GESTION ’UN CENTRE INFORMATIQUE

Dali
[Sélectionnez la date]

MAKKES Mounir et HADHRI Mohamed Ali

Fiche matière

Matière : **Gestion d'un Centre Informatique**

Public ciblé : Techniciens en informatique de gestion

Classe : 4ième niveau

Volume horaire : 22.5H de Cours Intégré

Coefficient : 1

Pré requis : Connaissance de :

- Matériel et programmes informatiques
- Réseaux informatiques
- Gestion et organisation

Moyens pédagogiques :

- Support de cours (sur papiers)
- Exposé du cours avec :
  - Indication des notes sur tableau
  - Tests d'attention et d'assimilation

Plan du cours :

Chapitre	***Durée***
I) Introduction aux Centres Informatiques	1.5H
II) Implantation d'un Centre Informatique	3H
III) Activités d'un Centre Informatique	4.5H
IV) Recensement du personnel d'un Centre Informatique	3H
V) Aspects de la gestion d'un Centre Informatique	4.5H
VI) Sécurité informatique	4.5H
VII) Eléments de réponses aux questions	1.5H

Annexes :

Des sujets d'examens

Bibliographie :

- Support du cours de Mr Med Ali ZOUGHLAMI
- Support de cours de Mr. Makkes Mounir
- Livre « La sécurité des systèmes informatiques » de Dhafrallah MHIRI, édité en janvier 2003 (les pages de 25 jusqu'à 29)

SOMMAIRE

Chapitre I

Introduction aux Centres Informatiques

Objectif
Connaître la mission d'un centre Informatique et ses relations

Eléments de contenu
1. Définition d'un Centre Informatique
2. Objectifs d'un Centre Informatique
3. Mission d'un Centre Informatique
4. Les Interactions
5. Questions de compréhension

I.1) Définition d'un Centre Informatique

Un Centre Informatique (C.I.) est un ensemble de moyens matériels et logiciels mis à la disposition d'un groupe d'utilisateurs destinés à rendre des services de nature informatique aux différentes personnes de l'entreprise.
Ces moyens sont gérés par le personnel informatique.

I.2) Objectifs d'un Centre Informatique

Un C.I. a pour objectifs :
a) Rendre au profit de différents utilisateurs des services de type traitement de l'information ainsi que d'assistance technique pour la réalisation des traitements.
b) Répondre aux besoins et aux exigences des utilisateurs d'une manière efficace.
c) Améliorer la productivité du personnel par satisfaction des besoins dans les limites des ressources prévues.

I.3) Mission d'un Centre Informatique

La mission d'un C.I. est définie comme un ensemble de services rendus aux utilisateurs leur permettant de faire les traitements sur les données et communiquer de l'information
Parmi ces services, on peut citer :
1. Acquisition et installation du matériel informatique.
2. Acquisition, installation et paramétrage des logiciels pour répondre aux besoins des utilisateurs en traitements; ces logiciels peuvent être des logiciels standards ou des applications spécifiques.
3. Formation et assistance des utilisateurs à l'exploitation
4. Installation d'un réseau local pour faire communiquer des données entre les différents utilisateurs de l'entreprise.

5. Connexion de l'entreprise à l'INTERNET pour s'ouvrir sur le monde extérieur et en particulier, sur ses clients et ses fournisseurs.

En offrant ces services, le C.I. est soumis aux contraintes suivantes :

- Plus court délai (le plus tôt possible ou bien à temps)
- Meilleure qualité
- Moindre coût
- Continuité du fonctionnement (disponibilité continue du système Informatique)
- Budget consacré au C.I. pour les investissements et les frais de fonctionnement
- Rentabilité des investissements
- Bonne compétence du personnel du C.I.
- Formation du personnel
- Evolution des moyens informatiques du centre
- Ouverture sur l'environnement extérieur
- Sécurité de tout le système informatique
- Confidentialité : certaines informations, professionnelles ou personnelles, doivent rester confidentielles au niveau du responsable du C.I.

I.4) Les Interactions

L'exploitation d'un C.I. est accompagnée par l'interaction avec les principaux intervenants suivants :

a) La Direction

Elle représente les décideurs qui détiennent le pouvoir de la décision.
La direction intervient dans tout ce qui concerne le budget, la stratégie, les objectifs, les contrats, la rentabilité des investissements, les rapports d'activité et le respect des engagements envers les fournisseurs.

b) Les utilisateurs

Ce sont les consommateurs de tout service offert par le C.I, donc, ce sont les clients du C.I.
Ils exploitent le matériel, le logiciel et le réseau qui sont gérés par le C.I.
C'est avec le degré de satisfaction des utilisateurs qu'on mesure le degré de la réussite ou d'échec du C.I.
Ce sont les utilisateurs qui doivent spécifier leurs besoins (en matériel ou en logiciel) dans un cahier des charges et le présenter au C.I. qui doit les satisfaire dans les brefs délais.

c) Les développeurs

C'est l'équipe du personnel informatique ou la société de services en développement qui assure le développement des applications spécifiques demandées par les utilisateurs. Elle doit tenir compte de la date de livraison des applications, de leur date de mise en exploitation et des préparations nécessaires : installation et configuration du matériel, paramétrage et formation des utilisateurs, etc …
Elle doit rédiger un manuel d'exploitation pour les utilisateurs.
Elle doit être prête à toute demande de maintenance des applications pour corriger des erreurs dans les traitements (maintenance corrective) ou pour faire évoluer les applications afin de répondre à de nouveaux besoins et appliquer de nouvelles

règles de gestion (maintenance évolutive) ou pour adapter les applications à une nouvelle plateforme de matériel d'exploitation (maintenance adaptative).

d) Les fournisseurs

Le C.I. doit établir des contrats avec les différents fournisseurs du matériel et du logiciel et doit s'engager à les renouveler et à les honorer à temps.
Il doit assurer le contrôle de la quantité et de la qualité des produits réceptionnés (PC, imprimantes, logiciels, licences, etc …)
Il doit discuter avec les fournisseurs la qualité, la quantité et le prix des produits à acheter pour acquérir avec le meilleur prix et dans le cadre du budget disponible.

Chapitre II

IMPLANTATION D'un C.I.

Objectif

Pour construire un centre Informatique, il faut établir les prévisions nécessaires en terme de bureaux, salle informatique, composants de base et réseaux.

Eléments de contenu

1. Introduction
2. Composants de base d'un système informatique
3. Construction d'une salle informatique
4. réseau informatique
5. Equipements électriques et de climatisation
6. faux plancher et faux plafond
7. Equipements de détection d'incendie
8. Issue de secours
9. Questions de compréhension

II.1) Introduction

De nos jours, les technologies de l'information et de communication ont pris une bonne place dans la société; elles sont devenues indispensables au fonctionnement et à la survie de toute entreprise.
Les décideurs donnent une grande importance aux moyens techniques de traitement, de sauvegarde et de communication de l'information.

