

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ IBN-KHALDOUN DE TIARET
FACULTÉ DES SCIENCES APPLIQUÉES
DÉPARTEMENT DE GENIE ELECTRIQUE



MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master

Domaine : Master Génie Electrique

Filière : Electronique

Spécialité : Electronique Des Systèmes Embarquées

THÈME

Gestion Electronique de la fiche circuit

*Préparé par : ZIADI Khadra
BOURIANE Amina*

Devant le Jury :

Nom et prénoms	Grade	Qualité
Mr. A. Benatia	MAA	President
Mr. M. Maaskri	MAA	Examineur 1
Mr. M. Goismi	MAA	Examineur 2
Mr. H. Benabid	MAA	Encadreur

PROMOTION 2017 /2018

“Whenever you read a good book, somewhere in the world
a door opens to allow in more light.”

Vera Nazarian

DEDICACES

C'est avec profonde gratitude et sincères mots, que nous
dédions ce modeste travail de fin d'étude à :

Nos chers parents ; qui ont sacrifié leurs vie pour notre réussite
et nous ont éclairé le chemin par leurs conseils judicieux. Nous
n'espérons qu'un jour, nous pourrons leurs rendre un peu de
ce qu'ils ont fait pour nous, que dieu leur prête bonheur et
longue vie.

Nous dédions aussi ce travail à nos frères, sœurs et toutes nos
familles.

Et à toute la promotion de 2ème année master électronique des
systèmes embarqués.

Khadra ZIADI & Amina BOURIANE.

REMERCIEMENTS

Nous tenons tout d'abord à remercier **Allah** le tout puissant et
miséricordieux, qui nous a donné la force et la patience
d'accomplir ce modeste travail.

Nous remercions vivement notre encadreur **Mr. BENABID
Houari** pour ses précieux conseils et ses aides durant toute la
période du travail.

Nous remercions nos enseignants dès la première année jusqu'à
ce jour.

Nos vifs remerciements vont également aux membres du jury
pour l'intérêt qu'ils ont porté à notre recherche en acceptant
d'examiner notre travail et de l'enrichir par leurs propositions.

Enfin, nous tenons également à remercier toutes les personnes
qui ont participé de près ou de loin à la réalisation de ce travail.

Nous remercions nos parents pour nous avoir soutenus le long
de nos études.

Sans oublier notre cher pays l'Algérie et que dieu la garde.

Sommaire

CHAPITRE I

I.1 Introduction.....	19
I.2 Définition	19
I.3 Intérêt des réseaux informatiques	19
I.3.1 Apport aux entreprises	19
I.3.2 Apport aux individus.....	20
I.4 Types des réseaux informatiques (la typologie).....	20
I.4.1 Le réseau personnel (PAN) Personal Area Network.....	20
I.4.2 Le réseau local (LAN).....	20
I.4.3 Le réseau métropolitain (MAN).....	20
I.4.4 Le réseau étendu (WAN)	20
I.4.5 Réseaux sans fil (Wireless networks).....	21
I.5 Topologie physique des réseaux	21
I.5.1 La topologie en bus (le support linéaire).....	21
I.5.2 La topologie en étoile.....	22
I.5.3 La topologie en anneau	22
I.5.4 La topologie en arbre	23
I.5.5 La topologie en maillage.....	23
I.5.6 La topologie bus en étoile	23
I.5.7 La topologie anneau en étoile	23
I.6 Architectures des réseaux informatiques (rôle).....	23
I.6.1 L'architecture client/serveur	23
I.6.6.1 L'architecture à deux (02) niveaux	24
I.6.1.2 L'architecture client-serveur à trois (3) niveaux	24
I.6.2 L'architecture poste à poste ou pair-à-pair (peer-to-peer).....	25
I.7 Le modèle de référence OSI.....	25
I.7.1 La couche physique.....	26
I.7.2 La couche liaison de données	26
I.7.3 La couche réseaux	26
I.7.4 La couche transport.....	26
I.7.5 La couche session.....	26
I.7.6 La couche présentation	26
I.7.7 La couche application	26
I.8 Le modèle TCP/IP	26
I.8.1 La couche hôte réseau	27
I.8.2 La couche internet	27

SOMMAIRE

I.8.3 La couche transport	27
I.8.4 La couche application	27
I.9 L'internet.....	28
I.9.1 Les services offerts par l'internet.....	28
I.9.2 Avantages de l'internet	29
I.9.3 Fonctionnement de l'internet.....	29
I.10 Les protocoles de communication (la topologie logique)	29
I.10.1 Le protocole TCP/IP	29
I.10.2 IP (Internet Protocol).....	30
I.10.3 Le protocole UDP (User Data Protocol).....	30
I.10.4 Le protocole BOOTP	30
I.10.5 Le protocole DHCP.....	30
I.10.6 Le protocole HTTP	31
I.11 Gestion de la communication.....	31
I.11.1 Sens de transmission	31
I.11.1.1 Le mode simplex	31
I.11.1.2 Le mode half- duplex.....	31
I.11.1.3 Le mode full-duplex	31
I.11.2 Les types de transmission	31
I.11.2.1 Le type synchrone.....	32
I.11.2.2 Le type asynchrone.....	32
I.11.3 Les méthodes d'accès au support	32
I.11.3.1 La contention	32
I.11.3.2 L'interrogation (polling).....	32
I.11.3.3 Le jeton passant.....	33
I.12 Les principes de la sécurisation des réseaux	34
I.12.1 L'authentification	34
I.12.2 La confidentialité.....	34
I.12.3 L'intégrité	34
I.12.4 La disponibilité.....	34
I.13 Conclusion	34

CHAPITRE II

II.1 Introduction	36
II.2 Définition.....	36
II.3 Objectif de la gestion électronique des documents.....	36
II.4 Les étapes de la chaîne de (GED).....	37
II.4.1 La création.....	37

SOMMAIRE

II.4.2 La gestion	38
II.4.3 La diffusion	38
II.4.4 La conservation	39
II.5 Méthodologie de mise en place	39
II.6 Les types de la GED.....	39
II.6.1 La GED bureautique.....	39
II.6.2 La GED documentaire.....	39
II.6.3 La GED administrative.....	40
II.6.4 La GED COLD (Computer Output on Laser Disc)	40
II.6.5 La GED technique	40
II.7 Les principes de la GED	40
II.7.1 Stockage de l'information	40
II.7.2 Accès à l'information	40
II.7.3 Echange de documents	40
II.8 Les différentes catégories de logiciels de GED	40
II.8.1 Les logiciels GED d'entrée de gamme	40
II.8.2 Les logiciels GED à composants	41
II.8.3 Les logiciels GED génériques	41
II.9 Analyse du logiciel.....	41
II.9.1 Les fonctionnalités offertes	41
II.9.2 L'architecture technique	41
II.9.3 L'offre de service de l'éditeur	41
II.9.4 Le coût.....	41
II.10 Avantages de la GED.....	41
II.10.1 Accès rapide et à distance aux documents.....	42
II.10.2 Base unique pour l'ensemble des documents de l'entreprise	42
II.10.3 Conservation des documents.....	42
II.10.4 L'organisation de l'information	42
II.10.5 La gestion du cycle de vie des documents.....	42
II.10.6 La centralisation et le partage des documents	42
II.10.7 La sécurisation de l'information	42
II.11 Les aspects techniques de la GED.....	42
II.11.1 Standards ouverts.....	42
II.11.2 Architecture logicielle et plate-forme technique	43
II.11.3 Gestion des droits d'accès	43
II.11.4 Administration	43
II.12 Enjeux relatifs à la GED	43
II.12.1 L'interopérabilité des formats	43

SOMMAIRE

II.12.2 La pérennité des formats et des supports de stockage.....	44
II.12.3 La sécurité des données	44
II.13 Les Risques.....	44
II.13.1 Mauvaise détermination des objectifs du projet.....	44
II.13.2 Mauvaise interface graphique	45
II.13.3 Sous-évaluation de la dimension humaine	45
II.13.4 Surévaluation de la dimension technique	45
II.13.5 Sous-évaluation de la charge de travail	45
II.14 Les facteurs clés de succès de projet GED	45
II.14.1 Volonté politique	45
II.14.2 Implication des acteurs	45
II.14.3 Découpage de projet.....	45
II.14.4 Coordinations entre les intervenants.....	46
II.14.5 Mise en place de retours d'expérience.....	46
II.15 Conclusion.....	46
CHAPITRE III	
III.1 Introduction	48
III.2 Définition.....	48
III.3 Les risques (attaques).....	48
III.3.1 Réalisation d'une attaque	48
III.3.2 Objectifs des attaques	48
III.3.2.1 Interruption	49
III.3.2.2 Interception.....	49
III.3.2.3 Modification	49
III.3.2.4 Fabrication.....	49
III.3.3 Typologie des attaques	49
III.3.3.1 Appropriation de mots de passe	49
III.3.3.2 Attaques fondées sur le leurre.....	50
III.3.4 Types des attaques	50
III.3.4.1 Attaques passives	50
III.3.4.2 Attaques actives.....	50
III.3.5 Description des attaques.....	51
III.3.5.1 L'usurpation d'adresse IP	51
III.3.5.2 Un analyseur réseau	51
III.3.5.3 ARP Poisoning.....	52
III.3.5.4 Balayage des ports	52
III.3.5.5 Fishing	52
III.4 Critères de la sécurisation (services).....	53

SOMMAIRE

III.4.1 La disponibilité	53
III.4.2 L'intégrité	53
III.4.3 La confidentialité	53
III.4.4 L'identification et l'authentification	53
III.4.5 La non-répudiation	54
III.5 Les domaines de la sécurité de l'information	54
III.5.1 La sécurité physique	54
III.5.2 La sécurité de l'exploitation.....	54
III.5.3 La sécurité logique.....	55
III.5.4 La sécurité applicative.....	55
III.5.5 La sécurité des télécommunications	55
III.6 Objectifs de la sécurité d'information.....	55
III.6.1 La localisation des données.....	55
III.6.2 La gestion du caractère privé des données	56
III.6.3 La disponibilité des services ou de l'information	56
III.6.4 Le contrôle des accès.....	56
III.6.5 L'environnement multi locataires complexe et les fuites de données	56
III.6.6 La perte de données	56
III.7 Architecture de la sécurité	56
III.8 Mécanisme de défense.....	57
III.8.1 Chiffrement.....	57
III.8.2 Signature numérique.....	57
III.8.3 Bourrage de trafic	57
III.8.4 Notarisation.....	57
III.8.5 Contrôle d'accès	57
III.8.6 Antivirus.....	57
III.8.7 Le pare-feu	57
III.8.8 Détection d'intrusion.....	58
III.8.9 Journalisation	58
III.8.10 Analyse des vulnérabilités (Security audit).....	58
III.8.11 Contrôle du routage.....	58
III.8.12 Contrôle d'accès aux communications	58
III.8.13 Horodatage.....	58
III.8.14 Certification	58
III.8.15 Distribution de clefs	58
III.9 Enjeux de la sécurisation	58
III.10 Cryptage	59
III.10.1 Méthodes de cryptage	59

SOMMAIRE

III.10.1.1 La méthode symétrique	59
III.10.1.2 La méthode asymétrique.....	60
III.10.1.3 Cryptage hybride.....	60
III.11 Conclusion.....	61
CHAPITRE IV	
IV.1 Introduction.....	63
IV.2 Outils de développement :.....	63
IV.2.1 EasyPHP version 14.1vc9.....	63
IV.2.2 Editeur de texte (sublime text3).....	63
IV.2.3 Serveur web (Apache).....	64
IV.2.4 Système de gestion de base de données (MySQL).....	64
IV.3 Langages de programmation.....	64
IV.3.1 HTML.....	64
IV.3.2 PHP	65
IV.3.3 CSS	66
IV.4 Conception et réalisation	67
IV.4.1 Conception de la base de données	67
IV.4.2 Etapes de conversion.....	68
IV.4.3 Architecture générale de notre site	71
IV.4.4 La page d'accueil du site.....	72
IV.5 Scénario d'exécution	72
IV.5.1 Boite de dialogue de La bibliothèque centrale.....	72
IV.5.2 Boite de dialogue de la bibliothèque de la faculté	73
IV.5.3 Boite de dialogue de Vice_doyen.....	73
IV.5.4 Boite de dialogue de chef de département	74
IV.5.5 Impression de la fiche circuit :.....	74
IV.6 Les scripts principaux.....	76
IV.7 Conclusion	77
Conclusion générale et perspectives	78
Références bibliographiques et webographies.....	79
RESUME.....	81

CHAPITRE I

Figure I. 1 : Topologie physique des réseaux.	21
Figure I. 2: La topologie en bus.....	22
Figure I. 3: La topologie en étoile.	22
Figure I. 4: La topologie en anneau.....	23
Figure I. 5: L'architecture client/serveur à deux niveaux.	24
Figure I. 6: Architectures client/serveur à trois niveaux.	25
Figure I. 7: Le modèle de référence OSI.....	25
Figure I. 8: Le modèle TCP/IP.	28
Figure I. 9: L'architecture TCP/IP.	30

CHAPITRE II

Figure II. 1: Architecture d'une solution de la gestion électronique de documents.	37
---	----

CHAPITRE III

Figure III. 1: Cryptage symétrique.	60
Figure III. 2: Cryptage asymétrique.	60
Figure III. 3: Cryptage hybride.....	61

CHAPITRE IV

Figure IV. 1: EasyPHP.	63
Figure IV. 2: Sublime text3.	63
Figure IV. 3: Apache.	64
Figure IV. 4: MySQL.	64
Figure IV. 5: HTML5.	65
Figure IV. 6: PHP5.	65
Figure IV. 7: CSS3.	66
Figure IV. 8: Sélection du format «Feuille de calcul OpenDocument ».	68
Figure IV. 9: Création de la base de données (etudiant).	68
Figure IV. 10: Importation du contenu de la base de données déjà convertit.	68
Figure IV. 11: Conversion de la base de données.	68
Figure IV. 12: Exécution de la conversion.	69
Figure IV. 13: L'architecture générale de notre site.	71
Figure IV. 14: La page d'accueil du site.	72
Figure IV. 15: La boîte de dialogue de la bibliothèque centrale.	72
Figure IV. 16: La boîte de dialogue de la bibliothèque de la faculté.	73
Figure IV. 17:La boîte de dialogue de Vice_doyen.	73
Figure IV. 18: La boîte de dialogue de chef de département.	74
Figure IV. 19: La fiche de circuit avant l'impression.	74
Figure IV. 20: La fiche de circuit après l'impression.	75

CHAPITRE IV

Tableau IV. 1: La base de données en format EXCEL..... 67
Tableau IV. 2: la base de données sous format MySQL..... 69
Tableau IV. 3: La table et_gc. 70
Tableau IV. 4: La table et_ge. 70
Tableau IV. 5: La table et_gm..... 71
Tableau IV. 6: Les scripts principaux. 76

TCP/IP: Transmission Control Protocol/ Internet Protocol.

PAN: Personal Area Network

LAN: Local Area Network

MAN: Metropolitan Area Network

WAN: Wide Area Network

AP: Access Point

SGBD : Systèmes de Gestion de Base de Données

OSI: Open System Interconnexion

HDLC: High-Level Data Link Control

UDP: User Datagram Protocol

MIME: Multipurpose Internet Mail Extension

ASCII: American Standard Code for Information Interchange

TFTP: trivial File Transfer Protocol

SMTP: Simple Mail Transfer Protocol

HTTP: HyperText Transfer Protocol

IRC: Internet Relay Chat

WWW: World Wide Web

Ftp: File Transfer Protocol

IMPAP: Internet Mail Access Protocol

RARP: Reverse Adresse Resolution Protocol

DHCP: Dynamic Host Configuration Protocol

BOOTP: Bootstrap Protocol

CSMA/CD: Carrier Sense Multiple Access Collision Detection.

CSMA/CA: Carrier Sense Multiple Access Collision Avoidance.

FDDI: Fiber Distributed Data Interface

MAU: Media Access Unit

GED: Gestion Electronique de Document

GED COLD: Computer Output on Laser Disc

DTD : Document Type Définition

DOS : Denial of Service ; Déni de service

ARP: Address Resolution Protocol

SI: Système d'Information

WAMP: Windows Apache MySQL PHP.

SQL: Structured Query Language

NOMENCLATURES

PHP: hypertext preprocessor

CGI: commun Getway interface

CSS: Cascading Style Sheet

INTRODUCTION

GENERALE

Toujours, l'homme fut obsédé par l'échange de biens et de ressources pour parvenir à satisfaire ses besoins et faciliter sa vie, comme l'informatique qui est apparu pour faciliter beaucoup de problèmes complexes et qui est aujourd'hui présent dans les différents domaines de la vie privée et professionnelle.

Le monde de l'informatique est sûrement l'un des milieux qui évolue le plus rapidement ; avec la révolution de l'Internet, le rêve de milliers d'entreprises s'est réalisé en apportant une incroyable possibilité d'extension et d'épanouissement au monde ainsi que dans les différentes relations humaines.

Les établissements scolaires et universitaires qui présentent le cerveau moteur de tout développement, doivent aussi bénéficier des avantages de l'internet en améliorant la qualité d'information fourni aux étudiants. Donc comment peuvent-ils atteindre cet objectif? Et qu'elles sont les principaux éléments qui permettent d'y aboutir?

