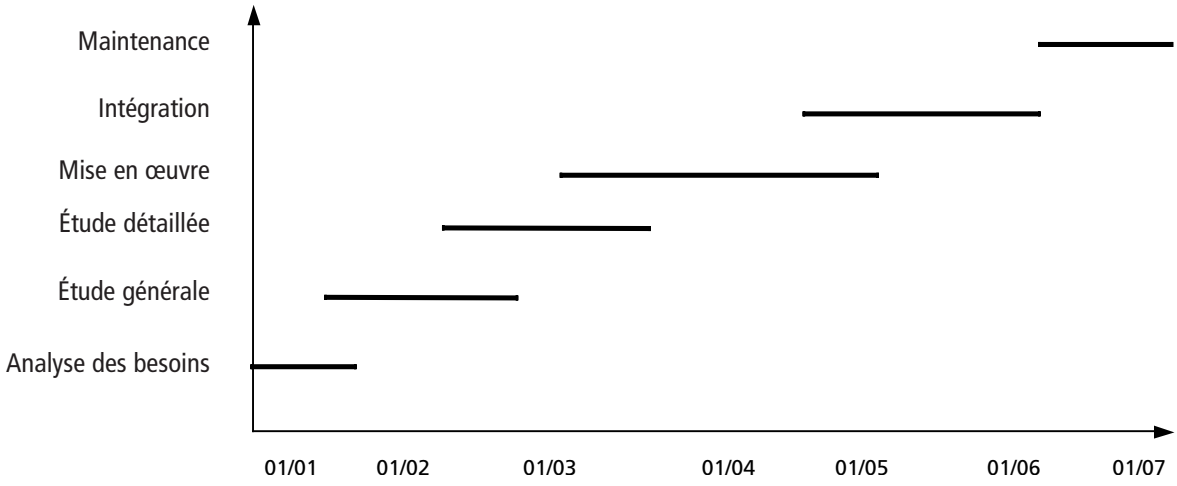
De plus, supposons que vous ne puissiez pas prendre votre petit déjeuner avant de vous être préparé. Comment organiser vos tâches pour aller au plus vite… afin de faire sonner le réveil au dernier moment ? Pour cela nous allons réaliser un mini planning.

Il est évident ici qu'il faudra réaliser la tâche numéro 2 (préparer le café), puis la numéro 1 puis la 3. Si le café met plus de 20 minutes à se préparer, on peut encore gagner du temps en séparant la tâche numéro 3 en deux : céréales et café. On pourra ainsi, en mangeant les céréales réduire le temps d'attente du café.

C'est ce type de planning et d'ajustement en fonction d'un aléa (ici le retard dans la disponibilité du café) que nous allons voir dans cette partie.

3B. *Le diagramme de Gantt*

Il répond à la question : « quelles sont les tâches qui doivent se réaliser à une date donnée ? ».
Ce diagramme se présente sous la forme d'un graphique avec la liste de tâches en ordonnée et le temps en abscisse.
Par exemple, si on suit les étapes préconisées par Merise pour un « petit » projet démarrant le 1er janvier d'une certaine année, on aura :



On voit sur ce schéma que la mise en œuvre peut commencer dès lors que les 2/3 (environ) de l'étude détaillée sont réalisés. En effet, l'étude détaillée s'étend du 15/02 au 01/04 et la mise en œuvre débute vers le 10/03 pour se terminer fin mai.
Ce type de schéma va nous permettre, en cas de retard ou d'allongement d'une tâche, de décaler toutes les autres en conséquence.

De nombreux logiciels de planification permettent de réaliser un diagramme de Gantt, ils sont couramment employés dans le monde industriel, en gestion de projet. Comme « Gestion de Projet » ou Open Workbench dans le monde du libre, Project de Microsoft, Gnt Planning de SodeaSoft… Certains sont téléchargeables, je vous conseille d'aller les consulter. Ils permettent de réaliser le planification initiale mais surtout de l'adapter au cours du temps en fonction des réalisations concrètes et des aléas que se présentent.

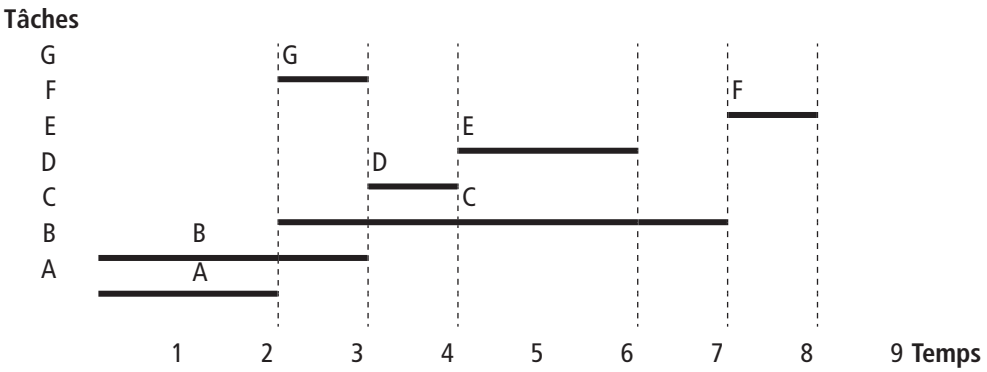
Exemple

Soit un projet pour lequel les diverses tâches (nommées ici A à G) ont été répertoriées ainsi que les relations d'antériorité entre elles. Nous allons réaliser le diagramme de Gantt correspondant.

Tâche	Durée en jours	Antériorité
A	2	–
B	3	–
C	5	A
D	1	B
E	2	D
F	1	E, C
G	1	A

La lecture de ce tableau nous informe que les tâches A et B peuvent commencer dès le début, qu'une fois que A est terminée on peut débuter en parallèle les tâches C et G et que la tâche F est obligée d'attendre que les tâches E et C soient terminées pour débuter.

Le diagramme de Gantt se présente alors ainsi :



On voit ici que le projet se terminera à la fin du 8e jour.
Les traits verticaux représentent les antériorités.
Ce diagramme nous permet de voir que seule la tâche G peut être retardée de 5 jours sans que le projet ne soit globalement retardé. On pourrait retrouver ceci par le calcul en faisant : 8 (date de fin de projet au plus tôt) – 1 (durée de G) - 2 (date de début au

plus tôt de G, sachant qu'elle ne peut commencer que lorsque A est achevée). 5 jours est la marge de manœuvre dont le responsable de projet dispose sur cette tâche (appelée la marge totale, voir ci-dessous).

De même à la lecture du diagramme on voit que les tâches A, C et F ne peuvent prendre aucun jour de retard sans retarder globalement le projet. Elles représentent ce que nous appellerons le chemin critique.

La tâche E peut prendre un jour de retard (on peut la translater d'une case vers la droite sans modifier le délai total de réalisation du projet). Mais si elle prend 3 jours de retard, le projet se terminera alors 2 jours plus tard (soit à la fin du 10e jour). En effet le retard de 3 jours absorbe la marge de 1 jour qui était disponible et retarde donc le projet de 2 jours (3-1). Si cela était le cas E se situerait alors sur le chemin critique.

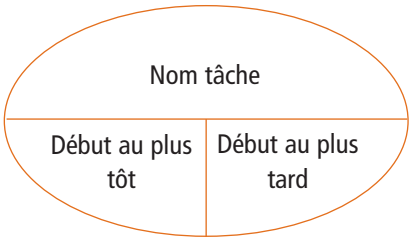
Le diagramme de Gantt est un bon instrument graphique pour la lecture des dates de début et de fin de tâches, il est relativement moins performant pour les prévisions en fonction des marges. Nous allons donc voir maintenant un outil un peu plus complet pour le calcul des marges : le MPM (méthode des potentiels métra)

3C. *Le graphe MPM*

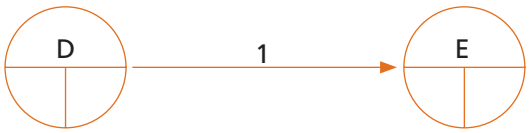
3C1. Présentation et construction

Cet outil se présente sous forme d'un graphe, il a donc des sommets, qui représentent les tâches, et des arcs (flèches) qui indiquent les relations d'antériorité.
Chaque sommet est présenté sous forme d'un rond avec le nom de la tâche, sa date de début au plus tôt, ainsi que sa date de début au plus tard.

On réalise tout d'abord le graphe en ne mettant que le nom des tâches et les flèches, sur lesquelles on porte la durée de la tâche.



Si on reprend l'exemple ci-dessus, la tâche D, qui dure un jour et qui précède la tâche E, est représentée ainsi :

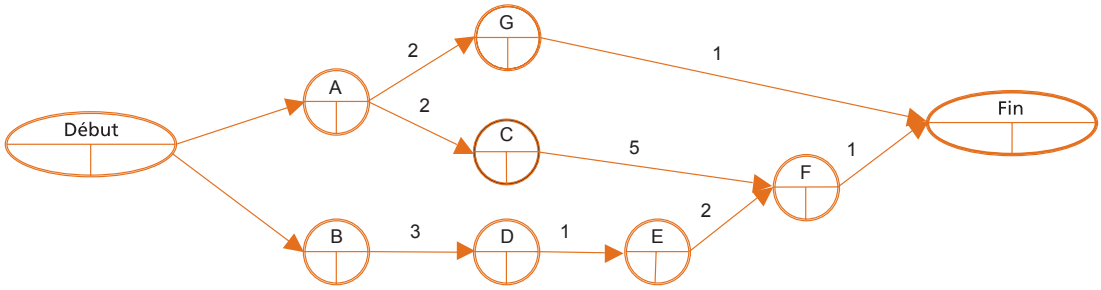


De plus, on dessine le graphe en tenant compte des niveaux. Le 1er niveau représente l'ensemble des tâches qui peuvent se réaliser dès le début, le niveau 2 celui qui peut se réaliser dès qu'une tâche de niveau 1 est terminé…

On rajoute deux tâches « début » et « fin » auxquelles sont reliées respectivement les tâches n'ayant pas d'antériorité ni de successeur.

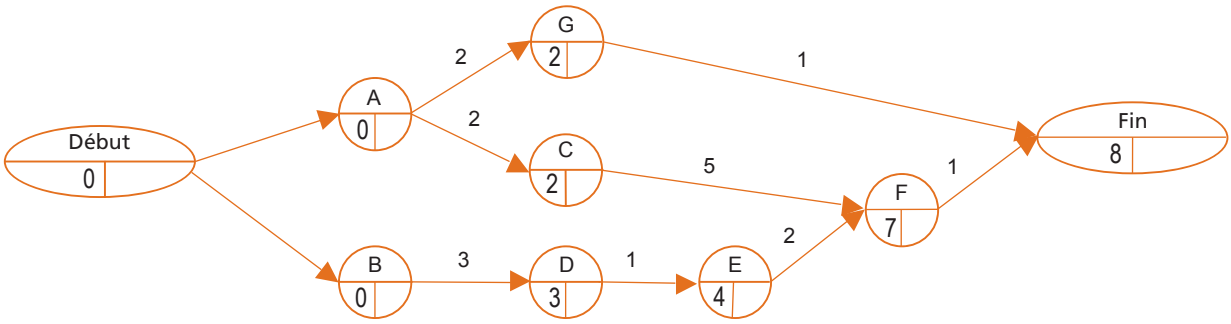
On obtient donc pour le graphe suivant :

Niveaux : 1 2 3 4



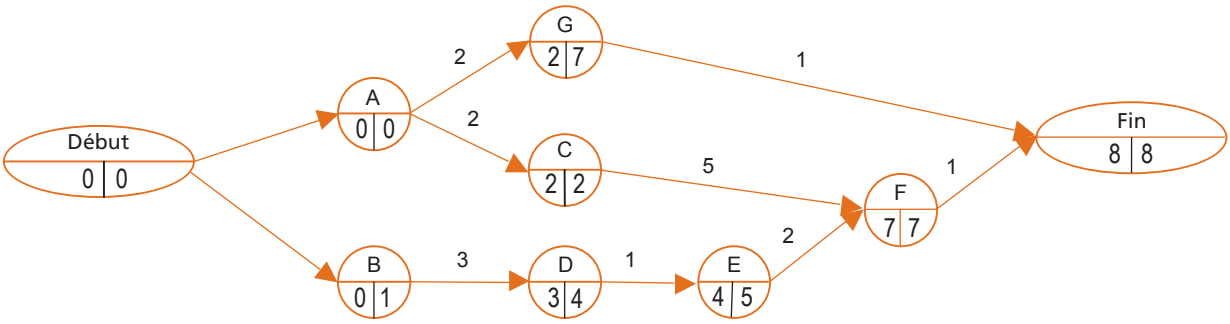
On s'occupe ensuite des dates de début au plus tôt. Pour cela on met 0 à la tâche de « début » puis, pour chaque tâche, on additionne le début au plus tôt et la durée de la tâche précédente, pour obtenir le début au plus tôt de la tâche courante. Par exemple pour E on a 4, soit 3 le début au plus tôt de D et 1 la durée de D.

Si une tâche a plusieurs prédécesseurs, on prendra la valeur la plus grande obtenue par chacune des flèches qui arrivent à la tâche. En effet la tâche doit attendre que tous ses prédécesseurs soient terminés, et donc, entre autre, le prédécesseur qui termine le plus tard. Par exemple pour F on a C et E comme tâches antérieures. Par le chemin qui provient de C, on obtient 7 (2+5) comme date au plus tôt. Par le chemin qui provient de E, on obtient 6 (4+2) comme date au plus tôt. On prend donc 7 pour attendre la fin de C.



Nous savons maintenant que le projet peut être réalisé, au plus juste, en 8 jours, nous allons donc calculer les dates de début au plus tard de chaque tâche pour ne pas retarder le projet global. On va faire ceci comme pour les dates au plus tôt sauf qu'on va partir de la fin et prendre à chaque fois les données les plus faibles obtenues.

Pour cela on part de la « fin » dans laquelle on reporte 8, la durée globale, puis on en déduit de proche en proche les dates de fin au plus tard en se servant des durées de chaque tâche. Pour G cela nous donne 7 (8 - 1). Si une tâche a plusieurs successeurs on prendra alors la valeur la plus petite obtenue, comme A pour laquelle on a le choix entre 5 (7 - 2) si on considère G comme successeur et 0 (2 - 2) si on considère C comme successeur, le début au plus tard est donc 0.



3C2. Indicateurs d'ordonnancement

Ce graphe MPM nous permet, pour chaque tâche, de calculer aisément la **marge totale** d'une tâche qui représente le retard qu'elle peut prendre sans retarder le projet global. La marge totale est obtenue en faisant, pour chaque tâche, la différence entre la date de début au plus tard et la date au plus tôt.

Marge totale = 7 – 2 = 5

La **marge libre** représente, pour chaque tâche du projet, la marge de manœuvre disponible sans modifier la date de début au plus tôt de tous les successeurs. Elle se calcule donc par « date de début au plus tôt » de la tâche suivante moins durée de la tâche considérée.

Une **tâche critique** est une tâche dont aucun retard n'est possible sans affecter la durée globale du projet. Sur le graphe MPM on les repère par le fait que les deux dates sont égales.

Marge totale = 2 – 2 = 0

Dans le graphe précédent, les tâches critiques sont donc A, C et F.

On appelle **chemin critique** la succession des tâches critiques. En général, sur le graphe MPM, on met en valeur ce chemin par des doubles flèches ou une couleur différente des flèches. Les tâches situées hors du chemin critique peuvent, dans une certaine mesure, être allongées ou retardées sans répercussion sur la durée totale du projet.

3D. La méthode PERT

Dans une première approximation, on peut dire que le graphe associé à la méthode PERT (program evaluation and review technic) est quasi identique au graphe MPM. Simplement, on va mettre le nom des tâches sur les arcs, suivi de la durée entre parenthèse. À la place du nom de la tâche (en haut du rond) on met un numéro de tâche.

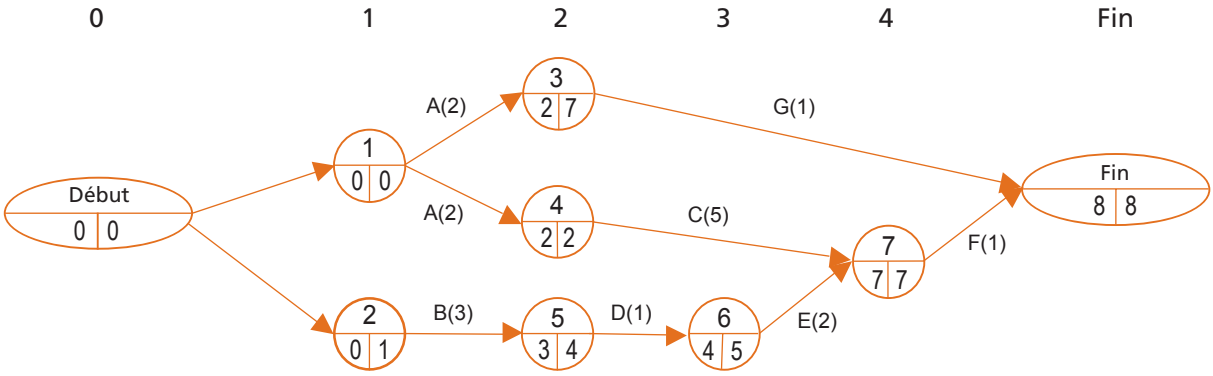
Il est important d'y faire apparaître le niveau, ce que nous avions déjà fait pour notre exemple de graphe MPM. Le niveau de chaque tâche est le fait qu'elle puisse être réalisée dès le début (niveau 1), ou après que les premières tâches soient terminées (niveau 2)…

Si on lit « verticalement » notre ancien graphe MPM, on voir que le niveau 1 est composé des tâches A et B qui n'ont aucun prédécesseur et donc peuvent commencer au début. Le

niveau 2 est composé des tâches G, C et D, qui ont toutes un prédécesseur de niveau 1. Le niveau 3 est composé de la tâche E, qui a comme seul prédécesseur D, de niveau 2. Le niveau 4 est composé de la tâche F dont le niveau le plus élevé parmi ses prédécesseurs (C et E) est 3.

Dans un graphe PERT la tâche fictive « fin » est toujours apparente, alors qu'on peut se passer de la tâche « début ».

Le graphe PERT de notre exemple se présente donc ainsi :



4. Le suivi des projets

Pour toutes les étapes que nous avons vues ci-dessus, l'essentiel n'est pas de prévoir toutes les opérations et leur planification, mais la maîtrise du déroulement du projet.

Pour cela le chef de projet doit suivre les conditions et l'état d'avancement du projet et agir par des actions correctrices au bon moment. De nombreux tableaux de bord (voir séquence consacrée à ce sujet) l'aident pour l'alerter des dérives. C'est à lui de prendre les bonnes décisions au bon moment. Ces décisions sont fonction des risques à prendre ou à éviter, de la rapidité de leur mise en œuvre, des marges de manœuvre données à chaque acteur du projet, de la mise à jour des informations…

Les outils mis à la disposition du responsable pour gérer ceci sont vus dans les séquences relatives au TIC (technologies de l'information et de la communication) et aux outils d'aide à la décision.

Exercice 1

Supposons que vous travailliez au service informatique d'un grand hypermarché avec une méthode de conception basée sur le langage UML et respectant les consignes de la méthode TTUP. Préciser, pour les exemples ci-dessous, la branche du processus TTUP (fonctionnelle ou technique) qui sera prise en compte.

1. L'hypermarché ouvre une section « agence de voyage », il veut créer un système d'information indépendant de celui de l'hypermarché, en pouvant assurer des échanges de données entre les deux systèmes d'information.
2. La section « agence de voyage » passe un accord de revente de certains voyages organisés avec une compagnie qui monte ces voyages. Des conditions particulières doivent être mises en place pour cette activité de revente.
3. La section « agence de voyage » décide d'ouvrir une rubrique de commerce électronique.
4. Le partenariat avec la compagnie précédente impose la mise en place d'un extranet avec des moyens techniques de synchronisation des deux systèmes.

Exercice 2

Dans une entreprise, on désire mettre en place un réseau local qui prendra en charge une soixantaine de postes clients. Le responsable informatique a dégagé les diverses tâches à réaliser pour mener à bien le projet. Il a quantifié leurs durées en jours de travail.

Référence tâche	Tâche	Durée en jours	Antériorité
A	Description détaillée des besoins	4	-
B	Détermination du budget	2	-
C	Recherche et choix des fournisseurs intervenant	6	A et B
D	Commande et réception du logiciel d'administration réseau	1	C
E	Commande et réception des équipements réseaux	4	C
F	Installation du logiciel d'administration réseau	1	D
G	Câblage	10	C
H	Formation de l'administrateur réseau	4	C
I	Mise à jour des postes au niveau matériel	3	E et G
J	Mise à jour des postes clients (logiciel et sécurité)	2	I
K	Intégration et mise au point serveurs et clients	5	F, H et J

Remarques

Le câblage est réalisé par une société extérieure qui a proposé deux devis : un premier de 3 000 € avec un délai de réalisation de 6 jours, et un second (celui retenu) de 2 000 € en 10 jours.

Pour la formation de l'administrateur réseau, l'organisme de formation qui la dispense n'organise que deux sessions par mois, les prochaines auront lieu le lundi 06/03/06 et le lundi 27/03/06 (soit exactement 3 semaines après la première session).

L'entreprise travaille cinq jours par semaine, du lundi au vendredi.

Au niveau du personnel, tous les travaux sont réalisés par des fournisseurs externes ; seul un administrateur réseau est nouvellement embauché pour assurer son administration (en plus de travaux de maintenance informatique). Il doit impérativement être présent pour les tâches A, C et K de ce projet.

1. ***Représenter graphiquement l'enchaînement des tâches de ce projet.***
2. ***À l'aide du graphe MPM, déterminer le nombre de jours que va durer la mise en place du réseau.***
3. ***Quelle est la tâche, sur le chemin critique, qui dure le plus longtemps ? Dans le cas où l'entreprise voudrait réduire le temps global d'installation du réseau, que proposez-vous pour cette tâche ?***
4. ***Sachant que le choix des fournisseurs (tâche C) auquel participe l'administrateur réseau, se termine le jeudi 2 mars 2006 et que ce dernier est inscrit pour la formation du lundi 6 mars, pourra t-il suivre cette session ? La participation à ce stage du 06/03/06 va-t-elle retarder le projet ?***
5. ***Si la session de formation du 06/03/06 affiche complet et que l'administrateur ne peut assister qu'à la suivante, quelle conséquence cela aura sur la durée globale de mise en place du réseau ?***
6. ***Pour aborder, comme sur un calendrier, la planification des tâches en termes de dates précises, quelle autre représentation (que le MPM) semblerait plus adaptée ?***
7. ***Quelles sont les marges totales des tâches D, E et G ?***
8. ***Lors de la réalisation concrète de ce projet, alors que l'entreprise est en train de réaliser la mise à jour des postes au niveau matériel (tâche I), on constate que les tâches ci-dessous ont pris du retard :***
   - ***suite à l'absence du principal décideur, la description détaillée des besoins a duré 7 jours ;***
   - ***retard de réception des équipements réseau de 2 jours ;***
   - ***allongement d'une journée pour l'installation du câblage.***

Quelle est l'incidence de ces trois retards sur la date de disponibilité générale du réseau ?

Séquence 9

Qualité et système d'information

Cette séquence va traiter de la qualité du système d'information principalement au travers de la conduite des projets informatiques. C'est pourquoi il est nécessaire de maîtriser la séquence 8 pour pouvoir aborder correctement cette séquence.

Vous avez déjà une idée de ce qu'est la qualité en général. Par exemple, vous achetez une chemise dans un magasin de prêt-à-porter, à quoi vous attendez-vous ? Tout d'abord, à ce qu'elle soit mettable (possibilité de s'habiller avec, la boutonner…) et qu'elle vous donne chaud, ou au moins vous couvre, c'est que nous appellerons la satisfaction des besoins de l'utilisateur. Puis vous voulez qu'elle vous embellisse, selon votre goût personnel (satisfaction des besoins selon le goût personnel et ergonomie). De plus elle doit être facile à mettre et vous devez vous y sentir bien (facilité d'apprentissage et d'utilisation).

Mais nous verrons que pour un logiciel, qui s'inscrit dans un système d'information (cadre beaucoup plus large que celui de porter une chemise !) ces seuls critères ne suffisent pas. En effet, il est important d'assurer la cohérence du système d'information, de respecter les délais, de produire au meilleur coût… La qualité au niveau informatique va aussi incorporer ces divers domaines.

1. De la qualité à la qualité totale

L'information est aujourd'hui une ressource stratégique pour la plupart des organisations, dans lesquelles de très nombreuses activités reposent sur l'exploitation d'applications informatiques. Pour ces organisations :

- la part consacrée aux logiciels est aujourd'hui prépondérante dans le coût total d'un système informatique ;
- la demande d'applications nouvelles, de plus en plus complexes, ne cesse de croître ;
- les utilisateurs sont de plus en plus exigeants en termes de fiabilité et de sécurité.

Parallèlement, on constate que :

- de nombreux projets en cours de développement sont abandonnés pour non-conformité, retard trop important, dépassement de budget... (voir séquence 8, les raisons de ces problèmes dans « Qu'est ce qu'un projet réussi ? ») ;
- les projets qui aboutissent ont souvent un retard considérable et le coût du produit développé est souvent bien supérieur aux prévisions.

Il est donc nécessaire :

- de prendre conscience que la satisfaction des besoins des utilisateurs est un critère essentiel dans tout projet informatique mais qu'il n'est pas le seul, dans l'intérêt de la cohérence globale du système d'information et la maîtrise de ses coûts ;
- d'accroître la qualité du produit logiciel, tant dans les domaines de leurs fonctionnalités, de la fiabilité, des performances… que dans les domaines de respect des délais et des budgets ;

– d'accroître la productivité et de réduire les coûts, non seulement lors de la production du logiciel, mais aussi de l'ensemble des activités mises en œuvre au cours de son cycle de vie.

La gestion de la qualité logicielle va donc s'intéresser à :

– la qualité du logiciel prise dans son sens général : satisfaction du besoin, facilité d'utilisation, limitation du nombre d'erreurs (bogues), convivialité, apprentissage aisé, interaction avec les autres modules ;
– la qualité du processus de production : découpage en unités correctes (voir gestion de projet), respect des délais et des coûts…

La **qualité totale** regroupe toutes ces notions et tient compte de l'évolution au cours du temps d'un produit ou service informatique (maintenance et évolution durant toute la durée de vie d'un élément). Par exemple, pour un logiciel comptable, il doit non seulement satisfaire ses utilisateurs au niveau des fonctionnalités proposées, de l'ergonomie, de son interfaçage avec les autres applications, de l'accessibilité des données en fonction du type d'utilisateur… mais il doit également satisfaire l'administration fiscale en lui transmettant l'information nécessaire au format imposé et s'adapter sans cesse aux nouvelles réglementations.

Pour un logiciel, un matériel ou un service informatique, la qualité va donc bien au-delà de ce que peut percevoir un utilisateur.

2. Évaluation de la qualité d'un logiciel

La métrologie du logiciel est un ensemble de méthodes qui permettent d'évaluer la qualité d'un logiciel et celle de son processus de développement. Elle a pour objet de définir :

– un ensemble de caractéristiques mesurables du logiciel ;
– des méthodes d'évaluation ;
– des outils d'évaluation (analyseurs, jeux de tests…).

2A. Présentation de la métrologie

Chaque caractéristique du logiciel peut être évaluée de manière quantitative (exemple : les temps de réponse) ou qualitative (exemple : l'ergonomie d'un certain écran) par la mesure d'un certain nombre d'indicateurs ou métriques. Une métrique peut être une valeur mesurée (temps en secondes), une note donnée (de 1 à 5), un taux ou un niveau (bon, moyen ou mauvais)...

Dans tous les cas, la valeur d'une métrique est ramenée à un niveau (bon, moyen ou mauvais) par application de seuils s'il s'agit d'une valeur mesurée ou calculée.

Par exemple, pour le code source d'un logiciel, on peut évaluer la longueur d'un programme (procédure, fonction ou module) et décider que s'il fait plus de 800 lignes, ou de 1000 instructions, il sera « mauvais » pour la maintenance, alors que s'il fait entre 500 et 300 lignes, il sera « moyen » et « bon » en deçà.