Au fil des années, on est passé d'un simple service informatique à un département puis à un Centre Informatique sous forme d'une Direction rattachée directement à la Direction Générale.

II.2) Les composantes de base d'un système informatique

Un Centre Informatique (C.I.) est créé pour abriter le personnel informatique et centraliser le système informatique de l'entreprise.
En effet, le C.I. se compose d'un certain nombre de bureaux pour accueillir le personnel informatique et d'une salle informatique où on trouve les composantes de base d'un système informatique et qui sont :

- Un ou plusieurs ordinateurs (PC puissants ou stations de travail) équipés chacun d'un ou de plusieurs processeurs pour assurer le traitement et le stockage des données.
- Un serveur de communication pour assurer la messagerie à l'intérieur et à l'extérieur de l'entreprise.
- Des dérouleurs de bandes magnétiques (ou lecteurs de streamers) pour assurer la sauvegarde et le stockage des fichiers et des données.
- Des imprimantes système pour imprimer les travaux.

- Des contrôleurs de communication destinés à gérer des lignes téléphoniques sur lesquelles sont connectés des postes de travail.
- Des modems pour connecter des postes distants à l'ordinateur central par des lignes de connexion : RTC (c'est Réseau Téléphonique Commuté), LS (c'est Lignes Spécialisées), réseau X25, etc…
- Du matériel de secours pour l'alimentation électrique (onduleurs, …)
- Du câblage et des connectiques du réseau local.
- Du matériel de communication permettant le partage de certains périphériques entre plusieurs ordinateurs (switchs, hubs, etc…)
- Des logiciels du système d'exploitation et d'administration des réseaux
- Des applications de gestion standard et de métier
- Du consommable informatique (listing, cartouches d'encres, rubans,)
- Et tout ce qui est nécessaire au bon fonctionnement du système informatique

II.3) La construction d'une salle informatique et des bureaux

Avant de construire un Centre Informatique (C.I.), il faut bien étudier et choisir le lieu destiné à l'accueillir.
En effet, l'emplacement de l'implantation physique doit être à l'abri de toute menace physique ou naturelle (inondations, séisme, incendies, …) et loin de toute perturbation ou bruit (vibration, rayonnement électromagnétique, …)

En plus, il ne faut pas oublier d'étudier et de prévoir l'emplacement des équipements et des accessoires nécessaires au bon fonctionnement du C.I. tels que :

- Pré-câblage de la salle et des bureaux en un réseau de transmission de données et en des réseaux des lignes électriques et téléphoniques (dans ce cas, on parle de bâtiment intelligent).
- Equipements électriques et de climatisation

Pour la salle informatique, prévoir :

- Le faux plancher et le faux plafond
- Les équipements de détection d'incendie
- Les accès de secours

Avant de commencer l'implantation physique d'un C.I., il est nécessaire d'étudier la surface globale du centre qui englobe la surface occupée par les unités de traitement, la surface du stockage des fournitures et des consommables, la surface pour les bureaux du personnel et les surfaces susceptibles d'accueillir les équipements électriques et de climatisation.

II.4) Conception d'un réseau informatique

Le but de l'informatique est le traitement, et la communication de l'information. Le traitement se fait à l'aide des applicatifs et des processeurs; par contre, pour faire communiquer l'information, on a besoin des réseaux locaux et des réseaux à grande distance en utilisant le réseau X25 ou Internet ou le RTC ou les L.S. ou ADSL.

Donc, il est nécessaire de prévoir un pré-câblage du réseau de transmission de données au moment de l'implantation du C.I.
Le choix du matériel et de la topologie de réseau est en fonction du volume des données qui devront être échangées.

L'installation d'un réseau informatique exige l'implantation du matériel suivant

- ☒ Des switchs ou hubs
- ☒ Des câbles RJ45 encastrés dans le mur
- ☒ Des prises RJ45 encastrées dans le mur
- ☒ Un tableau des platines de brassage
- ☒ Des modems qui ont pour rôle de transformer les signaux numériques en signaux analogiques lors de l'émission de données (c'est la modulation) et de faire l'inverse lors de la réception des données émises (c'est la démodulation).
- ☒ Une station d'administration du réseau
- ☒ Un serveur de communication connecté à l'Internet
- ☒ Des postes de travail pour se connecter au réseau; ces postes doivent être équipés de carte réseau et d'un câble de connexion.

II.5) Les équipements électriques et de climatisation

Le fonctionnement d'un C.I. peut être interrompu suite à des coupures électriques ou à des pannes engendrées par un sur-échauffement de certains composants électroniques du serveur.
Donc, il faut mettre des dispositifs permettant de les dépasser : Un générateur du courant de type groupe électrogène ou onduleur s'avère nécessaire pour éviter les pannes ou les micro-coupures. Il est possible aussi d'utiliser des régulateurs de courant afin de maintenir la tension stable.

Pour éviter le sur-échauffement des composants électroniques, il faut prévoir l'installation des équipements de climatisation suivants :

- ❖ Un système de refroidissement et de régulation de l'humidité de l'air
- ❖ Un système de chauffage
- ❖ Des ventilateurs ou des souffleries
- ❖ Un système de filtration d'air pour éviter des grains de poussières qui pourraient endommager les surfaces des disques durs

II.6) le faux plancher et le faux plafond

Le faux plancher se présente comme des dalles carrées sur lesquelles repose les tables des ordinateurs et des différents périphériques.
Ces dalles sont posées sur des vérins d'environ 60 cm de hauteur.
Le faux plancher permet d'accueillir l'air froid qui remonte à travers des grilles et il permet le passage des câbles de branchement du matériel installé.

Le faux plafond est attaché au plafond à l'aide des suspentes.
Son rôle consiste à reprendre l'air chaud de la climatisation pour le faire traiter, à encastrer les circuits électriques d'éclairage et éventuellement à abriter les détecteurs de fumée et le système d'extinction automatique.

II.7) les équipements de détection d'incendie

En vue de diminuer les risques d'incendie à l'intérieur d'un C.I., il est recommandé de prévoir des équipements de prévention et de détection d'incendie comme :

- Détecteurs de fumée
- Détecteurs ioniques qui permettent d'analyser la composition de l'air
- Détecteurs thermiques qui permettent d'analyser la température
- Extincteurs automatiques des incendies

II.8) Les issues de secours

Lors de la construction d'un C.I., il est recommandé de prévoir, en plus de l'entrée principale du centre, au moins, une issue de secours pour évacuer le personnel en cas d'un sinistre. Cette issue doit rester libre à tout instant (càd ne pas le condamner par un obstacle physique tq armoire) car, on ne sait jamais quand est ce qu'un danger puisse arriver.

Chapitre III

Les activités d'un C.I.