La société universitaire produit chaque année de larges nombres de documents ; les informations qu'ils contiennent sont de différents types et objectifs.

Parmi les documents sortant de l'université, on cite la fiche du circuit (certificat d'évacuation) qui est une pièce maitresse pour que les étudiants aient leurs diplômes de fin d'études. Vu le nombre important des étudiants sortant chaque année, un problème de gestion manuelle de leurs fiches s'est imposé au niveau des services concernés (départements, facultés et bibliothèques).

Et pour remédier à ce grand problème, on va proposer la création d'un site web dynamique pour gérer ce document (Fiche de circuit) d'une façon électronique, rapprochant et unifiant la procédure permettant d'en obtenir.

Dans ce nouveau contexte, les bibliothèques, les facultés et les départements d'université IBN KHALDOUN ont la responsabilité et la possibilité de créer et de fournir aux étudiants les moyens d'une gestion efficace de l'information ; qui est une mission de service publique traditionnelle mais qui nécessite de nouvelles méthodes de travail et une organisation administrative appropriée.

Ce manuscrit est subdivisé en quatre chapitres :

Le premier chapitre cite l'intérêt des réseaux informatiques, leurs types, leurs topologies et leurs architectures suivant le rôle de chaque réseau ; ensuite une brève description du modèle OSI, le modèle TCP/IP, l'Internet, les protocoles et la gestion de la communication.

Le second chapitre décrit la gestion électronique des documents, ces étapes, les différentes catégories de logiciel de GED, la gestion du cycle de vie des documents, les risques, les enjeux relatifs à la GED et les facteurs clés de succès de projet GED.

Le troisième chapitre cite les critères de la sécurité de l'information contre les différentes attaques. Le quatrième chapitre explique l'application réalisée (site web de gestion des fiches de circuit pour les étudiants) ainsi les outils informatiques utilisés.

Enfin, ce travail sera clôturé par une conclusion générale et quelques perspectives de recherche envisagées.

**INTRODUCTION AUX
RESEAUX
INFORMATIQUES**

CHPITRE I : INTRODUCTION AUX RESEAUX INFORMATIQUES

I.1 Introduction

Les réseaux informatiques sont nés pour faire Communiquer les terminaux distants avec un site central puis à des ordinateurs entre eux.

Dans un premier temps ces communications étaient juste destinées aux transports de données informatiques alors qu'aujourd'hui on se dirige plutôt vers des réseaux qui intègrent à la fois des données mais en plus la parole et la vidéo. [1]

Les réseaux informatiques sont devenus aujourd'hui une partie intégrante de l'entreprise, les individus, les professionnels et les universitaires ont également appris à s'appuyer sur des réseaux informatiques pour des capacités telles que le courrier électronique et l'accès à des bases de données distantes à des fins de recherche et de communication.

Les réseaux sont ainsi devenus une réalité mondiale de plus en plus répandue car ils sont rapides, efficaces et fiables. [2]

I.2 Définition

Un réseau en général est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations, et partager des services.

Le terme réseau en fonction de son contexte peut désigner plusieurs choses. Il peut désigner l'ensemble des machines, ou l'infrastructure informatique d'une organisation avec les protocoles qui sont utilisés, ce qui 'est le cas lorsque l'on parle de l'Internet.

Le terme réseau peut également être utilisé pour décrire la façon dont les machines d'un site sont interconnectées. C'est le cas lorsque l'on dit que les machines d'un site (sur un réseau local) sont sur un réseau Ethernet, Token Ring, réseau en étoile, réseau en bus,...

Le terme réseau peut également être utilisé pour spécifier le protocole qui est utilisé pour que les machines communiquent. On peut parler de réseau TCP/IP, NetBeui (protocole Microsoft) DecNet (protocole DEC), IPX/SPX,... [3]

I.3 Intérêt des réseaux informatiques

Les réseaux informatiques jouent un rôle très important que ce soit dans la vie publique ou privée :

I.3.1 Apport aux entreprises

Partage de ressources ; imprimantes, disque dur, processeur, etc.

- Réduction de coûts.
- Augmentation de la fiabilité ; dupliquer les données et les traitements sur plusieurs machines.

- Fournir un puissant média de communication: e-mail, VC
- Faciliter la vente directe via l'Internet. [1]

I.3.2 Apport aux individus

- Accès facile et rapide à des informations distantes: Informations de type financier: Paiement de factures, Consultations de solde, recherche d'informations de tout genre
- Accès à des journaux et bibliothèques numériques: News ...
- Communication entre les individus : Vidéoconférence, courrier électronique, groupes thématiques (newsgroups), clavardage (chat), communication poste-à-poste (peer-to-peer), téléphonie et radio via Internet, etc.
- Divertissements et jeux interactifs : vidéo à la carte et toutes sortes de jeux (jeux d'échec, de combats, etc.)
- Commerce électronique (e-commerce) : transactions financières, achats en ligne à partir de son domicile. [1]

I.4 Types des réseaux informatiques (la typologie)

Suivant la distance qui sépare les ordinateurs, on distingue plusieurs catégories de réseaux :

I.4.1 Le réseau personnel (PAN) Personal Area Network

La plus petite étendue de réseau. Elle désigne une interconnexion d'équipements informatiques dans un espace de dizaine de mètres. [4]

I.4.2 Le réseau local (LAN)

Local Area Network ; est un réseau local d'entreprise constitué d'ordinateurs et de périphériques reliés entre eux et implantés dans une même entreprise, et à caractère privé.

- Il ne dépasse pas généralement une centaine de machines.
- Le partage des ressources est ici fréquent et les vitesses de transmission vont de 10 à 100/s. [1]

I.4.3 Le réseau métropolitain (MAN)

Metropolitan Area Network Réseau métropolitain ou urbain. Il est nommé aussi le réseau fédérateur correspond à la réunion de plusieurs réseaux locaux (LAN) à l'intérieur d'un même périmètre d'une très grande entreprise ou d'une ville par ex, pouvant relier des points distants de 10 à 25 Km. [4]

I.4.4 Le réseau étendu (WAN)

Wide Area Network ; réseau grande distance. Il s'agit cette fois d'un réseau multi-services couvrant un pays ou un groupe de pays, qui est en fait constitué d'un ensemble de réseaux locaux interconnectés.

- Un WAN peut être privé ou public, et les grandes distances qu'il couvre plusieurs centaines de kms. [1]

I.4.5 Réseaux sans fil (Wireless networks)

Il est caractérisé par deux types

Connexion point à point ; Par une interface réseau sans fil, deux nœuds peuvent communiquer directement on parle également de liaison de type pair à pair (Peer to peer) ou ad hoc. Une telle configuration est possible dans les techniques Bluetooth ou Wi-fi.

Connexion multi-point ; Un élément centralisateur comme le (AP –Access point) point d'accès et wi-fi centralise les communications .Il permet également l'interconnexion avec le réseau filaire local.

- Avantages ; installation simple, facilité de déploiement, faible cout d'appartenance,
- Inconvénients ; débit de 1 à 2 Mb/s, taux d'erreurs élevé, sécurité, interférences. [4]

I.5 Topologie physique des réseaux

L'organisation physique concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile ...).

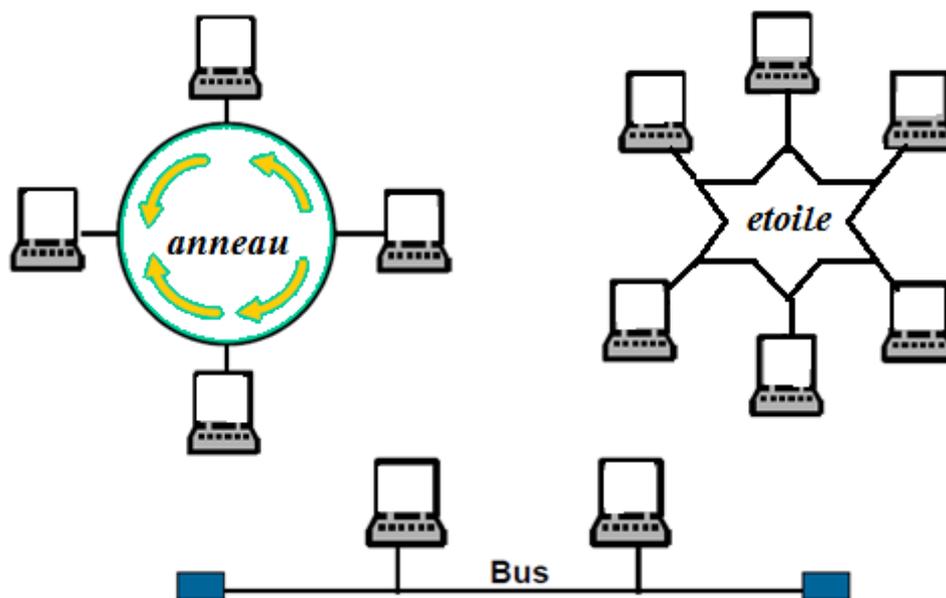


Figure I. 1 : Topologie physique des réseaux.

I.5.1 La topologie en bus (le support linéaire)

Un réseau de type bus est ouvert à ses extrémités. Chaque PC y est connecté par l'intermédiaire d'un connecteur spécial. Certains périphériques, comme des imprimantes, peuvent également être directement reliés au réseau. Ils doivent alors comporter une carte adaptateur réseau.

- Avantages ; simple à mettre en œuvre ; peu coûteux.
- Inconvénient : s'il y a rupture du câble, tout le réseau tombe en panne. [1]

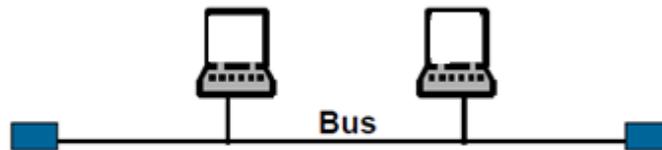


Figure I. 2: La topologie en bus.

I.5.2 La topologie en étoile

Dans un réseau en étoile, chaque nœud du réseau est relié à un contrôleur (ou hub) par un câble différent. Le contrôleur est un appareil qui recevant un signal de données par une de ses entrées, va retransmettre ce signal à chacune des autres entrées sur lesquelles sont connectés des ordinateurs ou périphériques, voir d'autres contrôleurs.

- Avantage ; un nœud peut tomber en panne sans affecter les autres nœuds du réseau.
- Inconvénients ; plus coûteux, longueur du câblage est important ; panne du contrôleur provoque la déconnexion du réseau. [1]

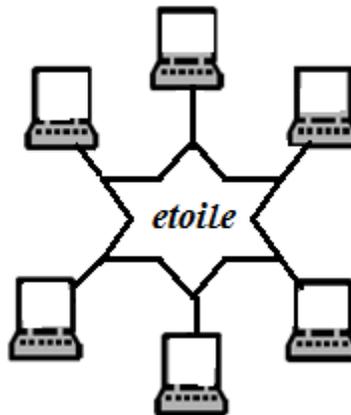


Figure I. 3: La topologie en étoile.

I.5.3 La topologie en anneau

Cette topologie repose sur une boucle fermée, en anneau (ring), constitué de liaisons point à point entre périphériques. Les trames transitent par chaque nœud, qui se comporte comme un répéteur (élément actif). Les concentrateurs en anneau permettent l'insertion de station dans un réseau. [4]

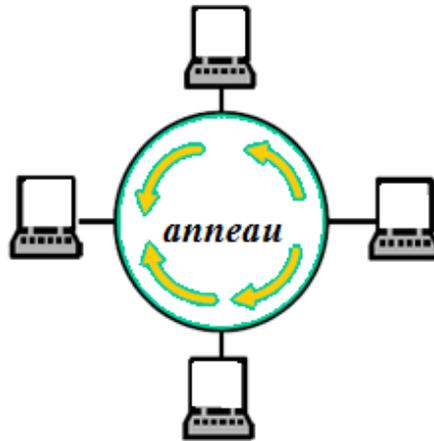


Figure I. 4: La topologie en anneau.

I.5.4 La topologie en arbre

Dans l'architecture en arbre, les postes sont reliés entre eux de manière hiérarchique, à l'aide de concentrateurs (stackable hubs), cette connexion doit être croisée. [4]

Les topologies dérivées :

I.5.5 La topologie en maillage

On parlera de réseau maillé lorsqu'il s'agit de décrire une architecture constituée de topologies mixtes, par exemple Internet. [4]

I.5.6 La topologie bus en étoile

Les éléments actifs du réseau, sur lesquels sont connectés les postes de travail, peuvent être reliés entre eux par un bus. [4]

I.5.7 La topologie anneau en étoile

Est la liaison de plusieurs anneaux entre eux.

Choix de la topologie réseau adaptée

Les réseaux locaux de bureau sont désormais standardisés, dans les protocoles utilisés comme dans les topologies. L'étoile est la norme, avec une connexion directe des postes de travail et serveurs à des commutateurs. Bien sûr, ceux-ci sont reliés entre eux, très souvent par des bus en fibres optiques. On trouve la topologie bus dans les réseaux industriels. [4]

I.6 Architectures des réseaux informatiques (rôle)

Les réseaux informatiques peuvent aussi être catégorisés par la relation fonctionnelle (le rôle) entre les équipements. On distingue par exemple :

I.6.1 L'architecture client/serveur

Qui centralise des ressources sur un serveur qui offre des services pour des clients. Le réseau Internet, basé sur cette architecture, peut être vu comme un réseau de services composés

exclusivement de serveurs. L'architecture client/serveur désigne un mode de communication à travers un réseau entre plusieurs programmes ou logiciels :

Le processus client envoie des requêtes pour demander un service.

Le client (le navigateur sur notre ordinateur) émet une requête vers le serveur grâce à son adresse et le port qui désigne un service particulier du serveur.

Le processus serveur attend les requêtes des clients et y répond en offrant le service.

Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

Le navigateur, sur la machine cliente interprète le code renvoyé par le serveur et l'affiche

Par extension, le client désigne également l'ordinateur sur lequel est exécuté le logiciel (processus) client, et le serveur, l'ordinateur sur lequel est exécuté le logiciel (processus) serveur. [5]

I.6.6.1 L'architecture à deux (02) niveaux

Dans une architecture deux tiers (niveaux), encore appelée client-serveur de première génération ou client-serveur de données, le poste client se contente de déléguer la gestion des données à un serveur spécialisé. Le cas typique de cette architecture est une application de gestion fonctionnant sous Windows ou Linux et exploitant un SGBD centralisé. [5]

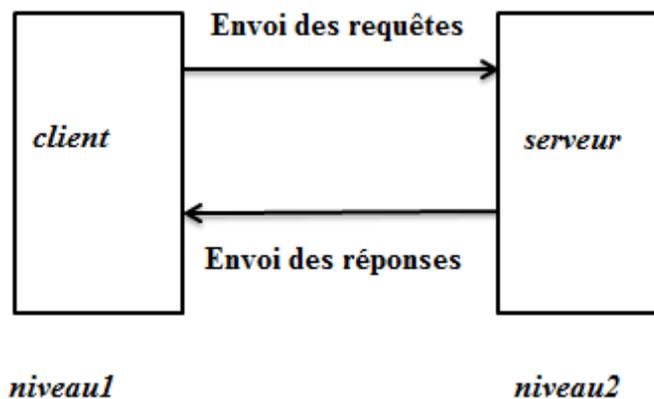


Figure I. 5: L'architecture client/serveur à deux niveaux.

I.6.1.2 L'architecture client-serveur à trois (3) niveaux

Cette architecture également appelée client-serveur de deuxième génération ou client-serveur distribué sépare l'application en 3 niveaux de services distincts :

- Premier niveau : l'affichage et les traitements locaux (contrôle de saisie, mise en forme de données ...) sont pris en charge par le poste client.
- Deuxième niveau : les traitements applicatifs globaux sont pris en charge par le service applicatif.
- Troisième niveau : les services de base de données sont pris en charge par un SGBD. [5]

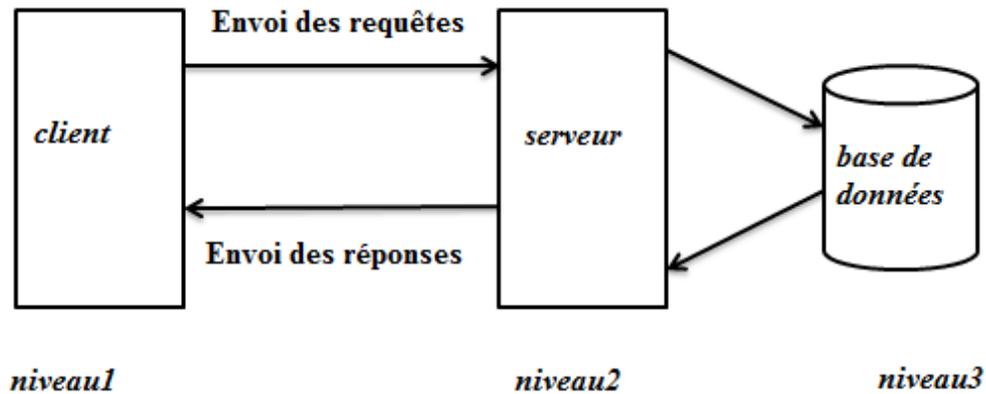


Figure I. 6: Architectures client/serveur à trois niveaux.