Une métrique peut influer plusieurs critères. Par exemple, le nombre de lignes d'un programme a des incidences sur sa simplicité et sur sa modularité. Il faut donc construire des modèles de simulation permettant de jouer sur plusieurs variables en même temps.
Ces modèles vont prendre en compte plusieurs métriques en donnant un poids à chacune et évaluer globalement, et par domaine, un produit ou service informatique.

Comme dans un tableau de bord (cf. séquence 3) c'est au décideur de mettre en place des indicateurs pertinents qui l'aideront à se procurer l'information dont il a besoin pour prendre ses décisions.

2B. *Contrôle de la qualité*

Ce contrôle va se réaliser en plusieurs étapes. Remarquez que la démarche suivie est identique à celle de mise en place des tableaux de bord vue à la séquence 3.

2B1. Choix des critères de contrôle

Comme lors de la détermination des indicateurs d'un tableau de bord, on va choisir les critères d'acceptabilité et des sous-caractéristiques que l'on retient par rapport aux objectifs fixés par l'utilisateur. Par exemple, si l'utilisateur désire une application ne fonctionnant qu'en monoposte pour un système donné, sans évolution future, la portabilité ne sera pas une caractéristique retenue ; alors que l'adaptation sans faille au système utilisé sera requise.

2B2. Choix des métriques

Pour chacune des sous-caractéristiques, on va choisir des mesures en essayant de gommer le plus possible la subjectivité. Cette phase n'est pas simple à mettre en œuvre, car certaines sous-caractéristiques ne sont pas facilement quantifiables, comme l'ergonomie.

On va construire un modèle prenant en compte le minimum de métriques. Par exemple, on établit un jeu d'essai et on mesure les temps de réponse par rapport à une liste prédéfinie de requêtes.

2B3. Choix des niveaux d'acceptabilité

Des échelles de classement sont alors indispensables. Les seuils définis correspondent à des niveaux de classement (excellent, bon, moyen, mauvais).

2B4. Pondération des métriques

On va enfin attribuer des coefficients à chaque sous-caractéristique et établir ainsi une pondération selon l'importance que l'on donne à chacun d'eux. Pour un économiseur d'écran, par exemple, le coefficient attribué à la sécurité sera de 0, alors que celui des rendements ou de l'esthétique sera important. On va fixer la note globale qui nous permet d'accepter ou de refuser le logiciel.

2B5. Exemple

On évalue un logiciel sur plusieurs critères dont chacun, qualitatif ou quantitatif, est ramené à une note de 0 à 10.

Critères	Pondération	Valeur	Points
Fonctionnalités	6	6	36
Fiabilité	3	6	18
Facilité d'utilisation	5	8	40
Rendement	4	6	24
Maintenabilité	1	0	0
Portabilité	1	0	0
Total	20	5,90	118

Cette note globale de 5,90 sur 10 n'est pas très satisfaisante. On peut prévoir de mettre en place des mesures correctrices de la qualité sur les critères à plus gros coefficients (comme le critère « fonctionnalités » qui n'obtient que la note 6 tout en étant l'essentiel dans un logiciel) ou sur des critères ayant obtenu des notes médiocres.

3. Certification qualité

Au niveau des logiciels, comme au niveau industriel, il existe des normes obligatoires ou optionnelles à respecter pour satisfaire à des critères de qualité.

Des organismes indépendants contrôlent le respect de ces normes de qualité et peuvent ensuite délivrer une certification qui atteste de la qualité au niveau des divers partenaires qui interviennent dans la mise en œuvre d'un projet.

La recherche de la maîtrise des processus dans l'entreprise étendue (entreprise en interne plus tous ses partenaires) d'aujourd'hui passe par la mise en place de certifications, ou tout au moins le respect de normes.

3A. Intérêt de la certification

La certification est un avantage concurrentiel. En effet, réalisée par un organisme extérieur à l'entreprise et ayant une certaine légitimité, elle garantit un niveau de qualité reconnu sur les marchés.

Pour atteindre certains clients, qui ne collaborent qu'à des projets certifiés, elle est un minimum obligatoire. Par exemple, un client certifié, et qui ne veut pas perdre sa certification, ne va collaborer qu'avec des fournisseurs certifiés afin de s'affranchir des problèmes de qualité qui pourraient exister en amont de son activité.

La certification assure le client que le fournisseur a soigné son processus de production et a mis en place une politique de gestion de la qualité.
La certification est basée sur le respect de procédures et processus prédéfinis et connus de tous. L'organisme certificateur vérifie leur mise en œuvre lors de la phase de certification puis contrôle ensuite périodiquement leur évolution.

3B. Présentation de quelques certifications

En informatique, les certifications ne cessent d'évoluer (nouvelles versions ou nouveaux axes de certification).

Présentons un exemple : la certification ISO 17799/2005 (cf. site de l'AFAQ : afaq.org) s'intéresse à la sécurité de l'information. Toute entreprise qui désire s'engager dans un processus de certification ISO 17799/2005 doit réduire ses éléments vulnérables et ses risques majeurs concernant la sécurité. Le document décrivant les procédures à suivre détaille comment procéder pour l'analyse des risques et la mise en place de la politique de sécurité de l'information.

De même, la norme ISO/CEI 90003:2004 couvre toutes les étapes de la gestion de projet du développement d'un logiciel (voir séquence 8). Elle fait appel à des normes plus anciennes qu'elle intègre. Elle renvoie, par exemple, à l'ISO/CEI 12207 concernant les modèles du processus du cycle de vie du logiciel et à l'ISO/CEI TR 15504 pour l'évaluation des fonctionnalités.

La plus connue de toutes les normes ISO dans le domaine de la qualité est la norme ISO 9000 et ses dérivées (9001...). Elle est maintenant ancienne mais sans cesse en réadaptation. Par « management de la qualité » cette norme recouvre :

– les exigences qualité du client ;
– les exigences réglementaires ;
– l'amélioration de la satisfaction du client ;
– l'amélioration des performances concernant tous ces objectifs.

3C. *Grandes étapes de la certification*

Le processus qui mène à la certification peut être long et coûteux pour une entreprise. Il faut tout d'abord adapter l'organisation et les procédures aux exigences préconisées dans les documents détaillant la norme.

Un organisme certificateur vient tout d'abord faire une première visite et rend son rapport dans lequel figurent des conseils. L'entreprise dispose d'un temps d'adaptation avant les visites d'audit suivantes, qui devraient la mener à la certification.

Une fois que ces divers contrôles ont eu lieu, l'entreprise reçoit une certification initiale, qui est en général valable pour trois années, puis des contrôles et audits viennent reconduire ou non cette certification.

L'entreprise peut ainsi, temporairement être fière d'être « **certifiée qualité** » (cf. tous les logos et messages que l'on voit sur les camions, publicités…) et va le faire savoir à ses partenaires.

4. Coût et surcoût de la qualité

4A. *Limite dans la recherche de la qualité*

L'objet de la qualité est de satisfaire avant tout le client mais aussi les processus internes et externes de l'entreprise (entreprise étendue). Mais tout ceci a un coût. En effet, se préoccuper de la qualité mobilise des ressources humaines, organisationnelles et financières. S'en préoccuper à outrance peut coûter à l'entreprise plus cher que cela ne lui rapporte.

Il faut donc savoir s'arrêter dans la recherche de la qualité. En effet, les corrections des premiers dysfonctionnements ou les premières améliorations sont souvent faciles à repérer et à mettre en œuvre, mais, plus on veut s'approcher de la perfection et plus les coûts vont augmenter plus que proportionnellement (exponentiellement).

Par exemple, au niveau de la création d'un logiciel, il est important de se fixer des objectifs réalistes. Un logiciel chargé de conserver et de traiter des dossiers médicaux de patients atteints de maladies graves doit viser la perfection même si son coût de développement est élevé. À l'inverse, un logiciel de migration de données peu importantes (comme des données de prospects éventuels destinées à des publipostages de masse) d'un système vers un autre, peut se permettre d'être peu fiable s'il fournit des listes de rejets que les responsables des services concernés vont décider de traiter « manuellement » ou d'abandonner.

Dans la réalité, cet arbitrage entre qualité et surcoût important dû à la mise en place de la qualité est chose commune. La prise de recul du gestionnaire est un élément impor-

tant dans son activité. L'objectif n'est pas d'atteindre la perfection absolue mais seulement de viser un meilleur niveau que celui des concurrents.

Dans le cas de recherche d'une certification, le niveau de perfection minimum recherché est imposé par les normes édictées dans les documents de certification.

4B. *Importance du facteur temps*

Comme toujours en gestion, le temps est une variable importante. En effet, il est souvent plus coûteux de corriger les erreurs que de « faire bien » dès le départ, et cela croît avec le moment où l'on se rend compte de l'erreur. Plus l'erreur est détectée et corrigée tôt et moindre sera le coût de cette erreur.

Le coût de la non-qualité est d'autant plus important qu'elle est détectée tardivement. Par exemple, il est largement préférable de se rendre compte qu'un produit fonctionne mal lors de contrôles en cours de production et de « rectifier le tir » immédiatement que de se rendre compte de ceci lorsqu'il est déjà présent sur le marché, en constatant que les ventes ne décollent pas car les clients ne sont pas satisfaits. Souvent ces éléments sont laissés de côté car les actions correctrices en cours de production vont prendre du temps et de l'argent, au moment où l'entreprise n'a qu'une hâte : sortir le produit sur le marché avant ses concurrents.

Au niveau de la qualité, le rôle du gestionnaire est donc de trouver le point d'équilibre idéal entre les contraintes internes de son entreprise et celles du marché, et au niveau financier entre une qualité et un coût acceptables par rapport à une « hyper » qualité à un coût faramineux.

Exercice 1

Voici un mini-glossaire présentant quelques éléments de vocabulaire qui pourraient se trouver dans des procédures de qualité relatives à la création de logiciels.

Adaptabilité : capacité du logiciel à évoluer. Facilité avec laquelle un programme peut être modifié pour y ajouter de nouvelles fonctionnalités au fur et à mesure que de nouveaux besoins apparaissent.

Conformité : aptitude d'un logiciel à satisfaire ses spécifications et à répondre aux besoins des utilisateurs.

Complétude : état du logiciel tel que toutes les exigences spécifiées sont réalisées.

Compréhensibilité : facilité avec laquelle un programme peut être compris par la lecture de son code source.

Disponibilité : aptitude du logiciel à assurer sa fonction pendant une période de temps donnée.

Efficacité : aptitude d'un logiciel à n'utiliser que les ressources strictement nécessaires à l'accomplissement de sa fonction. On distingue l'efficacité d'exécution (temps minimum d'exécution) et l'efficacité de stockage (capacité minimum de la mémoire en cours d'exécution).

Ergonomie : étude scientifique de l'homme au travail sous les aspects physiologiques, anatomiques, psychologiques et sociaux. La convivialité et la facilité d'apprentissage pour l'utilisateur font partie de l'ergonomie.

Fiabilité : aptitude du logiciel à accomplir sans défaillance l'ensemble des fonctions spécifiées, à fonctionner dans des conditions anormales sans mettre en cause ni les informations du système, ni leur cohérence.

Flexibilité : caractère d'un logiciel qui définit la facilité avec laquelle des fonctions peuvent être ajoutées, supprimées ou modifiées dans un programme opérationnel.

Intégrité : protection d'un logiciel contre des altérations ou l'accès par des utilisateurs non autorisés (sécurité).

Interopérabilité : capacité du logiciel à échanger des informations avec d'autres logiciels (importation et exportation de données).

Maintenabilité : facilité avec laquelle un défaut peut être localisé, identifié et corrigé.

Modularité : aptitude d'un logiciel à être structuré en composants ou modules indépendants.

Portabilité : capacité d'un logiciel à pouvoir être utilisé sur d'autres matériels ou avec d'autres systèmes d'exploitation sans modifications significatives.

Réutilisabilité : facilité avec laquelle un sous-ensemble du logiciel qui remplit une fonction donnée peut être isolé et employé dans une autre application.

Nous vous rappelons les principales étapes de la gestion de projet vues à la séquence précédente que nous allons appliquer à la création d'un logiciel :

– le schéma directeur ;
– l'étude préalable ;
– l'étude détaillée ;
– l'étude technique ;
– la réalisation ;
– la mise en œuvre ;
– la qualification et la livraison.

Pour chacune des étapes précédentes, indiquez les critères de qualité présents dans le glossaire, qui sont à prendre en compte. Un critère pouvant se retrouver dans plusieurs étapes.

Exercice 2

Un logiciel de gestion-qualité se vante d'avoir les fonctionnalités suivantes concernant chaque « événement qualité » :

– gestion des actions préventives et correctives ;
– gestion des risques associés ;
– affectations multiples des actions (organisation, activités, produits, projets…) ;
– propriétés de suivi des actions (intervenants, moyens, échéances) ;
– planification des actions et vérification d'efficacité ;
– tableaux de bord multiaxes des actions.

1. ***Au vu de ces critères, à quoi peut-on assimiler un « évènement qualité » dans le cadre de ce logiciel ?***
2. ***Quel peut être l'intérêt de la fonction « gestion des risques associés » ?***
3. ***Grâce à ce logiciel, peut-on assurer des « affectations multiples des fonctions » et des « tableaux de bord multiaxes » ? Quel problème cela soulève au niveau de la gestion de la qualité ?***

Séquence 10

La gestion de parcs informatiques

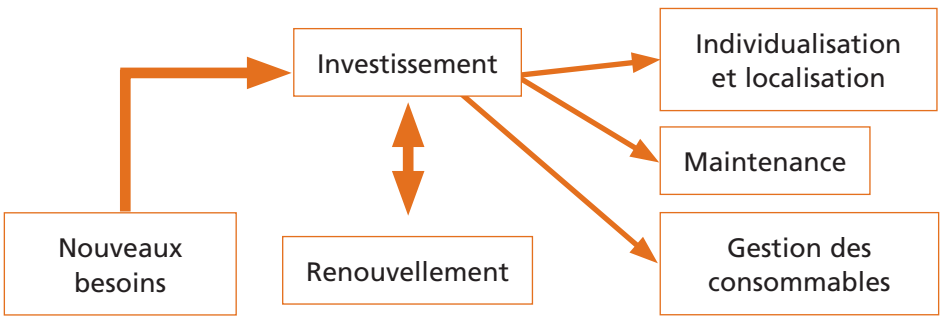
Cette séquence est explicitement au programme des étudiants qui font l'option ARLE mais il est conseillé de le lire, à titre de culture générale, pour le BTS par ceux de l'option DA.

Par « gestion de parc informatique » on pourrait penser à la gestion de l'ensemble des matériels et logiciels du domaine des TIC (technologie de l'information et de la communication) dont dispose l'organisation. De manière encore plus limitative, on pourrait axer cette gestion uniquement sur l'inventaire de ces matériels et logiciels et leur localisation physique. Cette vision de la gestion du parc informatique était certes valable il y a une dizaine d'années, mais aujourd'hui elle s'étend à son financement, à la gestion des immobilisations et au niveau technique à la synchronisation et à l'uniformisation des configurations ou à la gestion des incidents.

1. Qu'est-ce que la gestion de parcs informatiques ?

1A. Présentation

La gestion de parc informatique est un ensemble d'activités s'occupant de l'ensemble des moyens matériels, logiciels et de communication d'une Organisation.
Elle regroupe les activités présentées dans ce schéma :



1B. Objectifs

1B1. Inventorier et localiser les moyens informatiques

Répertorier les matériels et logiciels.

Pouvoir les individualiser (informations globales et précises).

Standardiser les matériels, les logiciels et moyens de communication pour une gestion plus rapide et efficace.

Affecter les matériels et logiciels en fonction de leur disponibilité (sans systématiquement en racheter de nouveaux sans savoir qu'ils existent et sont non-utilisés dans une autre unité de l'entreprise).

Pouvoir négocier plus facilement avec les fournisseurs en ayant un parc plus large et plus homogène.

1B2. Optimiser la maintenance

Gérer administrativement les interventions.

Diminuer les temps de diagnostic et d'intervention.

Suivre les coûts de maintenance et les contrats de prestataires.

1B3. Sécuriser le parc

Assurer une traçabilité du matériel pour repérer les vols ou déplacements inhabituels. Par exemple, pour les ordinateurs portables, il est important de connaître en temps réel l'utilisateur, son point de connexion…

Éviter, ou tout au moins réduire le piratage, par inventaire et standardisation du parc. En identifiant les postes sensibles.

2. Principales fonctionnalités d'un logiciel de gestion de parc

Les trois grands domaines de gestion suivants sont communs à tous les progiciels de gestion de parc. La sécurité n'est pas mentionnée ici comme élément principal car on suppose que toutes les fonctionnalités assurent leur rôle en tenant compte des impératifs de sécurité.

2A. L'inventaire et la localisation

L'inventaire est l'élément essentiel, mais non suffisant aujourd'hui, c'est celui qui a le plus changé dans l'offre logicielle du marché. Il se couple avec la localisation physique des matériels et logiciels, leur marquage et leur affectation à un responsable (ou utilisateur).

Le niveau de détail, la maintenabilité et les facilités d'interrogation de la base de données associée à ce recensement perpétuel sont des critères de choix importants.

La plupart des logiciels permettent de scanner automatiquement le réseau pour détecter les nouveaux matériels et les suppressions de matériels. Une gestion spécifique des matériels sans fils, et surtout de leurs connexions, est appréciée, notamment au niveau sécurité.

2B. Gestion des immobilisations et des licences

Le terme « immobilisations » n'est pas limité ici à son acceptation comptable. On entend, pour cette séquence, ce terme dans le sens des achats de matériels ou logiciels et de leur valorisation financière en tenant compte de leur dépréciation (vétusté et incompatibilité). Certains logiciels incluent une gestion des contrats de maintenance et de services et des interventions associées.

Au niveau des licences, on entend bien sur ici les licences logicielles (nombre, validité, contrats).

2C. Détection et résolution des incidents

L'idéal est un outil qui permette un premier niveau de diagnostic automatique et une prise en main à distance. De plus, certains couplent cette détection avec des logiciels de détection de SPAM (pourriels), ou d'intrusion suspecte. La qualité des statistiques produites par ce module est un élément important dans la disponibilité et la sécurité du système informatique.

Lorsqu'il y a des prises en main à distance pour la maintenance, certains logiciels proposent un suivi au niveau de chaque élément avec des notes horodatées et auto signées.

La gestion des « clients » (Help desk), fonctionnalité associée au module de détection et de résolution des pannes outrepasse en théorie la simple gestion des pannes. Elle concerne, outre les fonctionnalités vues ci-dessus :

- le suivi de tous les types d'interventions ;
- la valorisation de chaque appel pour refacturation ;
- l'historique et le suivi complet de tous les appels, avec accès par divers critères (type d'équipement, de demandeur, de priorité, de périodicité…) ;
- la mise à disposition de documentations pour les utilisateurs et pour les techniciens ainsi que de « foires aux questions » (FAQ : frequently asked questions).

Exercice

Une étude de cas serait trop théorique, ou trop complexe pour cette séquence. Nous vous proposons donc de rechercher quelques logiciels de gestion de parc informatique proposés sur le marché actuellement et de les comparer en définissant vous-même vos critères.

Unité 4

Les TIC au service du système d'information

▶ *Contenu*

Séquence 11

Les outils TIC au service du système d'information

Dans cette séquence et la suivante nous allons détailler quelques éléments des technologies de l'information et de la communication (TIC) et analyser leurs apports pour le SI.

Nous nous limiterons aux outils suivants :

– progiciel de gestion intégrée ;

– collecticiel et outil de travail collaboratif ;

– entrepôt de données ;

– informatique nomade ;

– internet, Intranet.

1. Les progiciels de gestion intégrée

Les progiciels de gestion intégrée PGI (ou en anglais ERP enterprise ressource planning) sont des progiciels qui permettent d'intégrer la gestion de tous les sous systèmes d'information que nous avons déjà analysés (séquence 2) :

– comptabilité et gestion des flux financiers ;

– gestion de production ;

– gestions des ressources humaines ;

– administration…

Dans un PGI, ces divers domaines utilisent une base de données unique au niveau logique. Ils couvrent l'ensemble des fonctionnalités nécessaires à la gestion de ces divers sous-SI.

Comme toutes les Organisations n'ont pas les mêmes besoins, le paramétrage d'un PGI peut s'avérer une tâche très importante, souvent gérée comme un projet à part entière.

Les PGI prétendent répondre à tous les domaines d'activités et les processus support d'une entreprise. Mais, dans la réalité, on constate qu'ils ont tendance à se spécialiser en fonction du niveau de détail de leur principale fonctionnalité : commerce (voir les progiciels de gestion de la relation client), bâtiment, comptabilité, professions médicales…

Ceci pour des raisons commerciales, mais aussi parce que lorsqu'un progiciel est spécialisé dans un « métier » spécifique, il peut gérer les autres domaines supports des entreprises de ce « métier » plus efficacement. Par exemple, un PGI spécialisé dans la gestion des dossiers médicaux, outre ses « compétences » médicales, ne va pas présenter les mêmes fonctionnalités pour le domaine (support) comptable qu'un PGI destiné aux professions de la construction. C'est pourquoi, il sera mieux adapté qu'un PGI plus général non seulement dans le métier principal de sa spécialité (« gestion médicale ») mais aussi dans les autres domaines de gestion de l'entreprise.

Un PGI unique est donc illusoire, trop difficile à paramétrer et difficilement adaptable à tous les cas d'entreprises. On lui préfère aujourd'hui un PGI spécialisé par métier qui est déjà pré-paramétré pour la profession et peut proposer des fonctionnalités spécifiques.

Un PGI est souvent vu comme un élément permettant de gagner en compétitivité par une automatisation globale et unique des divers processus de l'entreprise. Il y a partage des informations et synergie entre les divers processus qui permettent une meilleure gestion du système d'information de l'entreprise.

Le reproche essentiel qui est fait aux PGI est qu'en intégrant toute la gestion de la structure organisationnelle, cette dernière ne peut plus être spécifique à une entreprise particulière mais à des chances de se retrouver dans les diverses organisations qui acquièrent le même PGI. La structure organisationnelle d'une entreprise est donc moins spécifique, et ne représente plus un avantage concurrentiel déterminant.

2. Les collecticiels et la gestion de la connaissance

L'exemple type de collecticiel (ou synergiciel, ou en anglais groupware) est un outil qui permet de travailler à plusieurs personnes sur un même document ou un même projet. Mais ses fonctionnalités sont bien plus étendues.

Un collecticiel est basé sur un principe du partage de données et de connaissances entre personnes qui ne sont pas toutes au même endroit, et ne collaborent pas toutes spécialement au même moment. Elles disposent d'un environnement partagé où peuvent être coordonnées leurs diverses activités.

Quelques fonctionnalités classiques d'un collecticiel sont :

- le travail collaboratif avec participation de chaque membre du groupe ;
- une base de documents partagée ;
- des outils de coordination : gestion des flux, du temps et des tâches ;
- des agendas des divers collaborateurs interfaçables entre eux ;
- une messagerie électronique avec ses fonctionnalités de sécurité, classement, rappel, réponse automatique… ;
- des forums ;
- la possibilité de réunions à distance.

Aujourd'hui, ce type de travail collaboratif tend à évoluer vers la gestion des connaissances (knowledge management) qui, outre des bases de données conséquentes sur les savoirs, permet de décrire la connaissance d'une personne en faisant ressortir son savoir-faire tout autant que son savoir. Ces savoir-faire sont souvent difficiles à formaliser car ils sont tacites et « font partie » de chaque personne. Une mission de la gestion des ressources humaines est d'inciter les individus à collaborer à ce recueil et cette mise en forme des savoirs et savoir-faire.

Au niveau des outils informatiques de gestion de la connaissance on trouve tout d'abord les (anciens) systèmes experts qui simulent le raisonnement d'un expert dans un domaine précis et les agents intelligents qui exécutent en tâche de fond et périodiquement des opérations précises, souvent sur Internet, pour aider les décideurs.

La gestion des connaissances, faisant partie du capital immatériel de l'entreprise, n'est pas valorisée financièrement mais représente un capital-réussite pour une entreprise dans le futur. Elle ne peut se dissocier de facteurs humains et organisationnels.

3. Les entrepôts de données et leurs outils de forage

Nous pourrions assimiler un entrepôt de données (data warehouse) à un entrepôt classique où seraient stockées toutes les informations d'un système d'information. Cependant trois différences cruciales sont à noter.

- Toutes les données ne sont pas physiquement présentes dans l'entrepôt, mais des liens vers des bases de données externes permettent d'accéder à certaines d'entre elles.
- Le rangement est bien différent de celui d'un entrepôt classique car chaque donnée peut être multi-indexée et donc accessible à partir de divers critères (notion d'accès multidimensionnel). Comme si un objet placé dans un entrepôt pouvait être accessible directement de plusieurs points géographiquement différents de cet entrepôt. Prenons l'exemple du chiffre d'affaires réalisé au mois de décembre 2006. Ce dernier peut être accessible directement au niveau comptable ou reconstitué instantanément à partir des ventes par type d'article, type de commercial, type de point de vente…
- Certaines données ne sont pas présentes dans l'entrepôt, on retrouve seulement des données agrégées issues de traitements précédents sur des données de base. Par exemple, le chiffre d'affaires ci-dessus a pu être calculé à partir de toutes les factures du mois qui elles, ne sont pas dans l'entrepôt mais dans des bases de données annexes. Ce chiffre d'affaires global a donc été calculé à partir des données de base et ce n'est que son résultat qui est stocké dans l'entrepôt.

Le stockage des données ne rassemble que logiquement les diverses données éparpillées dans les bases de données de l'entreprise. Cependant, pour des questions de rapidité, des copies peuvent être partiellement réalisées. Des solutions mixtes telles que la création d'une nouvelle base de données centralisée pour les données agrégées, et le fait de laisser les données opérationnelles sur les bases initiales, sont souvent adoptées.

Des outils d'extraction et d'agrégation de données sont donc des éléments importants d'un entrepôt de données. On les appelle aussi des outils de forage (ou anglais data mining).

Au niveau de la consultation, l'entrepôt de données ne peut se dissocier, ou possède lui même, des outils d'aide à la décision (foreurs de données, requêteurs…). En effet, les données d'un entrepôt de données sont essentiellement utilisées par des outils d'aide à la décision (voir séquence 3) pour aider les dirigeants. La technologie la plus connue est OLAP (online analytical processing) qui fournit au demandeur des données déjà regroupées par thème sous forme d'un ensemble de données. Les thèmes des paquets sont prédéfinis et l'utilisateur en retire les éléments qu'il désire grâce à des outils d'aide à la décision. Par exemple, si on reprend le chiffre d'affaires, un paquet peut fournir les données du chiffre d'affaires selon divers critères et chaque utilisateur ira rechercher les informations pertinentes pour lui dans le paquet.

On représente souvent ces différents modes d'accès multidimensionnels par un cube ou une structure à plusieurs dimensions. Cette représentation illustre le fait qu'une donnée peut être accessible par divers critères.

4. L'informatique nomade

Il serait prétentieux de vouloir faire la liste des outils d'informatique nomade car ces derniers ne cessent d'évoluer au niveau logiciel comme matériel.

L'ordinateur portable et la possibilité de se connecter au réseau de l'entreprise à distance, sont des outils TIC qui rendent d'importants services à l'entreprise. Ceci surtout pour les salariés amenés à se déplacer constamment. Ils leurs permettent de consulter les données de l'entreprise et d'envoyer à celle-ci les données qu'ils viennent d'acquérir ou de créer.

La possibilité d'accéder à Internet ou à un Intranet par téléphone portable n'est pas que l'outil préféré des commerciaux mais aussi des artisans, constructeurs, hauts cadres… qui peuvent décider de recevoir tous ou certains mèls ou messages d'alerte importants (voir séquence 3, les tableaux de bord) sur leurs outils mobiles.

5. Internet et Intranet

Internet, et Intranet (un réseau limité à une Organisation) ne sont plus à présenter. Ils permettent d'accéder à tous les outils TIC que nous avons présentés et favorisent la mise en place des pratiques liées au TIC que nous analyserons dans la séquence suivante.