Objectif

Recenser les différentes activités d'un centre Informatique

Eléments de contenu

1. Introduction
2. Recensement des tâches d'un C.I.
3. Acquisition des applications
4. Gestion de la documentation technique
5. Elaboration et réalisation d'un schéma directeur informatique opérationnel
6. Connexion de l'entreprise à l'Internet
7. Questions de compréhension

III.1) Introduction

La création d'un C.I. au sein d'une entreprise a pour but d'apporter une efficacité et une performance de toute l'activité de l'entreprise et ce afin d'augmenter la productivité du personnel, d'accroître le chiffre d'affaire et de multiplier le profit.
Ceci n'est possible que si on assure un bon fonctionnement de tout le système informatique. C'est le Centre Informatique qui en est le premier responsable devant la Direction Générale.
Pour remplir sa mission, le C.I. doit assurer un certain nombre de tâches et d'activités qu'on verra dans ce chapitre.

III.2) Recensement des tâches d'un C.I.

Pour remplir sa mission, le C.I. doit réaliser les tâches suivantes :

- ✓ Elaboration des Schémas directeurs Informatique Opérationnels
- ✓ Planification et préparation des travaux
- ✓ Contrôle de la bonne exécution des traitements
- ✓ Administration et maintenance du système
- ✓ Acquisition, installation et maintenance du matériel informatique
- ✓ Acquisition des logiciels ou développement des applications
- ✓ Acquisition du consommable informatique
- ✓ Administration des réseaux
- ✓ Administration et sauvegarde des Bases de Données
- ✓ Reprise du fonctionnement après incident
- ✓ Assistance et formation des utilisateurs
- ✓ Rédaction des cahiers des charges techniques
- ✓ Connexion de la société à l'Internet
- ✓ Ouverture de la société sur ses clients et ses fournisseurs
- ✓ Gestion de la sécurité du C.I.
- ✓ Contrôle d'environnement du C.I. (électricité, climatisation etc…)

III.3) Acquisition des applications

Pour répondre aux besoins des utilisateurs en termes d'applications de gestion, le C.I. doit procéder :

a) soit à l'acquisition des progiciels de gestion pour les tâches standard telles que Comptabilité, Gestion des stocks, etc.…

Dans ce cas, il faut préparer un cahier des charges (qui contient trois parties : C.C. administratif préparé par le service financier et juridique, le C.C. fonctionnel où on trouve les spécifications fonctionnelles préparées par l'utilisateur décideur et le C.C. Technique où on trouve les spécifications techniques de la plateforme d'exploitation et il est préparé par le C.I.

Avec les 3 parties du C.C., le C.I. peut lancer un appel d'offres (national ou international) pour l'acquisition d'un logiciel.

Après la réception des offres des soumissionnaires, pour chaque offre, on vérifie la présence des papiers administratifs demandés (affiliation à la CNSS, Non faillite, etc ..) puis on procède au dépouillement technique (suivant une méthodologie de dépouillement fixée avant le lancement de l'appel d'offres) : si la note technique dépasse un certain seuil fixé auparavant, alors on passe au dépouillement financier et on attribue une note financière puis on calcule la note globale par une formule fixée auparavant

On choisit le fournisseur dont l'offre a eu la meilleure note globale et on signe avec lui un contrat d'acquisition de logiciel.

Une fois le logiciel est acquis, il suffit de le paramétrer suivant les spécificités de l'entreprise ou de lui faire adapter l'organisation de l'entreprise pour en tirer le meilleur profit.

b) Soit à sous traiter le développement des tâches métiers qui sont très spécifiques à l'entreprise et pour lesquelles on ne trouve pas des logiciels qui répondent aux besoins des utilisateurs.

Dans ce cas, il faut préparer les mêmes documents et suivre les mêmes étapes mais cette fois ci, c'est pour sélectionner une Société de Services et d'Ingénierie en Informatique (SSII) qui va assurer le développement des tâches spécifiques de la société.

Après le choix de la société sous traitante, il faut rédiger :

- Un contrat où on spécifie les responsabilités de chacun des C.I. et de la société
- Un Cahier des charges fonctionnel très précis et validé par les utilisateurs décideurs
- Un contrat précisant les modalités de réception et de paiement.
- Un contrat mentionnant les délais prévus pour le début et la fin du développement des applications et précisant les pénalités des retards.

Dans les deux cas, le responsable du C.I. doit établir un contrat de maintenance des applications acquises avec le fournisseur pour corriger des éventuelles erreurs (maintenance corrective) ou pour les faire évoluer afin de répondre à des nouveaux besoins (maintenance évolutive) ou pour les faire adapter à une nouvelle plateforme technique (maintenance adaptative).

La valeur de ce contrat est de l'ordre de 10% du coût des applicatifs.

III.4) Acquisition et maintenance du matériel Informatique

Le C.I. assume toute la responsabilité pour l'acquisition et la maintenance de tout type du matériel informatique qui existe dans l'entreprise.

Pour l'acquisition du matériel, le C.I. doit, d'abord, rédiger un cahier des charges où il spécifie les caractéristiques techniques du matériel tout en tenant compte des besoins des utilisateurs et des contraintes des logiciels à acquérir; puis lancer une consultation ou un appel d'offres suivant l'enveloppe prévue du coût du matériel; Généralement, si elle est inférieure à 30MD alors il doit consulter au moins trois fournisseurs sinon il doit lancer un appel d'offres.
Après la vérification des papiers administratifs des offres, il faut procéder au dépouillement technique des offres valables puis passer au dépouillement financier de celles qui ont une note technique qui dépasse un certain seuil fixé dans la méthodologie de dépouillement. On leur attribue des notes financière puis on calcule la note globale de chaque offre suivant une formule fixée auparavant.
On sélection l'offre qui a la meilleure note globale et on rédige un bon de commande pour inviter le soumissionnaire à livrer le matériel proposé dans son offre.
Lors de la livraison du matériel, seul le C.I. qui peut procèder à la réception quantitative et qualitative du matériel commandé et l'affecter aux utilisateurs demandeurs.

Pour la maintenance du matériel, il y a, généralement trois cas :

a) Si le matériel informatique est neuf et encore en période de garantie alors il vaut mieux, au pire des cas, réparer coup par coup.
b) Si on a des techniciens de maintenance et un grand parc informatique alors il vaut mieux avoir un petit stock de pièces de rechanges et des outillages pour essayer de faire une réparation en interne pour les petites pannes sinon, envoyer le matériel à une société de maintenance.
c) Si le parc informatique est grand et le matériel tombe fréquemment en panne alors il vaut mieux choisir une société de maintenance et établir avec elle un contrat de maintenance avec une somme annuelle forfaitaire. Dans ce cas, à chaque appel de dépannage et de réparation le sous traitant est obligé de venir rapidement et de réparer le plus tôt possible le matériel tombé en panne; ainsi la société peut gagner en temps (elle n'a pas à chercher à chaque fois la société qui va réparer) et en argent (car c'est une somme forfaitaire quelque soit le nombre des interventions).