I.6.2 L'architecture poste à poste ou pair-à-pair (peer-to-peer)

Qui permet de partager simplement des fichiers le plus souvent, mais aussi des flux multimédia continus (streaming) ou du calcul réparti. Les systèmes peer-to-peer permettent une décentralisation des systèmes, en permettant à tous les ordinateurs de jouer le rôle de client et de serveur. (Tous sont client tous sont serveur). [5]

I.7 Le modèle de référence OSI

(Open System Interconnexion) Le modèle OSI propose le découpage de la communication en 7 couches, afin de permettre de normaliser les méthodes d'échange entre deux systèmes. Chaque couche a un rôle bien particulier et communique sur requête (sur demande) de la couche supérieure en utilisant des services de la couche inférieure (sauf pour la couche physique).

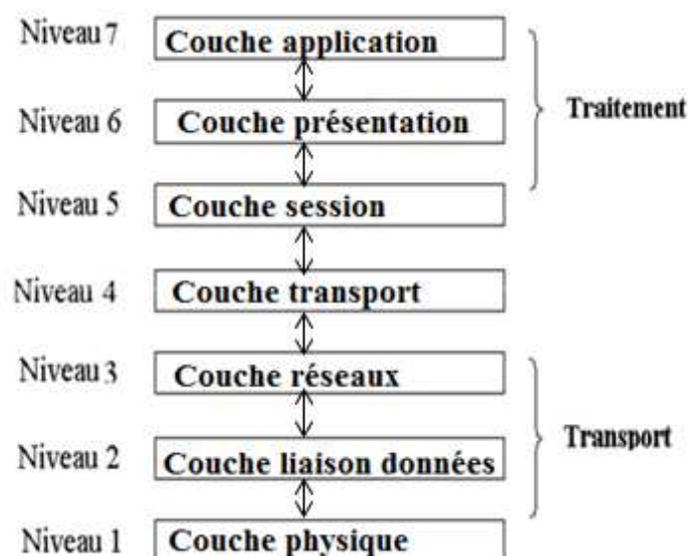


Figure I. 7: Le modèle de référence OSI.

I.7.1 La couche physique

Elle assure le transfert de bits, on trouve dans cette couche : l'étude des interfaces de connexion et l'étude des modems, des multiplexeurs et concentrateurs [4]

I.7.2 La couche liaison de données

Elle est responsable de l'acheminement d'unités de données appelées trames en assurant la meilleure qualité de transmission possible, le protocole standard est HDLC. [4]

I.7.3 La couche réseaux

Ce niveau permet l'interconnexion des réseaux physiques différents, dans le modèle TCP/IP, il constitue la deuxième couche nommée internet, elle transporte des unités de taille fixe appelées paquets exemple de protocoles standards : X25 et IP. [4]

I.7.4 La couche transport

Elle constitue les applications de types client/serveur utilisant TCP/IP peuvent utiliser deux modes de transport ; connecté grâce à TCP, non connecté, ou datagramme, avec UDP.

-Transport des unités de données appelées messages. [4]

I.7.5 La couche session

Cette couche gère également un mode connecté, à ce niveau que sont gérés les points de synchronisation. [4]

I.7.6 La couche présentation

Elle assure la mise en forme des données, des paramètres internationaux, pages de code et format divers. Cette couche peut également exploiter des fonctions de chiffrement et de compression, des codages comme MIME (Multipurpose Internet Mail Extension), ASCII (American Standard Code for Information Interchange), c'est typiquement le rôle du langage HTML. [4]

I.7.7 La couche application

Elle assure l'interface de communication avec l'utilisateur, à travers des logiciels adéquats, elle gère également la communication entre applications, comme pour le courrier, SSH... [4]

I.8 Le modèle TCP/IP

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qu'on utilise "par-dessus" un protocole réseau, IP (Internet Protocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP. [6]

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

I.8.1 La couche hôte réseau

Cette couche est assez étrange. En effet, elle regroupe les couches physiques et liaison de données du modèle OSI. En fait, elle n'a pas vraiment été spécifiée ; la seule contrainte de cette couche, c'est de permettre un hôte d'envoyer des paquets IP sur le réseau. L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche hôte-réseau. [6]

I.8.2 La couche internet

Cette couche est la clé de voûte de l'architecture. Cette couche réalise l'interconnexion des réseaux distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement de ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

La couche internet possède une implémentation officielle : le protocole IP. [6]

I.8.3 La couche transport

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation. Officiellement, cette couche n'a que deux implémentations : le protocole TCP et le protocole UDP. [6]

I.8.4 La couche application

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage que les logiciels réseau n'utilisent que très rarement ces 2 couches, et finalement, le modèle OSI dépouillé de ces 2 couches ressemble fortement au modèle TCP/IP. Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol). Le point important pour cette couche est le choix du protocole de transport à utiliser. [6]

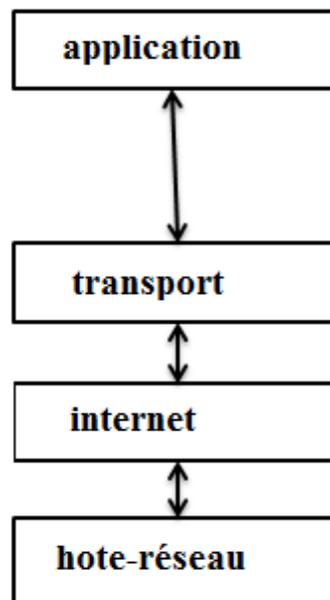


Figure I. 8: Le modèle TCP/IP.

I.9 L'internet

Internet est un ensemble de réseaux interconnectés utilisant une suite protocolaire appelée TCP/IP (Transmission Control Protocol/Internet Protocol) pour échanger des informations à travers le monde. En termes simples : Internet est un immense réseau d'ordinateurs qui peuvent communiquer entre eux en utilisant TCP/IP. [6]

I.9.1 Les services offerts par l'internet

Sur le plan pratique, Internet est un outil capable de nous rendre un certain nombre de services. Ces services sont réalisables à travers les différents protocoles de l'Internet (Les protocoles de la couche application TCP/IP).

- **IRC** (Internet Relay Chat) : pour discuter en direct (chat) avec des gens du monde entier. Le dialogue s'effectue par échange de texte, mais il est possible de dialoguer aussi en temps réel avec la voix et la vidéo (vidéoconférence).
- **Http** (ou *World Wide Web* ou *www* ou tout simplement le *web*) pour accéder à des pages web. Le web est l'application Internet la plus populaire. Grâce à un navigateur web (browser), un utilisateur (internaute) peut lire des pages web stockées sur un ordinateur serveur situé n'importe où dans le monde.
- **Ftp** (File Transfert Protocol) pour le transfert électronique de fichiers entre des machines distantes. Avec FTP on peut charger des fichiers sur des ordinateurs serveurs connectés à Internet, ou télécharger des fichiers sur le poste client. [6]
- **Telnet** (Connexion à un ordinateur distant) : tout utilisateur d'Internet peut travailler à distance sur une machine, sur laquelle il dispose d'un compte utilisateur et dont il a

accès. Il peut utiliser Telnet ou d'autres programmes de contrôle à distance (rlogin, rsh...)

- **SMTP, POP et IMAP:** pour la messagerie électronique (ou mail)
- **SMTP** (Simple Mail Transfer Protocol) pour l'envoi du courrier.
- **POP** (Post Office Protocol) permet à l'utilisateur de récupérer les messages qu'il a reçu sur le serveur de messagerie hébergeant sa boîte aux lettres en les déplaçant sur son ordinateur local.
- **IMPAP** (Internet Mail Access Protocol) un autre protocole qui permet aussi de consulter notre boîte aux lettres sur le serveur de messagerie.

La boîte aux lettres est aussi un moyen de stockage de courrier et les pièces jointes (les fichiers joints aux différents mails). [6]

I.9.2 Avantages de l'internet

- Accès à l'information d'une manière continue et à partir de n'importe quel point du monde et ce pour un coût d'accès limité.
- Communication sous toutes formes (d'une personne à une autre, d'une personne à un groupe, d'un groupe à un autre, d'un groupe à une personne) à partir d'un même outil.
- Échanger tous types de données numérisées (documents, dessins, photos, son, vidéo, logiciels, etc.).
- Permettre le commerce électronique grâce à des échanges sécurisés.
- Permettre l'enseignement/apprentissage à distance en synchrone ou en asynchrone. [6]

I.9.3 Fonctionnement de l'internet

Internet est un réseau basé sur le modèle client / serveur :

- L'ordinateur client, utilise un logiciel spécifique (le navigateur : par exemple Google Chrome, Mozilla Firefox ou Microsoft Internet explorer) pour aller chercher l'information numérique auprès d'un autre ordinateur distant : le serveur.
- Le serveur, ou hôte, stocke les données numériques sur des disques durs et les envoie, à la demande, sur l'ordinateur client. [6]

I.10 Les protocoles de communication (la topologie logique)

Un protocole est un ensemble de règles et des conventions décrivant la syntaxe et la sémantique des messages échangés et la façon dont la transmission se déroule. [1]

I.10.1 Le protocole TCP/IP

La famille TCP/IP, comportant plusieurs dizaines de protocoles, définit un modèle en quatre (4) couches réseau, il s'agit des protocoles de communication et d'application les plus populaires pour connecter des systèmes hétérogènes, indépendamment de la couche physique.

TCP (Transmission Control Protocol) est un protocole de transport qui assure un service fiable, orienté connexion pour un flot d'octets, il permet de s'assurer de la bonne arrivée de toutes les informations, en contrepartie, cette fonction peut ralentir la communication. TCP complète les manques de IP en assurant une fiabilisation du service, pour cela, un accusé de réception (ACK-Acknowledgement) répond systématiquement aux paquets. [4]

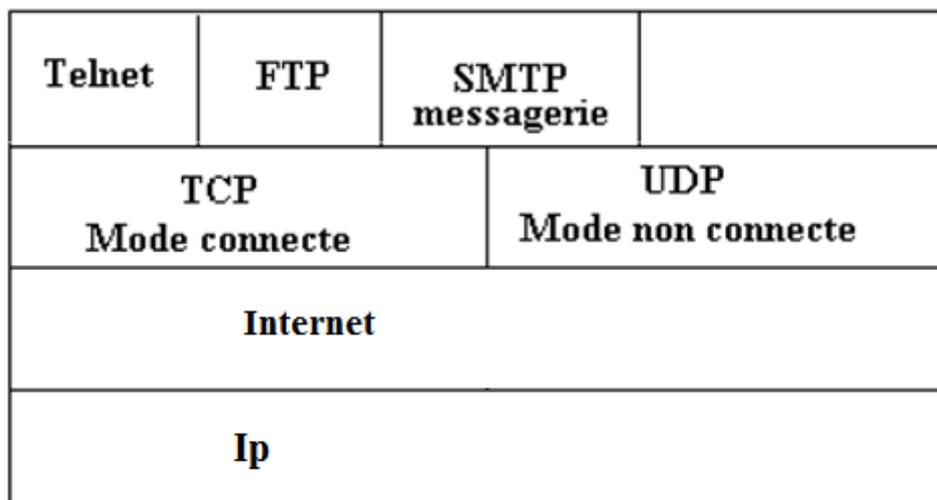


Figure I. 9: L'architecture TCP/IP.

I.10.2 IP (Internet Protocol)

Il fournit un système de livraison de paquet, sans connexion et non fiable, il gère des adresses logiques, qui décomposent l'identifiant de chaque nœud en un numéro de réseau logique et un numéro de périphérique sur quatre (4) octets (en IP version 4).

I.10.3 Le protocole UDP (User Data Protocol)

Contrairement à TCP, UDP n'assure pas de connexion et reporte le processus de fiabilisation à la couche supérieure (applicative), il fonctionne en mode non connecté, ce qui permet de gagner un débit pour les transmissions gourmandes, telles que vidéos et sons, il est donc très rapide mais surtout plus fiable. [4]

I.10.4 Le protocole BOOTP

Il constitue une évolution de RARP (Reverse Adresse Resolution Protocol), et de BOOTPARAM, autorisant la fourniture d'autres paramètres que la seule adresse IP. [4]

I.10.5 Le protocole DHCP

(Dynamic Host Configuration Protocol) : constitue une évolution de BOOTP, en ce sens, qu'il permet aussi au client d'envoyer des informations au serveur, de plus contrairement à BOOTP, qui gère pas de durée d'acquisition de paramètres TCP/IP, DHCP est capable d'associer des paramètres pendant une durée donnée. [4]

I.10.6 Le protocole HTTP

Hyper Text Transfer Protocol, il s'agit d'une norme régissant les échanges (demande d'un document, envoi d'informations, envoi d'un document) entre un client web (navigateur) et un serveur web. HTTP est un protocole texte (sur 8 bits) qui utilise une liaison TCP pour la communication entre le client et le serveur.

Le client établit une connexion TCP Avec le serveur web (souvent sur le port 80) et émet une demande de document en se servant de l'instruction GET du protocole http.

Le serveur reçoit la demande, l'examine et en cas de succès retourne le document demandé. [4]

I.11 Gestion de la communication

La circulation des informations sur le réseau, le type de transmission et le partage du média sont des aspects importants de l'architecture.

I.11.1 Sens de transmission

Il existe différentes directions du flot de données selon le support de transmission et des techniques utilisées. [4]

I.11.1.1 Le mode simplex

Ce mode n'exploite qu'un seul sens de transfert de l'information, il correspond généralement à l'usage d'un seul émetteur pour n récepteurs (l'émission de programmes radio).

La fibre optique ne permettant que le mode simplex, au moins deux fibres sont utilisées, en multi mode, pour permettre une communication bidirectionnelle. [4]

I.11.1.2 Le mode half- duplex

Les deux sens de communication sont alternés, chaque interface étant successivement émettrice et réceptrice.

Le câble coaxial représente un bon exemple de support half-duplex. [4]

I.11.1.3 Le mode full-duplex

Les deux extrémités peuvent être transmettre simultanément (les communications téléphoniques).

Le support filaire pair torsadé est un média de transmission full-duplex. Une carte réseau connectée à l'équipement adéquat peut utiliser simultanément une paire de fils pour l'émission et une autre pour la réception. [4]

I.11.2 Les types de transmission

Les données transmises doivent être synchronisées par le récepteur afin d'être lues, pour cela plusieurs types de transmission peuvent être utilisés :

I.11.2.1 Le type synchrone

Une horloge pour transmettre à flots continus. [4]

I.11.2.2 Le type asynchrone

Permettant de gérer un échange imprévisible ou occasionnel, débutant par un bit de démarrage. [4]

I.11.3 Les méthodes d'accès au support

Sur un canal point à point, un émetteur peut transmettre librement. En revanche, lorsque le support est partagé par plusieurs périphériques, il est nécessaire de gérer la façon dont les données sont échangées, ces échanges dépendent de l'architecture réseau, c'est-à-dire de la topologie logique, une méthode d'accès décrit les règles qui régissent pour chaque matériel, l'accès, la transmission et la libération du canal partagé. On distingue essentiellement trois méthodes : la contention, le polling et le jeton passant. [4]

I.11.3.1 La contention

Les deux implémentations les plus répandues de contention sont CSMA/CD et CSMA/CA, CSMA correspond à l'écoute de la porteuse (Carrier Sense) sur un support partagé (Multiple Access).

Les deux mises en œuvre se distinguent par le fait que l'une détecte les collisions (Collision Detection), et l'autre tente de les éviter (Collision Avoidance).

CSMA/CD correspond à l'implémentation Ethernet, tandis que CSMA/CA elle est adoptée par la norme 802.11 (wi-fi).

- Avantages ; le principal avantage de cette gestion du support est sa simplicité.
- Inconvénients ; la méthode n'est pas déterministe, car le temps d'accès au canal n'est pas prévisible, de plus aucune gestion de priorité n'est possible pour des matériels qui ont besoins d'accéder rapidement au support partagé. [4]

I.11.3.2 L'interrogation (polling)

Ici, un équipement du réseau est désigné comme administrateur de l'accès au canal, ce matériel, le maître interroge dans un ordre prédéterminé chacun des autres nœuds et leur demande s'ils ont des informations à transmettre.

Souvent, le maître est un concentrateur et les matériels secondaires sont les nœuds de l'étoile.

- Avantages ; l'avantage de cette méthode est que tous les accès au canal sont centralisés.

Le temps d'accès et le volume des données manipulées sur le support sont prévisible et fixés.