C'est tout d'abord grâce à la mise en réseau, et donc aux connexions et échanges à distance, que les outils TIC tels que les collecticiels peuvent être mis en place et reliés aussi bien sur un réseau local que global.

Intranet et Internet, outre l'aspect communication et gestion, ont apporté de nouvelles possibilités d'exploitation au système d'information de l'entreprise, nous allons donc voir tout d'abord leurs apports avant de rechercher leurs limites.

Au niveau des avantages techniques, on peut citer :

- la personnalisation du poste client (concept de client/serveur) qui peut être un avantage concurrentiel important, surtout pour les partenaires (clients, fournisseurs…) ;
- la meilleure gestion de parc informatique (voir séquence correspondante) ;
- le fait que l'on peut communiquer avec des matériels hétéroclites sans même le savoir (entre un Mac et un PC par exemple).

Au niveau des avantages organisationnels la communication interne, inter-organisationnelle ou externe est un premier atout général, ne serait-ce qu'avec le courrier électronique.

On trouve également de nouvelles possibilités d'organisation dans le partage d'informations et de connaissances entre personnes d'une même société situées dans des lieux géographiques différents, et très reculés pour certains. Si on reprend l'exemple du collecticiel, rien n'empêche aujourd'hui de créer un groupe de projet avec des personnes situées à des points du globe diamétralement opposés (affranchissement des contraintes de localisation et de décalage horaire). Globalement Internet et Intranet améliorent la réactivité de l'entreprise si l'information est correctement (*et rapidement !*) recueillie et traitée en interne.

Au niveau des limites techniques, plus l'ouverture extérieure du SI d'une entreprise s'ouvre et plus la sécurité prend de l'importance (voir dernières séquences). De même, la puissance des moyens informatiques (capacité, rapidité…) devra suivre le développement des outils Internet ou Intranet sous peine de minimiser leurs avantages (temps d'accès…).

Au niveau des limites organisationnelles, les problèmes naissent souvent de l'aspect humain. Des réticences à faire confiance aux outils Internet ou Intranet, ou tout simplement le fait d'oublier de les utiliser et de passer beaucoup plus de temps à recherche ou traiter l'information sont encore d'actualité. À l'inverse, dans une organisation, Internet (et la messagerie électronique) ne sont-ils pas des perturbateurs ou « mangeurs de temps » pour des considérations personnelles des salariés au détriment des considérations professionnelles ?

Séquence 12

Les pratiques TIC au service du système d'information

Cette séquence va nous permettre de présenter d'autres outils TIC en nous axant davantage sur les pratiques organisationnelles qui leur sont liées. Comme dans toute séquence faisant appel à l'analyse d'une organisation ou au SI (système d'information), nous vous invitons à faire le lien entre ce cours et celui d'économie d'entreprise.

Nous aborderons les points suivants :

– gestion électronique de documents ;

– gestion de processus et de flux ;

– échange de données informatisé ;

– commerce électronique.

1. La gestion électronique de documents

Dans un garage automobile si une secrétaire veut retrouver une facture suite à l'appel d'un client elle a généralement deux possibilités : rechercher dans le classeur des dernières factures ou des factures de telle période le document ou consulter son logiciel de facturation et y chercher la facture par client ou type de client. Ces recherches ont des chances d'aboutir si la secrétaire est bien organisée, surtout au niveau de son classement.

En revanche, si demain, un constructeur l'appelle en lui disant de rechercher toutes les réparations dans lesquelles a été utilisée la pièce XF15 car cette dernière possède des défauts entravant la sécurité des véhicules, l'opération sera beaucoup plus compliquée.

La GED (gestion électronique de documents), ou GEIDE (gestion électronique d'informations et de documents pour l'entreprise) pourrait l'aider à classer et ainsi retrouver un document au regard de divers critères : date, type de client, type de véhicule, modèle de véhicule…

La GED permet de dématérialiser, d'indexer, de classer, de recueillir, de rechercher et de stocker des documents. Ces documents peuvent être de diverses formes : textes, images, sons… Elle dispose pour cela de divers moyens informatiques et organisationnels.

1A. Les étapes de la GED

Pour mettre en place un projet GED (ou GEIDE, son homologue qui incorpore la notion de gestion des contenus) les documents doivent passer par les étapes suivantes.

1A1. Le recueil et la numérisation de documents

Dans un premier temps, on va numériser les documents, ou stocker ceux qui sont déjà sous forme numérique. Ce stockage permet de diminuer leur volume, d'assurer leur

pérennité, d'éviter les nombreuses tâches d'archivage, d'économiser sur les coûts papier ou supports multimédia. Le but principal étant qu'ils soient accessibles et consultables par tous les acteurs qui en ont besoin et qui y sont autorisés. Des outils de numérisation (scanners…), de duplication, de reconnaissance de documents ou de caractères (ROC : reconnaissance optique de caractères) sont utilisés pour cela.

1A2. L'indexation

L'indexation est la phase la plus importante car un document qui n'est pas atteignable par un mot clé pertinent ne pourra être facilement accessible. Comme disent les documentalistes « tout ouvrage mal rangé peut être considéré comme perdu », nous pourrions adapter ceci à la GED en disant qu'un document mal indexé peut être considéré comme non accessible.

1A3. Le stockage sécurisé

Une fois les documents indexés, il est important d'organiser leur stockage en ayant mûrement réfléchi à l'arborescence des dossiers, sous-dossiers… (voir cours d'ALSI). Ceci pour les recherches et accès futurs.

De plus, des procédures de sécurité (voir dernières séquences) devront être mises en place car le contenu des documents manipulés par la GED contient des informations précieuses pour l'organisation qui les possède. L'entreprise ne peut se permettre de perdre ou détruire certains documents, surtout s'ils n'existent que sous forme électronique.

1A4. La recherche et la diffusion de documents

La base d'une bonne recherche réside avant tout dans une excellente indexation. Les outils de recherche (butineurs, moteurs de recherche…) doivent être efficaces, conviviaux et souples.

Une fois le document trouvé, il est important de pouvoir le publier dans le format que l'on désire : impression papier, visualisation, intégration dans un autre document ou un outil de présentation…

1B. La distinction entre contenu et présentation

Aujourd'hui un même document peut servir dans diverses applications informatiques et nécessiter des présentations différentes (graphisme adapté à l'application et/ou l'utilisateur, sélection de certaines données…) alors que son contenu est identique. À l'inverse, une même présentation peut contenir des données différentes selon les circonstances.

De plus, le développement des outils Web, nécessite des outils graphiques de plus en plus sophistiqués et faisant appel à des spécialistes à part entière (les graphistes Web). C'est pourquoi, à la fois au niveau du développement et du stockage, on distingue de manière séparée le contenu de la présentation d'un document.

Traditionnellement les pages du Web sont établies en HTML (hypertext mark-up language). Mais lorsque la dynamique et la structuration deviennent obligatoires, il faut passer à un langage de description de données tel XML (extensible markup language) qui est aussi un langage à balises mais dont l'utilisateur peut les définir à sa guise.

L'avantage d'XML est de stocker des données indépendamment de leur présentation et de pouvoir les échanger avec d'autres outils dans un format standard. Les outils « destinataires » pourront à leur tour les afficher ou les traiter selon leurs besoins.

1C. *Les gains induits par la GED*

Le coût du papier étant souvent abordable pour une entreprise, et les habitudes anciennes aidant, ce n'est pas le critère financier mais plus des critères socio-écologiques qui ont participé à faire accepter la GED comme élément faisant faire des économies. Le coût des multiples archives (photocopies) a été réduit considérablement.

Le gain se retrouve essentiellement dans les avantages de la consultation en ligne : rapidité, partage, accès direct, accès sans connaître au préalable l'existence du document.

La GED ne peut réellement se dissocier des flux de travail dans une organisation.

2. Gestion des processus et des flux

La gestion des processus et des flux (ou en anglais workflow) tente d'automatiser le circuit de traitement d'un document, et plus généralement les flux de travail.

Par exemple, si un employé veut remplir une fiche de demande de congés, on peut imaginer les flux concernant l'automatisation d'un seul et même formulaire de demande de congés, qui subira le circuit suivant :

Étape	Employé	Supérieur hiérarchique	Service du personnel
1	Remplit le formulaire avec sa demande		
2		Consulte et apprécie la demande	
3	Reçoit le formulaire avec la réponse		Reçoit l'information pour décompter des jours de congés du salarié

Comme vous le voyez tous ces flux sont automatisés étape par étape. Chaque acteur rajoute une information ou prend en compte une information pour un autre traitement qui le concerne.

La gestion des processus et des flux et donc basée sur trois éléments :

- la circulation d'un document électronique avec la possibilité d'enrichissement de ce document par les divers acteurs : on prédéfinit quel type d'acteur peut consulter et/ou modifier quelle donnée ;
- le rôle des divers acteurs : un acteur peut être un groupe de personnes (ex : tous les chefs de service d'un même niveau, toutes les personnes d'un certain secteur d'activité…) ;
- la coordination de ces diverses étapes par un système de règles qui décrivent comment les acteurs interviennent sur les documents : à quelles étapes et pour quel type de modification ou de consultation.

Le workflow permet donc d'automatiser les processus et de réduire la circulation du papier.

Au niveau de l'implémentation, la gestion des flux et des processus se base sur un collecticiel pour les interventions successives et programmées des divers acteurs et sur la GED au niveau du document lui-même.

Ces systèmes fonctionnent correctement à condition que le troisième élément fondamental : la coordination, soit bien organisée. Supposez, dans l'exemple ci-dessus, que le seul destinataire possible du formulaire de demande de congés soit le supérieur hiérarchique direct de chaque salarié. Si ce supérieur est absent pour une longue durée et qu'il n'est pas prévu que dans ce cas le document puisse être rerouté vers une personne, le salarié ne pourra jamais émettre sa demande de congés.

De même, la gestion des flux et des processus implique que tous les acteurs participent activement à cette gestion. En effet, si le supérieur hiérarchique ne consulte que rarement les documents qui arrivent pour validation, le demande de congés sera bloquée. Les outils GED, proposent de pouvoir relancer automatiquement une personne en retard, ou de rediriger un flux vers un autre acteur. Il faudra donc prendre soin de leur paramétrage dans un souci de souplesse organisationnelle afin de ne pas paralyser le système.

3. L'échange de données informatisé

Si un client veut envoyer, sous forme électronique, un bon de commande à un fournisseur, il faut que ce document soit intégré dans les deux systèmes d'information (SI) des partenaires. L'EDI (échange de données informatisé ou en anglais electronic data interchange) s'occupe du fait que le bon de commande puisse être prélevé dans le logiciel de génération des commandes du client, puis traduit dans un format transportable, puis retraduit dans le format de fichier du SI du fournisseur qui gère l'arrivée des commandes.

Historiquement les partenaires se mettaient d'accord entre eux sur un format de fichier structuré (voir cours de DAIGL). Le client transformait le fichier initial dans le format négocié entre les deux parties. Puis, à l'arrivée, le fournisseur tenait compte du format en question pour le remettre au format nécessité par son logiciel de gestion des commandes arrivées. Plus tard, le besoin de rédiger des normes standard s'est fait sentir. Les premières normes concernaient des secteurs d'activité : transport, échanges interbancaires... Des organismes de normalisation, ont alors vu le jour et ont rédigé des normes telle EDIFACT (EDI for administration, commerce and transport) qui est toujours utilisée aujourd'hui. Ces normes sont internationales et concernent l'échange de données dans le milieu des affaires.

Comme nous l'avons vu dans le premier point concernant la GED (gestion électronique de documents), XML (extensible markup language) est un langage à balises qui décrit la structure des données d'un document. Il permet de structurer, de définir le vocabulaire et la syntaxe des données.

XML répond donc à la problématique de l'EDI ; à savoir, définir un format d'échange selon les besoins. Il offre également des mécanismes de vérification de la validité d'un document. Des analyseurs (ou parseurs) permettent d'extraire le contenu d'un document XML.

XML est donc en passe de devenir le langage de description de l'EDI grâce à l'incorporation, dans XML de la description des données normalisée d'EDIFACT.

Quel que soit le type de normalisation utilisée pour les échanges, l'EDI est un atout important pour les entreprises au niveau de la rapidité des échanges (moins de ressaisie, intégration automatique dans les divers SI, ...) et de leur fiabilité. Ces deux avantages liés à la qualité des échanges aident à créer de meilleures relations entre les partenaires.

4. Le commerce électronique

Le commerce électronique (e-commerce ou electronic commerce) n'est plus à présenter aujourd'hui vu son essor considérable dans les dernières années. Cet essor vient entre autres :

- du développement du nombre de sites qui présentent un choix plus large au consommateur ;
- des sites comparateurs dont certains sont spécialisés par domaine ;
- de l'abolition partielle des contraintes géographiques dans les possibilités d'achat ;
- de l'augmentation de la confiance associée aux paiements en ligne ;
- de l'augmentation du nombre d'accès à Internet par les clients potentiels ;
- de l'efficacité accrue des problèmes de logistique qui se sont posés aux fournisseurs lors des premiers temps ;
- des améliorations graphiques qui permettent de mieux présenter, voire de personnaliser la présentation des produits…

Le commerce électronique ne se limite pas aux relations entre distributeur et consommateur final, il gère aussi les relations inter organisationnelles par le commerce entre entreprises (B to B business to business) ou les relations des entreprises avec les administrations (B to A business to administration)

De même, les sites Internet de commerce ne se limitent pas à la vente, ils participent à la promotion des produits, à l'image de marque, à la mise en ligne de notices et autres documents qui allègent les services après-vente.

En mercatique, le profilage des consommateurs permet de restreindre le champ des cibles visées. Le profilage est le fait que l'on peut mémoriser les pages visitées par un consommateur, ses achats ou les réponses à des questions pour, lors de ses prochaines visites, lui proposer directement les produits auxquels il est sensible. Visitez les grands sites de ventes de produits multimédia et vous pourrez vous rendre compte de la précision de ses investigations.

Le commerce électronique est donc un créneau à part entière pour le commerce et tend à influencer également le commerce traditionnel.

En revanche, le commerce électronique ne présente pas que des atouts pour une entreprise.

Au niveau de la structure organisationnelle et de la participation du personnel aux diverses activités, des refontes ont été nécessaires. Le traitement des ventes électroniques ne peut se réaliser en interne comme sur un point de vente classique. Le personnel s'est donc vu imposer cette évolution avec tous les problèmes de résistance au changement que cela pose.

La logistique (stockage, préparation des colis, transport, livraison…) a mis du temps à s'adapter à cette nouvelle forme de commerce. La réactivité étant de mise dans ce type de commerce, la logistique doit viser le « zéro défaut ». Les entreprises vendeuses externalisent plus en plus les fonctions logistiques en se concentrant sur leur métier de base. En revanche, les entreprises de logistique ont développé des organisations et des compétences performantes pour répondre à ce type de commerce.

Des entreprises qui ne travaillaient auparavant qu'au niveau national, ont vu les portes internationales s'ouvrir à elles sans s'être réellement préparées aux problèmes liés au commerce international : droits de douane, TVA …

De même, il a fallu réagir pour certains, et profiter de nouvelles opportunités commerciales pour d'autres, à la réticence des consommateurs face aux paiements en ligne.

La carte bancaire reste le moyen privilégié pour ce type de commerce. Les protocoles de cryptage et de sécurisation des transferts tels SET ou SSL ont été développés. Tout d'abord, le numéro de carte bancaire va être crypté (par un système comme SIPS) avant d'être transmis sur le réseau. Un protocole de sécurité comme SSL (secure sockets layers), ou SET, basé sur un système de clé publique permet de sécuriser la transaction (voir dernières séquences sur la sécurité).

Unité 5

Sécurité du SI

▶ *Contenu*

▶ *Introduction*

Bienvenue dans cette partie du cours de GEOSI, qui traite de **cindynique informatique.**

Kesako la cindynique ? C'est la science qui étudie les risques (industriels, sociaux, économiques, informatiques…).

Le terme **cindynique** vient du grec **kindunos**, qui signifie **danger**.

Cette appellation a été créée en 1987 lors d'un colloque tenu à la Sorbonne.

Son objectif est de répondre aux questions : comment identifier le risque, comment le mesurer, quelles en sont les conséquences et comment le contourner ?

La cindynique utilise souvent la notion d'**événement non souhaité** (ENS), et d'**effet pervers**.

La cindynique a été introduite en 1989 dans la maîtrise des activités informatiques par Didier **Hallépée**. Selon celui-ci, la cindynique devrait être considérée comme une branche spécialisée de l'axiologie, qui est la science de la qualité.

Face aux risques informatiques, il est nécessaire d'organiser la **sécurité informatique**.

La sécurité informatique est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des risques accidentels ou intentionnels.

Les dispositifs de sécurité sont devenus incontournables, surtout avec l'ouverture des frontières du SI hors de l'entreprise.

Le thème de cette 5e partie du cours de GEOSI est un recensement des risques et des solutions face à la sécurisation du système d'information.

Le but de ce cours est de vous sensibiliser aux problèmes de sécurité, de vous initier à être capable d'évaluer et relativiser les risques, et à rechercher les moyens pour s'en prémunir (gestion de la sécurité, sauvegardes et procédures de reprise, contrôle d'accès, audit, etc.).

Dans le Larousse de l'informatique, la définition du système d'information d'une organisation est la suivante :
« Ensemble constitué par :
– les données nécessaires au fonctionnement de l'organisation ;
– les moyens informatiques et bureautiques nécessaires à leur traitement et leur circulation. »

Le **système informatique** est la partie technique du système d'information.
Donc, la sécurité du système d'information nécessite la sécurisation du système informatique, et recouvre les aspects **matériels** et **logiciels**.

Bien entendu, la sécurité est un thème transversal, qui n'est pas traité que dans cette partie du programme de BTS. Voici ci-dessous ce que l'on trouve dans le référentiel du BTS, concernant la sécurité.

La sécurité et le référentiel du BTS IG

Parties du référentiel concernées par la sécurité informatique
Les informations écrites en *italique* concernent l'option ARLE.
Les autres informations concernent les deux options.

Contenus	Capacités attendues
S13. Technologie des périphériques Dispositifs de sécurité	– Décrire le rôle et les principales caractéristiques techniques et fonctionnelles des périphériques. – Identifier les technologies et normes relatives aux périphériques. – Installer et configurer un périphérique.
S23. Techniques d'administration d'un réseau – Administration de réseaux, gestion du parc matériel, télécollect. – Gestion des logiciels et des licences, télédistribution. – Maintenance, surveillance, télé-diagnostic, télémaintenance. – Métrologie et sécurité, intégrité des données, sauvegardes.	– Administrer un réseau local. – Assurer la sécurité d'un réseau local. – Assurer la gestion d'un parc matériel et logiciel. – Assurer la surveillance et la maintenance d'un réseau local. – Installer le système d'exploitation d'un réseau.
S25. Système de gestion de base de données relationnel Administration de la base de données. Protection, sécurité, sauvegarde, restauration, gestion des accès concurrents, journalisation, paramétrage.	– Administrer une base de données non répartie et en assurer la sécurité.
S44. Sécurité informatique Objectifs et enjeux Typologie des risques informatiques Principales techniques de sécurisation	– Mettre en œuvre un logiciel « antivirus ». – Évaluer tout ou partie de la sécurité d'un système informatique et mettre en œuvre des dispositifs de sécurité. – Participer à la réalisation d'un plan de reprise. – *Repérer les problèmes de sécurité posés par l'accès à des réseaux d'échanges de données.*

Dans le référentiel réseau, outre les savoirs inscrits dans le tableau ci-dessus, on trouve une liste de compétences spécifiques à la sécurité, compétences que doivent acquérir les administrateurs de réseaux locaux d'entreprise.
Je ne traiterai pas dans ce cours la partie « Mains dans le cambouis » spécifique à l'option ARLE.

Par contre, je traiterai l'aspect « culturel », « veille technologique », et je m'appuierai pour construire ce cours, sur le tableau ci-dessus, mais aussi sur le tableau ci-dessous, qui recense les compétences de l'option ARLE relatives à la sécurité.

Pourquoi ?
Ce référentiel a presque dix ans. Depuis qu'il a vu le jour, il s'est produit une montée en puissance de l'utilisation des réseaux, locaux, virtuels, éloignés, Internet, Intranets, etc. Tout développeur qui se respecte doit connaître ces différents types d'infrastructures, mais aussi tous les risques et solutions liés à la sécurisation de ces environnements plus ou moins ouverts.

Depuis un certain nombre d'années, à l'examen, on trouve, y compris dans les études de cas de l'option développeur, des questions concernant la sécurité. Vous devez donc, toutes options confondues, être capables de répondre à ces questions.

En outre, un développeur développe, la plupart du temps, des applications en environnement réseau. Il doit donc savoir tenir compte de l'environnement réseau dans sa façon de développer, savoir sécuriser ses applications, et savoir aussi tenir compte des risques et des dispositifs de sécurité présents dans l'environnement d'exécution des logiciels qu'il développe.

Je recommande donc vivement à tous de travailler tout le cours, même si à l'origine, certaines compétences sont spécifiques aux ARLE.
Voici ci-dessous le tableau des compétences spécifiques aux ARLE et relatives à la sécurité.
J'ai mis en gras tous les mots liés aux thèmes des risques et de la sécurité. J'ai sélectionné seulement les passages directement liés à ces thèmes.

<table>
<tr><th colspan="2">Compétences spécifiques aux ARLE</th></tr>
<tr><td colspan="2">C2. INSTALLER ET CONFIGURER
Contexte général de réalisation : les interventions d'installation et de configuration d'une solution réseau local sont envisagées dans le strict respect des consignes de sécurité et par application d'une démarche rationnelle.
Critères généraux d'évaluation :
– utilisation cohérente des concepts et de la terminologie de référence ;
– conformité et qualité des éléments installés ;
– maîtrise de l'ordonnancement des tâches ;
– optimisation de la procédure d'installation ;
– respect des délais.</td></tr>
<tr><th>Compétence</th><th>Situation</th></tr>
<tr><td>C23. Installer et configurer un dispositif de sécurité, matériel ou logiciel.</td><td>• Un réseau en état de fonctionnement.
• Un dispositif de sécurité à installer.
• Une documentation technique.
• Les consignes d'installation.</td></tr>
<tr><td colspan="2">C3. Administrer et maintenir
• Contexte général de réalisation : les interventions d'administration d'un réseau local et de maintenance de ses différents composants, sont assurées dans un environnement technique maîtrisé.
• Critères généraux d'évaluation :
– réactivité et adaptation aux pannes ;
– respect des règles de sécurité.</td></tr>
<tr><th>Compétence</th><th>Situation</th></tr>
<tr><td>C33. Assurer la sécurité du réseau.</td><td>• Maîtrise des risques associés à l'utilisation d'un réseau.
• Connaissance et respect des consignes de sécurité permettant de prévenir les risques, de les réduire ou de les corriger.</td></tr>
<tr><td>C34. Surveiller et optimiser le trafic sur le réseau ainsi que le niveau d'activité des serveurs, diagnostiquer et mesurer les pannes. Identifier la nature des anomalies et effectuer le dépannage de premier niveau.</td><td>• Un réseau en état de fonctionnement dégradé ou de dysfonctionnement.
• Des outils de surveillance du trafic et de l'activité des serveurs.
• Précision de l'identification des symptômes de dysfonctionnement du réseau.
• Pertinence du choix de la réponse à apporter et de l'intervenant à solliciter.</td></tr>
</table>

Vous avez peut-être remarqué, à la lecture des textes officiels reproduits ci-dessus, que dans cette partie du cours de GEOSI, il n'est pas uniquement question de sécuriser le **système d'information** en tant que base de données, mais aussi le **système informatique**, c'est-à-dire qu'en fait, il faut qu'on s'intéresse à au moins trois niveaux de sécurité :
– la sécurité au niveau du matériel, y compris en environnement réseau ;
– la sécurité au niveau du système d'exploitation, y compris en environnement réseau ;
– la sécurité au niveau logiciel, y compris en environnement réseau.
Le système d'information de l'entreprise s'appuie en effet sur le matériel informatique,

sur le système d'exploitation et sur les applications. C'est cet ensemble que désigne l'expression **système informatique**.

Les configurations matérielles et logicielles possibles sont nombreuses : postes locaux, postes en réseau, réseau fermé ou ouvert, réseau standard ou intranet,…

En ce qui concerne la partie logicielle du système d'information (les bases de données et les applications), appelé le SIA (pour SI automatisé), on a aussi un grand nombre d'implantations possibles : système centralisé, réparti, au sein d'un réseau local, d'un réseau étendu, données centralisées ou réparties, traitements centralisés ou répartis, etc.

La logique métier gravitant autour du SIA a également son importance : les données manipulées sont-elles sensibles ? À caractère confidentiel ? Font-elles l'objet de transfert via des lignes réseau ? Etc.

Bien entendu, on ne choisira pas la même politique de sécurité selon, par exemple, que notre SIA abrite des recettes de cuisine et leurs ingrédients, accessibles depuis une interface web, ou selon qu'il héberge des données à caractère personnel ou des données sensibles.

La stratégie de sécurité sera plus importante dans certains cas que dans d'autres.

Il est important d'être conscient du degré minimum de sécurisation, mais il faut aussi être conscient que certains outils de sécurisation sont inutilement coûteux parfois.

Par exemple, pour notre site hébergeant et rendant accessibles des recettes de cuisine et leurs ingrédients, on ne va pas sortir l'artillerie lourde, cela coûterait beaucoup d'argent pour rien. On va se contenter de sécuriser le serveur et de protéger le SIA de la destruction et de l'endommagement.

Pourquoi prévoir un cours spécifique sur la sécurité ?

Ce cours a pour but de recenser le plus exhaustivement possible tous les risques existants et les solutions pour s'en prémunir.

Il vient en complément de ce qui est abordé plus ponctuellement dans les autres cours à propos de la sécurité. Je souhaite rassembler ici, en une sorte de synthèse, les concepts, techniques et outils liés à la sécurité, que l'on aborde ici de manière transversale, alors que dans les autres cours, le traitement du thème est lié au thème du cours (réseau, base de données, matériel…).

La sécurité et la prévention des risques font désormais l'objet de métiers à part entière, comme le métier d'**Architecte en sécurité**, par exemple. Il s'agit, dans ce travail, de déterminer la stratégie globale de sécurité informatique de l'entreprise, des couches matérielles aux couches logicielles, en passant par les couches réseau, ceci sans oublier l'aspect humain.

Les compétences visées par ce cours sont donc un peu, toutes proportions gardées, celles d'un consultant (connaître à peu près tout ce qui existe en matière de sécurité). Nous resterons bien modestes par rapport à cet objectif.

Il s'agit en fait pour vous de :

– connaître les différents types de risques représentant un danger pour un environnement informatique ;
– savoir choisir le bon dispositif de sécurité, de prévention, en fonction des besoins exprimés concernant une politique de prévention, un risque, une défaillance éventuelle… ;
– savoir comment est organisé un plan de reprise en cas de défaillance, ou comment organiser une politique de sécurité préventive.

C'est quoi au juste, la sécurité du système informatique ?

Une définition

C'est l'ensemble des mesures prises pour assurer, la confidentialité, l'intégrité, la disponibilité et l'authentification.

La sécurité informatique recouvre donc les situations, l'organisation, les conditions matérielles et logicielles qui correspondent à l'absence réelle de danger dans la saisie, le traitement, la télétransmission, la consultation des fichiers et la fourniture des résultats.

Mais puisque ça coûte cher, est-ce vraiment indispensable ?

Oui, ça l'est. Quelques chiffres pour vous convaincre :

– plus de 50% des entreprises qui ont connu un sinistre informatique majeur n'existent plus deux ans après ;

– il est reconnu que 80% des problèmes de sécurité sont internes à l'entreprise, d'où la nécessité d'être conscient des risques et de pouvoir ainsi organiser la sécurité au sein de l'entreprise.

Voici le plan général prévu :

Séquence 13 : Risques informatiques
Séquence 14 : Organisation de la sécurité
Séquence 15 : Les moyens de prévention

Nous allons commencer par recenser les risques pouvant porter atteinte à la sécurité du système.