III.5) Gestion de la documentation technique

Il est fréquent de trouver plusieurs produits installés dans un C.I., (matériel et logiciels). A chacun de ces produits est rattachée une documentation technique telle que : manuel d'installation, manuel utilisateurs, fonctionnalités du produit, etc…
Cette documentation peut être incluse dans le logiciel lui-même ou exister sur différents supports physiques : papiers, CD, DVD ou même sur un site WEB sur Internet.
C'est le C.I qui doit créer une bibliothèque pour les supports physiques et bien l'organiser pour retrouver rapidement le support et le manuel en cas de besoin.
Ceci pourrait éviter un long arrêt de l'exploitation du système ou de logiciel et faire gagner du temps pour la société et même gagner de l'argent si on ne sera pas obligé d'appeler le fournisseur ou le sous traitant pour débloquer la situation.

III.6) Elaboration et réalisation d'un Schéma Directeur Informatique Opérationnel

Avant d'élaborer un Schéma Directeur Informatique Opérationnel (SDIO), il faut :

1- Créer un comité de pilotage informatique, composé :
   - Du P.D.G. de la société
   - Du responsable du C.I. et ses collaborateurs
   - Des utilisateurs décideurs
   - Du représentant du ministère de tutelle
   - Du représentant du Secrétariat d'Etat à l'Internet et à l'Informatique
   - Eventuellement, d'un bureau de conseil

2- Préparer un Cahier des Charges qui doit être validé par le comité de pilotage
3- Lancer un appel d'offres pour l'élaboration du SDIO
4- Faire le dépouillement des offres pour le choix d'un bureau d'études afin d'élaborer le SDIO en collaboration avec le comité du pilotage informatique

Le Bureau d'étude choisi doit faire les tâches suivantes :

a) Audit de l'existant (matériel, logiciel, personnel, organisation, sécurité, etc…)
b) Etude des nouvelles orientations de la Direction Générale
c) Etude des nouveaux besoins des utilisateurs (en matériel, application, formation)
d) Proposition d'un nouveau système d'information de l'entreprise
e) Proposition d'au moins deux scénarios pour réaliser le nouveau système d'information. Pour chaque scénario, proposer une architecture matérielle, des solutions logicielles, moyens de communication, moyens de sécurité, plan de formation et il faut estimer son coût de réalisation.
f) Choix d'un scénario en collaboration avec le comité de pilotage.
g) Développement détaillé du scénario retenu
h) Etablir un plan de sécurité
i) Etablir un plan de bureautique
j) Estimation de l'investissement nécessaire et élaboration d'un planning de réalisation sur trois ans.
k) Prévision du budget nécessaire pour l'investissement et le fonctionnement pour chacune des trois années.
l) Elaboration d'un rapport final du SDIO et le faire approuver par le département informatique du ministère de tutelle et le Secrétariat d'Etat à l'Internet et l'informatique.

Le C.I. doit assurer, ensuite, :

m) Réalisation, sur trois ans, du SDIO approuvé.
n) Prévision des modalités de suivi de la réalisation du SDIO (faire des rapports annuels et des états de rapprochement par un comité de suivi.

III.7) Connexion de l'entreprise à l'Internet

Il y a ceux qui se demandent encore est ce qu'il faut se connecter dès maintenant à l'Internet ou attendre jusqu'à …quand ?

Or, Avoir une connexion à Internet (le fameux réseau des réseaux) n'est plus facultative aujourd'hui; c'est très nécessaire pour pouvoir faire communiquer des informations

(données, voix, images, vidéos) avec les autres, surtout les clients et les fournisseurs qui sont éparpillés dans le monde entier.

Le responsable du C.I. doit savoir convaincre la D.G. de la rentabilité d'une connexion professionnelle à l'Internet et doit réfléchir et trouver des solutions aux points suivants :

- Comment faire pour se connecter à l'Internet ?
  - ☞ faire un abonnement professionnel chez un Fournisseur d'Accès à l'Internet tel que Planet Tunisie, Hexabyte, etc… et de préférence avec une connexion ADSL pour gagner du temps.

- Comment faire pour obtenir une adresse e_mail ?
  - ☞ Créer, au moins, un compte E_mail sur un moteur de recherche tq YAHOO, Google, voilà, etc…
- Comment faire pour créer un nom de domaine de la société pour avoir une présence sur Internet ?
  - ☞ faire un abonnement professionnel chez un Fournisseur d'Accès à l'Internet pour héberger et publier le site web de la société.
- Comment s'ouvrir aux clients et aux fournisseurs à travers l'Internet ?
  - ☞ Créer un portail d'entreprise pour pouvoir accéder aux B.D. à travers l'Internet.
- Comment sécuriser les données de la société et être sûr qu'aucun pirate ne pourra attaquer la Base de données ou le réseau de la société ?
  - ☞ Installer un serveur proxy avec un logiciel de firewall, utiliser des protocoles de sécurité sur Internet (tels que : IP'sec, http's et SSL) et faire le cryptage (ou le chiffrement) des e_mails.

Chapitre IV

Recensement du personnel d'un C.I.

Objectif
Inventorier les différents services (ou départements) d'un C.I.

Eléments de contenu
1. Introduction
2. Structure d'un C.I.
3. Directeur du C.I.
4. Personnel du service étude et développement
5. personnel du service exploitation
6. responsable de la sécurité
7. Coordination entre les différents services
8. Questions de compréhension