- Inconvénients ; elle utilise une partie de la bande passante du réseau pour émettre des messages de gestion (interrogations, avertissements, acquittements...), ce qui est coûteux en bande passante. [4]

I.11.3.3 Le jeton passant

Dans cette méthode, les trames circulent de poste en poste, chacun se comportant comme un répéteur. Ce jeton est en quelque sorte un message d'autorisation, qui offre l'exclusivité du support à la station qui le possède. Il existe plusieurs normes à jeton passant, sur des topologies en anneau (IEEE 802.5, Token Ring ou FDDI), aussi sur des topologies en bus (IEEE 802.4), on trouve encore des réseaux implémentant Token Ring ou FDDI. [4]

- Token ring ; l'anneau à jeton, plus connu internationalement sous le terme de Token Ring, est un protocole de réseau local qui fonctionne sur la couche *Liaison* du modèle OSI. Il utilise une trame spéciale de trois octets, appelée jeton, qui circule dans une seule direction autour d'un anneau. Les trames Token Ring parcourent l'anneau dans un sens qui est toujours le même. [5]
- FDDI ; Fiber Distributed Data Interface (FDDI) est un type de réseau informatique LAN ou MAN permettant d'interconnecter plusieurs LAN à une vitesse de 100 Mbit/s sur de La fibre optique (ce qui lui permet d'atteindre une distance maximale de 200 km). La technologie LAN FDDI est une technologie d'accès au réseau sur des lignes de type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit primaire, l'autre, permettant de rattraper les erreurs du premier, est dit secondaire). FDDI est un protocole utilisant un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance). Le jeton circule entre les machines à une vitesse très élevée. Si celui-ci n'arrive pas au bout d'un certain délai, la machine considère qu'il y a eu une erreur sur le réseau. [5]

La topologie FDDI ressemble de près à celle de token ring à la différence près qu'un ordinateur faisant partie d'un réseau FDDI peut aussi être relié à un concentrateur MAU (Media Access Unit) d'un second réseau. [5]

- Ethernet

Ethernet est un protocole de réseau local à commutation de paquets. Depuis les années 1990, on utilise très fréquemment Ethernet sur paires torsadées pour la connexion des postes clients, et des versions sur fibre optique pour le cœur du réseau. Tous les ordinateurs d'un réseau Ethernet sont reliés à une même ligne de transmission, et la communication se fait à l'aide d'un protocole appelé CSMA/CD. Avec ce protocole toute machine est autorisée à émettre sur la ligne à n'importe quel moment et sans notion de priorité entre les machines. Cette communication se fait de façon simple :

- Chaque machine vérifie qu'il n'y a aucune communication sur la ligne avant d'émettre

Si deux machines émettent simultanément, alors il y a collision (c'est-à-dire que plusieurs trames de données se trouvent sur la ligne au même moment)

- Les deux machines interrompent leur communication et attendent un délai aléatoire (9,6 μ s pour l'Ethernet 10 Mbps), puis la première ayant passé ce délai peut alors réémettre

Ce principe est basé sur plusieurs contraintes :

Les paquets de données doivent avoir une taille maximale (64 octets) et il doit y avoir un temps d'attente entre deux transmissions. [5]

I.12 Les principes de la sécurisation des réseaux

La sécurité réseau s'appuie sur quatre thèmes clés :

I.12.1 L'authentification

Permettant de s'assurer de l'identité pour connaître l'origine des opérations.

I.12.2 La confidentialité

Qui a pour but d'éviter toute divulgation d'information.

I.12.3 L'intégrité

Pour interdire ou connaître les modifications et se préserver des pertes d'informations.

I.12.4 La disponibilité

Qui permet d'assurer un service en toutes circonstances. [4]

I.13 Conclusion

Les réseaux informatiques constituent un domaine vaste, qu'il est bien souvent difficile d'appréhender parce que le sujet sous-tend de nombreux domaines techniques complexes, qui œuvrent dans des directions divergentes.

Même si la complexité est un problème majeur pour l'apprentissage de nouvelles notions ou le renforcement des connaissances, il n'en reste pas moins qu'une décomposition des problèmes, associée à des nombreuses illustrations, permet d'aborder facilement de ces notions.

Le chapitre suivant présentera la gestion électronique des documents.

**GESTION
ELECTRONIQUE
DES DOCUMENTS**

CHAPITRE II : GESTION ELECTRONIQUE DES DOCUMENTS

II.1 Introduction

La gestion électronique des documents est aujourd'hui une réalité qui touche de nombreux organismes, dont les centres de documentation qui se lancent dans des opérations de numérisation de leurs fonds documentaires. Et l'on constate une grande variété de ces projets de gestion électronique qui résultent d'objectifs différents et de choix techniques variés.

Une entreprise acquiert et produit tout au long de son activité un grand nombre de documents. Certains sont vitaux (les titres de propriété ou les contrats), et doivent être conservés pour répondre à l'environnement réglementaire. D'autres encore, les documents dits « de travail » tels que les comptes-rendus, les rapports, les documents bureautiques, peuvent être consultés dans le but de prendre une décision. Par conséquent, la gestion et la conservation des documents au sein de l'entreprise sont des activités essentielles. Elles répondent à des objectifs d'ordre juridique et légal, à des enjeux patrimoniaux (constituer une mémoire d'entreprise et conserver les documents relatifs à l'histoire et à l'activité de l'entreprise) et à des enjeux stratégiques.

Les premières solutions développées pour permettre la gestion des documents produits dans l'entreprise ont été les tableurs ou les systèmes de gestion de bases de données (SGBD). Ceux-ci rendaient possible le traitement de documents externes au système de gestion, le plus souvent papiers : catalogues de bibliothèque, bases de références. [7]

II.2 Définition

Dans le Dictionnaire encyclopédique de l'information et de la documentation, Jacques Chaumier définit la GED ou Gestion Electronique de Documents comme un « ensemble de logiciels concourant à réaliser les diverses étapes de la chaîne de traitement d'un document : acquisition, restitution, diffusion ». Un système de GED est donc une application logicielle qui vise à gérer, organiser dématérialiser, stocker et distribuer des informations documentaires produites par l'entreprise sous forme électronique. [7]

II.3 Objectif de la gestion électronique des documents

D'un point de vue stratégique, la mise en place d'une solution de GED rend possible une rationalisation des flux d'informations et donc un gain de temps. Elle permet notamment de :

- faciliter l'accès aux documents par les membres de l'entreprise,
- localiser plus rapidement l'information,
- éviter la perte de documents,
- éviter le redoublement des processus.

La GED présente également de nombreux avantages pour la production de documents de manière collaborative. Couplée avec une fonctionnalité de Workflow¹, une solution de GED permet d'optimiser le processus d'édition des documents. [7]

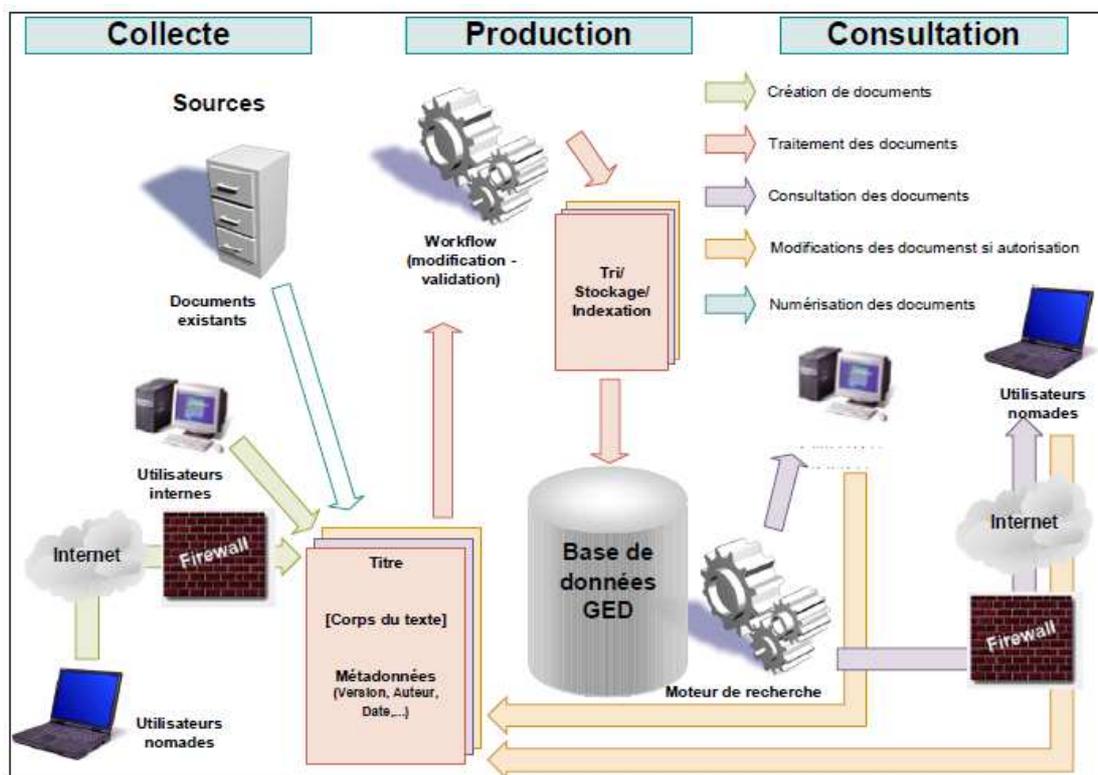


Figure II. 1: Architecture d'une solution de la gestion électronique de documents.

II.4 Les étapes de la chaîne de (GED)

Pourquoi parler de cycle de vie du document numérique ? Le document numérique s'impose de plus en plus dans les entreprises (qu'elles soient publiques ou privées). Il est donc nécessaire de s'interroger sur la gestion de ces documents au fil du temps. Le document numérique ne se traite pas comme un document papier. Il nécessite un ensemble de procédures adaptées. [7]

L'Aproged (Association des Professionnels de la GED) dans son référentiel *La maîtrise du cycle de vie du document numérique*, définit 4 grandes étapes présentées ci-dessous :

II.4.1 La création

La création du document numérique : Il peut être le résultat d'un traitement automatisé (création directement sous forme numérique), ou le résultat d'une numérisation de documents papiers. Dans

¹ Un **workflow** : anglicisme pour flux de travaux, est la représentation d'une suite de tâches ou opérations effectuées par une personne, un groupe de personnes, un organisme, etc. Le terme flow (flux) renvoie au passage du produit, du document, de l'information, etc. d'une étape à l'autre.

ce cas, il est nécessaire d'avoir des consignes pour la création et la mise en forme du document pour pouvoir en garantir l'exploitation ultérieure. [7]

L'enregistrement : On parle également de copie numérique. Cette phase correspond à la mémorisation du document pour des utilisations ultérieures (conservation, diffusion, archivage) ; on peut également inclure un système de workflow lors de l'enregistrement. [7]

Le classement : Il est nécessaire de ranger le document dans un espace informatique (serveur, disque de stockage,...) accessible aux utilisateurs. L'organisation du classement doit être compatible avec le plan de classement. [7]

L'indexation : L'indexation d'un document consiste à décrire celui-ci pour permettre son exploitation. C'est une des étapes cruciales de la GED. Elle doit être la représentation la plus fidèle et la plus exhaustive du contenu, du sens du document afin de faciliter les recherches et d'en garantir la pertinence. Il est important de concevoir une politique d'indexation (construction des index et leur maintenance dans de grandes bases documentaires). Cela va conditionner le bon fonctionnement de la GED.

Il existe deux grandes catégories d'indexation :

- l'indexation classificatoire : consiste à donner une description externe et synthétique du document. Elle n'est pas adaptée pour l'indexation de documents numériques destinés à un système de GED.
- l'indexation par concepts ou par langages combinatoires : consiste à donner une description du contenu du document. Elle se veut riche, exhaustive et dépassant la rationalité parfois trop univoque de la classification. [7]

II.4.2 La gestion

La gestion concerne les opérations qui interviennent sur le document après sa création. On parle souvent de sécurité et de droits d'accès ; cela peut passer par des opérations de cryptage, de restriction d'actions sur le contenu ou d'occultation de champs. Il s'agit de rendre le document accessible aux personnes autorisées. Le document numérique étant facilement reproductible et modifiable, il est également nécessaire de pouvoir gérer les différentes versions de ce document. [7]

II.4.3 La diffusion

On distingue deux techniques de restitution du document :

- le mode push : c'est la mise à disposition des documents que l'utilisateur va chercher dans la base. Il doit alors se connecter au système de GED. Il lui est possible de visualiser les documents après une recherche et une sélection (si celui-ci est autorisé à accéder au document).

- le mode pull : c'est la distribution du document. Le système transfère automatiquement les documents (souvent par la messagerie électronique) à des destinataires qui sont désignés préalablement. Il faut alors bien gérer les listes de diffusion (changement d'adresses électroniques, départ de l'entreprise, ...) pour que les bonnes personnes puissent avoir les bons documents. [7]

II.4.4 La conservation

L'objectif de la conservation des documents est de prouver, de mémoriser, de comprendre et de communiquer. Il faut donc conserver dans le temps la lisibilité des documents numériques et de ses composants. Cela implique un choix de formats judicieux. [7]

II.5 Méthodologie de mise en place

La mise en place d'une solution de gestion documentaire est souvent abordée selon une approche uniquement technique. Or, le système de GED mis en place va avoir un impact sur l'organisation et la définition des tâches dans l'entreprise : il va modifier les modes de travail, le processus de production et d'accès aux documents, les relations entre les services. Il est également nécessaire de prendre en considération l'environnement technique et juridique de mise en œuvre. [7]

II.6 Les types de la GED

On distingue cinq(05) types de GED :

II.6.1 La GED bureautique

Cette GED gère les documents bureautiques de l'entreprise. Elle vient compléter les applications bureautiques, et intervient au niveau des échanges et des flux entre les postes de travail producteurs.

Ce type de GED doit présenter les caractéristiques suivantes :

- La GED doit être fortement intégrée à l'environnement de productivité. C'est un élément fédérateur des échanges, car elle se trouve au niveau de la gestion et de la traçabilité des flux. Elle permet notamment la gestion de l'archivage des documents ainsi que le contrôle des différentes versions d'un document.
- Elle doit permettre une indexation rapide au moment de la production du document.
- Elle doit également gérer les documents vivants, et faire à tout moment un lien vers le document natif.
- Elle intègre des fonctions de messagerie, d'annotations, de workflow. [7]

II.6.2 La GED documentaire

Ce type de GED gère les documents de référence de l'entreprise. Elle permet de conserver la mémoire de l'activité de l'organisme.

Elle nécessite un langage d'indexation (thésaurus). Ce langage doit être assez générique afin d'être partagé par tout le monde, mais aussi spécifique pour que le moteur de recherche soit pertinent et précis. Le rôle du professionnel de l'information prend toute son ampleur ici dans la construction d'un langage d'indexation. [7]

II.6.3 La GED administrative

Elle consiste à numériser puis à classer les divers documents administratifs (factures, fiches techniques, bons de commande, formulaires, devis,...). Ces fichiers numérisés pourront être classés et conservés sur différents supports numériques. Ils pourront être éventuellement diffusés via le réseau interne de l'entreprise. [7]

II.6.4 La GED COLD (Computer Output on Laser Disc)

Elle permet d'archiver sous une forme électronique les états produits par l'informatique d'un organisme (relevés de compte, factures...). [7]

II.6.5 La GED technique

La GED technique ou GED métier qui concerne la manipulation de documents dont le format et le contenu sont propres à un métier (plans, schémas etc..). [7]

II.7 Les principes de la GED

II.7.1 Stockage de l'information

Une fois numérisés, les documents sont stockés et indexés selon des règles déterminées au préalable. [8]

II.7.2 Accès à l'information

Ils sont alors accessibles, selon une thématique, en recherche par mots clés ou en recherche intégrale. [8]

II.7.3 Echange de documents

La facilité d'échange offerte par la dématérialisation n'est pas le seul avantage. En un même instant, plusieurs correspondants peuvent tout à fait travailler autour d'un même document en des lieux différents. [8]

II.8 Les différentes catégories de logiciels de GED

II.8.1 Les logiciels GED d'entrée de gamme

Ils ne représentent actuellement qu'une très infime partie du marché, mais touche un très large public du fait de leur prix attractifs. Ils correspondent en général à des solutions monopostes destinées à des entreprises artisanales ou individuelles. La majeure partie de ces applications ne fonctionnent qu'avec des scanners de bureau et ne permettent de saisir qu'un nombre limité de documents par jour. [8]

II.8.2 Les logiciels GED à composants

Cette catégorie recouvre des modules logiciels intégrables à des applications au travers d'outils de développement (Visual C++) ou d'API (Application Programming Interface, une « interface de programmation applicative).