Séquence 13

Les risques informatiques et leurs conséquences

Dans cette séquence, nous allons recenser les différents types de risques, et donner une première approche des moyens de préventions possibles.

Certains dégâts peuvent empêcher l'entreprise de fonctionner longtemps, d'où un manque à gagner important, des licenciements, etc.

D'autres dégâts peuvent par exemple provoquer la perte de données accumulées depuis longtemps et utiles au fonctionnement de l'entreprise…

Les risques sont généralement classés par catégorie, dans des documents portant le titre « Typologie des risques »… Moi, j'ai fait une classification assez simple, en ne recensant que des risques de base.

1. Risques matériels

On a tous déjà eu au moins une coupure d'électricité qui nous a fait perdre une partie du travail qu'on était en train de faire. C'est rageant !

Certain(e)s parmi vous ont peut-être vécu la malchance d'avoir un disque dur qui tombe en rade… alors qu'aucune sauvegarde récente n'avait été faite… Arghh ! Le matériel !

Nous allons, dans cette partie, recenser les risques liés à des défaillances matérielles ou ayant pour conséquence du matériel endommagé.

Voici ci-dessous un tableau récapitulant les risques classés dans ceux qui peuvent porter atteinte au matériel, ainsi qu'une présentation très sommaire de quelques moyens de prévenir ces risques.

Certains moyens de prévention font l'objet d'une explication plus développée dans la séquence 15.

Risques liés au matériel ou concernant le matériel	Quelques exemples de moyens de prévention (c'est très incomplet…)
1A. Accidents	
1A1. Accidents naturels	
• Inondation, dégâts des eaux. • Séisme. • Incendie, explosion.	• Ne pas choisir un local dans zone inondable. • Ne pas choisir un local au rez-de-chaussée ni au dernier étage. • Dispositif de climatisation et d'incendie en état de marche et conforme aux normes de sécurité.
1A2. Accidents non naturels	

• Choc, bris, panne, de machine ou de support de stockage entraînant une machine inopérante et/ou une perte d'informations. • Pollutions physiques, magnétiques.	• Formation du personnel manipulant le matériel. • Utiliser une salle blanche (c'est une salle protégée de toute pollution pouvant endommager les composants).
1A3. Problèmes électriques	
• Surtension (il y a ici risque d'endommager les composants). • Micro-coupures (ici, il y a risque de perdre des données). • Coupure d'une durée conséquente.	• Équiper le système informatique d'onduleurs. • Être équipé de groupes électrogènes.
1A4. Pannes dues à des défaillances du matériel	
• Composants défaillants : disque dur… • Serveur hors service. • Liaisons réseau défaillantes.	• Avoir un serveur secondaire de secours. • Sauvegarder les données, notamment par l'utilisation d'un système RAID.
1B. Malveillance (vols, sabotage)	
• PC, composants.	• Accès réglementé aux salles, alarmes,
• Périphériques. • Usage abusif de ressources.	• Cadenas et colliers.

Bien entendu, lorsque le matériel informatique est endommagé, il y a de gros risques que les données stockées sur les unités de stockage endommagées soient devenues irrécupérables.

Mais à côté de cette catégorie de risques, il y a la catégorie des risques dangereux uniquement pour les informations et pas pour le matériel, je veux parler des risques à caractère logiciel, que nous allons aborder maintenant.

2. Risques au niveau logiciel

Vous constaterez que dans les risques logiciels, rien n'arrive par accident… lorsqu'un sinistre survient, il est du soit à de la malveillance, soit à des erreurs.

Risques logiciels	Quelques exemples de moyens de prévention
2A. Accidents Les seuls accidents pouvant survenir au niveau logiciel sont ceux issus d'accidents matériels. Au niveau strictement logiciel, rien n'arrive par accident…	
2B. Malveillance 2B1. Atteinte à la disponibilité des données	
• Mise en indisponibilité par attaque en déni de service (en anglais DoS pour Denial of Service et DdoS, qui désigne les attaques distribuées de déni de service). Les attaques par Déni de service consistent à paralyser temporairement (rendre inactif pendant un temps donné) des serveurs afin qu'ils ne puissent être utilisés et consultés. Elles sont un fléau touchant tous serveurs (Lan, Wan…) mais aussi tous particuliers reliés à l'internet via les protocoles de la suite TCP/IP. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à des sociétés dont l'activité repose sur un système d'information en l'empêchant de fonctionner. • Mise en indisponibilité par flooding (inondation : envoi massif d'informations à une machine ou un réseau, ce qui provoque sa saturation et son indisponibilité). • Mise en indisponibilité par attaque virale.	• Voir sur : http://www.securiteinfo.com/attaques/hacking/dos.shtml (c'est très bien expliqué et très simple à comprendre). • Anti-virus.
2B2. Atteinte à la cohérence des données	
Mise en état d'incohérence des données par usurpation, intrusion, ou par attaque virale.	Protection des accès, pare-feu (Firewall), gestion des droits d'accès, système d'authentification ou d'identification, chiffrement, anti-virus…
2B3. Atteinte à la confidentialité des données	
Vol, détournement, divulgation de fichiers, de logiciels, de données par : – copie ou téléchargement illicite ; – usurpation d'identité ; – intrusion illicite ; – interception.	Protection des accès, pare-feu (Firewall), gestion de droits d'accès, système d'authentification ou d'identification, formation des utilisateurs, instauration de systèmes intuitifs, chiffrement…
2C. Erreurs 2C1. Atteinte à l'intégrité, à l'accessibilité des données	
Mise en état d'incohérence et/ou d'inaccessibilité des données par erreur de manipulation (erreurs de saisie, mauvaise gestion des incidents, mauvais programmes).	Formation des utilisateurs et des développeurs et instauration de systèmes ergonomiques. sauvegardes
2C2. Atteinte à la qualité et à l'éthique des données	
• Mauvaise qualité des données (données erronées ou non mises à jour), mauvaise qualité du logiciel. • Données au contenu choquant ou déplacé.	• Éducation du sens critique, confrontation, consultation de la date de dernière mise à jour. • Systèmes de filtrage (exemple : verrouillage parental).

Avant de passer un peu plus en détail à la description de certains risques, je souhaite également vous parler de **l'ingénierie sociale.**

Sous ce nom à l'apparence bien sérieuse et bien sympathique, on regroupe ensemble des techniques de **manipulation psychologique** ou **comportementale** d'un individu ou d'un groupe d'individus dans le but d'amoindrir, contourner ou supprimer les mesures de sécurité d'un système.

Exemple : *pendant la phase de renseignement (indispensable pour toute attaque extérieure), obtenir des informations précises sur un contrat en cours de négociation afin d'être crédible vis-à-vis de l'administrateur système et de lui soutirer un mot de passe (on se fait par exemple passer pour un salarié qui voit son mot de passe refusé…).*

Les conséquences de ces techniques peuvent être multiples et la seule solution préventive est la formation des utilisateurs.

3. Détails sur certains risques logiciels

3A. Les risques issus de l'usurpation d'identité et de l'intrusion

Ce type de risque existe pour les données stockées sur une machine dès que celle-ci est connectée à un réseau, qu'il s'agisse d'un réseau local (un collègue trop curieux peut très bien tenter d'accéder à vos données, vos mails...), ou d'un réseau ouvert (je ne vous apprends rien en vous disant qu'on peut récupérer plein de « saletés » sur notre machine lorsqu'on est connecté à Internet).

Voici ci-dessous quelques exemples de comportements risqués.

Fournir des informations personnelles (notre nom, notre numéro de téléphone, notre numéro de carte de crédit,…) représente un risque. Ces informations peuvent être, par exemple, vendues pour des opérations commerciales, interceptées et être utilisées pour usurper notre identité…

À partir du moment où l'intrusion est possible, aucune donnée contenue sur notre machine n'est à l'abri des risques de destruction, piratage…

Alors vous allez me dire : « il suffit d'avoir mis en place un mot de passe pour protéger l'accès à notre machine »… Oui… Mais hélas pour nous, tout mot de passe, comme toute combinaison de coffre fort, peut être trouvée. Si ce mot de passe est long, il faudra simplement plus de temps aux logiciels spécialisés pour le trouver.

Il existe plusieurs méthodes pour calculer le mot de passe permettant l'intrusion sur une machine ou l'usurpation d'identité.

- **Utilisation d'un dictionnaire de mots de passe** : le dictionnaire de mots de passe est en fait un fichier contenant certaines combinaisons de chiffres, de lettres… ces combinaisons sont les mots de passe possibles. Pour tenter une intrusion, on utilise un programme qui lit ce dictionnaire et essaie de se connecter en utilisant une par une les combinaisons contenues dans le dictionnaire jusqu'à ce que la connexion soit acceptée.
- **Utilisation de la technique de la force brute :** cette technique utilise le même principe que précédemment, sauf que les mots de passe possibles sont générés par le programme, qui teste donc toutes les combinaisons possibles de chiffres et de lettres jusqu'à ce qu'il trouve la bonne combinaison.
- **Utilisation d'un logiciel espion :** ce logiciel est installé sur la machine à l'insu de son propriétaire (souvent à l'occasion d'une connexion réseau non sécurisée). Une fois ins-

tallé sur la machine, cet espion peut récupérer les mots de passe et autres informations en captant les saisies clavier.

- **Utilisation des différentes techniques d'usurpation d'adresses** (également appelé **spoofing**). La récupération d'adresses IP, MAC ou même d'adresses e-mail permet à l'usurpateur de se faire passer pour la machine ou la personne dont il a usurpé l'adresse. Ces informations une fois détournées, il est possible d'accéder aux machines ou aux applications qui se fient à ces adresses pour autoriser les connexions. Cela une fois fait, on peut effectuer tout traitement comme si on était la machine ou la personne dont on a usurpé l'adresse.

Exemple : *l'**IP spoofing** (ou forgeage d'adresses IP). L'IP Spoofing est une technique largement utilisée dans beaucoup des cas d'attaques logicielles cités ci-dessus. Du fait de la possibilité de forger des paquets bruts à l'aide de la programmation RAW SOCKET, il est possible d'envoyer des paquets avec une fausse adresse IP de source. Cependant il ne faut pas penser que la tâche soit aussi simple que ça, en effet, IP ne fonctionne pas tout seul et il est toujours (ou presque) utilisé avec un protocole de niveau supérieur. L'IP Spoofing en utilisant TCP est le plus difficile à mettre en œuvre surtout lorsqu'elle est utilisée en dehors d'un réseau local, on a donc là affaire à des personnes malveillantes, mais qui « touchent leur bille », hélas. Celles et ceux d'entre vous intéressés par cette technique peuvent chercher de plus amples informations sur la toile, en tapant par exemple IP spoofing dans un moteur de recherche.*

Qui peut avoir envie de se livrer à des intrusions et pourquoi ?

Il peut s'agir d'un concurrent peu scrupuleux, d'un pirate mercenaire payé par la concurrence, d'un truand, ou, d'un point de vue moins professionnel, d'un « bidouilleur » curieux, d'un personnage mal intentionné.

Les motivations peuvent être de natures très diverses : financière, sociale (besoin de reconnaissance, vengeance personnelle), technique (le piratage est considéré comme une performance par certains), politique…

3B. Les risques issus des attaques virales ou des attaques par envahissement

Une récente étude du fournisseur d'accès AOL révèle que près des trois quarts des internautes français ont déjà été infectés par un virus informatique.

Une autre étude du CLUSIF (Club de la sécurité des systèmes d'information) de juin 2004 montre que 40 % des causes de panne informatique sont dues à des virus.

Il importe donc de pouvoir identifier les différents parasites informatiques, de les prévenir et d'adopter un comportement qui garantisse la pérennité des données dont chacun est responsable.

Qu'est-ce qu'un virus, un ver ou un cheval de Troie ?

Ces 3 termes désignent des réalités différentes.

Un **virus** est un programme dont le but est de se reproduire. Sa technique est de s'accrocher à un programme existant, à la manière d'un parasite.

Un **ver** (ou *worm* en anglais) est également un programme auto-reproducteur. Mais à la différence du virus, il se suffit à lui même : il n'a pas besoin d'un programme hôte pour se reproduire. La méthode la plus courante de propagation des vers est l'envoi de courriers électroniques avec copie du ver en pièce jointe.

Un **troyen** ou **cheval de Troie** (ou **trojan** en anglais) est un programme qui permet de prendre le contrôle à distance de votre machine et de lui faire exécuter des commandes à votre insu (vol des mots de passe, accès à distance aux ressources de la machine, destruction de données, etc.). Il n'a pas de facultés auto-reproductrices.

3B1. Les virus et les vers

Un virus, vous le savez déjà, est un programme qui endommage d'une façon ou d'une autre la machine sur laquelle il s'exécute, à l'insu de l'utilisateur, bien sûr.

Pour la petite histoire, c'est Xerox, qui, sans le faire exprès, a créé le premier virus en 1980 : il s'agit d'un programme créé par les ingénieurs de Xerox mais devenu incontrôlable, nécessitant un vaccin pour l'arrêter.

En 1988, le premier antivirus commercial pour PC arrive sur le marché, pour protéger les machines du virus Brain, apparu deux ans plus tôt.

En 1989, IBM commercialise IBM Scanning Software, pour désinfecter les machines touchées par le virus Cascade.

Depuis 1999, on subit des attaques massives de toutes sortes de virus. Les virus utilisent les failles des logiciels du marché.

Les virus se propagent par **duplication**. Pour cela, ils infectent d'autres programmes d'ordinateur en les modifiant de façon à ce qu'ils puissent à leur tour se dupliquer.

Ils agissent lorsqu'ils sont chargés en mémoire au moment de l'exécution du logiciel infesté.

La plupart des virus **visent à déclencher une action**.

Certaines actions sont sans danger : affichage d'un message, exécution d'une musique, dessin d'une spirale sur l'écran, etc.

D'autres ont une action beaucoup plus nuisible.

Voici ci-dessous un rapide panorama des différentes sortes de virus, à compléter avec des lectures puisées sur internet.

Notez que la tendance actuelle des virus est d'arrêter les antivirus fonctionnant sur l'ordinateur contaminé. Si bien que plus que jamais, c'est la vigilance de l'utilisateur qui protège en dernier ressort.

- **Virus système ou virus de boot :** ils infectent le système en remplaçant le secteur d'amorce par leur propre code.

Exemples : *Stoned (1988), Form (1991), AnticMos (1994).*

- **Virus programme (ou virus d'application) :** il infecte les programmes exécutables. Il se glisse dans une partie du code et sera exécuté en même temps que l'application. Il en profitera pour se reproduire, contaminer d'autres exécutables et déclencher l'action prédéterminée par son auteur.

Exemple : *Tchernobyl (1998).*

- **Virus réseau :** il sait se dupliquer tout seul et se propager dans un réseau via les voies logicielles du système ou du réseau.
- **Bombe logique :** ces programmes ont la particularité de se lancer à une date précise, ou lors d'une action utilisateur précise.
- Le **virus de script** infecte les pages HTML chargées par un internaute. Une page HTML est composée de balises interprétées par le navigateur. Il est possible d'ajouter dans une page HTML des programmes écrits dans un autre langage pour enrichir les pages et les rendre dynamiques. Les plus utilisés sont VB-Script et JavaScript. VB-Script est à l'origine de nombreux virus.

Exemple : *I love you (mai 2000).*

- **Les virus macro :** ces virus se transmettent par l'intermédiaire de documents créés avec une application (courriers, tableaux, documents texte…). Ces macro commandes sont écrites en langage de haut niveau (***exemple :*** *macro commande écrite dans microsoft word*) et sont attachées à un document, qui est donc infecté. Dès l'ouverture de ce document infecté avec l'application source, l'application est infectée et infectera tous les documents créés ensuite.

Exemple : *Concept (1995).*

- **Les virus de messagerie** ou **vers :** ils se transmettent le plus souvent par les courriels, soit en pièce jointe, soit en étant carrément stockés dans l'entête SMTP du message (SMTP : Simple Mail Transfer Protocol, c'est le protocole utilisé pour l'envoi de messages), soit c'est le message lui-même qui est le ver. Il suffit, pour certains d'entre eux, que le message soit prévisualisé pour se déclencher.

Le ver sait se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses. Le ver est une variante de virus qui a la particularité de ne pas avoir besoin de support pour se reproduire, il se suffit à lui-même.

Exemples : *KakWorm (1999), Melissa (1999), Happy99 (1999).*

Les virus essaient de se rendre indétectables par diverses techniques de dissimulation…

- **Les polymorphes :** polymorphe signifie que le virus est capable d'avoir plusieurs morphologies, ou de changer de morphologie (plus exactement de signature) après chaque infection. Ce type de virus est capable de se déguiser sous diverses noms, signatures… ce qui le rend plus difficile à éradiquer.

Pour pouvoir s'auto-modifier, le corps du virus est chiffré avec une clé différente, et la routine de déchiffrement, qui reste en clair, est modifiée aléatoirement en insérant des instructions parasites ou choisies parmi des routines connues.

- **Les furtifs** : ils interceptent les demandes du système d'exploitation et présentent les informations telles qu'elles étaient avant l'infection, l'objectif est de ne pas être décelé.
- **Les rétrovirus** : ils attaquent les antivirus en bloquant leur exécution et leur redémarrage.
- **Les hybrides** : ils combinent les caractéristiques de plusieurs familles.

Les virus par e-mail savent également se déguiser, en fichier texte, image, son, vidéo... Un double clic ou bien l'ouverture automatique de ces fichiers multimédia active le virus.

3B2. Les chevaux de Troie ou troyens

Ces programmes ont l'air tout à fait anodin (mél, bandeau publicitaire, jeu en téléchargement) mais possèdent des fonctionnalités cachées à caractère malveillant (comme, par exemple, la récupération de mots de passe ou des fonctionnalités d'intrusion dans des fichiers pour les consulter, les transférer, les modifier ou les détruire).

Les troyens permettent aux pirates de s'introduire dans une machine sans le consentement de l'utilisateur. Dans ce cas, ils insèrent un logiciel « serveur » qui offrira au pirate toutes les informations dont il a besoin. Le pirate pourra prendre à distance le contrôle de l'ordinateur infecté.

À la différence d'un virus, les troyens ne cherchent pas à se reproduire.

L'objectif est de récupérer des informations confidentielles : codes de carte bancaire, identifiant et mots de passe, documents personnels.

Mais, le cheval de Troie est avant tout un **moyen de transport d'un parasite** plus ou moins dangereux, comme un ver, par exemple. Il utilise souvent une faille de sécurité pour s'introduire dans un ordinateur.

Voici un cheval de Troie qui a connu ses heures de gloires.

Client de Microsoft,

Voici la dernière version de mise à jour de sécurité « Correctif cumulatif, septembre 2003 », mise à jour qui élimine toutes les vulnérabilités qui affectent MS Internet Explorer, MS

Outlook et MS Outlook Express, ainsi que trois nouvelles vulnérabilités récentes.

Installez cette mise à jour immédiatement pour préserver la sécurité de votre ordinateur face aux vulnérabilités, la plus importante d'entre elles peut permettre à un pirate d'exécuter des programmes sur votre ordinateur. Cette mise à jour se cumule avec les précédents correctifs.

Remarque

Un correctif est un programme qui corrige des dysfonctionnements, bogue ou faille de sécurité, découverts dans un logiciel.
Ce message, accompagné d'une pièce jointe, précisait également qu'il fallait exécuter la pièce jointe…

MISE EN GARDE - Correctif Microsoft ou simple ver ?

Si vous avez reçu un e-mail « aux couleurs » de Microsoft vous proposant d'installer un soi-disant correctif, détruisez-le au plus vite.
Sachez que Microsoft ne distribue jamais de logiciels en pièce(s) jointe(s) par courrier électronique. Il s'agit en réalité d'un nouveau ver qui une fois installé exécutera des actions dangereuses pour l'ordinateur.

Et sur le site de Microsoft, on pouvait lire :

Politique Microsoft de diffusion des mises à jour des logiciels

Pour une informatique sûre et fiable, il est important de ne jamais utiliser de logiciels provenant de sources inconnues.

Comme indiqué dans un avis du CERT, des utilisateurs malveillants emploient souvent des « chevaux de Troie » pour introduire des logiciels pernicieux dans les ordinateurs d'utilisateurs imprudents.

- Un **cheval de Troie** est un logiciel qui, sous l'apparence d'un logiciel utile, réalise en fait de façon cachée des **actions dangereuses pour l'ordinateur infecté**. Par exemple, un pirate peut développer un programme de jeu qui efface délibérément des fichiers sur l'ordinateur qui l'héberge, puis il se propagera via la messagerie de l'utilisateur.
- Un autre mécanisme, fréquemment utilisé et qui s'apparente au cheval de Troie, consiste à envoyer par courrier électronique un **programme malveillant**, en annonçant qu'il s'agit d'une mise à jour d'un logiciel et **en se faisant passer pour l'éditeur de ce logiciel**. Récemment, de nombreux courriers de ce type sont apparus sur Internet, annonçant des mises à jour de logiciels Microsoft ou d'autres éditeurs. Il ne s'agit que de **logiciels dangereux** destinés à endommager les fichiers des utilisateurs qui les auraient exécutés.

Sachez que Microsoft ne distribue jamais de logiciels en pièce(s) jointe(s) par courrier électronique.

Nous distribuons des logiciels sur des supports physiques comme des **CD-ROM** et des **disquettes**.

Nous distribuons les mises à jour sur Internet **exclusivement** via nos sites Web américain et français, ou via le centre de téléchargement.

Nous envoyons parfois des courriers électroniques à nos clients pour leur **signaler la parution d'une mise à niveau**.

Toutefois, ces courriers contiennent **uniquement des liens** vers nos sites de téléchargement ; **nous ne mettons jamais en pièce jointe de logiciels à nos messages**. Les liens mènent toujours vers notre site Web ou notre site FTP.

Nous utilisons toujours Authenticode pour **signer numériquement nos produits**, ce qui permet aux utilisateurs de vérifier qu'ils ont reçu la bonne version.

Si vous recevez un courrier électronique se faisant passer pour Microsoft et contenant un logiciel joint, n'exécutez pas ce logiciel. Supprimez complètement ce message avec sa pièce jointe.

Si vous souhaitez aller plus loin, signalez ce message au fournisseur d'accès Internet (FAI) dont dépend l'expéditeur. De nombreux FAI offrent la possibilité de signaler de tels abus.

3B3. Les spywares ou espiogiciels

Ce sont des logiciels qui sont transmis en pièce jointe, ou bien encore qui s'infiltrent dans votre machine en empruntant un port ouvert (comme par exemple le port http). Cela une fois fait, ils espionnent le contenu de votre machine, à des fins toujours assez peu recommandables.

L'objectif des espiogiciels n'est pas de détruire, mais d'envoyer des informations à une société ou à un pirate sans se faire remarquer. Ces logiciels sont parfois présentés par des sociétés commerciales comme des outils de suivi des habitudes d'un utilisateur dans le but d'améliorer les produits de la société, mais cette collecte effectuée sans le consentement de l'utilisateur est une intrusion dans la vie privée.

On les trouve notamment dans les bandeaux publicitaires de pages HTML, dans les logiciels de téléchargement et d'échange de morceaux de musique.

Certains sont installés par des chevaux de Troie et peuvent collecter des informations privées comme l'identité, le carnet d'adresses, les mots de passe ou les codes de carte bancaire.

3B4. Les spams ou pourriels

Après la boîte aux lettres de votre domicile, le pare-brise de votre voiture, le fax de votre société, voici que c'est votre boîte aux lettres électronique qui récolte les tracts et les pubs. Dans le jargon, on appelle ça *spam* ou *spamming*, *polluriel*, *pourriel*, *courrier-rebut*... Selon les études, ce fléau représenterait aujourd'hui de 30 à 40 % du trafic e-mail !

Les spams sont des messages qui inondent le réseau, envoyés par des émetteurs appelés des spammeurs.

Il s'agit d'un procédé très peu coûteux pour expédier des offres commerciales à des millions d'adresses. Des logiciels spécialisés appelés « robots » parcourent le Web pour y récupérer les adresses. L'envoi des courriels est quasiment gratuit. Le taux de retour est extrêmement faible mais suffisant.

Ce ne sont pas des virus proprement dit, mais ils encombrent le réseau et inondent nos boîtes aux lettres. On les appelle des pourriels car ils pourrissent nos boîtes aux lettres.
Exemple : *vous trouverez en encadré page suivante le genre de message que l'on peut recevoir.*

Le spam présente deux inconvénients majeurs. Il parasite Internet, en monopolisant plus de 50 % du trafic du courrier électronique, et dévalorise les démarches commerciales responsables sur Internet.

Les acteurs de l'Internet s'efforcent donc de limiter le phénomène par des moyens techniques, et les États tentent d'y mettre fin par des dispositions législatives. Mais l'aspect international du phénomène et l'inventivité des spammeurs rendent l'éradication du fléau très difficile.

Par exemple, j'ai du, pour ma part, et malgré un anti-spam, arrêter de me servir d'une de mes adresses de messagerie car ma boîte aux lettres était inondée de spams.

Mais comment les spammeurs récupèrent-ils votre adresse e-mail ?

Les spammeurs peuvent en fait récupérer votre adresse par de nombreux moyens…

Votre fournisseur a cédé votre adresse e-mail

C'est la toute première fuite : votre fournisseur d'adresse électronique (FAE) a revendu tout ou partie de sa liste d'abonnés à un tiers, qui lui-même l'a revendu à un autre, etc. Au final, votre adresse s'est diffusée à de nombreux exemplaires sur le Net.
L'opération peut être faite dans la légalité, mais ce n'est pas toujours le cas.

From: "bc1234" < bc1234@fai.com>
To: clambey@fai.fr, ckel@fai.fr, christiane.deschambr@fai.fr, christine.dufond@fai.fr, clambey@fai.fr, ckel@fai.fr
Subject: !cid_yiprtvmv_iwpjxbnd_jwzaesmk
Date: Tue, 26 Oct 2004 13:24:00 -0300

Votre adresse a été générée au hasard

Prenez d'un côté les listes des noms et prénoms les plus courants, de l'autre celle des fournisseurs d'adresses les plus populaires. En utilisant toutes les combinaisons possibles (prenom.nom, nom.prenom, nprenom2, etc.), vous pouvez générer des centaines de milliers d'adresses e-mail... qui ont de fortes chances d'exister ! Et bien c'est ce que font certains spammeurs.

Avec une adresse du type *johnsmith2@hotmail.com*, ne vous attendez donc pas à être tranquille bien longtemps...

Vous avez communiqué votre adresse à un site Web

Vous avez passé une commande sur un site de commerce électronique ? Vous avez souscrit aux services d'un site ? Vous vous êtes inscrit à une liste de diffusion par courrier électronique ? Dans tous les cas, vous avez dû laisser votre adresse électronique.

Si vous avez oublié de cocher (ou décocher) une petite case, vous avez autorisé la diffusion de votre adresse électronique. Peut être même n'avez-vous pas eu ce choix...

Vous avez publié votre adresse sur le Net

Vous avez affiché votre adresse électronique sur votre page personnelle ? Vous avez laissé votre adresse sur des forums de discussion sur le Web ou dans les newsgroups ? Sachez que des logiciels permettent de récolter automatiquement les adresses e-mail publiées sur le Net.

À partir du moment où vous contribuez à un forum ou laissez votre adresse électronique sur une page perso, vous êtes donc susceptible d'intégrer un fichier d'adresses.

3B5. Les faux virus ou canulars ou hoax

Ce sont généralement des messages alertant leur lecteur d'un fait quelconque (arrivée d'un nouveau virus, collecte pour un enfant malade…) et demandant à ce lecteur de transmettre l'information à la plus grande quantité d'adresses e-mail possible. Le résultat est un encombrement du réseau et un ralentissement de son fonctionnement et la transmission d'informations erronées.

3C. Les risques d'interception

Outre le risque d'intrusion sur notre machine, il existe également le risque que des informations soient interceptées au cours de leur transit sur le réseau.

Il existe pour cela des logiciels appelés **renifleur** (également appelé **sniffer**). Ce sont des programmes permettant d'intercepter les informations qui transitent.

N'importe quelle information peut être interceptée si elle n'est pas protégée lors de son transit : adresses IP, MAC, e-mail, informations diverses…

Tout échange d'informations sur le réseau est donc susceptible d'être détourné.