IV.1) Introduction

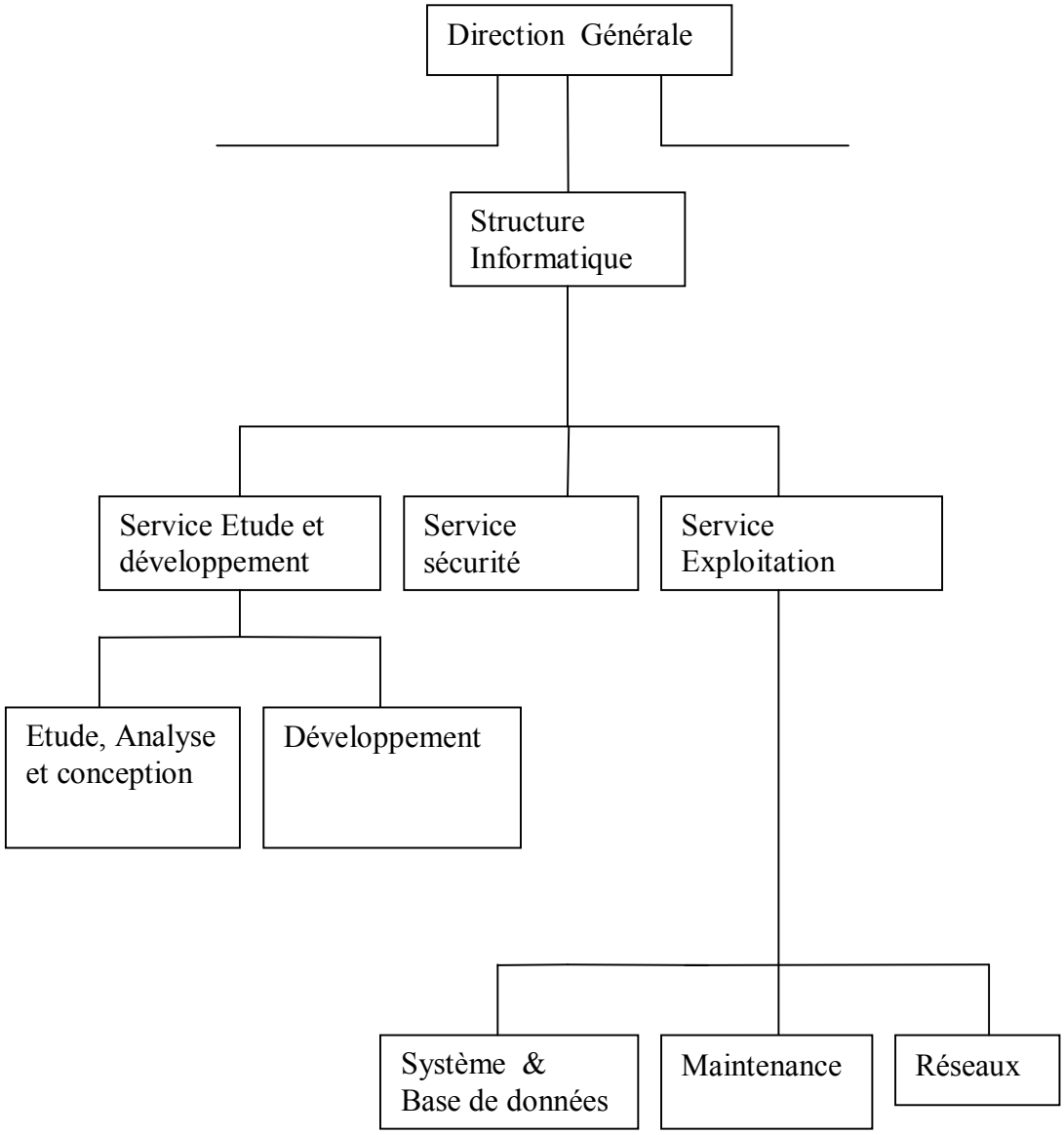
Si une entreprise décide de créer un C.I., c'est dans le but d'atteindre des objectifs préalablement tracés par la Direction Générale. Ces objectifs ne peuvent être réalisés en absence des moyens humains.

En effet, le fonctionnement d'un C.I. est conditionné par la mise à disposition des ressources financières, matérielles, logicielles et humaines. Ces dernières ont des qualités et des profils hétérogènes. Le personnel comprend un directeur, des ingénieurs informaticiens, et des techniciens.

IV.2) Structure d'un C.I.

La structure d'un C.I. peut être une Direction ou un département ou simplement un service informatique; ça dépend de l'ampleur et du degré de l'informatisation au sein de l'entreprise.
Toutefois, Pour maîtriser la gestion des informations de tous les processus de l'entreprise, la structure du C.I. doit être rattachée à la direction Générale.

Généralement, la hiérarchie de la structure d'un C.I. suit le modèle présenté dans la page suivante :


Direction Générale
Structure Informatique
Service Etude et développement
Service sécurité
Service Exploitation
Etude, Analyse et conception
Développement
Système & Base de données
Maintenance
Réseaux

IV.3) Le directeur du C.I.

C'est le premier responsable du C.I., il définit les objectifs en fonction de la stratégie globale de l'entreprise et de son plan informatique qui sont rassemblés dans un schéma Directeur informatique.
Il est chargé de :

- ✓ Fixer l'organisation générale du centre et le plan de carrière de son personnel
- ✓ Réaliser le schéma directeur informatique dans la durée prévue
- ✓ Coordonner les activités de ses collaborateurs
- ✓ Définir et gérer le budget
- ✓ Assurer l'esprit d'équipe et l'image de marque du centre
- ✓ Apporter de l'encadrement à son équipe

a) Formation requise
Le poste de Directeur informatique est souvent occupé par des universitaires de formation poussée (facultés, grandes écoles d'ingénieurs, etc ….) ayant une expérience dans les différentes disciplines de l'informatique et dans la gestion d'un C.I.

b) Qualités demandées
Un candidat au poste du directeur doit avoir :

- Esprit critique et de synthèse et une maîtrise des problèmes
- Le flair d'un psychologue
- Esprit d'imagination, d'innovation et de création de nouveaux projets
- Connaissance de l'organisation informatique, des possibilités des moyens matériels, logiciels et humains
- Connaissance en gestion des contrats et du personnel
- Sens de contact, de responsabilité et de bonnes relations humaines

IV.4) Personnel du service Etude et développement

Le service étude et développement a la responsabilité de l'analyse des besoins, la conception et la réalisation ou l'acquisition des applications informatiques de l'entreprise.

IV.4.1 le responsable de l'équipe Etude et développement

Il dirige toute l'équipe du développement et il assume la responsabilité d'acquisition des applications standards et le développement des applications spécifiques soit par l'équipe interne soit par sous traitement chez une SSII.
Pour se faire, il doit planifier la charge de travail de ses collaborateurs et contrôler le respect des délais de réalisation des différentes applications.

a) Formation requise
Le responsable des études doit avoir une formation supérieure poussée en informatique et doit avoir une expérience dans le développement des applications dans une SSII.

b) Qualités demandées
Il doit avoir :

- Connaissances parfaites des méthodologies de conception et des outils de développement
- Bonne connaissance des logiciels de base (syst. Exploitation, etc…)
- Sens de contact et de responsabilité

IV.4.2 Le chef d'un projet

Il est chargé de superviser et de coordiner les travaux d'études, d'analyses, de conception et de développement des applications. Il doit établir un planning détaillé depuis la conception jusqu'à la mise en production (càd exploitation quotidienne) de l'application. Il valide avec son équipe d'analystes et de programmeurs les méthodes à utiliser et les outils permettant de développer le projet afin de respecter les critères et les besoins demandés par les utilisateurs afin d'augmenter leur productivité.

a) Formation requise
   Formation d'un ingénieur informaticien et avec une expérience dans le développement

b) Qualités demandées
   - Connaissance parfaite des environnements de développement
   - Connaissance de génie logiciel
   - Connaissance dans la conduite des projets informatiques
   - Sens d'organisation et bonnes relations humaines

IV.4.3 l'Analyste-programmeur

Il étudie et analyse de façon détaillée la conception des applications. Il rencontre fréquemment les utilisateurs et prépare le dossier de programmation puis il passe au codage et au test des différents modules. Une fois approuvé, il élabore un manuel utilisateur et le transmet à l'utilisateur pour l'exploitation.

a) Formation requise
   - Technicien supérieur en informatique de gestion expérimenté, ou
   - Maîtrisard en informatique de gestion

b) Qualités demandées
   - Connaissance des méthodologies d'analyse et de conception
   - Connaissance des outils et des langages de programmation
   - Esprit de logique et d'algorithmique
   - Aptitude à la collaboration avec le chef de projet et les utilisateurs

IV.5) Personnel du service Exploitation

Le département exploitation est le responsable du bon fonctionnement du système informatique et de la qualité du service rendu aux utilisateurs.
Le personnel de ce département travaille en collaboration étroite avec le département étude et développement parce qu'il va faire exploiter les applications développées ou acquises par le responsable du développement.