Ces modules : numérisation, reconnaissance optique de caractères, indexation automatique et lecture de codes à barres sont destinés aux programmeurs ou aux sociétés de services informatiques désirant ajouter des fonctions de GED à leurs logiciels. [8]

II.8.3 Les logiciels GED génériques

Ce sont des solutions s'intégrant en complément des applications informatiques, bureautiques, documentaires, et transactionnelles. Ils sont disponibles pour de nombreux systèmes d'exploitation et s'intègrent généralement dans une architecture client/serveur, en connexion ou non avec l'informatique centrale. Ils jouent le rôle de fédérateur au sein du système de gestion d'informations de l'organisation. [8]

II.9 Analyse du logiciel

La mise en place d'une solution de GED passe par l'analyse du logiciel. Plusieurs éléments doivent être analysés :

II.9.1 Les fonctionnalités offertes

Acquisition et/ou création de document, stockage et archivage, recherche, consultation des documents, diffusion, fonctions spécifiques à l'entreprise. [9]

II.9.2 L'architecture technique

Relations stations serveur / stations clientes, réseau, protocole, développement spécifique du logiciel de GED, intégration à l'environnement bureautique. [9]

II.9.3 L'offre de service de l'éditeur

Paramétrage, installation, formation, maintenance, support technique, reprise de l'existant, conception d'un thésaurus, numérisation. [9]

II.9.4 Le coût

- Prix des licences, du développement, des services.
- Implantation de la société de services (pour les logiciels libres), de l'éditeur (pour les logiciels propriétaires).
- Références de la société de services ou de l'éditeur et les sites installés.
- Politique de mise à jour. [7]

II.10 Avantages de la GED

La mise en place d'une GED dans une entreprise présente notamment les avantages suivants :

II.10.1 Accès rapide et à distance aux documents

Le réseau permet l'accès à la base de GED et rend possible une consultation immédiate des documents. [9]

II.10.2 Base unique pour l'ensemble des documents de l'entreprise

Les documents produits dans l'entreprise sont tous stockés dans une même base, prévenant ainsi le risque d'une dispersion des documents. [9]

II.10.3 Conservation des documents

Le système de GED garantit la conservation des documents produits dans l'entreprise, et assure la pérennité dans l'accès aux documents. [9]

II.10.4 L'organisation de l'information

La GED est un moyen d'organisation de l'information documentaire, elle constitue un outil de dématérialisation qui limite la masse importante de papiers présentent dans les organisations, elle garantit l'homogénéité du support documentaire et permet de standardiser les documents. [9]

II.10.5 La gestion du cycle de vie des documents

La GED prend en charge l'ensemble du cycle de vie des documents, depuis leur création jusqu'à leur archivage, elle garantit ainsi la traçabilité de leur traitement et leur contrôle centralisé, elle gère aussi les relations entre les documents et ainsi la cohérence de la configuration documentaire, de ce fait la recherche et la mise à jour de l'information s'en trouvent optimisées. [9]

II.10.6 La centralisation et le partage des documents

La GED constitue un outil de centralisation et de partage de documents d'informations, et de connaissance, elle permet de disposer d'une interface d'accès unique et de moyens adéquats de recherche qui garantissent une acquisition rapide et pertinente de l'information, de ce fait elle facilite également les contrôles extérieurs comme par exemple les audits. [9]

II.10.7 La sécurisation de l'information

La GED permet l'accès aux documents par la gestion des différents niveaux d'habilitation à la consultation et à la diffusion des données. La fiabilité de l'information peut être assurée via des systèmes automatiques de contrôle. [8]

II.11 Les aspects techniques de la GED

La GED s'appuie sur des technologies dont le choix peut décider du succès du projet.

II.11.1 Standards ouverts

L'entreprise doit choisir des standards technologiques ouverts pour se protéger de tout risque d'abandon de la technologie par l'éditeur et s'offrir des possibilités d'évolution et de compatibilité

avec d'autres logiciels. Des formats de structure de contenu tels que XML par exemple sont aujourd'hui largement utilisés par les éditeurs. [9]

II.11.2 Architecture logicielle et plate-forme technique

L'architecture technique et la plate-forme technologique doivent permettre une montée en charge simple et rapide si cela est nécessaire. Des systèmes d'archivage, de compression, de sauvegarde évoluée peuvent rapidement s'avérer nécessaire pour permettre le traitement d'une grande masse de documents. [9]

II.11.3 Gestion des droits d'accès

Pour des raisons de sécurité, la gestion des droits d'accès peut s'appuyer sur un annuaire unique centralisé ou sur un méta-annuaire par exemple qui permet la consolidation de plusieurs référentiels (Active Directory, annuaire au format LDAP v3...). [9]

II.11.4 Administration

L'application d'administration, sous forme d'interface de type web, doit permettre l'administration des différents paramètres de la GED : canaux d'accès, contenu... Elle peut aussi fournir des indicateurs statistiques sur l'ensemble du processus de gestion des documents. [9]

II.12 Enjeux relatifs à la GED

II.12.1 L'interopérabilité des formats

Dans l'environnement de l'entreprise, il est important que le document soit réutilisable et interchangeable. Lors de l'enregistrement d'un document dans un format donné, il faut qu'il puisse être accessible pour différents acteurs de l'entreprise et pour des usages divers (lecture à l'écran, impression, stockage, insertion d'objets, modification). L'interopérabilité des formats caractérise notamment la faculté pour ces formats d'être reconnus et lus sur des plates-formes, des logiciels et des médias différents. Les enjeux actuels consistent en la création de standards favorisant l'interopérabilité et la portabilité des fichiers. L'élaboration du standard XML est sensée répondre à ces objectifs. XML favorise notamment la diffusion et la consultation des documents sur des applications et des médias divers, tout en conservant le document dans son intégrité et en garantissant sa pérennité. [7]

-Le standard XML

XML (Extensible Mark-up Language) est une famille de langages qui fait l'objet d'une recommandation par le W3C. Le fichier XML est accompagné d'une feuille de style décrivant l'apparence physique du document et d'une DTD (Document Type Définition) précisant la structure logique du document. [7]

- Avantages

- Il est extensible : un auteur peut définir de nouvelles balises

- Il décrit la structure du document : l'intérêt est de pouvoir conserver la structure du document indépendamment de la plate-forme utilisée et donc de garantir l'interopérabilité du fichier.
- Il dissocie la structure et la présentation du document. [7]

II.12.2 La pérennité des formats et des supports de stockage

La mise en place d'une solution de GED vise également à garantir la conservation des documents dans leur intégrité et la pérennité dans l'accès à ceux-ci.

Plusieurs éléments doivent être pris en compte : la durée de vie des supports de stockage et celle des systèmes de lecture utilisés, format d'enregistrement et systèmes de lecture.

Outre les problèmes d'interopérabilité présentés plus haut, le choix d'un format de document soulève la question de la pérennité dans l'accès au document. En effet, la lecture de documents numériques nécessite de recourir à un appareillage spécifique à la fois matériel (micro-ordinateur, lecteur) et logiciel (système d'exploitation, logiciel d'application). Or, le matériel et les logiciels d'application évoluent. Certaines versions de logiciels ne sont plus capables de lire les documents produits dans les versions précédentes. Il s'agit donc de permettre l'adaptation du document aux évolutions techniques grâce à :

- La migration (changement de support, de version du logiciel)
- La recodification (changement du format de présentation et de structuration). [7]

II.12.3 La sécurité des données

Les enjeux relatifs à la sécurité des données conservées dans une base de GED sont identifiés dans l'ouvrage de Jacques Chaumier².

- Garantie de l'authenticité des documents : la sécurisation du système de GED permet d'attester que le document n'a pas subi de modification.
- Préservation de la confidentialité des informations présentes dans la base.
- Protection contre l'altération volontaire des documents : modification, brouillage des données.
- Protection contre l'altération involontaire des documents : erreurs de saisie par exemple.
- Protection contre les dommages physiques (panne de matériel, incendie...). [7]

II.13 Les Risques

Dès le lancement du projet de mise en place d'une GED, le chef de projet doit prendre en considération les sources potentielles d'échec.

II.13.1 Mauvaise détermination des objectifs du projet

Il est essentiel que la direction de l'entreprise assigne des objectifs clairs et tangibles au chef de projet. [9]

² Jacques Chaumier : est diplômé de l'Institut national des techniques de la documentation. Jacques Chaumier est l'auteur de nombreux ouvrages sur l'information et la documentation.

II.13.2 Mauvaise interface graphique

La première impression qu'à l'utilisateur de la GED est celle laissée par l'interface graphique, si cette dernière est médiocre, il y'a de fortes chances qu'il utilise peu l'outil. [9]

II.13.3 Sous-évaluation de la dimension humaine

Pour la réussite de la pérennité du projet d'implémentation de GED, il est primordial de prendre en considération les besoins et les attentes des futurs utilisateurs. [9]

II.13.4 Surévaluation de la dimension technique

Un projet informatique quel qu'il soit est avant tout 80% de contraintes organisationnelles et humaines et 20% de contraintes technologiques, il faut donc veiller à bien identifier les priorités. [9]

II.13.5 Sous-évaluation de la charge de travail

Cette source d'échec concerne la charge de travail supplémentaire gérée par le projet ainsi que les modalités d'administration et de mise à jour de la GED, il est important que tous les acteurs aient de vision objective de l'investissement humaine, financier,... nécessaire à la réussite du projet, par ailleurs, lors de la déploiement de la GED et de sa montée en charge une phase de test et de correction doit être prévue. [9]

II.14 Les facteurs clés de succès de projet GED

Un projet d'implémentation de GED, comme tout projet informatique, nécessite une gestion efficace et adaptée.

II.14.1 Volonté politique

Un projet de mise en place d'une GED implique les diverses fonctions de l'entreprise, afin d'éviter une lutte de pouvoir pour l'obtention de la direction de projet, il est indispensable que la direction définisse les rôles et les responsabilités de chaque service. [9]

II.14.2 Implication des acteurs

Les acteurs doivent être convaincus de l'importance accordée par la direction de projet, cela suppose une campagne de communication efficace. [9]

II.14.3 Découpage de projet

La complexité de projet peut obliger la maîtrise d'ouvrage à la scinder en plusieurs lots, ce découpage présente plusieurs avantages :

- Réduction des risques technologiques.
- Forte visibilité auprès des utilisateurs.

Il est donc avantageux de déterminer dans le cahier des charges un cœur fonctionnel de la GED et de concevoir des lots successifs couvrant le reste des objectifs de projet. [9]

II.14.4 Coordinations entre les intervenants

L'entreprise peut être amenée à devoir faire appel à des prestataires externes (notamment par la maîtrise d'œuvre s'il s'agit d'un développement propre).

La coordination entre les équipes internes et externes est capitale car les prestataires doivent assimiler les connaissances métiers de l'entreprise et s'imprégner de sa culture. [9]

II.14.5 Mise en place de retours d'expérience

Lorsque les échéances de déploiement d'une GED sont trop éloignées, le projet GED risque d'être considéré comme (vaporware), le déploiement rapide d'une première version permet de juguler ce risque et de recueillir les premiers jugements des utilisateurs afin d'améliorer le fonctionnement dans ses versions ultérieures. [9]

II.15 Conclusion

Aujourd'hui, les acteurs de l'entreprise utilisent de plus en plus le document numérique. Celle-ci doit pouvoir réagir rapidement, en sollicitant les connaissances qui sont à sa portée afin d'être et de rester compétitive. La GED est donc un outil incontournable.

En effet, la GED permet de localiser rapidement l'information, en quelques clics. Le document est facilement accessible. Il peut être partagé par plusieurs personnes au même moment. La GED garantit également la sécurité des données et crée une dynamique de travail collaboratif. Le seul bémol à ce système réside dans les supports de stockage ; il convient de veiller particulièrement à ceux-ci afin de garantir la pérennité des données et des documents.

On peut donc dire que la GED est un composant majeur dans le système d'information de l'entreprise. En plus des changements techniques qu'elle suppose, la mise en place d'une solution de GED a des incidences sur l'organisation du travail et sur la culture d'entreprise. Elle instaure notamment de nouvelles pratiques de recherche de documents et systématise les processus de création et de publication de ceux-ci.

Un projet GED est sujet à beaucoup plus de risque de perte de données et de piratage des informations, le chapitre qui suit propose des solutions pour sécuriser ce projet.

SECURITE DE L'INFORMATION

CHAPITRE III : SECURITE DE L'INFORMATION

III.1 Introduction

Toute entreprise est exposée au risque de perte ou de détournement de l'information ; vol de support informatique, interception de communication.... La protection des informations sensibles doit être une préoccupation de l'ensemble des acteurs de l'entreprise. Il est important que chacun retrouve sa lucidité en gardant en esprit la sensibilité et la vulnérabilité des informations qu'il détient.

La sécurité d'information recouvre des réalités très variées, souvent complexes et imbriquées. On peut la définir comme l'ensemble des moyens actifs et passifs assurant la sauvegarde du patrimoine industriel, informationnel et immatériel de l'entreprise ainsi que ses activités. Il est clair qu'il n'existe pas de risque zéro ; tout l'enjeu pour l'entreprise est donc de réduire les risques à un niveau acceptable sans entraver son fonctionnement. [10]

III.2 Définition

La protection de l'information est une démarche consciente visant à protéger, au sein de l'entreprise étendue, ce qui vaut la peine d'être protégé, tant au niveau des données que des supports d'information. Cette démarche implique un système de gestion, une identification des informations sensibles, une analyse de risques, des acteurs, avec des rôles et responsabilités et un programme de réduction des risques. [10]

III.3 Les risques (attaques)

Une attaque n'importe quelle action qui compromet la sécurité des informations, elle conduisant à un déni ou refus de service peut être réalisé en sollicitant excessivement des ressources.

Les attaques occasionnant un déni de service sont considérées par la loi comme un acte criminel. [11]

III.3.1 Réalisation d'une attaque

Phase 1 : est la collecte d'information et la recherche de vulnérabilité,

Phase 2: savoir-faire et exploitation des informations recueillies et des failles,

Phase 3: création de l'attaque débouche sur l'intrusion,

Phase 4: exfiltration rester anonyme et donc ne pas laisser de trace sur le système utiliser l'identité d'une autre personne connu du système. [11]

III.3.2 Objectifs des attaques

Les attaques portées à la sécurité d'un ordinateur ou d'un réseau sont mieux caractérisées en considérant le système en tant que fournisseur d'information. En général, il existe un flot d'information issu d'une source, un fichier ou une zone de la mémoire centrale, vers une

destination, un autre fichier ou utilisateur. Il existe quatre catégories d'attaques : interruption, interception, modification et fabrication. [11]

III.3.2.1 Interruption

Un atout du système est détruit ou devient indisponible ou inutilisable. C'est une attaque portée à la **disponibilité**. La destruction d'une pièce matérielle (tel un disque dur), la coupure d'une ligne de communication, ou la mise hors service d'un système de gestion de fichiers en sont des exemples. [11]

III.3.2.2 Interception

Une tierce partie non autorisée obtient un accès à un atout. C'est une attaque portée à la **confidentialité**. Il peut s'agir d'une personne, d'un programme ou d'un ordinateur. Une écoute téléphonique dans le but de capturer des données sur un réseau, ou la copie non autorisée de fichiers ou de programmes en sont des exemples. [11]

III.3.2.3 Modification

Une tierce partie non autorisée obtient accès à un atout et le modifie de façon presque indétectable. Il s'agit d'une attaque portée à **l'intégrité**. Changer des valeurs dans un fichier de données, altérer un programme de façon à bouleverser son comportement ou modifier le contenu de messages transmis sur un réseau sont des exemples de telles attaques. [11]

III.3.2.4 Fabrication

Une tierce partie non autorisée insère des contrefaçons dans le système. C'est une attaque portée à **l'authenticité**. Il peut s'agir de l'insertion de faux messages dans un réseau ou l'ajout d'enregistrements à un fichier. [11]

III.3.3 Typologie des attaques

Les attaques sont le plus souvent basées sur l'appropriation de paramètres de connexion, de mots de passe, sur le leurre et l'exploitation de failles et de vulnérabilités : [12]

III.3.3.1 Appropriation de mots de passe

Tout simplement par l'utilisateur qui lui établit son mot de passe ou parce que ce mot de passe est beaucoup trop évident.

-Utilisation d'une complicité,

-Il peut leurrer les utilisateurs, par téléphone ou email, en se faisant passer pour l'administrateur du réseau,

-Par écoute passive du réseau, d'où l'utilité de chiffrer les mots de passe pendant les transferts ou de ne pas les transmettre,

-En cas de découverte de mots de passe cryptés, le pirate va tenter de les découvrir par brute force ou par dictionnaire,

-Utilisation de cheval de Troie : Cette technique évite d'attirer l'attention sur un éventuel dysfonctionnement. (Programme qui substitue au programme de connexion pour la première connexion uniquement, ensuite il redonne la main de bon programme de connexion),

-Activation d'un périphérique comme un micro ou une webcam à l'insu de l'utilisateur. [12]

III.3.3.2 Attaques fondées sur le leurre

Basé sur les sources de vulnérabilités des environnements Internet. Les leurres permettent :

-D'usurper les identités des utilisateurs ou des adresses IP,

-De voler des sessions TCP.

Elles exploitent les propriétés de certains protocoles de communication. [12]

III.3.4 Types des attaques

Il peut être utile de distinguer deux catégories d'attaques : les attaques passives et les attaques actives. [11]

III.3.4.1 Attaques passives

Écoutes indiscrettes ou surveillance de transmissions sont des attaques de nature passive. Le but de l'adversaire est d'obtenir une information qui a été transmise. Ces attaques passives sont la capture du contenu d'un message et l'analyse de trafic. [11]

- a) **-La capture du contenu de messages** : est facilement compréhensible. Une conversation téléphonique, un courrier électronique ou un fichier transféré peuvent contenir une information sensible ou confidentielle. [11]
- b) **-l'analyse de trafic** : est plus subtile. Supposons qu'un moyen de masquer le contenu des messages ou des informations soit à disposition (par exemple, un système de chiffrement), de sorte que les adversaires, même en cas de capture, ne pourront en extraire l'information contenue. Cependant l'adversaire pourra être en mesure d'observer le motif de ces messages, déterminer l'origine et l'identité des systèmes en cours de communication, et observer la fréquence et la longueur des messages échangés. Cette information peut être utile pour deviner la nature de la communication. Les attaques passives sont très difficiles à détecter car elles ne causent aucune altération des données. [11]

III.3.4.2 Attaques actives

La seconde catégorie d'attaques est l'attaque active. Ces attaques impliquent certaines modifications du flot de données ou la création d'un flot frauduleux ; elles peuvent

être subdivisées en quatre catégories : mascarade, rejeu, modification de messages et déni de service. [11]

- a) - **Déni de service** : empêche l'utilisation normale ou la gestion de fonctionnalités de communication. Cette attaque peut avoir une cible spécifique ; par exemple, une entité peut supprimer tous les messages dirigés vers une destination particulière. Une autre forme de refus de service est la perturbation d'un réseau dans son intégralité, soit en mettant hors service le réseau, soit en le surchargeant de messages afin de dégrader ses performances. [11]
- b) - **mascarade** : a lieu lorsqu'une entité prétend être une autre entité. Une attaque de ce type inclut habituellement une des autres formes d'attaque active. Par exemple, des séquences d'authentification peuvent être capturées et rejouées, permettant ainsi à une entité autorisée munie de peu de privilèges d'en obtenir d'autres en usurpant une identité possédant ces privilèges. [11]
- c) - **Rejeu** : implique la capture passive de données et leur retransmission ultérieure en vue de produire un effet non autorisé. [11]
- d) - **Modification des messages** : signifie que certaines portions d'un message légitime sont altérés ou que les messages sont retardés ou réorganisés. Par exemple, le message " autoriser X à lire le fichier confidentiel comptes " est modifié en " autoriser Y à lire le fichier confidentiel comptes. [11]

III.3.5 Description des attaques

III.3.5.1 L'usurpation d'adresse IP

L'usurpation d'adresse IP (mystification ou spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement.

Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

En effet, un système pare-feu (firewall) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines internes au réseau.

L'usurpation d'IP permet de contourner le mur de feu. [13]

III.3.5.2 Un analyseur réseau

Sniffer ou renifleur est un dispositif permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent. En effet, dans un réseau non commuté, les données sont envoyées à toutes les machines du réseau. Toutefois, dans une utilisation normale les machines ignorent les paquets qui ne leur sont pas destinés. Ainsi, en utilisant l'interface réseau dans un mode

spécifique il est possible d'écouter tout le trafic passant par un adaptateur réseau (une carte réseau Ethernet, une carte réseau sans fil, ...). [13]

III.3.5.3 ARP Poisoning

Une des attaques les plus célèbres consiste à exploiter une faiblesse du protocole ARP (Address Resolution Protocol) dont l'objectif est de permettre de retrouver l'adresse IP d'une machine connaissant l'adresse physique (adresse MAC) de sa carte réseau.

L'objectif de l'attaque consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet falsifié indiquant que l'adresse MAC de l'autre machine a changé, l'adresse ARP fournie étant celle de l'attaquant. De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice. [13]

III.3.5.4 Balayage des ports

Un scanner de vulnérabilité appelé analyseur de réseaux ; est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts (port scanning) sur une machine donnée ou sur un réseau tout entier. Le balayage se fait grâce à des sondes (requêtes) permettant de déterminer les services fonctionnant sur un hôte distant. Un tel outil permet de déterminer les risques en matière de sécurité. Il est généralement possible avec ce type d'outil de lancer une analyse sur une plage ou une liste d'adresses IP afin de cartographier entièrement un réseau. Un scanner de vulnérabilité est capable de déterminer les ports ouverts sur un système en envoyant des requêtes successives sur les différents ports et analyse les réponses afin de déterminer lesquels sont actifs.

En analysant très finement la structure des paquets TCP/IP reçus, les scanners de sécurité évolués sont parfois capables de déterminer le système d'exploitation de la machine distante ainsi que les versions des applications associées aux ports et, le cas échéant, de conseiller les mises à jour nécessaires, on parle ainsi de caractérisation de version.[13]

III.3.5.5 Fishing

Le phishing (fishing ou Phreaking ; désignant le piratage de lignes téléphoniques), traduit parfois en « Hameçonnage », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes.

La technique du phishing est une technique d'ingénierie sociale c'est-à-dire consistant à exploiter non pas une faille informatique mais la faille humaine en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de commerce.

Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et les invite à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, ... [13]

III.4 Critères de la sécurisation (services)

Les solutions de sécurité doivent contribuer à satisfaire au moins les critères suivant:

III.4.1 La disponibilité

Est de pair avec son accessibilité. Une ressource doit être accessible, avec un temps de réponse acceptable. La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié, ou par une gestion opérationnelle des ressources et des services.

Ce paramètre est mesuré par une montée en charge du système afin de s'assurer de la totale disponibilité du service. Un service doit aussi être assuré avec le minimum d'interruption en respect avec l'engagement établi.

De plus des pertes de données sont possibles si l'enregistrement et le stockage ne sont pas gérés correctement, d'où l'importance d'une haute disponibilité d'un système et de la mise en place d'une politique de sauvegarde. [12]

III.4.2 L'intégrité

Permet de certifier que les données, les traitements ou les services n'ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle.

L'altération est principalement occasionnée par le média de transmission mais peut provenir du système d'informations.

Il faut également veiller à garantir la protection des données d'une écoute active sur le réseau. [12]

III.4.3 La confidentialité

La confidentialité est le maintien du secret des informations ; dans le cadre d'un système d'information, cela peut être vu comme une protection des données contre une divulgation non autorisée.

Deux(02) actions complémentaires permettant d'assurer la confidentialité des données :

- a)- Limiter leur accès par un mécanisme de contrôle d'accès,
- b)- Transformer les données par des procédures de chiffrement. [12]

III.4.4 L'identification et l'authentification

L'identification de l'auteur d'un document peut être aisé par contre être en mesure d'assurer l'authenticité du document est plus délicate.

Ces mesures doivent être mises en place afin d'assurer :

- a)-La confidentialité et l'intégrité des données d'une personne,
b)-La non répudiation, c'est à dire qu'une personne identifiée et authentifiée ne peut nier une action.
L'identification peut être vue comme un simple login de connexion sur un système.
L'authentification peut être un mot de passe connu seulement par l'utilisateur. [12]

III.4.5 La non-répudiation

Est le fait de ne pouvoir nier ou rejeter qu'un événement a eu lieu. À cette notion sont associées :

- ✓ **L'imputabilité:** une action a eu lieu et automatiquement un enregistrement, preuve de l'action, est effectué,
- ✓ **La traçabilité:** mémorisation de l'origine du message,
- ✓ **L'auditabilité:** capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement.

L'existence de fichiers journal permet de garantir l'imputation et l'auditabilité. [12]

III.5 Les domaines de la sécurité de l'information

Tous les domaines de l'informatique sont concernés par la sécurité d'un système d'information :

III.5.1 La sécurité physique

Concerne tous les aspects liés de l'environnement dans lequel les systèmes se trouvent. La sécurité physique passe donc par :

- Des normes de sécurité,
- Protection de l'environnement (incendie, température, humidité, ...),
- Protection des accès,
- Redondance physique,
- Plan de maintenance préventive (test, ...) et corrective (pièce de rechange, ...). [12]

III.5.2 La sécurité de l'exploitation

Rapport à tous ce qui touche au bon fonctionnement des systèmes, cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic et de mise à jour.

La sécurité de l'exploitation dépend fortement de son degré d'industrialisation qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches. [12]

Quelques points clés de cette sécurité :

- ✓ Plan de sauvegarde, de secours, de continuité, de tests,
- ✓ Inventaire réguliers et si possible dynamique,
- ✓ Gestion du parc informatique, des configurations et des mises à jour,
- ✓ Contrôle et suivi de l'exploitation.... [12]

III.5.3 La sécurité logique

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel. Elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation.

Elle repose également sur :

- ✓ Les dispositifs mis en place pour garantir la confidentialité dont la cryptographie,
- ✓ Une gestion efficace des mots de passe et des procédures d'authentification,
- ✓ Des mesures antivirus et de sauvegarde des informations sensibles.

Pour déterminer le niveau de protection nécessaire aux informations manipulées, une classification des données est à réaliser pour qualifier leur degré de sensibilité (normale, confidentielle, top secrète, ...). [12]

III.5.4 La sécurité applicative

Faire un développement pertinent et l'intégrer harmonieusement dans les applications existantes.

Cette sécurité repose essentiellement sur :

- ✓ Une méthodologie de développement,
- ✓ La robustesse des applications,
- ✓ Des contrôles programmés,
- ✓ Des jeux de tests,
- ✓ Un plan de migration des applications critiques,
- ✓ La validation et l'audit des programmes,
- ✓ Un plan d'assurance sécurité. [12]

III.5.5 La sécurité des télécommunications

Offrir à l'utilisateur final une connectivité fiable et de qualité de bout en bout .Il faut donc mettre un canal de communication fiable entre les correspondants, quels que soient le nombre et la nature des éléments intermédiaires.

Cela implique la réalisation d'une infrastructure réseau sécurisée au niveau des accès, des protocoles de communication, des systèmes d'exploitation et des équipements. [12]

III.6 Objectifs de la sécurité d'information

Les objectifs de sécurité sont élaborés grâce à une échelle de besoin :

III.6.1 La localisation des données

Prévoir les dispositions permettant de réduire l'impact des écarts entre les exigences légales et réglementaires sur les plans de la compétence, de la divulgation des données, des droits de

propriété et du maintien de ces droits dans le cas où les actifs d'un client seraient considérés comme ceux du prestataire dans le cas d'une échec. [12]

III.6.2 La gestion du caractère privé des données

Définir les mesures de sécurité de l'information à instaurer pour assurer la protection d'information. [12]

III.6.3 La disponibilité des services ou de l'information

Définir les critères de choix d'un fournisseur à considérer pour éviter de s'exposer à une performance inadéquate, une capacité limitée du réseau, une mauvaise tolérance aux pannes ou un arrêt des services de télécommunication. [12]

III.6.4 Le contrôle des accès

Définir les mesures de sécurité de l'information à appliquer pour assurer un contrôle d'accès adéquat aux données stockées ou traitées. [12]

III.6.5 L'environnement multi locataires complexe et les fuites de données

Définir les mesures de sécurité de l'information pour se prémunir contre les risques de fuite de données dans un environnement caractérisé par des ressources partagées entre plusieurs clients. [12]

III.6.6 La perte de données

Définir les mesures de sécurité de l'information à appliquer pour éviter les conséquences d'une perte de données à la suite de la suppression accidentelle causée par le prestataire, de désastres naturels ou encore par un ou des intervenants malveillants. [12]

III.7 Architecture de la sécurité

Cette architecture est indispensable si l'on veut prendre en compte l'ensemble des problèmes de sécurité d'une entreprise,

- ✓ Elle permet d'identifier les critères minimaux de sécurité pour chacun des éléments,
- ✓ Permet également d'harmoniser le niveau de sécurité dans toutes les dimensions,
- ✓ Elle permet de visualiser toutes les dimensions de la sécurité :
- **Dimension technique et opérationnelle :**
 - ✓ Sécurité matérielle,
 - ✓ Sécurité environnementale,
 - ✓ Sécurité des télécommunications.

➤ **Dimension organisationnelle et économique :**

- ✓ Méthodologie,
- ✓ Budget,
- ✓ Evaluation,

➤ **Dimension humaine :**

- ✓ Surveillance,
- ✓ Ethique,
- ✓ Formation. [12]

III.8 Mécanisme de défense

Il est obligatoire d'établir tous ces mécanismes de défense pour sécuriser les informations, aucun des mécanismes de sécurité ne suffit par lui-même. Il les faut tous.

III.8.1 Chiffrement

Algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs. [14]

III.8.2 Signature numérique

Données ajoutées pour vérifier l'intégrité ou l'origine des données. [14]

III.8.3 Bourrage de trafic

Données ajoutées pour assurer la confidentialité, notamment au niveau du volume du trafic. [14]

III.8.4 Notarisation

Utilisation d'un tiers de confiance pour assurer certains services de sécurité. [14]

III.8.5 Contrôle d'accès

Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité. [14]

III.8.6 Antivirus

Logiciel censé protéger ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire. [14]

III.8.7 Le pare-feu

Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur. [14]

III.8.8 Détection d'intrusion

Repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime. Mauvaise détection : taux de faux positifs, faux négatifs. [14]

III.8.9 Journalisation

Enregistrement des activités de chaque acteur. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas. [14]

III.8.10 Analyse des vulnérabilités (Security audit)

Identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu. [14]

III.8.11 Contrôle du routage

Sécurisation des chemins (liens et équipements d'interconnexion). [14]

III.8.12 Contrôle d'accès aux communications

Le moyen de communication n'est utilisé que par des acteurs autorisés. Par VPN ou tunnels. [14]

III.8.13 Horodatage

Marquage sécurisé des instants significatifs. [14]

III.8.14 Certification

Preuve d'un fait, d'un droit accordé. [14]

III.8.15 Distribution de clefs

Distribution sécurisée des clefs entre les entités concernées. [14]

III.9 Enjeux de la sécurisation

Il existe un certain nombre de tendances de fond et de ruptures d'ordre économique, réglementaire et sociologique, qui obligent à repenser de façon plus globale la protection de l'information. [15]

❖ Parmi les **évolutions internes** on peut citer les tendances suivantes :

- a) L'explosion des services dématérialisés et des volumes d'information : (structurée mais surtout non structurée) circulant dans les entreprises et sur Internet. Cette volumétrie croissante des contenus oblige à repenser la démarche de protection de l'information ; [15]
- b) L'environnement décentralisé des entreprises et l'hétérogénéité des niveaux de sécurité interne : qui peuvent justifier la mise en place d'un référentiel de protection de l'information. [15]

❖ Parmi les **évolutions externes** on peut mentionner :

- a) La tendance à la convergence des usages domestiques et professionnels des SI : Wifi, messageries instantanées, réseaux sociaux, blogs, wikis...sont d'utilisations courantes dans la sphère privée mais souvent incompatibles avec les usages et les besoins dans l'entreprise. Ceci oblige à revoir les règles d'usages des SI (chartes) mais aussi à redéfinir plus précisément la valeur de ces systèmes d'information pour l'entreprise, [15]
- b) L'émergence de l'entreprise étendue : impliquant un changement des modèles d'affaire, des relations avec les clients, les partenaires, les fournisseurs, les salariés et conduisant à étendre le périmètre de protection de l'information au-delà des frontières traditionnelles de l'entreprise, [15]
- c) L'exigence de transparence et de reporting : accru avec un renforcement des contraintes légales, réglementaires, contractuelles. Cette tendance conduit d'un côté à publier davantage d'informations mais d'un autre côté à contrôler en amont beaucoup plus finement leur origine, et véracité et en aval les destinataires de l'information, [15]
- d) La complexité et l'interaction croissante avec l'environnement : ce qui se traduit par exemple par une diversification et une dangerosité croissante des menaces, obligeant les entreprises à repenser leur politique de protection de l'information et à se préparer au changement. [15]

III.10 Cryptage

Chiffrer des données, ou crypter, c'est rendre un document incompréhensible pour toute personne ne possédant pas la clé de chiffrement (ou l'algorithme, pour les méthodes de cryptage simple). [15]

III.10.1 Méthodes de cryptage

Il n'existe en réalité que deux façons de cryptage :

III.10.1.1 La méthode symétrique

La méthode symétrique utilise une clé secrète pour crypter un message, et cette même clé pour le décrypter. Un système symétrique peut être d'une grande robustesse, seulement, il faut transmettre la clé de façon sécurisée, [15]



Figure III. 1: Cryptage symétrique.

Le seul moyen certain de transmettre la clé de façon sécurisée, c'est de se connecter sur un canal sécurisé au préalable, ou d'échanger une clé de façon physique. Il existe en fait un autre moyen de transmettre une clé de façon sécurisée. Il faut utiliser un système de chiffrement asymétrique. [15]

III.10.1.2 La méthode asymétrique

Ce système fonctionne avec deux clés différentes. Une clé publique, que tout le monde peut voir, et une clé privée, gardée secrète. A l'inverse de la méthode symétrique, pour la méthode asymétrique, on utilise des fonctions à sens unique et à brèche secrète. Ce sont des fonctions facilement calculables, mais très difficiles à inverser.

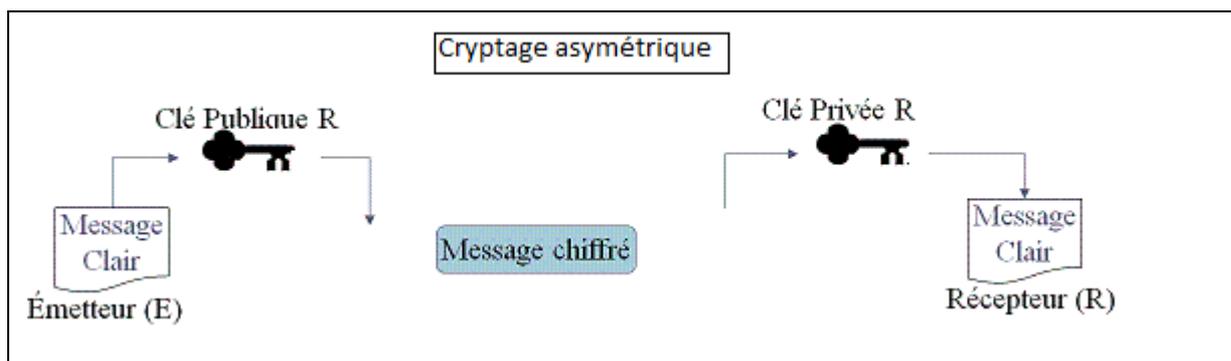


Figure III. 2: Cryptage asymétrique.