Une fois que le sniffer a intercepté les informations, il peut les utiliser, notamment pour usurper des identités.

Une adresse à consulter :
Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques : http://www.certa.ssi.gouv.fr/site/CERTA-2003AVI-084/index.html

4. Risques sociaux

On n'y pense pas toujours, techniciens que nous sommes, mais les risques sociaux existent bel et bien et peuvent également avoir des conséquences bien lourdes.

Parmi ce type de risques, on recense principalement :

- des interruptions des traitements pour cause de grève (du personnel ou de sous-traitants) ;
- le départ de membres stratégiques du personnel ;
- l'insertion de nouvelles méthodes de travail, entraînant éventuellement des réactions de la part du personnel, un changement dans la répartition des fonctions, et des conséquences au niveau de la productivité.

Avant de passer à la séquence 14, qui traite de l'organisation de la sécurité, nous allons rapidement passer en revue les conséquences éventuelles issues de sinistres matériels, logiciels ou sociaux.

5. Conséquences possibles

Perte de chiffre d'affaires
Un sinistre peut entraîner erreurs, impossibilité ou retards dans les traitements, les commandes, la facturation, les comptes clients/fournisseurs/relances, les stocks, la production.

Atteinte à l'image de marque
Les erreurs de commandes, de facturation, les retards peuvent être considérés comme des infractions aux réglementations, comme un non respect des contrats commerciaux, ce qui nuit à l'image de l'entreprise.

Prise de décisions erronées
L'imprécision, l'inadaptation, l'inexactitude ou l'inaccessibilité des informations peut en effet entraîner une mauvaise prise de décision lourde de conséquences néfastes à l'entreprise.

Distorsion de concurrence
La revente à la concurrence de fichiers, de logiciels, de données, de documentation volés est également une atteinte à la compétitivité de l'entreprise.

Dégradation de la qualité du service
L'emploi de personnel intérimaire, le mécontentement du à des temps de réponse trop longs, des ruptures des stocks, des erreurs, l'absence de moyens pour une bonne prise de décision, des difficultés d'exploitation sont autant de conséquences possibles nuisibles à l'entreprise.

Dépenses imprévues
Suite à un sinistre matériel, logiciel ou social peuvent en effet survenir des surcoûts sous forme :

– d'heures supplémentaires ou de personnel intérimaire ;
– de travaux de réfection ;
– de coûts de développement ou de maintenance supplémentaires.

6. En guise de conclusion…

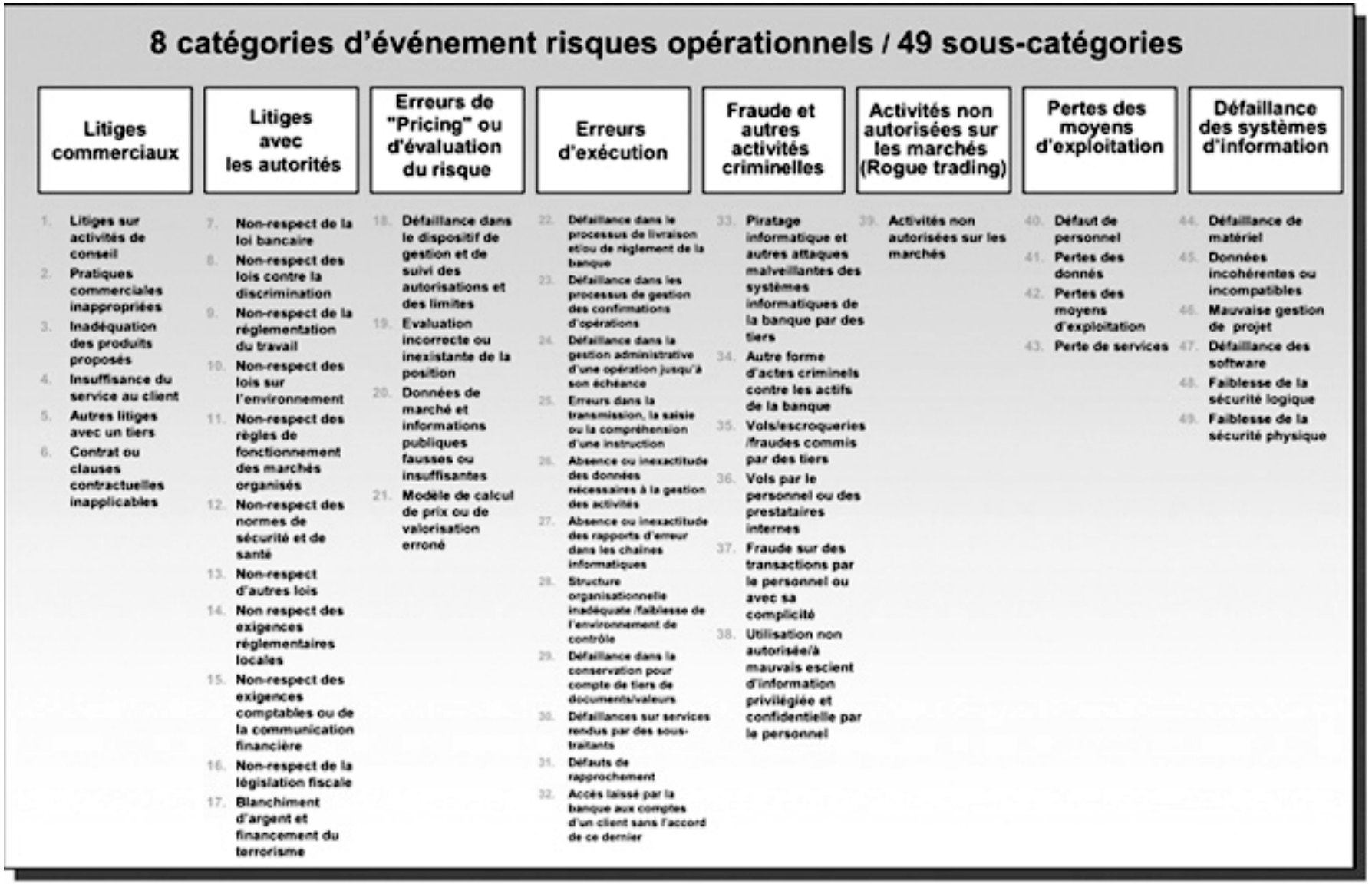
Voici, ci-après, un schéma représentant une classification de risques, dont certains ont fait l'objet d'un relatif développement ci-dessus.

Vous constatez qu'on parle ici de **risque opérationnel**.

Le risque opérationnel se définit comme le risque de perte résultant de l'inadaptation ou de la défaillance de procédures, de personnes ou de systèmes internes ou encore d'évènements extérieurs (catastrophes naturelles, incendie, agression, etc.).

Le risque opérationnel est inhérent à chacun des métiers et des activités de l'entreprise.

Bon, nous allons maintenant aborder la séquence 14, qui traite de l'organisation de la sécurité.



PRES/BA2/OPE – 26 juin 2003

Séquence 14

Organisation de la sécurité

Avant de se lancer dans la description des moyens de protection, à la séquence 15, nous allons aborder les différentes solutions existantes à un niveau plus global et concernant la sécurité.

1. Les différents types de solutions sécuritaires

On peut avoir deux attitudes opposées face à la sécurité : une attitude **active**, et une attitude **passive**.

1A. Sécurité active

Il existe principalement deux modes actifs de gestion de la sécurité du système.

1A1. Le mode préventif

On organise la sécurisation afin que le sinistre ne se produise pas.
Exemple : *antivirus*

Dans la séquence précédente, dans les tableaux de présentation des risques, je vous ai indiqué quelques exemples de moyens de prévention.

Généralement, lorsqu'on veut organiser la sécurité d'un système, on réfléchit avant.

Il existe des méthodes pour aider à organiser la sécurité préventive d'un système, ce sont des méthodes dites d'**analyse des risques**.

Pour ma part, je vous citerai deux méthodes d'analyse des risques :

- une méthode relativement simple et rapide à mettre en œuvre, appelée **MARION,** qui permet de faire un diagnostic de la sécurité dans une organisation et de proposer des solutions ;
- une autre méthode plus sophistiquée et donc plus lourde à mettre en œuvre, appelée **MEHARI** (méthode harmonisée d'analyse de risques informatiques).

Ces deux méthodes vous sont présentées synthétiquement plus bas dans ce cours.

1A2 Le mode curatif

On réagit après que le sinistre se soit produit afin de revenir à une situation normale.
Exemple : *restauration des sauvegardes.*

Dans ce mode de gestion de la sécurité, il faut réfléchir à la façon dont on va remettre le système en état.

On définit alors un **plan de reprise** à mettre en œuvre après le sinistre. La notion de plan de reprise vous est présentée plus loin.

1B. *Sécurité passive*

On trouve dans ce domaine essentiellement la souscription d'une **assurance**.

Dans toute entreprise, et ce, malgré la mise en place de moyens de sécurisation et l'application d'une politique de sécurité, un contrat d'assurance spécifique est souvent nécessaire pour l'informatique, car le matériel informatique et les données de l'entreprise ne sont pas systématiquement couverts par les polices d'assurance générales.

Ce contrat doit prévoir d'indemniser les sinistres informatiques quelles qu'en soient les causes (incendie, inondation, attaque virale), car la perte du matériel informatique ou des données fragilise les entreprises, quand elle ne les pousse pas à la faillite.

En général, les pertes d'exploitation résultant d'une défaillance informatique sont couvertes par les contrats habituels. La plupart du temps, les ordinateurs de bureau sont assurés et considérés comme du mobilier, à l'exception des stations et autres serveurs.

En revanche, la perte et les frais de récupération des données ne sont en général pas indemnisés dans les contrats traditionnels, de même que les logiciels. L'assurance spécifique doit donc couvrir ce type de sinistre, tout en sachant qu'il est rarissime de trouver un contrat d'assurance qui prend en charge les sinistres concernant les applications développées au sein même de l'entreprise.

Curieusement, malgré la couverture, de nombreuses entreprises hésitent à faire jouer les assurances lors d'un sinistre, à cause de l'obligation de déclaration à la police en cas d'attaque de virus ou de malveillance, et aussi à cause du malus qui s'ensuit.

En outre, les assureurs soumettent leurs clients à une analyse des risques. Plus on a d'incidents, plus il est difficile de se prémunir.

2. Méthodes d'analyse des risques (sécurité préventive)

Je vous présente deux méthodes, une assez simple (MARION) et l'autre plus élaborée (MEHARI).
Grosso-modo, bien que différentes, ces deux méthodes s'appuient sur des principes relativement similaires.
La démarche d'analyse des risques peut, de manière générale, se résumer comme suit :

- identification des ressources ;
- établissement des scénarios des risques encourus ;
- calcul des pertes face à ces événements ;
- détermination des moyens de sécurité nécessaires ;
- évaluation des contraintes techniques et financières ;
- choix final des solutions.

2A. *La méthode Marion*

MARION signifie méthode d'analyse de risques informatiques optimisée par niveau.

2A1. Description des étapes

Voici la démarche en cinq grandes étapes préconisée dans cette méthode.

Étape 1 : quels risques court-on ?
Au cours de cette étape, on organise des brainstormings par groupe de travail incluant tout le personnel.

Les résultats attendus sont :

– une liste exhaustive des risques ;

– l'élaboration de scénarios catastrophe ;

– une hiérarchisation des risques.

On passe ensuite aux étapes 2 et 3 qui peuvent être menées en parallèle et débouchent toutes deux sur l'étape 4.

Étape 2 : peut-on accepter ces risques ?
Au cours de cette étape, on procède à une estimation de rapport entre le coût du sinistre et le coût du moyen préventif.

Étape 3 : quel est le niveau actuel de la sécurité ?
Cette étape consiste en un audit, un inventaire de la sécurité au travers d'une batterie de questions.

Étape 4 : que faire ?
La réflexion et les résultats de l'étape 4 se nourrissent des résultats des étapes 2 et 3.

Lors de cette étape, il y a mise au point :

– de la liste des moyens à mettre en œuvre ;

– de la définition des priorités ;

– du degré d'amélioration à atteindre.

Étape 5 : comment faire ?
Cette étape consiste en l'élaboration du plan technique détaillé. On recense également ici quels sont les moyens financiers, techniques, humains nécessaires.

2A2. Un exemple concret de cas

Nous allons dérouler la démarche en cinq étapes de la méthode MARION en l'appliquant au cas d'une salle informatique en accès libre dans un établissement scolaire.

Supposons que le contexte soit le suivant : un établissement scolaire possède une salle informatique en accès libre de 8 h 00 à 17 h 30 sans interruption. Toutefois, cette salle peut être réservée et utilisée par un enseignant pour une utilisation avec une classe.

De nombreux problèmes (dont l'origine n'a pas été déterminée avec précision car l'établissement ne possède pas de personnel compétent techniquement) ont entraîné des gênes voire des impossibilités d'utilisation (logiciels absents, bureaux Windows farfelus, connexions au réseau local perdues, lenteur de connexion au serveur et à internet, etc.).

La méthode MARION peut permettre de mener un **audit global** des risques informatiques liés à l'utilisation de cette salle.

Le résultat sera un rapport intégrant pour chaque risque, une solution technique précise et chiffrée.

Appliquons la méthode MARION à ce cas simple.

Étape 1 : quels sont les risques ?
Il s'agit ici d'établir la liste exhaustive des risques pour cette salle, en ne se limitant pas aux risques évidents, mais en creusant la question en profondeur.
Pour les risques les plus importants, on propose un scénario « catastrophe ».
À l'issue de cette étape, on doit disposer d'une liste de risques la plus exhaustive possible, ainsi que de scénarios catastrophe issus des risques les plus importants.

Étape 2 : peut-on accepter ces risques ?
Le cas étant simple et l'établissement scolaire ayant peu de moyens, ce que l'on peut faire ici, c'est, dans la liste des risques, créer deux catégories de risques…

Ceux pour lesquels une solution préventive raisonnable peut être mise en œuvre,

Ceux pour lesquels une solution préventive est trop coûteuse à mettre en œuvre, soit parce que l'établissement n'a pas les moyens financiers, soit parce qu'elle couvre un risque négligeable.

À l'issue de cette étape, on doit disposer de la liste de risques retenus comme devant être pris en compte, ainsi que de la ou des solutions préventives pour chaque risque.

Étape 3 : quel est le niveau actuel de la sécurité ?

Pour chaque risque devant être traité, on conçoit des questionnaires d'audit qui diffèrent en fonction des catégories de personnes concernées, et ce afin de déterminer le niveau actuel de la sécurité.

Exemple de question : *on peut par exemple demander aux utilisateurs (profs, élèves…) comment ils s'y prennent pour retenir leur mot de passe.*

Étape 4 : que faire ?

Pour chaque risque à traiter :

- on dresse la liste des moyens à mettre en œuvre pour assurer la sécurité préventive ;
- on définit des priorités en fonction de l'importance du risque et de l'urgence à le traiter ;
- on détermine le degré d'amélioration à atteindre.

Étape 5 : comment faire ?

Rédaction du plan technique détaillé : ici, on rédige toutes les procédures de conception, développement, installation, configuration et maintenance des moyens de sécurité mis en place.

Moyens financiers, techniques, humains associés : on estime le coût de chaque solution préventive retenue, on décrit ce qu'il faut acheter, on dit aussi combien de personnes il faut, quelle doit être leur qualification…

2A3. Conclusion

Cette méthode est relativement simple et est adaptée aux structures d'envergure modeste. Il est possible qu'une entreprise plus volumineuse ait besoin d'une démarche et d'outils adaptés à son envergure. C'est l'ambition annoncée par les concepteurs de la méthode MEHARI, que je vous présente rapidement ci-dessous.

2B. MEHARI

Cette méthode a été développée par le CLUSIF (le club de la sécurité des systèmes d'information français) dont le site se trouve à l'URL https://www.clusif.asso.fr.

Je vous présente très synthétiquement cette méthode et vous invite à compléter votre culture en allant sur le site du CLUSIF.

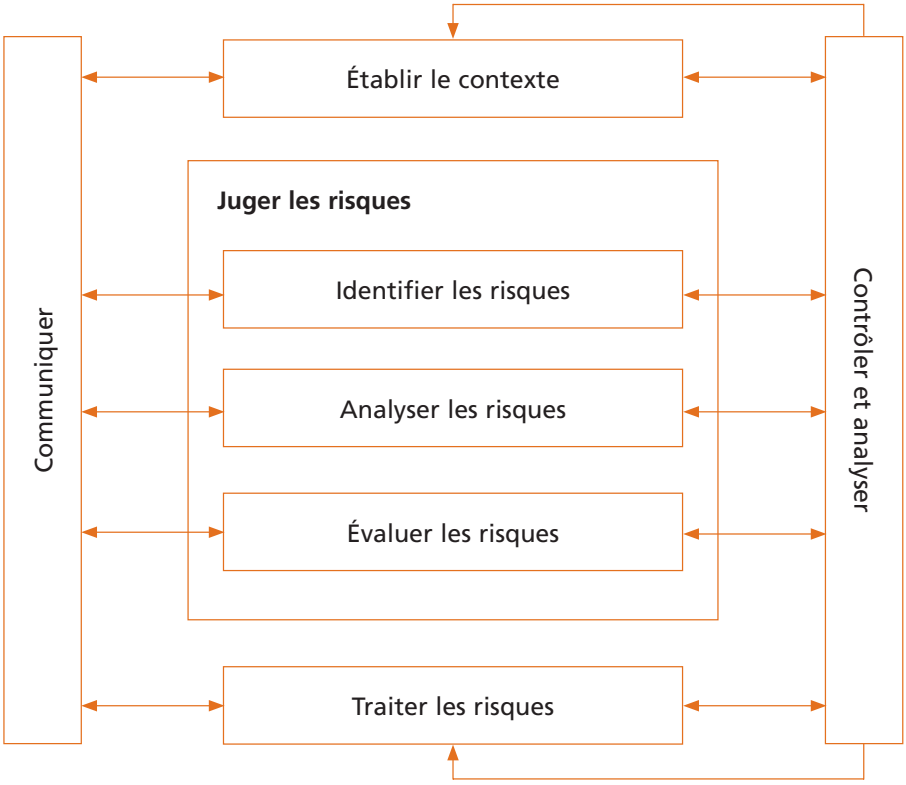
MEHARI signifie méthode harmonisée d'analyse des risques.

Cette méthode concerne l'analyse des risques liés à l'information.

Selon ses concepteurs, MEHARI fournit un cadre, des méthodes et des bases de connaissance permettant de préciser les points suivants, essentiels pour la sécurité de l'information :

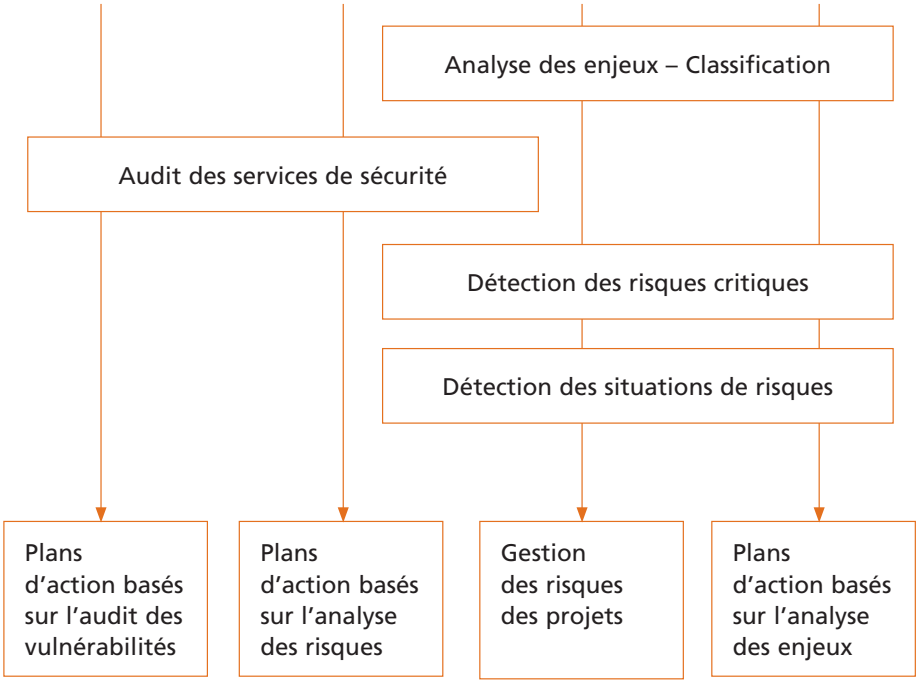
- enjeux majeurs ;
- vulnérabilités ;
- risques et niveaux de gravité de ces risques ;
- pilotage de la sécurité à mettre en œuvre.

Cette méthode de management des risques s'appuie sur le modèle ISO 13335, dont voici la démarche schématisée :



MEHARI propose quatre modules indépendants (analyse des enjeux, audit des services de sécurité, détection des risques critiques, détection des situations de risques…).

Ces modules permettent d'atteindre des objectifs variés, comme le montre le schéma ci-dessous :



La méthode fournit un cadre de travail, des démarches, une documentation relative aux risques, à leurs remèdes, des bases de connaissances sous forme de fichiers excel (avec des liens, des calculs automatiques…).

La méthode fournit aussi un modèle de risque dont voici un schéma simplifié :

Voici ci-dessous une présentation rapide des différents aspects de cette méthode.

2B1. Analyse des enjeux de la sécurité

Ce thème, dans la méthode, a pour buts :

– l'identification des dysfonctionnements pouvant être causés ou favorisés par un défaut de sécurité ;

– l'évaluation de la gravité de ces dysfonctionnements.

Les résultats :

– un document de référence, contenant une hiérarchisation des dysfonctionnements en fonction de leur impact au niveau du fonctionnement de l'entreprise ;

– une classification des informations et ressources du système informatique.

Utilité :

– être sélectif dans les moyens à mettre en œuvre et ne pas engager de moyens là où les enjeux sont faibles (définir des priorités, ne faire que ce qui est nécessaire) ;

– éviter des contraintes inutiles aux utilisateurs.

2B2. Analyse des vulnérabilités

Ce thème sert à :

– l'identification des faiblesses et défauts de la sécurité ;

– l'évaluation quantitative de la qualité de la sécurité.

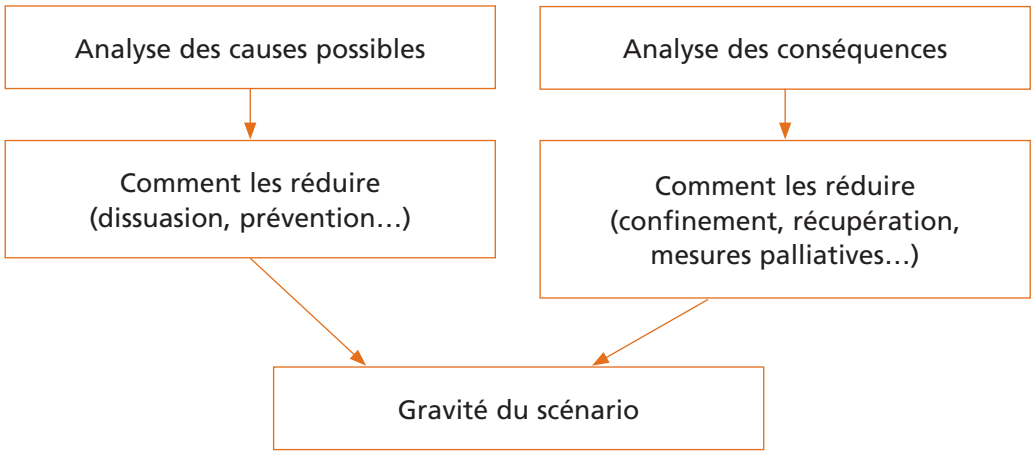
Utilité :

– vérifier l'absence de points faibles inacceptables, le résultat possible étant la mise en œuvre de plans d'action immédiats ;

– évaluer et garantir l'efficacité de la sécurité ;

– se comparer aux normes et usages en vigueur en matière de sécurité.

MEHARI fournit des questionnaires type et l'analyse des risques inhérents à tout point faible détecté.



2B3. Analyse des risques

Dans MEHARI, l'analyse des risques comprend :

- l'identification des situations représentant un risque pour l'entreprise ;
- l'évaluation de la probabilité que ces situations à risque ne surviennent, de leurs conséquences possibles, de leur caractère acceptable ou non ;
- le recensement des mesures à prendre, susceptibles de ramener chaque risque à un niveau acceptable.

Utilité :

- définir les mesures les mieux adaptées à l'entreprise ;
- mettre en place un management des risques et être sûr que tous les risques sont identifiés ;
- analyser et gérer les risques de tout nouveau projet.

MEHARI fournit, outre le modèle de risques, des métriques (c'est-à-dire de quoi mesurer les risques), une démarche et des guides de mise en œuvre.

Les résultats attendus ici sont des plans d'action.

2B4. Le pilotage de la sécurité

Il s'agit ici de définir :

- les objectifs annuels ;
- les étapes de plans d'action, à l'aide d'indicateurs définis par la méthode.

2B5. Conclusion

Cette méthode est assez lourde et importante en volume, elle me paraît surdimensionnée pour des petites structures. La démarche qu'elle préconise est très «carrée». L'application de cette méthode nécessite des moyens humains conséquents, mais son utilisation garantit une stratégie, un pilotage de la sécurité adapté à l'entreprise.

Nous allons maintenant aborder la stratégie à adopter lorsque le choix de sécurité est curatif.

3. Plan de reprise (sécurité curative)

Un **plan de reprise**, c'est l'ensemble des mesures nécessaires au redémarrage, sous des délais et conditions appropriées aux critères de survie de l'entreprise, d'une production informatique bloquée, détruite ou endommagée.
L'élaboration d'un plan de reprise se déroule généralement en cinq étapes.

Étape 1 : étude préalable
On décrit les objectifs généraux du plan de reprise, ainsi que la situation de l'entreprise.

Étape 2 : étude de faisabilité
On élabore un « algorithme » général (entre 5 et 10 étapes) du plan de reprise,
On évalue quelles doivent être les conditions initiales pour que le plan de reprise soit faisable.

Étape 3 : rédaction des fiches de procédure
Ici, on rédige de façon très précise la liste des manipulations à réaliser pour que la reprise soit effective.

Étape 4 : test
On teste si ce qu'on a élaboré permet effectivement une reprise.
Sinon, on procède à des remèdiations dans les étapes précédentes, puis on teste à nouveau.

4. En conclusion, quelques mots sur les politiques de sécurité

La politique de sécurité de l'information est l'aboutissement des réflexions menées concernant les choix opérés (active/passive, curative/préventive…) pour sécuriser un système informatique. L'établissement d'une politique de sécurité du système est indispensable.

Bien sûr, il est impossible de sécuriser un site informatique à 100%, aucune entreprise n'est complètement à l'abri d'un sinistre informatique.

Bien sûr encore, la sécurisation d'un site informatique a forcément un coût et les éléments constituant le site informatique ont eux aussi une valeur.

Lors de l'établissement d'une politique globale de sécurité, il faut donc comparer la valeur des données, logiciels et matériels que l'on protège (dans le cas d'une sécurité préventive) ou que l'on remet en état (dans le cas d'une sécurité curative) et ce que coûte l'action de protéger ou de réparer.

Il faut penser aux différents niveaux de sécurité (matériel, logiciel, humain). Pourquoi ?

Il existe une règle d'or qui dit que la sécurité est **une chaîne qui ne vaut que par son maillon le plus faible**.

Qu'est-ce que ça signifie ?
Cela signifie que si un aspect de la sécurité est négligé ou n'est pas appliqué, le niveau global de sécurité rejoint le niveau de cet aspect négligé ou non appliqué.