IV.5.1 le responsable de l'équipe Exploitation

Il est chargé de fixer le planning de lancement des nouvelles applications, il organise le travail de son équipe et leurs affectations. C'est lui le responsable de la

qualité du service rendu aux utilisateurs qui sont responsables de l'exploitation des applications et de la qualité des résultats obtenus.

a) Formation requise
Ingénieur informaticien avec quelques années d'expérience

b) Qualités demandées
- Sens de responsabilité
- Méthodique dans l'exploitation
- Sens d'initiative
- Connaissance du matériel d'exploitation

IV.5.2 L'ingénieur système

Il s'occupe du système informatique, en particulier, en ce qui concerne :
- ☒ Le système d'exploitation du serveur central
- ☒ L'administration des Bases de Données
- ☒ La détermination des caractéristiques des serveurs
- ☒ la préparation des appels d'offres
- ☒ Evaluation des propositions techniques et financières des fournisseurs.

a) Formation requise
Ingénieur informaticien ou maîtrisard en informatique

b) Qualités demandées
- Connaissance approfondie des systèmes d'exploitation et des SGBD les plus utilisés.
- Esprit logique et méthodique
- Aptitude de collaboration avec les autres

IV.5.3 L'ingénieur réseau

Il a comme tâches :
- ☒ Administration des réseaux et de la connexion à l'Internet
- ☒ Gestion des utilisateurs (logins et mots de passe)
- ☒ Administration du site Web de l'entreprise

a) Formation requise
Ingénieur spécialisé en réseaux informatiques et télécommunication

b) Qualités demandées
- Connaissance des architectures des réseaux les plus utilisées
- Connaissances sur le développement des sites Web

IV.5.4 Technicien de maintenance

Il a comme charge la gestion de la maintenance du matériel informatique :
- Suivi de la maintenance du matériel
- Gestion du stock du consommable informatique
- Dépannage de certaines pannes

a) Formation requise
Technicien supérieur en maintenance du matériel informatique

b) Qualités demandées
   - Connaissance en matériel informatique
   - Connaissance en gestion de la maintenance
   - Connaissance des outils de diagnostic et de réparation
   - Expérience dans la réparation du matériel informatique

IV.5.5 Le Bandothécaire

C'est le technicien responsable de la gestion de la bibliothèque des supports physiques des documents techniques qui peuvent contenir des fichiers, des programmes et des données de l'entreprise (documents papiers, bandes magnétiques, streamers, disquettes, CD, DVD, etc …).

a) Formation requise

Technicien supérieur en informatique

b) Qualités demandées
   - Sens d'organisation
   - Connaissance de codification et de rangement des différents supports

IV.6 le responsable du service de sécurité

La personne assumant cette responsabilité est rattachée directement au directeur du C.I. car elle touche tous les aspects de la sécurité informatique.
Elle est chargée de :

- ✓ Définir les outils et les moyens à mettre en place pour sécuriser le C.I. (matériel, logiciels, procédures, B.D., etc …)
- ✓ Mettre en place ces moyens
- ✓ Mettre à jour et renouveler ces moyens
- ✓ Audit des moyens de sécurité
- ✓ Assurer la sécurité des réseaux et des accès à l'Internet

a) Formation requise

Ingénieur spécialisé en sécurité informatique

b) Qualités demandées
   - ✓ Avoir un master spécialisé en sécurité informatique
   - ✓ Avoir de l'expérience dans le domaine
   - ✓ Etre attentif et bien veillant
   - ✓ Avoir une réaction rapide et efficace

IV.7) Coordination entre les services

Au sein d'un centre informatique (C.I.), les responsables doivent tenir bon à l'esprit de travail d'équipe.

En effet, le bon fonctionnement du centre est conditionné par la coordination et la coopération des différents services (ou départements).

Effectivement, le responsable des études planifie les différentes interventions en coordination avec le responsable d'exploitation. Il doit être au courant de l'avancement des travaux, des dates prévues de démarrage, des plans et des dates de formation des utilisateurs, etc …De même, il doit assister les utilisateurs à l'exploitation des

applications et faire des réunions avec eux afin de se rendre compte des problèmes rencontrés par ces derniers et de leur trouver des solutions.

Chapitre V

Aspects de gestion d'un C.I.

Objectif
Présenter des différents aspects de la gestion d'un C.I.

Eléments de contenu
1. Introduction
2. Gestion des contrats de service
3. Gestion des ressources matérielles, logicielles et humaines
4. Gestion des sauvegardes et des reprises
5. Gestion des performances
6. Gestion des relations avec l'extérieur
7. Questions de compréhension

V.1) Introduction

La mission d'un C.I. est d'apporter une efficacité et une meilleure qualité aux services et aux produits fournis par l'entreprise à ses différents clients et ce afin d'atteindre les objectifs escomptés au paravent
De son côté, le directeur du C.I. peut se faire aider par les responsables des différents services du C.I. pour gérer des différents aspects tels que :

- gestion des contrats de service
- gestion des ressources
- gestion des incidents
- gestion de la sauvegarde et de la reprise
- gestion des performances
- gestion des relations avec l'extérieur

V.2) Gestion des contrats de service

Le suivi de la qualité du service informatique rendu par le C.I. aux utilisateurs se fait à l'aide d'indicateurs préalablement définis avec les utilisateurs et les responsables du C.I.. Ces indicateurs sont consignés dans un document appelé contrat de services qui précise les engagements respectifs du C.I. et des utilisateurs.
Les indicateurs fréquemment retenus sont les suivants :

- ✓ Le temps de réponse souhaité
- ✓ La fourchette horaire de disponibilité du système
- ✓ La date et l'heure de remise des états imprimés en batch
- ✓ La plan de survie et de reprise en cas de panne
- ✓ Le niveau de sécurité exigé

Dans le contrat de services, on détermine aussi les responsabilités des deux partenaires l'un vis-à-vis à l'autre, à savoir :

V.2.1) Les responsabilités du C.I.

- Assurer le bon fonctionnement du système informatique
- Assurer la continuité du fonctionnement

- Suivre les indicateurs des performances et du temps de réponse
- Appliquer les droits d'accès aux données
- Appliquer les droits d'exécution des logiciels
- Garantir la confidentialité des données
- Garantir le niveau de sécurité exigé
- Prévoir un plan de reprise en cas d'incident pour garantir la continuité du fonctionnement du système
- Assurer la formation des utilisateurs

V.2.2) Les responsabilités des utilisateurs :

- Assurer l'exploitation de leurs propres applications
- Préparer les modèles des états à imprimer
- Désigner les personnes qu'il faut former
- Fixer les droits d'accès et d'exécution
- Déterminer le niveau de sécurité minimum requis

V.3) Gestion des ressources

En plus de la gestion quotidienne des différentes ressources disponibles au C.I., la gestion des ressources concerne aussi l'évaluation des besoins en ressources humaines, matérielles et logicielles nécessaires au bon fonctionnement du C.I..
Pour estimer les besoins, les responsables de l'entreprise doivent faire un recensement des besoins ou des statistiques sur ce qui est consommé pendant l'année en cours et prévoir ce qu'il faudrait, en terme de ressources, pour réaliser ce qui est prévu dans le Schéma Directeur Informatique.