Il est presque impossible de trouver l'antécédent d'une telle fonction à moins de posséder une information secrète. En cryptographie asymétrique, cette information est appelée clé privée.

La clé publique sert à crypter, et la clé privée sert à décrypter.

La méthode asymétrique est essentiellement utilisée pour transmettre une clé secrète de façon sécurisée. Le système asymétrique est en réalité très lent. On le couple donc très souvent avec le système symétrique. On parle alors de cryptographie hybride. [15]

III.10.1.3 Cryptage hybride

Le chiffrement hybride utilise les deux types de chiffrements le chiffrement symétrique et le chiffrement asymétrique.

On utilise d'abord le chiffrement asymétrique pour communiquer une clé secrète. On utilise ensuite cette clé secrète pour communiquer avec le cryptage symétrique qui est plus rapide que l'asymétrique. [15]

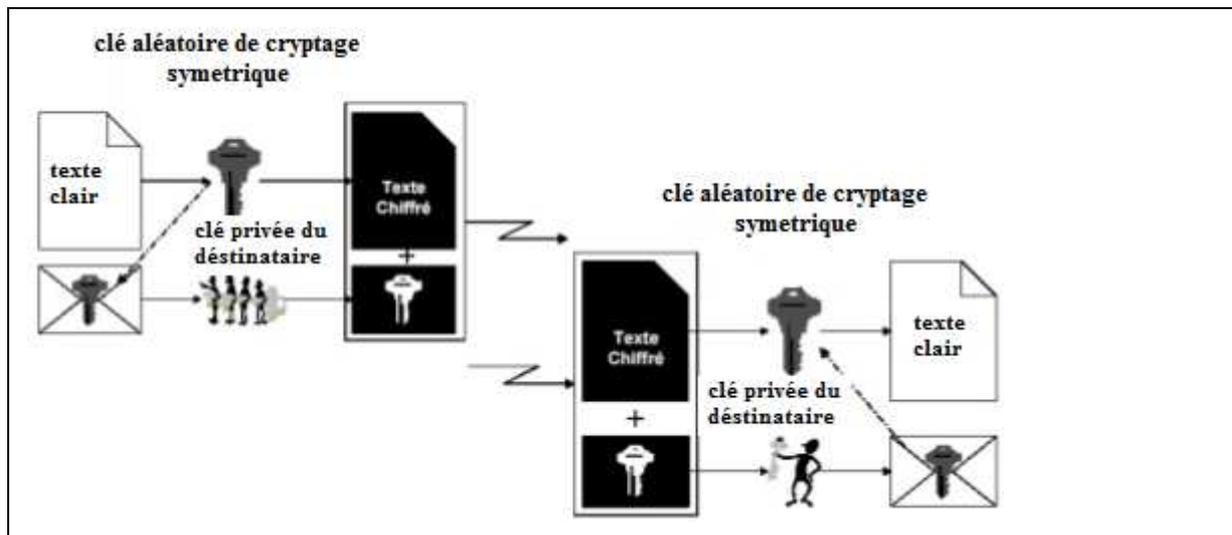


Figure III. 3: Cryptage hybride.

La cryptographie hybride utilise des algorithmes à clé publique et des algorithmes à clé privée, d'où l'adjectif hybride. Ce faisant, il combine les avantages des deux systèmes et pallie à certains inconvénients. En effet, un chiffrement hybride est rapide mais ne présente pas de faiblesse au niveau de la clé comme un chiffrement à clé publique. En effet, un algorithme symétrique oblige à conserver la clé sur le disque dur ou sur une clé USB, ce qui implique un risque qu'un pirate s'infiltrer dans la mémoire de l'ordinateur ou du support USB pour avoir accès à la clé.

III.11 Conclusion

Aujourd'hui, l'informatique est partout, il est donc très dur de se protéger face aux pirates qui sont de plus en plus rapides et efficaces. En effet, même si les pirates informatiques ont un avantage en technique, certains pirates contribuent à la sécurité d'autrui sur internet et autres réseaux sociaux. On peut donc en déduire que la sécurité informatique avance grâce au piratage. Les deux sont liés, donc un jour, peut-être que la sécurité contrera le piratage mais pour le moment, le piratage est omniprésent alors que la sécurité l'est peu. Il y'a de plus en plus de pirates informatiques ainsi, les lois évoluent au même rythme que le nombre de pirates augmente.

Le chapitre suivant présentera une explication de l'application réalisée ; site web dynamique de gestion des fiches de circuit pour les étudiants.

CONCEPTION

ET

REALISATION

CHAPITRE IV : CONCEPTION ET REALISATION

IV.1 Introduction

Ce chapitre a pour objectif de donner une explication de l'application réalisée (Site web de gestion des fiches de circuit pour les étudiants) ainsi les outils informatiques utilisés.

IV.2 Outils de développement :

Cette section permet de présenter brièvement les outils nécessaires pour la réalisation de l'application en question, à l'occurrence : EasyPHP, SublimText3, CSS3 et HTML5.

IV.2.1 EasyPHP version 14.1vc9

Fut le premier package WAMP (Windows Apache MySQL PHP). Il s'agit d'une plateforme de développement Web, permettant de faire fonctionner localement (sans se connecter à un serveur externe) des scripts PHP. EasyPHP est un environnement comprenant deux serveurs (un serveur web Apache et un serveur de bases de données MySQL), un interpréteur de script (PHP), ainsi qu'une administration SQLphpMyAdmin. Il permet donc d'installer en une seule fois tout le nécessaire au développement local du PHP. [16]



Figure IV. 1: EasyPHP.

IV.2.2 Editeur de texte (sublime text3)

Sublime Text est un éditeur de texte générique codé en C++ et Python, disponible sur Windows, Mac et Linux. Le logiciel a été conçu tout d'abord comme une extension pour Vim, riche en fonctionnalités. [17]

Depuis la version 2.0, sortie le 26 juin 2012, l'éditeur prend en charge 44 langages de programmation majeurs, tandis que des plugins sont souvent disponibles pour les langages plus rares. [18]



Figure IV. 2: Sublime text3.

IV.2.3 Serveur web (Apache)

Le logiciel libre Apache HTTP Server (Apache) est un serveur HTTP créé et maintenu au sein de la fondation Apache. C'est le serveur HTTP le plus populaire du World Wide Web. Il est distribué selon les termes de la licence Apache. [19]



Figure IV. 3: Apache.

IV.2.4 Système de gestion de base de données (MySQL)

MySQL est un système de gestion de base de données (SGBD) relationnelles basé sur le langage de d'interrogation SQL (Structured Query Language). Selon le type d'application, sa licence est libre ou propriétaire. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle et Microsoft SQL Server. MySQL est un serveur de bases de données relationnelles SQL développé dans un souci de performances élevées en lecture. [20]



Figure IV. 4: MySQL.

IV.3 Langages de programmation

IV.3.1 HTML

Hyper Text Mark-up Language ; est le langage de balise, permet de définir l'habillage d'un document, c'est-à-dire la façon dont il s'affiche à l'écran d'un navigateur.

Cette notion d'habillage est importante : elle signifie qu'une page écrite en HTML comportera du texte, bien sûr, mais aussi des codes ou balises permettant de modifier l'affichage de ce texte, à savoir sa forme, sa taille, sa couleur, le HTML permet également d'inclure des images, du son ou des animations dans une page web. [20]

HTML inclut les éléments qui permettent la communication entre un client web et un serveur capable de recevoir des informations de ce client de les stocker et ou d'effectuer des traitements en dépendant, la réalisation des sites web interactifs et la création des pages web dynamiques demandent que cette communication soit possible. [20]

HTML5 : Le langage HTML 5 est une amélioration du langage HTML 4, avec des simplifications par rapport à la version XHTML qui était de mise avant lui. HTML 5 déterminer une structure générale commune à toute page en conformité avec des spécifications.



Figure IV. 5: HTML5.

IV.3.2 PHP

PHP (hypertext preprocessor) est un langage de scripts open source. Comme beaucoup d'autres langages, il a été spécialement conçu pour le développement d'applications web, il peut être intégré au HTML. Pour ce faire, le code PHP est inclus entre une balise de début et une balise de fin qui permettent au serveur web de passer en mode PHP. La partie PHP correspond donc à la partie créative et dynamique du document HTML finalement envoyé par le serveur et que le navigateur transformera en page web. PHP est principalement conçu pour servir de langage de côté serveur. Il est capable de réaliser tout ce qu'un script CGI peut faire. Il est principalement utilisé pour écrire des scripts de collecte de données issues de formulaires, de stockage éventuel de ces données dans une base de données, de génération dynamique de contenu. C'est l'utilisation la plus traditionnelle et le principal objet de PHP. [20]

La version qu'on a utilisée est :

PHP5 : PHP5 n'est pas une révolution mais une évolution. Cette évolution introduit quelques changements majeurs tout en conservant une compatibilité totale avec la version antérieure.



Figure IV. 6: PHP5.

Les principales nouvelles fonctionnalités sont:

- **SQLite:** Un SGBD embarqué dont nous verrons les principales forces et faiblesses,
- **SimpleXML:** Un nouveau parseur XML très efficace et très simple,
- **Un nouveau modèle POO:** Le modèle objet complètement remanié, l'ancien restant correctement interprété par PHP. [20]

IV.3.3 CSS

CSS signifie Cascading Style Sheet (feuille de style en cascade). C'est un langage dont l'objectif est de paramétrer finement la mise en forme des éléments d'un document HTML. Il convient d'en comprendre les principes et, notamment, le fonctionnement de la cascade. Il est également utile de se familiariser avec la syntaxe de langage. L'utilisation de CSS permet de réfléchir à des stratégies efficaces de conception en prenant en compte, dès le départ, les possibles mises à jour. Le concept de feuille de style est un concept abstrait qui trouve sa concrétisation sous de multiples formes. Une feuille de style est un ensemble de règles utilisées par le navigateur pour la mise en page et en forme des différents éléments (au sens de HTML). [20]



Figure IV. 7: CSS3.

IV.4 Conception et réalisation

IV.4.1 Conception de la base de données

Nous avons convertit la base de données des étudiants disponible au niveau de l'université du format EXCEL au format MySQL suivant ces étapes :

Le tableau suivant montre la base de données en format Excel.

A	B	C	D	E	F	G	H
N°		Nom Prénoms			Date Naiss	Etat	Matricule
1		ABDELLI YAHIA ABDELKADER			18/12/1994	N	38009554
2		AISSA FATMA			02/06/1994	N	37048234
3		AIT ANTAR BELKACEM			10/08/1993	N	38010390
4		AIT HAMMOU ABDELHAMID OUSSAMA			30/06/1994	N	38023222
5		BADACHE ROUBA			27/03/1994	N	38011819
6		BELKHEIR HOUSSAM EDDINE			28/11/1991	N	8014580
7		BENZIANE MOHAMMED OMAR FARROU			01/03/1992	N	8012150
8		BOCOUM RAMATA DITE KOUMBEL			25/09/1995	N	1869
9		BOURIANE AMINA			22/08/1994	N	38009027
10		DAHMANE BELQASSIM			09/12/1992	N	8012061
11		LAOUNI RIM			12/06/1995	N	38015973
12		MAROC MOHAMED			25/09/1992	N	380117096
13		MIMOUNI HANANE			22/09/1993	N	8017029
14		MOUSSAOUI ABDELKADER			27/10/1991	N	8011272
15		OUAHRANI YACINE			1993	N	38007363
16		OUGGADA MOHAMED SALAH			04/07/1992	N	38010382
17		SAIS DJIHAD NOUR ELHOUDA			22/07/1994	N	38009615

Tableau IV. 1: La base de données en format EXCEL.

IV.4.2 Etapes de conversion

a)- Enregistrer la base de données Excel sous format **Feuille de calcul OpenDocument** :

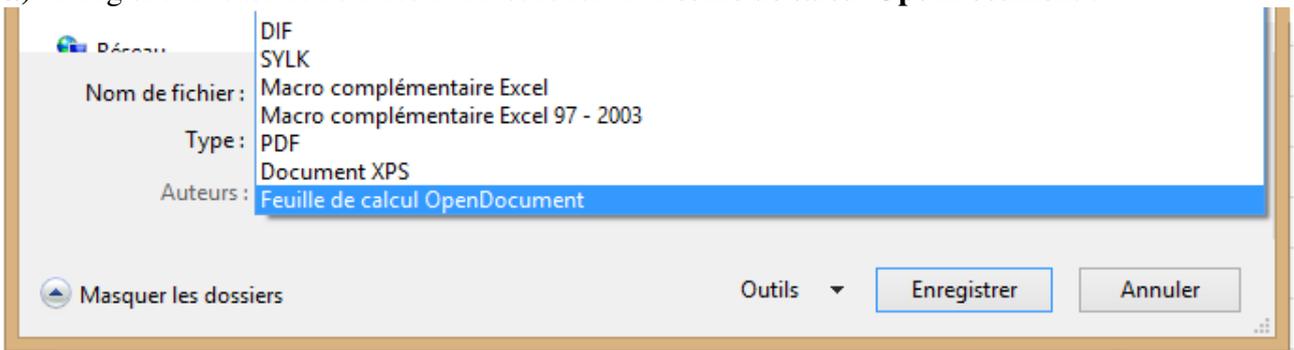


Figure IV. 8: Sélection du format «Feuille de calcul OpenDocument ».

b)- Créer une nouvelle base de données sous MySQL :

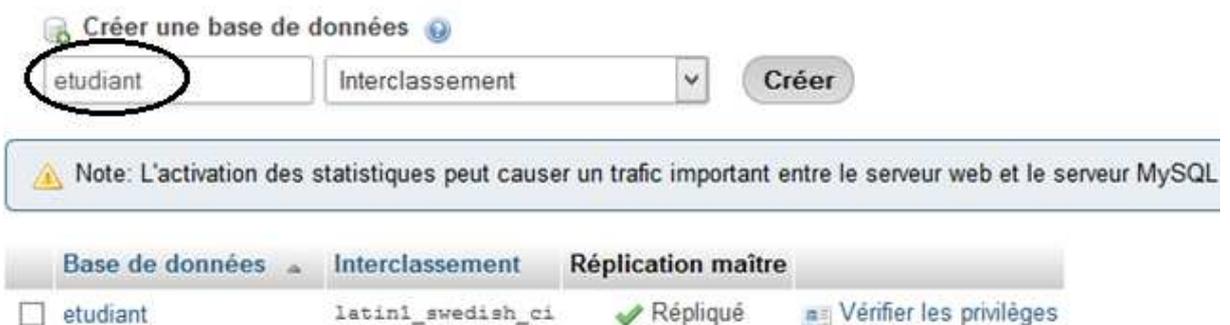


Figure IV. 9: Création de la base de données (etudiant).

c)- Importation de la base de données sous format Feuilles de calcul OpenDocument.

On clique sur l'icône **importer** situant dans la barre menu comme indique la figure suivante :



Figure IV. 10: Importation du contenu de la base de données déjà convertit.

d)- Conversion de la base de données :

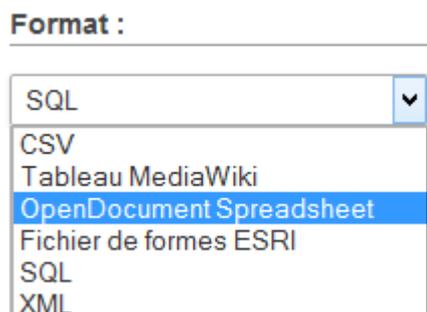


Figure IV. 11: Conversion de la base de données.

e)- Exécution de la conversion :

Format :

OpenDocument Spreadsheet ▾

Options spécifiques au format :

- La première ligne du fichier contient le nom des colonnes de la table (si ceci n'est pas coché, la première ligne fait partie des données)
- Ne pas importer les lignes vides
- Importer les pourcentages en tant que décimales (12.00% devient .12)
- Importer les valeurs de monnaie (\$5.00 devient 5.00)

Exécuter

Figure IV. 12: Exécution de la conversion.

La base de données sous format MySQL :

mat_etudiant	nom_etudiant	bibcen	bibfac	departement	vice_doyen
38009554/13	ABDELLI YAHIA ABDELKADER	ok	ok	ok	ok
37048234/13	AISSA FATMA	ok	ok	ok	ok
38010390/13	AIT ANTAR BELKACEM	ok	ok	ok	ok
38023222/13	AIT HAMMOU ABDELHAMID OUSSAMA	ok	ok	ok	ok
38011819/13	BADACHE ROUBA	ok	ok	ok	ok
8014580/13	BELKHEIR HOUSSAM EDDINE	ok	ok	ok	ok
8012150/13	BENZIANE MOHAMMED OMAR FARROU	ok	ok	ok	ok
1869/13	BOCOUM RAMATA DITE KOUMBEL	ok	ok	ok	ok
38009027/13	BOURIANE AMINA	ok	ok	ok	ok
8012061/13	DAHMANE BELQASSIM	ok	ok	ok	ok
38015973/13	LAOUNI RIM	ok	ok	ok	ok
380117096/13	MAROC MOHAMED	ok	ok	ok	ok
8017029/13	MIMOUNI HANANE	ok	ok	ok	ok
8011272/13	MOUSSAOUI ABDELKADER	ok	ok	ok	ok
38007363/13	OUAHRANI YACINE	ok	ok	ok	ok
38010382/13	OUGGADA MOHAMED SALAH	ok	ok	ok	ok
38009615/13	SAIS DJIHAD NOUR ELHOUDA	ok	ok	ok	ok
8010241/13	SAKRANE SADDAM HOSSEIN	ok	ok	ok	ok
38009599/13	ZIADI KHADRA	ok	ok	ok	ok

Tableau IV. 2: la base de données sous format MySQL.

f)-Création des tables de la base de données :

La base de données comporte trois tables :

(et_gc) : étudiant Génie civil, (et_ge) : étudiant Génie électrique et (et_gm) : étudiant Génie mécanique :

1)- La table et_gc :

#	Nom	Type	Interclassement	Attributs	Null	Défaut
<input type="checkbox"/> 1	mat_etudiant	varchar(11)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 2	nom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 3	prenom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 4	bibliotheque_centrale	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 5	bibliotheque_fac	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 6	departement	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 7	vice_doyen	varchar(50)	latin1_swedish_ci		Non	Aucune

Tableau IV. 3: La table et_gc.