Une politique de sécurité doit donc :

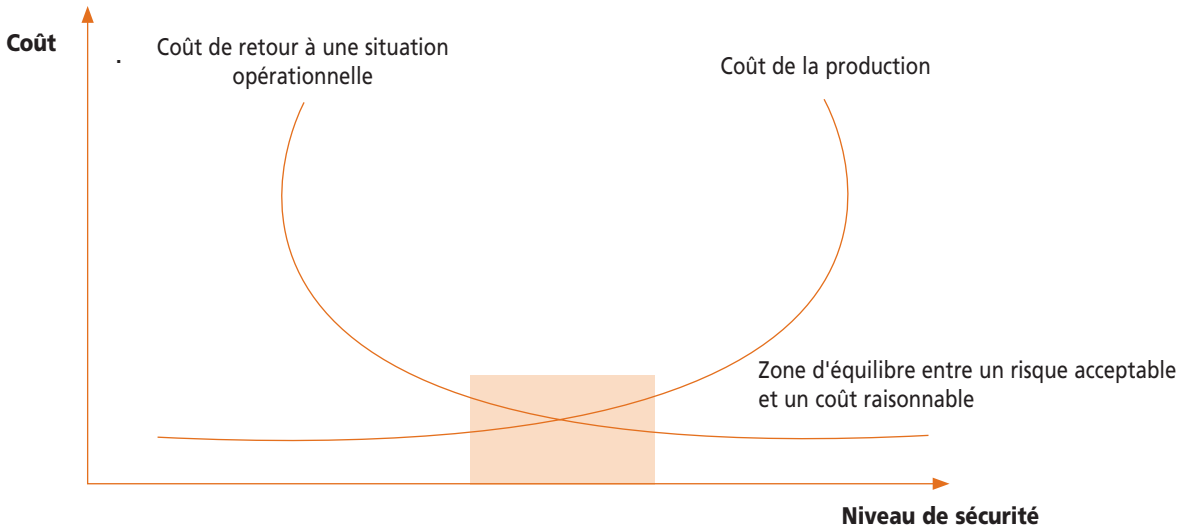
- définir une politique globale à l'organisation puisque la sécurité est une chaîne ;
- être chapeautée par une personne possédant une autorité en matière de sécurité (« architecte sécurité », « responsable sécurité ») ;
- inclure une veille technologique permanente ;
- associer l'ensemble des acteurs, en particulier les utilisateurs ;
- sensibiliser tous les acteurs aux risques et aux moyens de s'en prémunir ;
- élaborer des règles et des consignes de sécurité.

Et le coût ?
La sécurisation d'un système d'information peut représenter des coûts très importants. Elle a pour particularité de porter sur un aspect de l'entreprise qui est difficilement chiffrable : l'information.

Ne rien protéger ne coûte rien, tant qu'aucun incident ne se produit. C'est pour cela qu'il est très important d'évaluer les risques et les coûts associés à un plan de reprise, dont le rôle est de remettre le système dans son état initial.

De la même manière, se protéger de tout entraîne un coût extrêmement élevé, dépassant celui des éléments à protéger.

Le schéma ci-après illustre le point optimal entre risque et sécurité.



Nous allons maintenant étudier de plus près différents moyens de prévention, dans la séquence 15.

Séquence 15

Les moyens de prévention

Nous allons présenter ici les moyens existants de protéger le matériel d'une part, les données et les logiciels d'autre part, avec toujours à l'esprit la règle suivante : une dégradation matérielle peut endommager la couche données/logiciels, mais une dégradation logicielle ne peut pas endommager le matériel. Tout au plus, une dégradation au niveau des données ou des logiciels pourra provoquer un dysfonctionnement du matériel, mais pour des raisons logicielles.

1. Les moyens de protection du matériel

On peut tout d'abord commencer par noter que certaines technique de sécurisation entrent actuellement au niveau des puces, comme par exemple dans **Next Generation Secure Computing** (NGSC), c'est à dire le Palladium (sécurité microsoft), qui, depuis mai 2003, repose sur l'implémentation de technique de sécurisation au niveau des puces, donc du matériel.

Je vous présente ci-dessous les moyens les plus répandus de protéger le matériel.

1A. Les onduleurs

Je pense que la plupart d'entre vous savent ce qu'est un onduleur. Pour ceux et celles qui ne sont pas vraiment au point sur ce type de matériel, voici ci-dessous quelques points essentiels à connaître.

Un onduleur est un boîtier que l'on intercale entre la prise électrique murale et l'ensemble du matériel informatique.

Un onduleur comporte une batterie électrique qui produit du courant continu, ainsi que des composants capables de transformer le courant continu en courant alternatif.

Il existe de nombreuses gammes d'onduleurs, à tous les prix. Bien entendu, plus c'est cher, plus l'autonomie électrique est longue.

L'onduleur permet de protéger le système informatique de la détérioration du matériel ou de la perte de données pour des raisons de dysfonctionnement électrique.

L'onduleur permet de protéger le matériel contre différents types de dysfonctionnements :

- Les coupures d'électricité (très courtes, comme les micro-coupures) ou plus longues. L'onduleur est capable dans ce cas de continuer à alimenter le matériel informatique en électricité.
  Le temps d'autonomie électrique varie d'un onduleur à l'autre, mais au moins, lors des coupures, on a le temps d'enregistrer son travail avant de ne plus avoir de courant pour alimenter le système informatique.
- Les pics de tension ou les chutes de tension électrique survenant dans le secteur. Ces variations d'alimentation sont préjudiciables aux composants matériels (par exemple, en cas d'orage, la foudre est capable de créer d'énormes pics de tension, ce qui peut

faire « griller » les composants). L'onduleur est capable de réguler la tension arrivant au matériel qu'il dessert.

- Des **parasites** électriques peuvent être produits par d'autres appareils électriques ou par une ligne électrique de mauvaise qualité. L'onduleur est capable de protéger le matériel de ces perturbations.

Un onduleur est caractérisé par sa **puissance** et la par la **technologie** qu'il utilise.

La puissance

La **puissance** d'un onduleur s'exprime en **voltampère**. Cette puissance est en fait la puissance de protection que l'onduleur est capable de déployer en cas de dysfonctionnement électrique.

Pour savoir si un onduleur donné est suffisamment puissant pour protéger une configuration informatique, il faut faire la somme de la consommation électrique de chaque appareil composant la configuration (unité centrale, moniteur, imprimante, clavier, souris, modem, disque de sauvegarde externe, scanner, enceintes…). Cette consommation se calcule en ampères. On trouve la consommation des appareils généralement sur les appareils eux-mêmes (sur des étiquettes collées au dos des appareils).

La somme des consommations une fois effectuée, on la multiplie par 230. Le résultat de cette multiplication s'exprime en **volts-ampères.**

Bien entendu, la puissance de l'onduleur, afin que celui-ci soit efficace pour protéger la configuration informatique concernée, doit être supérieure au résultat du calcul d'apothicaire décrit ci-dessus.

La technologie

Sur le marché, il existe différentes technologies en ce qui concerne les onduleurs actuels.

- La technologie **off line**. C'est la technologie la plus sommaire. On la trouve dans les modèles les moins chers. Avec ce type d'onduleur, la batterie prend le relais pour une durée plus ou moins limitée en cas de coupure de courant.
- La technologie **on line**. Ce type d'onduleur travaille en permanence, et pas seulement en cas de problème électrique. Le courant électrique est traité en permanence par l'onduleur. Le courant électrique du secteur est systématiquement transformé en courant continu puis retransformé en courant alternatif par les différents matériels de l'onduleur. Le résultat est un courant dit **régulé** ou **stabilisé** ou **lissé**.
  Cette technologie protège donc le matériel de toute variation intempestive de courant. Ce type d'onduleur coûte très cher et est surtout utilisé par les professionnels.
- La technologie **interactive**. Ce type d'onduleur fonctionne comme ceux de la catégorie **off-line**, mais ils sont équipés, en plus, d'un régulateur de tension, afin de réguler les variations importantes pouvant survenir sur le réseau électrique d'alimentation.

Le prix de ce type d'appareil est raisonnable.

Voilà ce qu'on peut dire en gros des onduleurs. Ils protègent des dysfonctionnements électriques.

À côté de ce risque électrique, il y a le risque que, sans aucune panne de courant, la machine tombe en panne.
Afin, dans ce cas, de ne pas perdre de données, ou de ne pas mettre les données dans un état d'incohérence, il faut prévoir un système de sauvegarde. Il existe plusieurs façons de mettre en place des sauvegardes, dont le système RAID. Cette technologie, plus qu'un

simple système de sauvegarde, permet d'augmenter la tolérance aux pannes des machines équipées.

Ci-dessous, nous allons d'abord parler des systèmes de sauvegardes, puis nous passerons à une description sommaire de ce qu'est le système RAID.

1B. *Les sauvegardes*

Pour donner une définition simpliste, une sauvegarde, c'est une copie de ce qu'on a sur le disque dur de notre machine, copie que l'on stocke ailleurs, au cas où notre machine viendrait à ne plus fonctionner.

La nécessité d'effectuer des sauvegardes n'est pas uniquement dictée par le fait que le disque dur de notre machine puisse tomber en panne ou que notre local a été inondé, mais aussi par des risques non matériels comme la corruption des données (suite à un plantage système, par exemple), les fausses manips (du genre : « Mince, j'ai effacé la bonne version du cours de GEOSI que je suis en train d'écrire, et j'ai gardé l'ancienne… »), virus destructeurs, malveillance, inondation...

Selon l'entreprise editomac (voir http.//www.editomac.fr), les statistiques d'assurance disent que 80% des entreprises qui ont un sinistre informatique sans réelles sauvegardes font faillite dans l'année qui suit.

Les différentes façons de faire des sauvegardes dépendent à la fois des supports physiques et des méthodes et outils que l'on utilise.

1B1. Les supports physiques de sauvegarde

On peut sauvegarder tout ou partie de nos données.

• Sur un **deuxième disque dur**. Ce disque peut être interne ou externe à notre machine.

Attention, il ne faut pas confondre deuxième disque dur interne et deuxième partition de disque dur. Une partition de disque dur, c'est une partie de disque dur à laquelle on a alloué un nom d'unité logique. On peut donc très bien avoir un seul disque dur dans notre machine, et plusieurs partitions sur ce même disque. Le partitionnement de disque dur permet par exemple de pouvoir faire cohabiter plusieurs systèmes d'exploitation sur le même disque dur, c'est très pratique mais par contre, si le disque dur de la machine tombe en panne, les données de toutes les partitions deviennent inaccessibles.

On est donc bien d'accord : lorsque je parle de sauvegarde sur un deuxième disque dur interne, cela suppose que dans l'ordinateur, il y ait un deuxième disque dur, et donc un deuxième contrôleur de disque dur.

Si le disque dur est externe, il se branche à la machine via une prise USB ou FireWire (**note à l'attention de ceux et/ou celles qui ne connaissent pas la signification du terme FireWire :** FireWire est un standard matériel au même titre qu'USB. Ce standard correspond à la norme **IEEE1394**, il est également appelé **iLink** chez Sony. Ce type de prise est majoritairement utilisé pour récupérer sur une machine les films contenus dans les caméscopes numériques. Elle s'utilise aussi avec certains disques et graveurs externes, et fournit des performances en général légèrement supérieures à celles de l'USB 2.0. Par contre, les machines n'en sont pas systématiquement équipées, ce standard a moins bien percé qu'USB).
Bref, que le disque dur soit externe ou interne, la sauvegarde, dans ce cas, consiste en une recopie disque à disque des données que l'on veut conserver en cas de panne.

• Sur un CD ou un DVD. Dans ce cas, cela suppose que notre machine soit équipée d'un graveur de CD/DVD. La sauvegarde est plus longue que si on utilise un deuxième dis-

que dur car là, il s'agit de graver, et pas de simplement recopier. On doit donc utiliser un logiciel de gravure. En outre, l'espace disponible sur un CD (environ 800 Mo) ou un DVD (environ 4 à 5 Go) est beaucoup moins important que sur un disque dur, ce qui peut nous obliger à réaliser la sauvegarde en plusieurs fois, pour la répartir sur plusieurs CD ou DVD. Mais bon, un CD vierge est aussi beaucoup moins cher qu'un deuxième disque dur, qu'il soit interne ou externe !

- Sur d'autres supports externes (par exemple de type cassettes DAT), à partir du moment où on possède le matériel permettant de lire et d'écrire sur ce support.

1B2. Les méthodes et outils de sauvegarde

Plusieurs stratégies de sauvegarde sont possibles.

On peut décider, lors de chaque sauvegarde, d'effectuer juste une sauvegarde dite **incrémentale**. Dans ce cas, on se contente de sauvegarder uniquement les fichiers ayant été modifiés depuis la dernière sauvegarde.

On peut, au contraire, lors de chaque sauvegarde, opter pour une **sauvegarde complète** lors de chaque sauvegarde. Cette stratégie prend, bien sûr, plus de temps que la sauvegarde incrémentale.

Quelle que soit la stratégie de sauvegarde choisie, il est important d'effectuer les sauvegardes sur plusieurs supports, et de placer les supports de sauvegarde dans des endroits différents du système à sécuriser, ceci afin d'éviter leur destruction simultanée, dans le cas d'un incendie ou d'une inondation, par exemple.

En deçà d'une méthode de sauvegarde, et pour parer à toutes éventualités en terme de dysfonctionnement, quelques mesures de bon sens s'imposent, comme par exemple :

- ausculter régulièrement le disque dur à l'aide des outils système livrés avec le système d'exploitation ;
- consigner l'ensemble de ses mots de passe ;
- faire des captures d'écran des paramètres de configuration importants ;
- se donner le moyen de pouvoir redémarrer le système à l'aide d'un support externe (comme un CD bootable, par exemple)…

Même si on a effectué une sauvegarde complète des données, et même si on a conservé les informations importantes de configuration et les mots de passe, en cas de disque dur illisible, remettre un nouveau disque dur dans le même état est un travail long et assez fastidieux.

Pour pallier cela, il existe des **outils logiciels** capables de reproduire à l'identique l'état d'un disque dur. Ces outils permettent de sauvegarder l'intégralité du disque dur, et de créer ce qu'on appelle une **image** du disque dur. Cette **image** une fois créée, il suffit de la stocker sur un support externe.

À chaque fois que l'on veut reproduire l'état de ce disque dur sur une autre machine, il suffit d'utiliser l'outil ayant permis de créer l'image pour installer cette image sur un autre disque dur.

Le logiciel le plus connu dont le rôle est de créer des images s'appelle **ghost** (il est édité par **Norton**), mais il en existe d'autres. Il existe même un utilitaire de ce type fourni dans windows, par exemple. Sous windows, cet utilitaire s'appelle **Sauvegarde** sous Windows 98, **Sauvegarder** sous Windows 2000 ou encore **Utilitaire de sauvegarde** sous Windows XP.

Ces utilitaires permettent généralement d'effectuer des sauvegardes partielles, différentielles, incrémentales ou totales, et de créer des images.

Il existe également, dans les outils cités plus haut ou dans des outils à part, des utilitaires permettant de :

– programmer des sauvegardes à intervalles de temps réguliers ;
– synchroniser ses fichiers ;
– récupérer des fichiers perdus ;
– restaurer son système...

Parallèlement à tous ces outils permettant soit de prévenir le risque, soit de le réparer, on peut aussi citer le choix que font de plus en plus d'entreprises, qui est de faire des sauvegardes en ligne, en louant de l'espace disque chez des hébergeurs accessibles via le net ou via des lignes spécialisées. Dans ce cas, les données à sauvegarder sont envoyées (souvent de manière sécurisée) et hébergées par ces hébergeurs spécialisés dans le stockage des données.

Pour connaître quelques prestataires délivrant ce type de service, il vous suffit de taper le mot **sauvegarde** dans votre moteur de recherche préféré.

1B3. Et si malgré toutes les précautions prises, il y a perte de données : solution curative

En dernier recours, si on a perdu ses données, il existe des entreprises spécialisées dans la récupération de données sur des supports endommagés. Ca coûte cher, mais c'est parfois efficace.

Voir par exemple http.//www.ontrack.fr/recuperationdedonnées/, il s'agit du site d'une entreprise spécialisée dans la récupération de données perdues.

Voilà à peu près ce qu'on peut dire en gros sur les sauvegardes.

Passons maintenant à une technique relevant de la sauvegarde, tout en étant plus élaborée, je veux parler ici du système **RAID**.

1C. Le système RAID

C'est un système de stockage ultra fiable sur disques durs multiples.

De même que pour les onduleurs, certain(e)s parmi vous sont peut-être d'ores et déjà très au point sur la technologie RAID, mais d'autres peut-être moins.

Voici donc un petit topo sur l'essentiel à savoir à propos de cette technologie.

Le sigle RAID signifie **Redundant Array of Inexpensive Disks**, ou parfois, ce sigle est indiqué comme signifiant **Redundant Array of Independent Disks**. En français, on peut dire que ce sigle signifie **Ensemble redondant de disques indépendants.**

La technologie RAID permet de constituer **une** unité de stockage **virtuelle** de grosse capacité (donc coûteuse), à partir de plusieurs disques durs peu onéreux.

L'unité ainsi créée est appelée une **grappe** et a une grande tolérance aux pannes (haute disponibilité), et aussi une plus grande vitesse d'écriture.

C'est ici la répartition des données sur plusieurs disques durs qui permet d'assurer la sécurité des données.

Cette technologie a été mise au point en 1987 par trois chercheurs (*Patterson*, *Gibson* et *Katz*) à l'Université de Californie (Berkeley).

Depuis 1992, c'est un organisme, le RAID Advisory Board, qui gère les spécifications caractérisant les différentes catégories de RAID.

Pourquoi je parle de **différentes catégories de RAID** ? Parce que, les disques assemblés selon la technologie RAID peuvent être utilisés de différentes façons, appelées **Niveaux RAID**.

Chacun de ces niveaux décrit la manière avec laquelle les données sont réparties sur les disques. Pour l'instant, il existe 7 niveaux répertoriés, numérotés de 0 à 6, mais le niveau 2 a été déclaré obsolète par le RAID Advisory Board.

En fait, chacun de ces niveaux constitue un mode d'utilisation de la grappe, en fonction des performances, du coût et des accès disques.

Dans le tableau ci-dessous, je vous donne une description rapide de chacun de ces niveaux.

Niveau	Nom(s) donné(s) au niveau	Description sommaire
RAID-0	Striping	Le terme **striping** se traduit généralement par **entrelacement** ou **agrégat par bande**. Cette technique consiste à stocker les données en les répartissant sur l'ensemble des disques de la grappe. En RAID-0, il n'y a pas de redondance, et donc pas de tolérance aux pannes (en cas de défaillance de l'un des disques, les données sont perdues). Par contre, ce niveau de RAID permet une vitesse de transfert élevée. En RAID-0 les données sont écrites par «bandes» (en anglais, **bande** se dit **stripe**), c'est à dire en fragments. Exemple : si on a 3 disques durs en RAID-0, le premier fragment sera écrit sur le premier disque, le deuxième fragment sur le deuxième disque, le troisième fragment sur le troisième disque, le quatrième fragment sur le premier disque, le cinquième fragment sur le deuxième disque etc. On appelle **facteur d'entrelacement** la taille des fragments. Plus les fragments sont petits, plus la vitesse de transfert est élevée. Le remplissage par fragments devient impossible lorsque le plus petit disque dur de la grappe est plein. Il vaut donc mieux utiliser des disques de même taille pour faire du RAID-0, car dans le cas contraire, les disques de plus grande capacité ne sont pas pleinement exploités. La capacité de stockage de la grappe est égale à la capacité du plus petit des disques, multipliée par le nombre de disques.
RAID-1	Mirroring, shadowing	Chaque fragment est dupliqué au même endroit sur chaque disque dur de la grappe. En cas de panne du système, RAID 1 opère une recopie disque à disque. La lecture des données est également beaucoup plus rapide (On accède en parallèle à des fragments différents sur des disques différents). Le système peut continuer à fonctionner même si un des disques est en panne. **Remarque :** cette solution est performante mais coûteuse, puisque la capacité de stockage est égale à celle du plus petit disque dur, quel que soit le nombre de disques de la grappe.
RAID-2	Déclaré obsolète, mais il a quand-même un nom : striping with parity	Ce niveau est obsolète car il propose un contrôle d'erreur par code de Hamming (codes **ECC** – Error Correction Code), or ce code est désormais intégré dans les contrôleurs de disques durs. Le principe du niveau 2 était le suivant : niveau RAID-0 en écrivant, en plus, sur un disque supplémentaire les valeurs des bits de contrôle ECC. Le RAID 2 se caractérisait par des piètres performances mais un niveau de sécurité élevé.

RAID-3	Disk array with bit-interleaved data (le moins qu'on puisse dire, c'est que c'est un nom à rallonge!)	Les données sont stockées octets par octets sur chaque disque et un des disques est dédié au stockage d'un bit de parité suivant le schéma suivant : **Disque 1** **Disque 2** **Disque 3** **Disque 4** Octet 1 Octet 2 Octet 3 Parité 1+2+3 Octet 4 Octet 5 Octet 6 Parité 4+5+6 Octet 7 Octet 8 Octet 9 Parité 7+8+9 Si un des disques tombe en panne, on peut reconstituer les octets perdus à partir des autres disques. Après reconstitution, le contenu du disque défaillant est de nouveau intègre. Par contre, si deux disques tombent en panne en même temps, les informations restantes ne permettent pas de reconstituer les informations manquantes.
RAID-4	Disk array with block-interleaved data	Les principes sont les mêmes que ceux du niveau 3 sauf que les informations ne sont pas réparties octet par octet, mais bloc par bloc. C'est donc la valeur du facteur d'entrelacement qui n'est pas la même entre le niveau 3 et le niveau 4.
RAID-5	Disk array with block-interleaved distributed parity	Ce niveau est proche du RAID-0 en terme de performance, mais avec, en plus, une bonne tolérance de panne. Les principes sont les mêmes que ceux du niveau 4 sauf que les informations de parité ne sont pas toutes stockées sur le même disque, mais réparties sur l'ensemble des disques de la grappe, ce qui améliore les performances d'accès aux données. Exemple : Disque 1 Disque 2 Disque 3 Disque 4 Octet 1 Octet 2 Octet 3 Parité 1+2+3 Octet 4 Octet 5 Parité 4+5+6 Octet 6 Octet 7 Parité 7+8+9 Octet 8 Octet 9 En cas de panne du système, RAID-5 reconstruit le disque manquant à partir des informations stockées sur les autres disques.
RAID-6	Disk array with block-interleaved distributed parity	Ce niveau utilise 2 fonctions de parité, dont les résultats sont stockés sur deux disques dédiés. Ceci permet de reconstituer les données même si deux disques sont en panne en même temps. Il faut au moins 4 disques pour mettre en œuvre un système RAID-6.

Les solutions RAID les plus couramment utilisées sont le **RAID-1** et le **RAID-5**.

Le choix entre l'une ou l'autre de ces solutions RAID doit prendre en compte les trois critères suivants :

- **la sécurité** : RAID 1 et 5 offrent tous les deux un niveau de sécurité élevé, toutefois la méthode de reconstruction des disques varie entre les deux solutions ;
- **les performances** : RAID 1 offre de meilleures performances que RAID 5 en lecture, mais pas lors d'importantes opérations d'écriture ;
- **le coût** : le coût est lié à la capacité de stockage devant être mise en oeuvre pour avoir une certaine capacité effective. La solution RAID 5 offre un volume utile représentant 80 à 90% du volume alloué (le reste servant au contrôle d'erreur). La solution RAID 1 n'offre par contre qu'un volume disponible représentant 50 % du volume total (étant donné que les informations sont dupliquées).

Sur un serveur, on peut mettre en place une solution RAID de plusieurs façons :

- **mise en place logicielle** : dans le système d'exploitation, on rajoute un pilote (c'est-à-dire, en anglais, un driver) capable de créer un seul volume logique avec plusieurs disques ;
- **mise en place matérielle** : là encore, il existe plusieurs choix possibles dont…

Le rajout de contrôleurs de disques RAID. Ce sont des cartes que l'on rajoute dans la machine et sachant contrôler plusieurs disques durs.

L'utilisation de matériels DASD (direct access stockage device). Ce sont des unités de stockage externes pourvues d'une alimentation propre.

Voilà, j'ai fini cette partie sur les solutions de prévention au niveau matériel.

Passons aux solutions de prévention logicielles.

2. Les solutions de prévention au niveau logiciel

Dans cette partie, je parle très peu des actions que je qualifierais de « normales », sur poste individuel ou en réseau (local et étendu), et qui concerne la gestion des utilisateurs et de leurs droits en ce qui concerne l'accès aux ressources, l'accès au système d'information compris.

2A. Quelques règles tout de même concernant la sécurisation d'un réseau

La transmission de données sur un réseau doit pouvoir répondre aux impératifs de sécurité suivants :

- garantir la **confidentialité** des données (l'émetteur et le récepteur sont les seuls à pouvoir connaître le contenu d'un message) ;
- permettre l'**authentification** de l'auteur d'un message (celui qui reçoit un message doit pouvoir être sûr de l'identité de l'émetteur) ;
- garantir la **non-répudiation** des données (c'est-à-dire empêcher quelqu'un de renier le fait d'avoir envoyé un message) ;
- garantir l'**intégrité** des données (c'est-à-dire qu'elles ne seront pas modifiées en cours de route).

Pour prendre en compte ces impératifs, il est indispensable que l'accès aux machines source et destination soit sécurisé : contrôle de l'utilisateur, contrôle de l'intégrité des machines (virus, logiciels admis), contrôle de l'accès aux ressources (droits d'accès).

2A1. Authentification des utilisateurs

Le contrôle de l'identité d'un utilisateur peut se faire par :

- mot de passe (il ne doit pas être facile à deviner, doit être modifié régulièrement, doit être crypté lors de sa transmission sur le réseau) ;
- dispositif électronique porté par l'utilisateur comme carte magnétique, à puce, bar code, à passer dans un lecteur, système à proximité (Porte clé, scanner) ;
- biométrie (L'authentification d'un utilisateur par biométrie se base sur la reconnaissance d'une caractéristique physique de l'utilisateur ou d'une manière de se comporter qui lui est unique).

On utilise les paramètres suivants : empreinte digitale, forme de la main, visage, iris, rétine, voix, signature, frappe du clavier.

Dans le cas, par exemple, de l'authentification par **empreinte digitale**, l'utilisateur appuie un doigt sur un capteur constitué d'un micro-scanner qui réalise une image de l'empreinte (= ensemble de sillons).

De cette image est extrait un certain nombre d'informations significatives qui sont comparées avec les données des utilisateurs enregistrés.

Plusieurs éléments caractéristiques peuvent être repérés dans une empreinte : fin de sillon, sillons bifurquants, sillons divergeants, îlots, sillons entourant un vide, petits sillons.

Tout ceci permet de réduire l'image à un ensemble de caractéristiques simples à mémoriser.

Exemple de lecteur d'empreinte digitale : *u-are-u de Digital Persona*

Dans le cas de l'authentification par la **forme de la main**, l'appareil mesure la longueur, la largeur, l'épaisseur et la surface de la paume et des doigts. Le dispositif utilisé est un scanner 3D, il permet la vérification, pas l'identification absolue.

Je ne vais pas plus loin dans le détail de chaque technique biométrique. Les deux techniques les plus fiables sont **l'empreinte digitale** et le scan de **l'iris**.

2A2. Contrôle de l'intégrité des machines

Ce contrôle consiste à empêcher :

- les virus, troyens, vers, à l'aide d'antivirus ;
- les spams, mail bombs, junk mails, par filtrage des adresses entrantes ;
- les attaques en déni de service (DoS et DdoS), l'IP spoofing et autres techniques d'inondation, de blocage de machines ou d'interception à l'aide de firewalls et de logiciels de filtrage… (voir pour une liste complète la RFC2196 sur les règles de sécurité. RFC signifie : Request For Comment, ce sont des recommandations émises par des organismes reconnus, comme par exemple le W3C) ;
- il fait également transiter les données de manière chiffrée.

Je reviens plus en détail sur certaines techniques plus bas dans ce cours.

2A3. Contrôle de l'accès aux ressources

Généralement, gérer les ressources d'un réseau présume qu'on dispose :

- d'un serveur gérant les autorisations d'accès aux ressources ;
- d'un serveur hébergeant les espaces de travail des utilisateurs ;
- de postes clients à partir desquels chaque utilisateur peut ouvrir une session à l'aide de son nom d'utilisateur et de son mot de passe.

Selon la ressource, l'accès peut être réservé à une seule personne (espace personnel) ou bien autorisé à plusieurs utilisateurs définis (espaces communs).