V.3.1) Prévision des ressources matérielles

Cette prévision est indispensable pour prévoir le budget nécessaire au financement des acquisitions du matériel qui sont approuvées dans le SDIO.
Pour connaître les performances du matériel à acquérir, il faut prendre en compte :

- ❖ Le temps de réponse maximal qu'on pourrait accepter
- ❖ Les conditions techniques pour exploiter à l'aise les applications
- ❖ Le nombre des utilisateurs connectés simultanément au serveur

Pour faire l'acquisition, il faut procéder comme décrit dans le paragraphe III.4).

V.3.1) Prévision des besoins en logiciels

Pour l'acquisition des logiciels, il faut tenir compte des prévisions approuvées dans le SDIO et des nouveaux besoins des utilisateurs qui doivent être spécifiés dans un cahier des charges fonctionnel et suivre les étapes décrites dans le paragraphe III.3).

V.3.2) Gestion du personnel

La gestion du personnel est plus délicate que celle de n'importe quelle autre chose.
En effet, lors de recrutement des informaticiens, il faut s'occuper :

- de leur profil de formation
- de leur compétences surtout en nouvelles technologies
- de leur disponibilité et leur motivation au poste offert

En cours d'activité du personnel, il faut bien gérer :

- le pointage et l'absentéisme de chaque personne
- le calendrier des congés annuels ou particuliers

- la formation et la mise à niveau du personnel
- les encouragements et la promotion professionnelle
- éventuellement, l'aspect social et familial de l'employé
- Les heures supplémentaires en particulier la nuit ou pendant les week ends pour assurer des traitements en batch

De même, il faut faire très attention :

- Au départ imprévu de certain personnel, donc il faut prévoir un certain système pour ne pas perdre avec lui son savoir faire, par exemple prévoir des documents, des dossiers et des manuels à tous les niveaux
- A la fuite de certaines informations confidentielles
- Au chantage de certain personnel compétent surtout si le marché informatique peut être demandeur à cette compétence
- L'absence d'une personne compétente qu'on ne peut pas remplacer
- Au mécontentement du personnel informatique
- A la démission d'une ou de plusieurs personnes

V.4) Gestion des sauvegardes et des reprises

Une sauvegarde physique est une copie d'une unité de disque dur sur un support magnétique (disquettes, streamer, CD, DVD, etc…) et ce afin de se protéger contre les pannes du disque dur et contre la perte des données.
L'opération inverse, c'est la restauration qui consiste à réinstaller les fichiers sur le disque dur à partir de la copie.
Il faut gérer les sauvegardes et surtout les supports de sauvegarde en leur attribuant des noms, des numéros de version et dates des copies et le lieu de leur rangement.
La reprise est le fait de reprendre le fonctionnement du système informatique après incident. Il faut reprendre à partir d'une situation cohérente et intègre et non pas à partir d'un état de base de données transitoire.
Pour assurer la continuité du fonctionnement du système sans dégradation de services (lenteur, pas de sauvegarde immédiate, ou autres contraintes), il faut faire une reprise à chaud càd restaurer les données ou changer l'unité de disque dur sans éteindre le système et ceci n'est possible que si on a les ressources critiques du serveur dupliquées. (Deux unités de disques, deux processeurs et double alimentation)

V.5) Gestion des performances

Le suivi des performances du système informatique est important., car c'est souvent avec la mesure du temps de réponse que l'utilisateur évalue le degré de qualité du service rendu par le C.I.
La performance d'un système ne se limite pas seulement au facteur temps de réponse, elle peut être mesurée en fonction :

- ✓ du débit des lignes de transmission
- ✓ de la durée d'exécution des traitements par lots
- ✓ du nombre d'utilisateurs potentiel simultanés
- ✓ Nombre des postes qu'on peut connecter
- ✓ Caractéristiques techniques du serveur central

Ces éléments sont proportionnels ou inversement proportionnels au temps de réponse :
En effet,

- ☞ Plus le débit augmente, plus le temps est petit donc meilleur
- ☞ Plus la durée d'exécution est petite, plus le tps de réponse est meilleur

- ☞ Plus les caractéristiques sont performantes, plus le temps est meilleur
- ☞ Plus le nombre des utilisateurs est grand, plus le temps est grand donc mauvais
- ☞ Plus le nombre des postes connectés est grand, plus le temps est grand donc mauvais.

V.6) Gestion des Relations avec l'extérieur

Pour un C.I., On sous entend par extérieur les fournisseurs du matériel et des logiciels et les sociétés des services.
Avec ces partenaires, le C.I doit entretenir des bonnes relations professionnelles et même personnelles. Donc, Il est souhaitable d'établir avec eux des relations sérieuses et des réunions amicales qui dépassent les relations contractuelles; à savoir :

- Des réunions mensuelles (ou périodiques) avec les représentants des fournisseurs pour voir l'avancement de réalisation des différents projets et étudier les problèmes rencontrés
- Des invitations aux différents fournisseurs pour assister à l'exploitation de leur produits et logiciels et proposer des améliorations
- Envoi des cadeaux à l'occasion de la fin d'année ou de certaines fêtes
- Entretiens conversationnels (dialogues et discussions) concernant les nouveautés technologiques et tout ce qui pourrait intéresser le C.I..

Ainsi, on trouvera le partenaire externe tout prêt à répondre aux différents besoins du C.I de la société.

Chapitre VI

La sécurité informatique

Objectif

Savoir les différents aspects de la sécurité globale d'un système informatique et connaître les moyens disponibles.

Eléments de contenu

1. Introduction
2. Approche globale de la sécurité informatique :
   a) Sécurité organisationnelle
   b) Sécurité physique
   c) Sécurité des accès
   d) Sécurité des réseaux
   e) Sécurité des serveurs
   f) Sécurité des données
   g) Sécurité énergétique
   h) Sécurité antivirale
3. Stratégie de sécurité
4. Questions de compréhension

VI.1) Introduction

La sécurité des systèmes informatiques couvre généralement trois aspects :

- L'intégrité des données qui garantit l'authenticité des données càd les données sont bien celles qu'on croit être.
- La confidentialité qui consiste à assurer l'accès aux ressources uniquement aux personnes autorisées.
- La disponibilité qui permet de maintenir le bon fonctionnement du système informatique en tout temps et en toute circonstance.