2)- La table et_ge :

#	Nom	Type	Interclassement	Attributs	Null	Défaut
<input type="checkbox"/> 1	mat_etudiant	varchar(11)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 2	nom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 3	prenom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 4	bibliotheque_centrale	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 5	bibliotheque_fac	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 6	departement	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 7	vice_doyen	varchar(50)	latin1_swedish_ci		Non	Aucune

Tableau IV. 4: La table et_ge.

3)- La table et_gm :

#	Nom	Type	Interclassement	Attributs	Null	Défaut
<input type="checkbox"/> 1	<u>mat_etudiant</u>	varchar(11)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 2	nom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 3	prenom_etudiant	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 4	bibliotheque_centrale	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 5	bibliotheque_fac	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 6	departement	varchar(50)	latin1_swedish_ci		Non	Aucune
<input type="checkbox"/> 7	vice_doyen	varchar(50)	latin1_swedish_ci		Non	Aucune

Tableau IV. 5: La table et_gm.

IV.4.3 Architecture générale de notre site

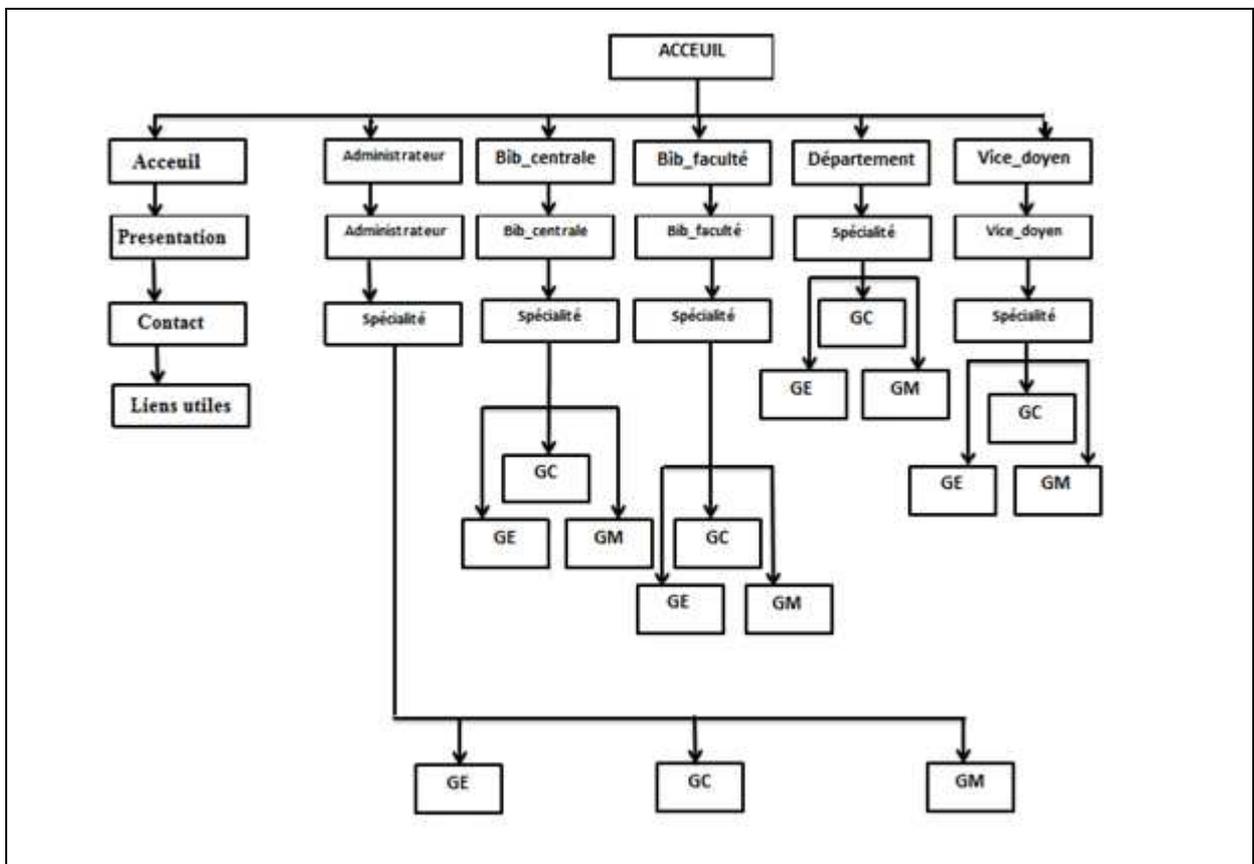


Figure IV. 13: L'architecture générale de notre site.

IV.4.4 La page d'accueil du site



Figure IV. 14: La page d'accueil du site.

IV.5 Scénario d'exécution

Durant toute l'année l'étudiant se déplace pour avoir des livres, mémoires, CD,etc.

A la fin d'année, il doit porter la fiche de circuit pour avoir son diplôme, cette fiche indique que l'étudiant n'a aucun document universitaire. Le chef de département vérifie l'état de l'étudiant (ok ou réserve) à partir de la communication entre les services concernés sans déplacement de l'étudiant.

Voici un exemple simple expliquant le déroulement de notre application :

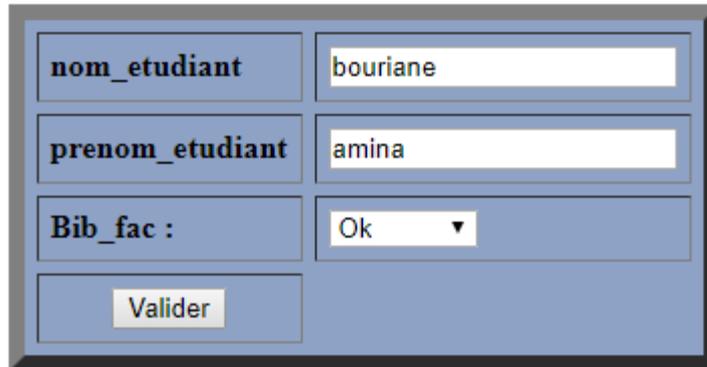
IV.5.1 Boite de dialogue de La bibliothèque centrale.

Le responsable de ce service est le seul qui a l'habilité pour modifier l'état de l'étudiant :

Figure IV. 15: La boite de dialogue de la bibliothèque centrale.

IV.5.2 Boite de dialogue de la bibliothèque de la faculté

Le responsable de ce service est le seul qui a l'habilité pour modifier l'état de l'étudiant :



nom_etudiant	bouriane
prenom_etudiant	amina
Bib_fac :	Ok ▼
Valider	

Figure IV. 16: La boite de dialogue de la bibliothèque de la faculté.

IV.5.3 Boite de dialogue de Vice_doyen

Le responsable de ce service est le seul qui a l'habilité pour modifier l'état de l'étudiant :



nom_etudiant	bouriane
prenom_etudiant	amina
bib_centrale	ok
bib_fac	ok
Vice_doyen :	Ok ▼
Valider	

Figure IV. 17: La boite de dialogue de Vice_doyen.

IV.5.4 Boite de dialogue de chef de département

Le responsable de ce service est le seul qui a l'habilité pour modifier l'état de l'étudiant :

nom_etudiant	bouriane
prenom_etudiant	amina
bib_centrale	ok
bib_fac	ok
vice_doyen	ok
Departement :	Ok ▼
Valider	

Figure IV. 18: La boite de dialogue de chef de département.

Après le remplissage de ces champs par les données, l'étudiant peut avoir sa fiche, et plutôt son diplôme.

IV.5.5 Impression de la fiche circuit :

Après la vérification de l'état d'étudiant par le chef département ; la fiche circuit peut être imprimé.

Imprimer
Total : 2 feuilles de papier

Destination: PDFCreator

Pages: Tous
 par exemple : 1-5, 8, 11-13

Copies:

Mise en page:

Couleur:

Imprimer via la boîte de dialogue du système...
(Ctrl+Shift+P)

Etudiant Genie Electrique

République Algerienne Démocratique et Populaire

Ministere de l'enseignement Superieur et de la Recherche Scientifique

Université Ibn Khaldoun de TIARET
Faculte des sciences appliquees

FICHE DE CIRCUIT

Mat_etudiant:

Nom_etudiant: Prenom_etudiant:

Services: Observations:

Bibliotheque centrale:

Bibliotheque de la faculte:

Vice_doyen:

Departement:

Figure IV. 19: La fiche de circuit avant l'impression.

La fiche circuit après l'impression :

Etudiant Genie Electrique	
République Algerienne Démocratique et Populaire	
Ministere de l'enseignement Superieur et de la Recherche Scientifique	
Université Ibn Khaldoun de TIARET	
Faculte des sciences appliquees	
FICHE DE CIRCUIT	
Mat_etudiant:	<input type="text" value="38009599/13"/>
Nom_etudiant:	<input type="text" value="ZIADI"/>
Prenom_etudiant:	<input type="text" value="Khadra"/>
Services:	Observations:
Bibliotheque centrale:	<input type="text" value="ok"/>
Bibliotheque de la faculte:	<input type="text" value="ok"/>
Vice_doyen:	<input type="text" value="ok"/>
Departement:	<input type="text" value="ok"/>

Figure IV. 20: La fiche de circuit après l'impression.

IV.6 Les scripts principaux

Puisque notre application est un site web dynamique nous avons basé beaucoup plus sur les langages de scripts PHP, HTML, et le SGBD MySQL.

Le principal objectif de nos scripts est l'interrogation et la gestion de la base de données.

Script	Explications
Index.html	Afficher l'interface générale
Administrateur.html	Accéder au page d'administration
Bibliothequecentrale.html	Modifier l'état des étudiants
Bibliotequefac.html	Modifier l'état des étudiants
Vice_doyen.html	Vérifier l'état des étudiants
Departement.html	Vérifier l'état des étudiants
Insertion1.php	Insérer des étudiants à la BD par l'administrateur
Insertion2.php	
Modification1.php	
Modification2.php	Modifier les données des étudiants par l'administrateur
Modification3.php	
Suppression1.php	Supprimer des étudiants par l'administrateur
Suppression2.php	
Fieldcen.html	
Fieldfac.html	Afficher les liens des 3 spécialités (GE, GC, GM)
Fieldvise.html	
Matriculegc.html	
Matriculege.html	Autoriser le responsable pour charger le matricule de l'étudiant
Matriculegm.html	
Test.php	Vérifier le nom d'utilisateur et le mot de passe
Geniecivil.html	Afficher le formulaire du nom d'utilisateur et de mot de passe pour chaque
Geniemecanique.html	département
Genieelectrique.html	
Imprimer.html	Imprimer la fiche circuit

Tableau IV. 6: Les scripts principaux.

IV.7 Conclusion

Dans ce chapitre , nous avons présenté notre site web permettant la gestion électronique de la fiche de circuit pour les étudiants sortant, ce qui va permettre de simplifier cette tâche pour l'étudiant lui-même et même pour l'administration concernée.

Ce chapitre, nous a permis de concrétiser ce que nous avons vu théoriquement dans les précédents chapitres et aussi d'apprendre les notions de la programmation du web dynamique et les outils nécessaires pour la réalisation de cette application comme EasyPHP, SublimText, MySQL,...etc.

Conclusion générale et perspectives

Ce mémoire de fin d'étude sert à une gestion électronique de la fiche circuit qui est un document pédagogique très important pour l'obtention du diplôme de fin d'études. Puisque elle est le seul moyen pour que les services universitaires puissent prouver qu'il y a rien à signaler pour chaque étudiant diplômé.

Raison pour laquelle on a réalisé une gestion électronique de la fiche circuit en se basant sur le développement d'un site web dynamique regroupant les différents services concernés.

Ce site web a comme objectif de simplifier et rendre facile la tâche d'extraction de cette importante pièce, par le biais d'un réseau local, on évite carrément, le déplacement de cet étudiant entre les services impliqués dans cette fiche de circuit.

Grâce à ce modeste PFE, nous avons acquis beaucoup de notions, que se soit, dans la rédaction de ce mémoire qui est le fruit d'un long travail et aussi dans le développement de l'application réalisée qui est le miroir du mémoire réalisé.

Perspective

Puisque le système embarqué se compose de la partie informatique et celle de l'électronique, dont la première est déjà réalisée par le développement d'un site web permettant la gestion électronique de la fiche de circuit. Donc, nous proposons comme futur projet ; la réalisation de la partie électronique qui s'occupe de la prise d'empreinte électronique pour plus de sécurité.

Aussi, nous proposons de généraliser l'application de ce site pour les enseignants et pourquoi pas au niveau de l'université en générale.

Références bibliographiques et webographies

- [1] : Rziza Mohammed /Cours des réseaux Informatiques / (2010-2011) rziza@fsr.ac.ma.
- [2] : coursinformatiquepdf.com/reseaux/introduction-general-au-reseaux-informatique.html
- [3] : Thierry Jeandel /généralité sur les réseaux informatiques (Cours en ligne destiné à des étudiants de BTS IG) / Lycée Chopin/3.
- [4] : José DORDOIGNE. / Réseaux informatiques/pearsonEducation/, 35,124 /5^e édition, 26 août 2011.
- [5] : La Salle Avignon/ CoursRéseaux-Généralité/frères des écoles chrétiennes/Saint-Jean-Baptiste de la salle Avignon.
- [6] : http://elearn.univ-ouargla.dz/2013-2014/courses/TIC/document/.../Ch1_Tweb.pdf?..
- [7] : Geraldine DESBETES, Lucile LEROY, Anne-Gaëlle LIEBERTY / Typologie des systèmes d'information /Mars 2008
- [8] : Desaubry Ludovic/ La dématérialisation des dossiers documentaires : les enjeux et les techniques/ Etude de faisabilité réalisée pour le centre de documentation des Arts Décoratifs/16novembre2009.
- [9] : Raphael SIBLER/ voirin-consultant/09/05/2003.
- [10] : Protection de l'information (CIGREF),www.cigref.fr/cigref_publications/.../Parus2008/Protection_information_2008.pdf
- [11] : Chap. I : Introduction à la sécurité informatique
Laurent Poinot UMR 7030 - Université Paris 13 - Institut Galilée Cours " Sécrypt "
- [12] : F-Nodot / les principes de la sécurité, critères fondamentaux/ université de REIMS Champagne-Ardenne
- [13] : Les menaces informatiques, <http://odile.papini.perso.luminy.univ-amu.fr/sources/SECURITE/cours-SSI-2.pdf>
- [14] : Bernard Cousin/Sécurité des réseaux informatiques/ Université de Rennes 1.
- [15] : RASIDY – DEBUYS Quentin – Lionel 6^oU – /Sciences informatiques/ 2011-2012.
- [16] : https://www.memoireonline.com/01/14/8689/m_Conception-et-realisation-d-un-site-web-dynamique-pour-la-gestion-du-lycee-Kateb-Yacine11.html
- [17]: Jon Skinner/Sublime Tex/Anatomy of a Next Generation Text Editor [archive]/ 3 novembre 2012.
- [18] : Sur sublimetext.com/8 novembre 2012.
- [19] : February 2005 Web Server Survey Finds 40 Million Sites on Apache.

[20] : Etienne Vandeput/développer une application avec PHP et MySQL/centre pour la formation à l'informatique dans le secondaire/ juin2005.

RESUME

Ce projet s'agit d'une application de site web dynamique, permettant la gestion électronique de la fiche circuit, en appliquant un processus de développement, et en utilisant un ensemble d'outils de programmation statiques et dynamiques (PHP, MySQL, HTML...etc.) pour répondre aux besoins de l'application, l'objectif de cette dernière vise à faciliter l'opération d'obtention de la fiche de circuit pour les étudiants sortants.

Mots clés

PHP, MySQL, HTML, site web, gestion électronique, réseau informatique.

الملخص

هذا العمل يتمثل في خلق موقع الكتروني يهدف الى تسهيل عملية ادارة وثيقة ابراء الذمة من طرف مختلف المصالح الادارية للجامعة لغرض تسليمها للطلبة في اطار التخرج. اعتمدنا في انجاز هذا العمل على مجموعة من وسائل البرمجة مثل PHP, MySQL, HTML

الكلمات الرئيسية

HTML , MySQL , PHP موقع الكتروني , الادارة الإلكترونية , شبكة الاعلام الالي .