L'accès à chaque espace peut se faire en lecture-écriture ou être limité à la lecture seule.

Les systèmes d'exploitation de type « serveur » permettent également de créer des groupes d'utilisateurs rassemblant les personnes disposant d'autorisations similaires.

Voilà pour cette petite synthèse sur la sécurisation d'un réseau.

2B. *Et quelques règles aussi concernant la sécurité du SI*

Pour rappel, le SIA, c'est un ensemble d'éléments logiciels qui permettent d'acquérir, de traiter et de mémoriser des informations et de les communiquer dans l'organisation.

Le SIA est composé par un ensemble d'informations formelles et de procédures et moyens utilisés pour le traitement de ces informations (en gros, des bases de données et des applications pour y accéder). En ce qui concerne les risques vis-à-vis du système d'information, on parle de **risque opérationnel**.

Je vous remets ci-dessous une partie de la classification des risques opérationnels, celle qui concerne spécifiquement le système d'information.

Le terme de système d'information est employé ici au sens de système d'information automatisé. Je ferai de même dans la suite de ce paragraphe.

Défaillance des systèmes d'information

4. Défaillance de matériel
5. Données incohérentes ou incompatibles
6. Mauvaise gestion de projet
7. Défaillance des software
8. Faiblesse de la sécurité logique
9. Faiblesse de la sécurité physique

Je vous fais une présentation assez théorique, mais somme toute assez utile, des risques opérationnels, puis nous passerons à un point de vue plus concret, celui de l'administrateur de base de données.

2B1. Définition des risques opérationnels

Comme je l'ai déjà expliqué dans la conclusion de la séquence 13, qui présentait les différents types de risques, le risque opérationnel se définit comme le risque de perte résultant de l'inadaptation ou de la défaillance de procédures, de personnes ou de systèmes internes ou encore d'évènements extérieurs (catastrophes naturelles, incendie, agression, etc.).

Il inclut le risque lié à la sécurité des systèmes d'information.

Le risque opérationnel est inhérent à chacun des métiers et des activités de l'entreprise.

Sa gestion repose sur un dispositif de **prévention**, de **contrôle** et de **couverture**. Ce dispositif intègre des procédures détaillées, une surveillance permanente, des polices d'assurance, auxquelles s'ajoutent des missions d'audit.

Pour bien gérer les risques, il est utile de disposer d'un historique de pertes opérationnelles internes, sous forme d'une base de données.

Cette base de données permet d'analyser les pertes (par nature d'évènements, par cause, par activité…) et de suivre leur évolution ainsi que les plans d'actions proposés. Ceci permet à l'entreprise de disposer d'une base de connaissance évolutive permettant d'établir une sorte de cartographie des risques intrinsèques caractéristiques de chaque activité.

L'objectif de ce mode de gestion des risques opérationnels est une alerte rapide, et donc une réaction rapide et une diminution des dégâts, ce qui permet une amélioration et une optimisation des actions correctives et préventives.

Bien entendu, pour bien gérer le risque lié au système d'information proprement dit, il est nécessaire d'être perpétuellement vigilant sur la qualité et l'efficacité du dispositif de

contrôle affecté à ces risques, l'efficacité de ce dispositif reposant en grande partie sur un système d'information fiable.

L'enjeu, dans un système d'information, c'est justement l'information.

Le SI est un outil stratégique (pensez à l'importance que peuvent avoir les bases de données dans une banque, par exemple, où tout, même nos sous à nous, est dématérialisé et géré par un système d'information).

Le SI doit donc être **sûr**, **fiable**.

Pour un établissement bancaire, par exemple, la perte du SI est extrêmement grave, car il s'agit de la perte de l'instrument de production, ce qui n'est pas le cas pour une entreprise industrielle.

2B2. Gestion des risques

Au vu des enjeux que représente le SI, il est essentiel de pouvoir mesurer le risque, afin de définir une stratégie de prévention et gestion de ces Risques (arbitrages, plannings, décisions).

Prenons le cas d'un établissement bancaire, car c'est le plus significatif.

Dans une banque, la principale mesure du risque est le risque maximum tolérable (RMT). C'est la valeur financière limite que la banque peut se permettre de perdre en cas de problème.

Voici la règle de calcul du RMT :

$$RMT = \alpha\,FondsPropres + \beta\,Bénéfices + \gamma\,Garanties$$

Avec : α, β, γ <= 1

Voici des précisions sur la valeur de α, β et γ :

α : le minimum réglementaire est de 8% des fonds propres (ratio de solvabilité), décision du comité de Bâle ;

β : c'est la capacité bénéficiaire prévisionnelle nette de l'année que la banque peut se permettre de perdre pour absorber le sinistre ;

γ : il est calculé à partir des garanties accordé par les assurances.

La politique de sécurité du SI est fondamentale.
Elle comprend la sensibilisation des acteurs face aux risques, un audit régulier du SI, la mise en place de mesures de sécurité pour diminuer la vulnérabilité (on en parle tout au long de cette séquence), et doit permettre à chaque instant : disponibilité, intégrité, confidentialité, preuve et contrôle.
Les quatre caractéristiques ci-dessus sont appelés les facteurs DICP.

Je vous les décris ci-dessous. Bien entendu, ce que j'explique ici à propos du système d'information proprement dit a un goût de déjà vu, car on a déjà parlé plus ou moins de tout cela à propos du système d'information au sens large.

Disponibilité : c'est l'aptitude du SI à remplir ses fonctions dans des conditions prédéfinies d'horaires, de délais, de performances à savoir :

- garantir la continuité du service, de l'activité ;
- assurer les objectifs de performance (temps de réponse) ;
- respecter les dates et heures de traitements.

Intégrité : c'est une caractéristique du SI qui assure que des informations sont identiques en deux points, dans le temps et dans l'espace, d'où la nécessité de :

– garantir l'exhaustivité, l'exactitude, la validité de l'information ;
– éviter la modification par erreur de l'information.

Confidentialité : c'est la caractéristique du SI qui assure la tenue secrète des informations avec accès aux seules entités autorisées. Pour ce faire, il faut :

– réserver l'accès aux seules personnes autorisées (système d'habilitation et d'authentification) ;
– garantir le secret des données échangées par deux correspondants, sous forme de messages ou de fichiers.

Preuve et contrôle : il s'agit de la non répudiation, déjà évoquée par ailleurs dans ce cours. C'est l'impossibilité pour une entité de nier avoir reçu ou émis un message.

Il faut pour cela garantir la possibilité de reconstituer un traitement à tous les niveaux (logique de programmation, déroulement du traitement, forme des résultats) à des fins de contrôle ou de preuve.

2B3. En pratique, quels sont les outils ?

Le DBA (DataBase Administrator, en français, on dit Administrateur de Base de Données) est garant de la sécurité et de l'intégrité du système d'information et doit travailler en collaboration avec l'administrateur du réseau, et participer à l'organisation de la sécurité, qu'elle soit préventive ou curative.

Il doit donner des droits aux utilisateurs des bases de données hébergeant les données du SI.

Je citerai ici trois grandes catégories d'utilisateurs :

– les développeurs, qui développent des applications de manipulation des données, ces applications sont destinées à l'utilisateur final (c'est-à-dire l'utilisateur des applications). Les développeurs ont généralement un accès direct aux bases de données qu'ils utilisent, via un logiciel client (pour accéder aux données de la base, ils tapent des requêtes en SQL), mais ils n'ont pas forcément accès à toute l'information ;
– l'utilisateur final, qui lui, ne tape pas de requête SQL, mais accède aux bases de données via les applications créées par les développeurs. Si les applications sont bien développées, l'utilisateur final a peu de chance d'endommager une base de données, à partir du moment où il est autorisé à utiliser l'application ;
– les applications, qui sont elles-mêmes des utilisateurs des bases de données qu'elles manipulent.

Pour ces catégories d'utilisateurs, il faut un système d'authentification afin :

– d'autoriser ou non l'utilisation de certaines applications (pour l'utilisateur final) ;
– d'effectuer ou non certaines opérations sur la ou les bases de données du système d'information (pour les développeurs et les applications).

Le DBA, pour garantir l'intégrité logicielle des données du SI, doit aussi mettre en place des contrôles lors de la modification de la structure ou du contenu des bases de données, afin, par exemple, qu'il n'y ait pas insertion d'une ligne mettant la base de données en état d'incohérence, ou bien encore, afin qu'il n'y ait pas de modification de la structure.

Les outils dont il dispose s'appellent contraintes d'intégrité, procédures stockées, gestion de transactions, gestion des droits… Je vous renvoie pour plus de détail à vos cours de base de données.

À son niveau, le développeur joue également un rôle de sécurisation, puisque l'utilisateur est limité dans ses possibilités d'intervention, par le biais des interfaces créées par le développeur.

Bien, revenons maintenant à une vision plus large du système d'information, et abordons les moyens de prévention concernant le système informatique.

2C. *Prévention contre les intrusions sur une machine : pare-feu, proxy, IDS*

2C1. Mettre un pare-feu

Un **pare-feu**, ou **firewall,** est un matériel ou un logiciel qui permet de protéger une machine ou un réseau des intrusions.

Il doit protéger aussi bien le poste des attaques provenant d'Internet que celles provenant d'un réseau interne.

En effet, Le pare-feu doit empêcher certains logiciels comme les chevaux de Troie d'entrer en contact avec d'autres ordinateurs situés dans un réseau local ou sur Internet et de leur fournir des informations présentes sur l'ordinateur.

Le pare-feu analyse tous les flux entrants et sortants dans le but de les bloquer s'ils ne sont pas autorisés à « entrer » ou s'ils s'adressent à un port bloqué, par exemple.

Les pare-feu ont généralement les fonctionnalités suivantes :

- création et mise à jour d'un journal du trafic, ce qui permet, par exemple, de connaître les tentatives d'intrusion ;
- filtrage des informations entrantes ou sortantes. Les informations acceptées le sont si elles respectent le paramétrage du firewall. Ce paramétrage peut concerner des adresses IP, un protocole particulier, un port d'entrée/sortie (comme par exemple le port 80, qui est le port http) ;
- le paramétrage du firewall permet aussi de déclarer quelles applications doivent être surveillées. Pour ces applications, il y a contrôle des tentatives de connexion ;
- si le firewall est chargé de protéger un réseau, il sait généralement traduire les adresses IP publiques (c'est-à-dire accessibles depuis Internet) en adresses IP privées différentes dans le réseau interne (j'entends par IP privées des adresses IP non accessibles depuis internet). La technologie permettant cette « translation d'adresse » est la technologie NAT (network address translation, en français, on peut traduire ça par la traduction d'adresses réseau.).

2C2. Utilisation d'un proxy

Un serveur proxy est une machine qu'on intercale entre internet et un réseau local pour protéger ce dernier des intrusions.

C'est une machine équipée d'au moins deux cartes réseau : une pour le réseau privé, interne et l'autre carte pour l'« extérieur » du réseau local, c'est-à-dire pour Internet.

Outre ces deux cartes réseau, le proxy est équipé d'un logiciel ayant les fonctionnalités d'un routeur (partage de connexion internet entre les machines du réseau local), d'un pare-feu et d'autres utilitaires de sécurité.

Il est capable de filtrer les accès à Internet (pour empêcher, par exemple, l'accès à certains sites depuis les machines du réseau local).

2C3. IDS

IDS signifie **système de détection d'intrusion.**

Ce système allie ressources logicielles et matérielles qui surveillent en temps réel les flux de données entrant dans un système d'information pour le protéger.

C'est un outil logiciel exploitant les fichiers journaux du système (*logs*) afin de repérer des comportements suspects.
Il compare les objets surveillés avec une base de signatures d'attaques connues, et détecte des anomalies de fonctionnement.

2D. *Prévention contre les virus, spams et espions : anti-virus, anti-spam, anti-spyware*

2D1. Antivirus

Il en existe tout un tas, plus ou moins gratuits, plus ou moins élaborés. Le plus important est qu'ils soient à jour, car de nouveaux virus sont conçus et injectés tous les jours.

On distingue deux grandes catégories de techniques utilisées par les anti-virus.

- **Technique de type « scanneur » :** ce type d'antivirus possède un dictionnaire qui contient **la signature** de chaque virus qu'il sait gérer.

Utilisée seule, cette technique n'est plus actuellement efficace à cause de la trop grosse quantité de virus à signatures différentes.

Qu'est-ce que c'est, la signature d'un virus ?
Lorsqu'un virus cherche à infecter un nouveau fichier, il commence par vérifier qu'il n'est pas lui-même déjà présent, car une nouvelle infection pourrait compromettre son efficacité. Il réalise ce contrôle par la recherche d'une séquence de code appelée **signature**.

Un anti-virus de type « scanneur » passe son temps à scanner toutes les informations stockées sur tout support de stockage connecté à la machine, cherchant les signatures des virus qu'il connaît. Ce type d'anti-virus, pour être efficace, doit donc être perpétuellement mis à jour afin d'intégrer dans son dictionnaire les signatures des nouveaux virus qui naissent tous les jours, ainsi que les signatures des différentes morphologies des virus polymorphes.

- **Antivirus générique** : il donne l'alerte si le comportement du système semble résulter d'une infection virale.

Plusieurs techniques :

- analyse **heuristique** : ce type d'analyse recherche les structures de code propres aux virus, telles des routines d'infection. En fait, la méthode permet de détecter les successions d'instructions pouvant correspondre à un virus. L'efficacité de ce type d'antivirus est valable à plus long terme que les anti-virus de type « scanneur » ;
- analyse **comportementale** : cette analyse fonctionne par exécution permanente d'un moniteur de comportement afin de détecter les détournements des appels systèmes fondamentaux (accès disque, déplacement mémoire…) pour les comparer à une base de règles définissant un comportement viral typique.
  Le moniteur de comportement n'est actif qu'à l'exécution du programme surveillé.
  L'inconvénient de ces deux méthodes génériques est qu'il y a beaucoup de fausses alertes,
- contrôle **d'intégrité** : l'antivirus calcule une empreinte cryptogaphique des fichiers système, et vérifie s'ils ont été modifiés. Lors de son installation, l'antivirus crée une base de données de tous les fichiers présents sur la machine basée sur la longueur des fichiers et d'autres paramètres.

Toute modification d'un fichier fera l'objet d'une alerte.

Les méthodes génériques ont deux inconvénients :

- l'alerte n'est donnée qu'après infection ;
- elles ne sont pas adaptées à un système dont les fichiers changent beaucoup comme Windows.

Les produits du marché

Les éditeurs d'antivirus se rapprochent actuellement des éditeurs de solutions anti-intrusion (IDS). Les logiciels antivirus combinent ces méthodes pour proposer les produits aussi performants que possible, notamment à cause des virus polymorphes.

La plupart du temps, les produits utilisent une base de signatures, couplée à un moteur générique, le plus souvent heuristique : Norton Anti Virus, VirusScan, VirusWall.

Aucune solution entièrement satisfaisante n'existe, c'est pourquoi il est parfois conseillé d'en utiliser plusieurs.

2D2. Et pour se protéger des autres « cochonneries » ?

Outre les virus, il faut aussi se protéger des spams, en installant un anti-spam. Pour choisir un anti-spam et en savoir plus sur la question, vous pouvez aller consulter le site http://www.secuser.com, sur lequel se trouve un dossier consacré au spamming et au mail-bombing.

Sous la pression des associations d'internautes et de consommateurs, avec la bienveillance des grandes agences de publicité et de marketing qui ont tout intérêt à assainir le domaine, une régulation de la publicité par e-mail se met progressivement en place.

Deux visions s'opposent pour la régulation du spam : l'*opt-in* et l'*opt-out*.
L'*opt-in* : cette option, également appelée « *permission marketing* », est la plus respectueuse de l'internaute. Elle consiste à ne lui envoyer des publicités ciblées que s'il y a clairement consenti.

L'*opt-out* : *opt-out* signifie désinscription. L'opt-out consacre l'existence d'un droit d'opposition a posteriori à recevoir des courriers électroniques. À cet effet, chaque mail publicitaire envoyé doit offrir la possibilité de se désinscrire du fichier. Les fichiers *opt-out* peuvent aussi bien être constitués de manière légale (par exemple d'un achat d'un fichier *opt-in*) qu'issus d'une collecte sauvage.

Enfin, pour se protéger des espiogiciels (les spyware), il faut s'équiper d'un anti-spyware, comme par exemple **spybot.**

2E. *Empêcher l'interception des informations que nous transmettons*

Tout échange d'informations sur le réseau est susceptible d'être détourné par des sniffers, à des fins de prospection commerciale, d'usurpation d'identité...

Il existe plusieurs moyens de protéger les informations qui transitent, je vous en présente plusieurs, mais d'abord, je vous présente les principes techniques permettant la sécurisation des échanges.

2E1. Principes techniques

Les principes techniques présentés sont utilisés pour pallier le risque suivant : d'une façon générale, tous les outils construits sur TCP/IP (telnet, ftp, web, email…) ne sont pas sécurisés. Tout transite en clair sur le réseau (on peut donc récupérer les informations qui transitent à l'aide d'utilitaires comme par exemple *dsniff*). Une personne mal intentionnée peut très facilement capturer les trames qui circulent. On souhaite donc chiffrer les messages afin de les rendre confidentiels.

Il y a deux grands principes utilisés dans la sécurisation des données lors de leur transit : le scellement et le chiffrement.

Le scellement par création d'une empreinte numérique.

À partir d'un message donné, une fonction de hachage génère un « hashcode » d'une taille déterminée.

Les fonctions de hachage utilisées doivent être telles que deux messages différents, même très voisins, ont une probabilité très faible de conduire au même code. On appelle parfois ces codes : résumés, empreintes numériques ou signatures.

Cette technique a pour but de vérifier que les données transmises n'ont pas été modifiées, falsifiées entre leur départ de chez l'émetteur et leur arrivée chez le destinataire.

Si on est certain de la validité d'une signature, on peut prouver qu'un message est ou n'est pas conforme à l'original : on en garantit **l'intégrité**.

Comment ?
Avant le départ de chez l'émetteur, un nombre (le résumé) est calculé en fonction des données à transmettre, ce nombre est l'empreinte numérique du message (le terme message est à prendre ici au sens large : une suite de bits pouvant correspondre à un texte, un logiciel…).

Les données sont transmises avec ce nombre. Lors de l'arrivée chez le destinataire, ce nombre est à nouveau calculé sur les données reçues. Les informations sont considérées comme intactes si l'empreinte numérique calculée à l'arrivée est égal au nombre calculé au départ.

Les empreintes numériques, comme expliqué plus haut, sont générées à partir d'un algorithme de ***hashage*** dont voici le principe.

Pour un message donné, l'algorithme génère une séquence de bits supposée unique (il n'existe aucune certitude, mais on n'a jamais prouvé le contraire…) et de taille fixe, quelle que soit la taille du message d'origine. Pour un même message, la séquence générée sera toujours la même. Mais la probabilité que deux messages différents, si proches soient-ils, donnent la même empreinte est infime (il semble donc que cette probabilité ne soit pas nulle, mais cela reste à démontrer…).

Exemple : *l'algorithme MD5 (RFC 1321 – Message Digest version 5 - 1992) génère une empreinte sur un nombre de bits fixe (16, 128, …) que l'on visualise généralement sous sa forme hexadécimale.*

La fonction SHA-1 est également une fonction de hachage.
Note : en principe, on ne peut pas retrouver le message initial à partir du hashage. Le crackage des messages scellés passe donc par une recherche exhaustive.

Le chiffrement

Attention, en ce qui concerne le vocabulaire : le **chiffrement** n'est pas l'équivalent du cryptage, et le **déchiffrement** n'est pas décryptage. Le terme **décryptage** est plutôt l'équivalent du terme **crackage**.

Le chiffrement permet de garantir :

- la confidentialité : protection de l'information contre une divulgation non autorisée ;
- l'intégrité : protection contre la modification non autorisée de l'information ;
- l'authentification : de l'émetteur et ou du destinataire ;
- la non-répudiation : offre la garantie qu'une partie ne pourra pas nier être impliquée dans une transaction (commerce électronique) ;
- la non-duplication : protection contre les copies illicites ;
- l'anonymat.

Les données sont codées suivant un certain algorithme, une certaine **clé de chiffrement**, puis elles sont transmises au destinataire qui dispose de l'algorithme de décryptage (de la **clé de déchiffrement**). Il existe différents types de chiffrement.

Symétrique

C'est la même clé qui est utilisée pour chiffrer et déchiffrer.

Les deux machines établissant un dialogue commencent par se communiquer la clé commune qu'ils vont utiliser.

Bien sûr, elle doit rester secrète mais elle peut être interceptée. Aujourd'hui, compte tenu des difficultés pour tenir la clé secrète, cette technique est plutôt réservée au **chiffrement de données locales** : par exemple, les mots de passe pour le *login* dans un réseau local.

Ensuite, l'échange d'informations peut commencer.
À un instant donné, il existe autant de clés que de « conversations ».

Une implémentation de ce principe se trouve dans l'algorithme DES (data encryption standard), très utilisé. C'est cet algorithme qui est utilisé dans le chiffrement des informations issues des paiements par cartes bleues et également dans les téléphones GSM (standard actuel de la télécommunication mobile).

Cet algorithme, qui utilise une clé de 56 bits, travaille sur des blocs de données de 64 bits à la fois et nécessite 19 étapes de manipulation des données. La clé utilisée pour chiffrer et déchiffrer est la même (il s'agit de la clé secrète devant être connue de l'émetteur et du récepteur).

DES peut être utilisé dans différents modes :

- ECB (electronic code book) : ne protège pas contre l'insertion d'un bloc étranger correctement codé ;
- CBC (chain block cipher) : le codage d'un bloc dépend du codage des blocs précédents, permettant ainsi de détecter toute intrusion dans le message ;
- CFM (cipher feedback mode) est une variante du mode précédent, travaillant sur des mots de 8 bits plutôt que de 64 bits.

Exemple : *par défaut, les mots de passe sous unix sont codés à l'aide de l'algorithme DES. Cet algo génère une clé de 56 bits en extrayant 7 bits des 8 premiers caractères du mot de passe.*

Afin que deux mots de passe ne donnent pas le même résultat, on calcule un *piment* à partir de l'heure, ce piment sera utilisé par l'algorithme.

Voici quelques exemples :

Mot de passe	Piment	Résultat
root	am	amfIADT2iqjAf
util1	7a	7azfT5tIdyh0I
util2	ri	ri79KNd7V6.Sk

Aujourd'hui, au vu des limites de cet algorithme, on préfère MD5 pour chiffrer les mots de passe sous Unix, même si le chiffrage est plus long (2000 clés générées par seconde avec MD5 contre plusieurs centaines de milliers avec DES).

Je m'explique ci-dessous à propos des limites de l'agorithme DES.

DES a été développé par le gouvernement US dans les années 70 pour protéger des données sensibles. Une association de laboratoires de recherche américain a démontré que l'algorithme de DES n'est pas suffisamment complexe. Elle a construit une machine dédiée à la recherche de clés DES (« Deep crack », un joujou à 250 000 $).

Avec DES, il existe 2^{56} (72 057 594 037 927 936) combinaisons possibles. Deep crack est constituée de 1 800 puces dédiées. Elle génère 92 milliards de clés à la seconde, il faut en moyenne 5 jours pour trouver un mot de passe (http://www.eff.org/descracker.html). Une clé DES a été crackée en 56 heures voici quelques années.

Ceci a conduit à développer une variante de l'algorithme DES, appelée « triple DES » travaillant avec deux clés de 56 bits : chiffrement avec la première clé, déchiffrement avec la seconde (c'est-à-dire brouillage des données car elle n'est pas la clé de départ), rechiffrement avec la première.

Le principal problème avec cet algorithme reste le fait que la clé doit être connue de l'émetteur et du récepteur et donc échangée à un moment donné avec les risques que cela implique.

C'est pour cela que la génération de clés différentes a été mise au point, comme expliqué ci-dessous.

Asymétrique

Cette technique est également appelée **ICP (infrastructure à clé publique)**.

Les ICP reposent sur le principe du chiffrement dit asymétrique, inventé en 1973 au sein des services secrets britanniques, puis redécouvert par des universitaires américains, Whitfield Diffie et Martin Helmann, qui, en 1976, en énoncent le principe : utiliser une paire de clés, dont l'une est publique, tandis que l'autre est secrète. L'une sert à signer ou chiffrer un document, l'autre à le déchiffrer.

En 1978, des universitaires, Ronald Rivest, Adi Shamir et Leonard Adleman, proposaient un algorithme permettant de réaliser cette prouesse à l'aide de nombres premiers. Leur système, baptisé RSA, est au coeur des solutions ICP proposées aujourd'hui, qui reposent sur l'attribution aux utilisateurs de cartes d'identité numériques, les certificats, normalisés et reconnus par la majorité des logiciels de navigation ou de messagerie. Il a suffi d'augmenter la longueur des clés pour les mettre à l'abri des attaques d'ordinateurs toujours plus puissants et capables, désormais, de travailler en réseau sur toute la planète.

À titre d'exemple, allez dans le menu **« À propos de Internet Explorer**, vous devez, sur la fenêtre qui s'ouvre, connaître la capacité de chiffrement de votre navigateur ».

Voici ce que j'apprends à propos de mon navigateur :

Je sais que le chiffrement se fait sur 128 positions binaires et que l'algo utilisé est RSA.

Le principe de fonctionnement

Dans le système à clef asymétrique, deux clefs sont utilisées, une clef publique et une clef privée. Les clefs publiques sont disponibles et accessibles à partir d'annuaires spécialisés. La clef privée de chacun est confidentielle.

C'est ce système qui est utilisé pour la **signature électronique, dans les logiciels de messagerie**.

La signature électronique est chiffrée avec la clef privée de l'émetteur.

Elle est déchiffrée par tous les destinataires avec la clé publique de l'émetteur.

Je vous présente un exemple dans le paragraphe ci-dessous, mais d'abord, je vous explique le principe du chiffrement.

Les implémentations du principe

Il existe différents algorithmes de calcul d'une clé privée par rapport à une clé publique. L'algorithme de chiffrement asymétrique le plus répandu est **RSA**, du nom de ses créateurs : Rivest, Shamir et Adleman. Cet algorithme est très largement utilisé, par exemple dans les navigateurs pour les sites sécurisés et pour chiffrer les emails.

RSA fait appel à des nombres premiers extrêmement grands pour garantir la sécurité du cryptage.

Voici en gros le principe de l'algorithme RSA.

Pour chiffrer un message, on fait : $\mathbf{c = m^e \bmod n}$

Pour déchiffrer : $\mathbf{m = c^d \bmod n}$

Avec :

m = message en clair,

c = message chiffré,

(e, n) constitue la clé publique,

(d, n) constitue la clé privée,

n est le produit de 2 nombres premiers,

mod est l'opération de modulo (reste de la division entière).

Comment e, d, et n sont-ils calculés ?
On prend deux nombres premiers **p** et **q** (de taille à peu près égale).
On calcule **n = pq**.
On prend un nombre **e** qui n'a aucun facteur en commun avec **(p-1)(q-1)**.
On calcule **d** tel que **ed mod (p-1)(q-1) = 1**
Le couple **(e,n)** constitue la clé publique. **(d,n)** est la clé privée.

Exemple :
Prenons deux nombres premiers au hasard : p = 29, q = 37
*On calcule n = pq = 29 * 37 = 1073*
On doit choisir e au hasard tel que e n'ait aucun facteur en commun avec (p-1)(q-1) :
(p-1)(q-1) = (29-1)(37-1) = 1008
On prend e = 71
*On choisit d tel que 71*d mod 1008 = 1*
On trouve d = 1079

On a maintenant nos clés :
La clé publique est (e,n) = (71,1073) (= clé de chiffrement)
La clé privée est (d,n) = (1079,1073) (= clé de déchiffrement)
On va chiffrer le message HELLO. On va prendre le code ASCII de chaque caractère et on les met bout à bout :
m = 7269767679

Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que n.
n comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres :
726 976 767 900 (on complète avec des zéros)

Ensuite on chiffre chacun de ces blocs :
726^71 mod 1073 = 436,
976^71 mod 1073 = 822,
767^71 mod 1073 = 825,
900^71 mod 1073 = 552.