VI.2) Approche globale de la sécurité informatique

Il faut traiter la sécurité d'un système informatique en sa totalité, car il est inutile d'avoir une porte blindée dans ma maison et en même temps les fenêtres sont ouvertes sur la rue càd sur le monde extérieur.
Partant de cette idée, on doit donc aborder la sécurité dans son contexte global :
Donc, on doit assurer les différents aspects de sécurité suivants :

a) La sécurité Organisationnelle
   - Définir les rôles des différents acteurs : Qui fait quoi ?
   - Sensibiliser les utilisateurs aux problèmes de la sécurité

- Intégrer le facteur sécurité dans tout projet informatique dès sa conception jusqu'à sa réalisation
- Arrêter les procédures d'organisation et de mise en œuvre de la sécurité

b) La sécurité physique
- Règles de sécurité des locaux qui abritent les serveurs sensibles et les équipements d'interconnexion : équiper ces locaux par des détecteurs d'incendie et par un système d'extinction automatique.
- Verrouillage des locaux contre le vol du matériel.
- Issue de secours dans les locaux
- Accès permis seulement aux personnes autorisées (utiliser des clés spéciales ou une carte à puce pour contrôler les accès à la salle informatique)

c) La sécurité des accès
- Sécurité des accès aux postes de travail et aux serveurs pour les utilisateurs et les administrateurs. L'accès doit être assuré par :
  - Nom utilisateur et mot de passe
  - Carte à puce : l'authentification par carte à puce est destinée à garantir l'identité d'une personne à assurer son identification via un code PIN et à protéger l'accès aux postes de travail par le biais d'un mot de passe dynamique (càd qu'il faut changer de temps en temps)
- Classification des données selon leur confidentialité et leur appartenance
- Gestion des droits d'accès aux données et aux fonctionnalités des logiciels en fonction des profils des utilisateurs

d) La sécurité des réseaux
- Assurer la sécurité des topologies LAN et WAN pour garantir la continuité de transmission des données à l'intérieur et à l'extérieur de l'entreprise
- Contrôler le flux des données entre le système d'information et le monde extérieur (càd l'Internet ou le WAN) pour éviter tout risque d'attaque (alors il faut installer serveur proxy avec un firewall)
- Détecter les intrusions qui viennent de l'extérieur et les éviter au préalable
- Assurer la sécurité de transmission de données sur l'Internet en implantant des protocoles sécurisés (SSL (Secure Sockets Layer), IPsec, etc…) et en faisant le cryptage des messages.

e) La sécurité des serveurs
- Classification des serveurs de l'entreprise (le serveur proxy doit être assez performant pour bien protéger le serveur de base de données)
- Audit sécurité des configurations des serveurs sensibles
- Sécuriser les procédures d'exploitation et d'administration (avec des mots de passe et arrêter qui fait quoi)

f) La sécurité des données
- Assurer une sauvegarde quotidienne et hebdomadaire des données
- Faire la sauvegarde sur des supports multiples

- Protéger les supports de sauvegarde, contre les incendies, dans une armoire ignifuge.

g) La sécurité énergétique

La sécurité énergétique est très importante quant au fonctionnement des équipements formant la plateforme technique.
Il est recommandé d'équiper les armoires abritant les différents éléments par des onduleurs performants pour remédier aux petites coupures du courant ou aux chutes de la tension électrique.
En revanche, pour les coupures de longue durée, il faut prévoir l'installation d'un groupe électrogène qui va assurer la continuité du courant nécessaire pour le bon fonctionnement.

h) La sécurité antivirale (c'est la sécurité contre les virus informatiques)

Un virus est un programme informatique qui peut infecter d'autres programmes dans le but de les modifier pour y ajouter une copie de lui-même, de gêner leur fonctionnement et voire même les supprimer ou nuire à certaines composantes de l'ordinateur. Les virus vont de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données et au le plus méchant qui formate le disque dur.
Les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection, d'où, outre les virus classiques, on distingue principalement quatre types de virus:

- Les VERS sont des virus capables de se propager à travers un réseau d'entreprise.
- Les chevaux de Troie (les troyens) sont des virus qui permettent de créer une faille dans un système, généralement, c'est pour permettre à leur programmeur de s'introduire dans le système infecté et de l'administrer à distance et faire tout ce qu'il veut.
- Les bombes logiques sont des virus capables de se déclencher suite à un évènement particulier (suite à une date système programmée, exemple : le virus de CHERNOBYLE)
- Les canulars sont des annonces publicitaires (les spams) qui arrivent à travers le courrier électronique et qui peuvent contenir des virus ou des fausses alertes ou des fausses informations.

Un antivirus est un utilitaire qui détecte les virus sur notre ordinateur par l'analyse (opération de scan) des fichiers sur tout support de données : Disque Dur, disquette, CD et même ceux qui sont encore en Mémoire centrale ou sur le secteur d'amorçage

Exemples d'antivirus :

- Symantec Norton Antivirus
- Mcafee Virusscan
- F-secure

Vu le nombre de virus existants et augmentant et vu leur nuisance, leur menace et leur rapidité de propagation accrue grâce au réseau Internet, la nécessité de se disposer d'un antivirus n'est plus à démontrer.

Mais vu la création et l'injection journalière, de nouveaux virus sur l'Internet, la possession d'un antivirus n'est plus suffisante pour s'assurer et dire qu'aucun virus ne passerait inaperçu car l'antivirus, lors de son analyse, fait référence à une liste de signatures numériques des différents virus établie lors de son développement; alors est ce qu'il peut reconnaître la signature de ceux qui sont créés après sa commercialisation ?

Reconnaître de façon automatique les nouveaux virus ; Non !

Mais, Oui, avec l'acquisition d'une nouvelle version d'antivirus ou par le téléchargement à partir de l'Internet de la liste de nouvelles définitions des virus de façon périodique et fréquente pour que l'antivirus puisse détecter les virus récemment créés et éventuellement désinfecter les fichiers touchés et ainsi éviter les risques de nouvelles infections.

VI.3) Stratégie de sécurité

Une bonne stratégie de sécurité ne permet pas de gagner de l'argent. Par contre, si elle est bien préparée et exploitée comme il le faut, elle nous évite d'en perdre.

Une bonne stratégie opérationnelle, doit passer par les trois étapes suivantes :

a) Une bonne Préparation
   - Une charte de sécurité
   - Un cahier des charges
   - Les moyens nécessaires à la mise en place de la sécurité

b) Une bonne application
   - Planification de la mise en place
   - Mise en place des procédures de différents aspects de la sécurité
   - Veiller à la disponibilité et au bon état du tout le système de sécurité

c) Un bon suivi
   - Contrôle et vérification périodique de l'efficacité du système sécurité (Audit de la sécurité)
   - Formation et recyclage du personnel de la sécurité
   - Renouvellement des moyens de sécurité obsolètes (dépassés).
   - Mise à jour périodique des antivirus
   - Mise à jour périodique des systèmes d'exploitation pour remédier à leur bug et à leur faille de vulnérabilités aux intrusions qui viennent de l'extérieur et en particulier de l'Internet.