Le message chiffré est 436 822 825 552.
On peut le décrypter avec d :
436^1079 mod 1073 = 726,
822^1079 mod 1073 = 976,
825^1079 mod 1073 = 767,
552^1079 mod 1073 = 900.

En enlevant les 0 (zéros) qu'on avait rajoutés tout à l'heure, on retrouve notre message en clair 72 69 76 76 79 : HELLO.

Dans la pratique, il faut trouver de grands nombres premiers (ça peut donc être très long à calculer).

Il faut obtenir des nombres premiers p et q de façon réellement aléatoire.
On n'utilise pas de blocs aussi petits que dans l'exemple ci-dessus.
Attention, avec RSA…

Pour ...	on utilise...	de qui ?
Envoyer un document crypté à quelqu'un	la clé publique	du destinataire
Envoyer une signature cryptée à quelqu'un	la clé privée	de l'expéditeur
Décrypter un document	la clé privée	du destinataire
Décrypter une signature	la clé publique	de l'expéditeur

Mais, il y a un mais…

En dessous d'une taille de 1024 bits ces clés ne sont pas considérées comme entièrement sûres. Évidemment plus la taille de la clé est grande plus le temps de codage est élevé.

Les algorithmes à clé publique sont efficaces, mais ils ont pourtant un défaut : ils sont beaucoup plus lents que les algorithmes de chiffrement symétrique. Pour des applications où il faut échanger de nombreuses données, ils sont inutilisables en pratique. On a alors recours à des cryptosystèmes hybrides. On échange des clés pour un chiffrement symétrique grâce à la cryptographie à clé publique, ce qui permet de sécuriser la communication de la clé. On utilise ensuite un algorithme de chiffrement symétrique. Le célèbre PGP, notamment utilisé pour chiffrer le courrier électronique, fonctionne sur ce principe.

PGP signifie pretty good privacy. Les données (volumineux) sont chiffrées en symétrique. La clé symétrique (faible volume) est chiffrée en asymétrique. Le principe, avec PGP, est le suivant :

– génération d'une clé de session (aléatoire) ;
– encodage des données avec la clé de session ;
– chiffrement des données avec la clé publique du destinataire ;
– envoi des données ;
– déchiffrement de la clé de session avec la clé privée du destinataire ;
– déchiffrement des données avec la clé de session.

Celles et ceux intéressés par plus de détails à propos de PGP peuvent aller consulter le site *http://www.pgpi.org/.*

2E2. Un exemple utilisant le chiffrement : la signature électronique lors de l'envoi de messages via une messagerie électronique

Madame Hixe veut envoyer un message numériquement signé à Madame Igrec. Madame Hixe dispose d'un logiciel de messagerie intégrant des fonctionnalités de cryptage (c'est-à-dire permettant de signer numériquement les messages envoyés).

Le texte écrit par Madame Hixe est tout d'abord compressé à l'aide d'une fonction de hachage, ceci donne ce qui est appelé un condensé ou résumé.

Le condensé est ensuite chiffré avec la clé privée de Madame Hixe, le résultat étant la **signature électronique**.

Le texte est ensuite envoyé en clair à Madame Igrec, accompagné de sa signature électronique, d'informations sur la fonction de hachage utilisée et de la clé publique de Madame Hixe.

Les clés publiques sont puisées dans des annuaires de clés publiques gérés par une autorité de gestion des clés. Cette clé peut-être connue d'autres personnes, cela ne permet pas pour autant de décrypter le message, car pour décrypter le message, il faut aussi la signature.

À réception du message, le logiciel de messagerie de Madame Igrec utilise à son tour la fonction de hachage sur le texte en clair transmis par Madame Hixe.

Le résultat est un condensé appelé **résumé calculé**.

Le logiciel de messagerie de Madame Igrec déchiffre la signature électronique qu'il a reçue en même temps que le message de sa copine Madame Hixe, et ceci à l'aide de la clé publique de Madame Hixe.

Le résultat du déchiffrage de la signature électronique à l'aide de la clé publique est un condensé appelé **résumé attendu**.

Le logiciel de messagerie de madame Igrec compare ensuite le **résumé calculé** et le **résumé attendu**.

Si les deux résumés sont identiques, madame Igrec a l'assurance que c'est bien madame Hixe qui lui a envoyé le message (authentification de l'expéditeur) et que le texte n'a pas été falsifié.

En bref, le message originel est crypté avec la clé privée de l'émetteur, cela donne la signature électronique, qui est déchiffrée avec la clé publique de l'émetteur. Le déchiffrage avec la clé publique est l'opération complémentaire du chiffrage avec la clé privée, puisque le résultat, c'est le message.

Bien sûr, la clé privée est calculée par rapport à la clé publique.

Remarque

Dans un environnement à clé publique, il est essentiel de s'assurer que la clé utilisée correspond à la bonne personne. Cette fonction est assurée par les ***certificats numériques****.*

2E3. Les certificats

La notion de certificat est décrite dans la RFC 2510.

Un certificat est un document électronique, il contient des informations sur la clé publique d'une personne ou d'un site, afin de garantir son authenticité.

Il est délivré par une **autorité de certification** (par exemple : *www.certplus.com* ou *www.verisign.com*), qui atteste de l'identité de son détenteur, pour prévenir la contrefaçon.

L'autorité de certification vérifie la concordance réelle entre la personne physique et la clé publique. Elle délivre un certificat qui joue le rôle d'une carte d'identité électronique.

Un certificat peut également identifier un serveur. Dans ce cas, le certificat est un document qui certifie que le site d'où les données vous sont transmises est bien le site auquel vous pensez être connecté. Le certificat vous est transmis par le site sur lequel vous vous connectez, et votre navigateur est capable de vérifier sa validité.

Un certificat Personnel contient les informations suivantes

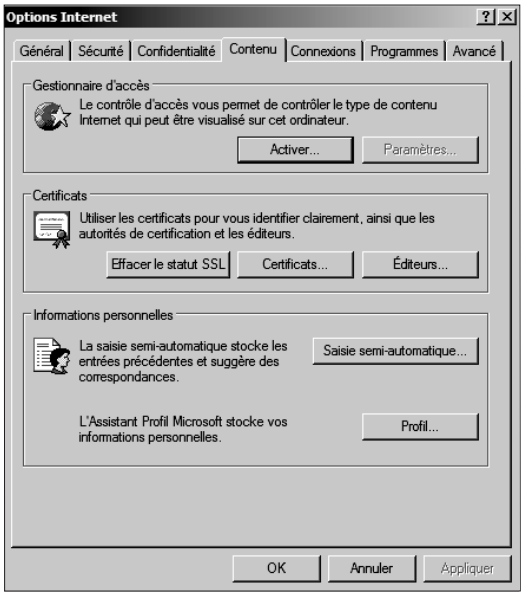
- Le nom de son propriétaire et éventuellement son adresse e-mail : Jean Dupont (jdupont@societe.Fr).
- Quelques informations optionnelles (adresse physique de la société, fonction de Jean Dupont, etc.).
- La clé publique de Jean Dupont à certifier.
- La date d'expiration du certificat.
- Un numéro de série unique.
- Le nom de l'autorité de certification qui a délivré le certificat numérique (banque, entreprise, administration, etc.).
- La signature de l'autorité de certification qui a délivré le certificat numérique (au moyen de la clé secrète de l'autorité de certification, sorte de « tampon » de validation d'un passeport électronique).

Un certificat Serveur contient les informations suivantes

- Le nom de domaine du serveur : www.societe.fr.
- Quelques informations optionnelles (nom et adresse physique de la société, etc.).
- La clé publique du serveur à certifier.
- La date d'expiration du certificat.
- Un numéro de série unique.
- Le nom de l'autorité de certification qui a délivré le certificat numérique (verisign trust network).
- La signature de l'autorité de certification qui a délivré le certificat numérique (au moyen de la clé secrète de l'autorité de certification, sorte de « tampon » de validation d'un passeport électronique).

Lorsqu'on utilise un certificat, le message peut être en clair ou crypté selon ce que l'on désire. Si les données ne sont pas confidentielles, le certificat est un moyen efficace de garantir leur origine et leur intégrité.

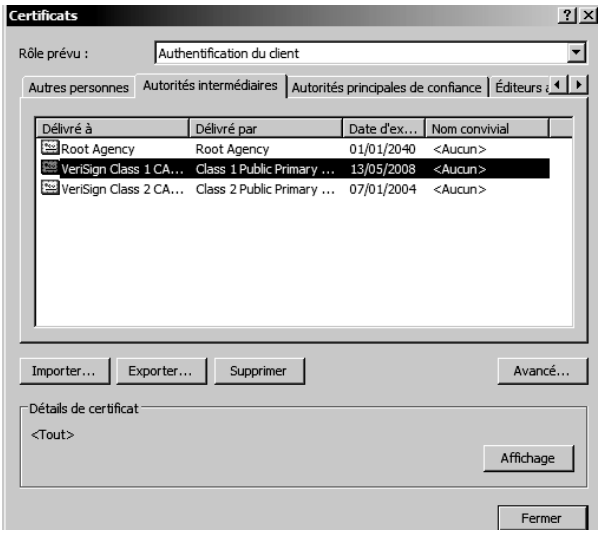
Vous pouvez, si vous le souhaitez, obtenir vous-même un certificat en allant sur le site : *http://www.certinomis.com*. Les certificats sont utilisés par exemple pour les échanges numériques d'informations entre des particuliers et des administrations en ligne.



Votre certificat une fois obtenu, vous pourrez signer numériquement vos messages depuis votre logiciel de messagerie.

On dispose aussi d'outils dans Internet Explorer (et dans les autres navigateurs) pour gérer les certificats.

Dans cette fenêtre, cliquez sur le bouton **Certificats**, et baladez-vous dans la fenêtre qui s'ouvre.



Si vous double-cliquez sur un des certificats, vous pouvez lire en détail les informations le concernant.

Par exemple, dans la liste suivante : je double-clique sur le certificat sélectionné et je peux accéder aux informations concernant le certificat, y compris à sa clé publique, si je clique sur l'onglet **Détails** de la fenêtre **Certificat**.

Remarque

Il existe un certain manque d'enthousiasme vis-à-vis de cette technologie qui était pourtant présentée comme le moyen idéal pour établir la confiance sur Internet. Elle permet, effectivement, de contrôler l'identité des internautes, de garantir la confidentialité et l'intégrité des messages transitant sur le réseau et de garder la preuve que l'échange de documents a bien eu lieu. Elle permet donc d'utiliser le réseau ouvert pour faire circuler des informations sensibles, pour passer des commandes, signer des documents, toutes choses coûteuses en temps et en argent dans le monde réel.

Ce n'est pas la technologie qui est en cause car elle est très efficace. C'est la lourdeur de sa mise en œuvre qui pose problème. La réglementation prévoit une pyramide d'acteurs. Elle comprend des distributeurs de certificats (en France, essentiellement Certplus et Verisign) agréés par des autorités de certifications (généralement des banques) qui, elles-mêmes, font l'objet de procédures de qualification. Il faut aussi des validateurs capables de tenir à jour les annuaires de certificats et d'en retirer ceux qui sont parvenus à expiration ou qui ont été révoqués. L'utilisateur final doit enfin être dûment identifié, ce qui suppose parfois une rencontre physique.

Outre le cas de la messagerie électronique évoqué ci-dessus, je vous présente deux solutions de sécurisation s'appuyant sur les principes de chiffrement que je vous ai présentés.

2E4. Recours à des protocoles sécurisés pour le transit des informations

Ce procédé est très fréquent lors d'achats sur internet ou de consultation de notre compte bancaire par internet, par exemple. On appelle ce type d'opérations sécurisées des **transactions commerciales**, ces opérations relèvent du **commerce électronique**.

Généralement, lors d'un achat en ligne, seule l'étape de paiement est sécurisée. Lorsqu'on utilise une banque en ligne par contre, on accède à son compte par un identifiant et un mot de passe et tout est sécurisé (consultation du compte, virements…).

Les principes généraux de ce type d'opération :

- la confidentialité (ne permettre l'accès qu'aux personnes autorisées) ;
- la traçabilité (avoir des preuves que l'opération a eu lieu).

Un exemple de solution sécurisée

Lors de ces échanges sécurisés, les adresses internet n'utilisent plus **http**, mais **https**. Dès qu'une requête **https** est tapée dans la barre d'adresse du navigateur du poste client, il y a démarrage par le navigateur d'une session **SSL** (secure socket layer), en français, on pourrait parler de sockets sécurisés (les sockets sont les fonctions permettant la communication entre deux machines distantes).

Cette solution de sécurisation, développée par Netscape, est la plus utilisée des solutions de sécurisation de transactions et est intégrée dans tous les navigateurs du marché.

Le protocole SSL permet une authentification forte des serveurs et des clients et des communications cryptées.

Conceptuellement, SSL s'insère entre la couche application du modèle OSI (http, telnet, …) et les couches logicielles réseau (TCP pour être précis). Lorsque la session est établie entre le client et le serveur, toutes les données qui transitent sur le réseau sont chiffrées et signées.

Techniquement, SSL rajoute une couche de chiffrement au dessus de TCP/IP, utilise le port 443 et intègre le système des certificats.

Le serveur présente son certificat au client pour authentification. Le processus d'authentification est basé sur l'utilisation des clés publiques et des signatures numériques. Dès que le client (ici, le navigateur du poste client) a la preuve que le serveur qui se présente

à lui est bien celui qu'il prétend être, le client utilise des techniques de chiffrement à clé symétrique pour chiffrer toutes les informations qu'il échange avec le serveur.

Si le serveur est configuré pour exiger une authentification du client, alors le client doit, lui aussi, présenter son certificat au serveur pour être authentifié avant l'établissement d'une communication SSL sécurisée.

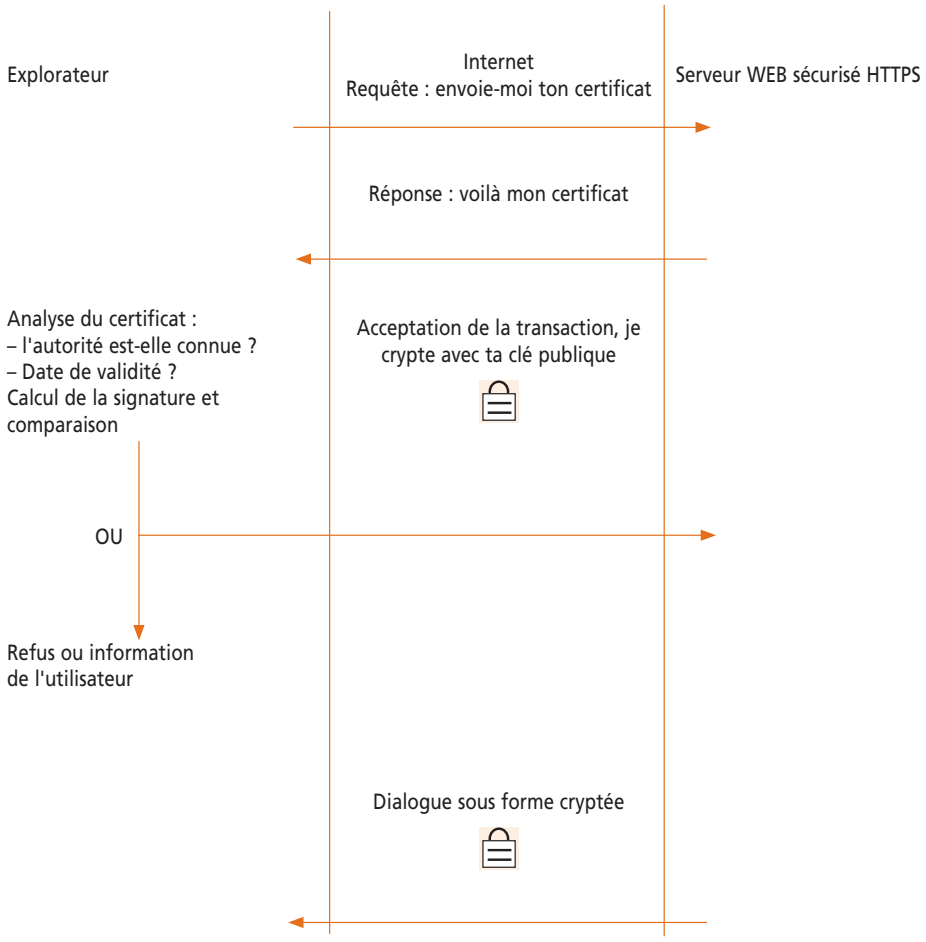
Pour authentifier un utilisateur sur un serveur, le logiciel client applique sa signature numérique sur une information quelconque générée aléatoirement. Le certificat et la donnée signée sont envoyés sur le réseau au serveur.

HTTPS est une variante de http qui utilise les sockets sécurisés.

Qu'est-ce qui se passe au démarrage d'une session SSL ?

Pour prévenir les risques d'usurpation, il y a **authentification** de l'émetteur et du récepteur de la requête https, puis il y a **chiffrement** des données avant envoi.

L'algorithme de chiffrement utilisé est décrit plus haut dans ce cours, il s'agit du chiffrement à clé publique **RSA**.



HTTPS avec SSL sont souvent utilisés en mode « dissymétrique », où uniquement le serveur possède un certificat, le client n'en possédant pas. Ce certificat du serveur permet de chiffrer (avec une clé de session) toutes les données transmises dans les deux sens et d'authentifier le serveur. Pour authentifier le client, le serveur demande classiquement un

mot de passe ou un numéro de carte bancaire au client. L'avantage est que ces données d'authentification ne circuleront pas en clair sur le réseau, tous les échanges étant chiffrés. C'est ainsi que fonctionne un serveur Web sécurisé, celui de votre banque peut-être.

Généralement, lorsqu'un client avec son navigateur se connecte sur un serveur Web sécurisé, ce dernier lui envoie son certificat (pour fournir sa clé publique…). Si ce certificat a été délivré par une autorité de certification reconnue par le navigateur du client, il est accepté de manière transparente pour l'utilisateur; sinon le navigateur demande à l'utilisateur s'il accepte ce type de certificat. HTTPS et SSL peuvent aussi fonctionner de manière symétrique où à la fois le serveur et le client ont un certificat. Dans ce cas, l'authentification du client pourra se faire avec le certificat de celui-ci, sans mécanisme supplémentaire de mot de passe.

2E5. Les réseaux privés virtuels

Les réseaux privés virtuels (dont le sigle anglais est VPN pour virtual private network) permettent de réaliser une liaison sécurisée entre deux réseaux distants à travers un réseau public. Ils permettent de relier deux sites informatiques distants sans recourir à des lignes spécialisées.

Lors d'une communication via un VPN, il y a création d'un tunnel virtuel, dont chaque extrémité est identifiée, et toutes les informations relevant de cette communication transitent par ce tunnel.

Lors d'une communication via un VPN, les techniques de chiffrement et d'authentification sont mises en œuvre.

L'émetteur, avant d'envoyer les données relevant de la communication qu'il a établie avec son interlocuteur, chiffre les données et les encapsule.

Actuellement, les réseaux privés virtuels ont du succès parce qu'ils sont fiables, mais aussi parce qu'ils coûtent moins cher que, par exemple, des lignes spécialisées.

Il existe plusieurs types de Réseaux Privés Virtuels, et notamment les RVP IP et les RPV Internet.

Les protocoles utilisés pour créer un tunnel sécurisé sont par exemple IPSec (protocole de la couche 3 du modèle OSI, voir la RFC 2411) ou PPTP (couche 2, accès par lignes téléphoniques).

Par exemple, le protocole IPSec utilise le format de base des trames IP en transformant le champ des données en deux parties :

- une partie qui contient un code de contrôle obtenu par un calcul avec une clé secrète sur le contenu du paquet ;
- une partie qui contient le paquet chiffré.

Voilà pour cette petite partie de cryptologie.

Abordons maintenant l'aspect des comportements humains.

2F. *Comportements préventifs*

Le CERTA (c'est-à-dire le centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques) certifie que le comportement de l'utilisateur est primordial dans la prévention contre les intrusions, les virus…

Outre les outils présentés ci-dessus, il est important de savoir adopter un comportement limitant les risques.

2F1. Pour limiter les risques de vol de mot de passe

Ne pas choisir un mot existant en guise de mot de passe, cela empêche les vilains pirates d'utiliser des dictionnaires dans leurs programmes de crackage de mot de passe.

Un mot de passe doit donc être une suite de chiffres, de lettres majuscules et minuscules, de caractères de ponctuation et de caractères peu utilisés (pour compliquer le calcul du mot de passe) sans signification particulière.

Choisir un mot de passe le plus long possible, pour ralentir les logiciels de type « force brute » dans leur recherche.
Exemple : *un logiciel de force brute parvient à trouver un mot de passe de moins de 6 caractères en assez peu de temps.*

N'écrire son mot de passe nulle part.

2F2. Pour se protéger des virus

Avoir un anti-virus régulièrement mis à jour.

Lors d'alertes par messagerie, vérifier qu'il ne s'agit pas d'un hoax en allant par exemple sur le site **hoaxbuster**.

Ne pas exécuter les programmes exécutables envoyés en pièce jointe avec les mails sans avoir au préalable vérifié la provenance du mail.

Ne pas ouvrir ni prévisualiser les mails envoyés par des adresses inconnues ou suspectes (désactiver le volet de prévisualisation dans votre logiciel de messagerie).

Ajouter sa propre adresse dans son carnet d'adresse pour détecter l'envoi automatique de courrier électronique en cas de contamination.

Ne pas connecter directement les serveurs d'une entreprise (intercaler un proxy, par exemple).

Désactiver l'exécution automatique des macros dans les applications bureautiques.

Définir des niveaux de sécurité dans tout logiciel où c'est possible…

2F3. Dix mesures pour sécuriser son poste de travail

Avoir un comportement préventif en appliquant les six règles suivantes :

1. sauvegarder ses données de façon régulière sur des supports fiables et stocker ses sauvegardes dans un endroit différent de celui du poste de travail ;
2. installer et activer un pare-feu ;
3. mettre à jour son système d'exploitation et ses applications, afin de bénéficier des corrections concernant les failles de sécurité ou les bogues utilisés par les parasites ;
4. installer et activer un anti-virus ;
5. installer et activer un anti-espiogiciels ;
6. utiliser un anti-spam.

Les six mesures précédentes visent à protéger le poste informatique des infections externes, mais le comportement de l'utilisateur joue un rôle non négligeable pour prévenir les désagréments liés aux parasites, d'où les quatre mesures suivantes, qui concernent l'adoption d'un comportement sans risque :

7. ne pas diffuser inutilement son adresse sur Internet, car lorsqu'on reçoit des spams, c'est que l'adresse que l'on possède circule sur le réseau Internet (sur des pages web, ou parce qu'on l'a saisie dans un formulaire, par exemple).

Pour toutes ces raisons, il est préférable d'utiliser un compte de messagerie dédié aux activités exposées et conserver une autre adresse pour les échanges professionnels ou personnels ;

8. ne pas répondre à un expéditeur inconnu ;

9. ne jamais transférer un message à tout son carnet d'adresses.
Cette pratique encouragée par le spam est à proscrire absolument. Elle encombre la messagerie, elle divulgue à chacun l'intégralité de vos correspondants.

Il est possible de transférer à certaines personnes un message reçu si ce message présente un intérêt pour elles, mais il est bon de vérifier avant qu'il ne s'agit pas d'un canular. Une recherche sur des sites spécialisés comme *www.hoaxbuster.com* ou *www.secuser.com/hoax*, peut éviter d'être piégé ;

10. régler soigneusement son client de messagerie.

Des règles anti-spam permettent d'envoyer dans un dossier réservé tous les messages filtrés, une observation régulière de son contenu lève le doute sur certains messages.

L'utilisation de règles de filtrage sur l'expéditeur, l'objet, le contenu permet de classer son courrier dans des dossiers prévus à l'avance, il ne reste plus que quelques messages dans la boîte de réception sur lesquels il sera plus facile de prendre une décision.

Certains messages sont écrits en HTML, ils sont plus attrayants mais potentiellement plus dangereux, on pourra régler, dans les options, la lecture en texte brut afin d'éviter une contamination par un code malveillant.

2F4. Comportements préventifs au sein de l'entreprise

La sécurité informatique d'une entreprise est tout d'abord une affaire de direction, qui, seule a les pouvoirs d'ordonner la mise en œuvre effective des recommandations. Mais tout le monde est concerné et doit coopérer à sa mise en place : les administrateurs qui ont la responsabilité du système, mais également les utilisateurs. Ces derniers doivent donc être largement informés et sensibilisés sur les risques encourus et leurs conséquences.

Pour être efficace, une stratégie de sécurité impose donc de respecter des règles, telles que sécuriser physiquement l'ordinateur, le protéger des attaques, assurer une restauration rapide après catastrophe et fixer les actions autorisées et interdites dans les domaines concernés. Mais la politique de sécurité impose également de veiller au respect de ces règles, en assurant une veille technologique et en auditant régulièrement.

Pour ce qui concerne les problèmes spécifiques rencontrés suite au développement d'internet, on manque de moyens juridiques pour freiner la criminalité (preuve du délit, application au national)…

Voilà, cette unité sur la sécurité est terminée. J'ai essayé d'être exhaustive, sans non plus écrire un roman fleuve…

Je vous propose maintenant de quoi faire des exercices sur le thème de la sécurité et des risques.

Séquence 16

Des exercices en guise de conclusion

Je n'invente aucun exercice, mais il faut que vous en fassiez.

Les questions inhérentes à la sécurité sont disséminées dans les études de cas.

Alors je suis allée consulter le site du CERTA (*http://www.reseaucerta.org/*). Non, ce n'est pas le site du Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques. Cette fois, c'est un site de l'éducation nationale, créé par les professeurs d'informatique de l'éducation nationale, et qui propose, libres en téléchargement, tout un tas de ressources dont :

– les exonets, des exercices à thèmes variés ;

– les sujets et corrigés des études de cas du BTS IG, option DA et ARLE.

Ça tombe bien, c'est la dessus que vous allez vous entraîner.

J'ai donc ausculté et sélectionné pour vous les exonets et les études de cas portant sur la sécurité.

Faites-les, ou, tout au moins, regardez les sujets et les corrigés.

Le public est souvent précisé (Option DA ou ARLE), mais je vous conseille de tout regarder, quelle que soit votre option.

Les exonets et les sujets d'examens sont directement accessibles depuis la fenêtre d'accueil du CERTA (dans la frame de gauche, vous avez un lien qui s'appelle **Exonets** et un qui s'appelle **Sujets d'examens**).

Voici ci-dessous un tableau récapitulant quels exonets et quelles études de cas me paraissent intéressants vis-à-vis du thème de la sécurité.

Pour les études de cas, lorsque le nom du fichier contient un **r**, c'est que c'est un sujet d'option ARLE, s'il contient un **d**, c'est que c'est un sujet d'option DA.

Pour ma part, je suis remontée jusqu'aux études de cas de 2004, mais rien ne vous empêche de remonter plus loin encore.

Référence de l'exonet ou de l'étude de cas	Thèmes
Exonet 34	Sauvegarde
Exonet 61	Sécurisation d'un réseau, routage, proxy, parefeu.
Exonet 72, exonet 73	Script de gestion des utilisateurs
Exonet 76	Tolérance de panne, sécurisation d'un réseau
Exonet 81	Cryptologie, chiffrement
edc05nr.zip	Tolérance aux pannes, filtrage, signature, chiffrement, VPN, gestion de droits.
Edc05nd.zip	Sécurisation d'un réseau sans fil
Edc05mr.zip	Sauvegardes, filtrage, droits…
Edc05mr2.zip	Sécurisation des accès, filtrage, droits, sécurisation de site, SSL
Edc05md.zip	DMZ, sécurité d'un réseau local, filtrage, pare-feu
Edc05m2.zip	Contrainte d'intégrité, sécurisation de réseau local, protocole NAT, filtrage de protocoles
Edc04nr.zip	Sécurisation d'accès distant
Edc04nd.zip	Gestion d'interconnexions, certificats SSL
Edc04mr.zip	Sécurité d'un réseau (dossier 2)
Edc04md.zip	Matériel d'interconnexion de réseau