Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université 08 Mai 1945 – Guelma

Faculté des sciences économiques, commerciales et sciences de gestion

Département de gestion

Mémoire de fin d'étude

En vue de l'obtention du diplôme du master

Spécialité : Technique d'information et de communication dans l'entreprise

Thème :

Utilisation des Tics dans la sécurité

Réalisé par :

Rihani Faiza

Bouarroudj Fouzia

Sous la direction de :

Mr. Toualbia Ilyes

Promotion Juin 2011

Remerciements

بسم الله الرحمن الرحيم

-Qu'il nous soit permis d'exprimer notre profonde gratitude et nos vifs remerciement à Allah le tout puissant de nous avoir donnée la force la volonté et le courage pour concrétiser notre travail nous ne serons pas comment remercier notre encadreur Toualbia Ilyes pour le grand honneur qu'il nous font en acceptant de nous encadrer, qui à mis toute sa compétence à notre disposition pour ses directives et conseils judicieux pour tous ses efforts et encouragement et les recommandations pertinentes qu'il nous ont prodigué lors de l'élaboration de ce projet avec beaucoup d'efficacité

Aussi nous tenons à remercier vivement tous nos enseignants chacun par son nom de première à 2ème année master qui sans leur savoir et leur compétence nous ne serions pas à ce niveau, nous leur devons respect et considération.

En fin c'est de notre devoir de remercier tous ceux de prés ou de loin qui ont contribué à notre formation et à l'élaboration de ce modeste travail trouvent ici l'expression de nos sentiments de reconnaissance et de respect.

Sommaire

Chapitre 2 : technologies et technique de l'information et de la communication

Chapitre 3 : utilisation des Tics dans la sécurité

Introduction générale

Vue sa nature sociale, l'homme a toujours cherché à mieux communiquer pour vivre en société : informer et s'informer, transmettre son expérience, expliquer ses idées, exprimer son avis et ses sentiments, etc. Cependant, avec l'évolution des techniques de l'information et les technologies de la communication, l'homme a pu utiliser ces méthodes et outils pour assurer d'autre tâches, des tâches exigeant la communication pour s'organiser et ordonner les efforts, utilisant les technologies de communication pour esquiver aux contraintes espace/temps et améliorer et/ou faciliter la communication elle-même. Aujourd'hui, les technologies de l'information et de la communication prennent de plus en plus de place dans la vie humaine et dans la société. En effet, on les retrouve dans plusieurs domaines : social, Commercial, économique, militaire, éducationnel, etc. Le développement des TIC est porteur de nouvelles opportunités, mais également de défis.

Les technologies de l'information et de la communication (TIC) permettent de fournir des services de base dans différents domaines, entre autres, de la télésanté, de la télé éducation, du commerce électronique et de la cybergouvernance aux populations des pays en développement dans lesquels de nombreux citoyens n'ont toujours pas accès à des infrastructures physiques telles que les hôpitaux, les écoles ou les services publics de l'administration.Grâce aux progrès réalisés dans le domaine des Tics, les transactions entre le médecin et le patient, l'accès aux services publics administratifs en ligne et l'utilisation de l'internet pour vendre des biens et des services à des clients situés dans des zones éloignées, sont désormais possibles.

Vivre dans un monde collectif, avec les différentestranches de la société ainsi les différentes mentalités, permet de profiter de différents services cités précédemment à l'aide des Tics, comme ça peut mener à des menaces telles que : le vol, les agressions, le terrorisme,

La sécurité des citoyens, des entreprises, des cadres d'état, des frontières du pays, des systèmes de gestion devient un des objets que lesTics doit satisfaire.

Dans le domaine de sécurité, les technologies de l'information et de la communication peuvent être utilisées comme un moyen efficace pour garantir la sécurité (vidéosurveillance,

identification biométrique, etc.), comme elles peuvent être la cause de l'insécurité (virus, intrusion, etc.) où le monde partage ses ressources ce qui va conduire les pirates à vouloir intercepter des informations, voler des données et des biens et détruire des systèmes et des dispositifs publiques. L'un des défis consiste à renforcer la sécurité et la confiance à l'égard des Tics afin que la population soit en mesure d'appréhender leurs dangers et de les utiliser correctement. De plus, il est intéressant de les utiliser pour renforcer le système sécuritaire mis en place pour veiller et garantir la sécurité des personnes, des biens et des entreprises.

Le présent travail intitulé : « Utilisation les technologies de l'information et de la communication (TIC) » vise à présenter les différents concepts et techniques liés aux Tics afin de comprendre cet outil en tant que moyen efficace et vital dans la vie quotidienne de l'être humain en citant les différents services offerts;entre autre, la sécurité. Et comment ces Tics offrent l'opportunité pour assurer cette dernière.

Donc, dans ce mémoire nous présentons les possibilités d'utilisation des Tics dans la sécurité et les outils et/ou techniques utilisés dans ce contexte, ce mémoire est organisé comme suit :

Le premier chapitre sera consacré à la présentation de différentes notions et concepts liés à la communication et à l'information.

Dans le second chapitre, nous présentons les différentes techniques d'échange d'informations et de communication ainsi que les différentes technologies sur lesquelles se base cette dernière.

Le troisième chapitre est dédié à la présentation des différentes opportunités offertes par les Tics pour assurer la sécurité des personnes, des biens et des entreprises ainsi que les différents techniques et/ou outils utilisés dans ce contexte.

Le quatrième chapitre résume le travail du stage réalisé au niveau de l'université 8 mai 1945 de Guelma qui porte sur l'utilisation des Tics pour assurer la discipline et la sécurité au niveau de l'université. Ici la sécurité concerne la discipline dans la bibliothèque, l'accès à l'université, la surveillance, etc.

Enfin nous terminons par une conclusion générale dans laquelle nous évaluons notre étude.

Chapitre 1 : Concept de base de la communication et de l'information

Introduction

Dans ce chapitre, nous avons abordé les différents notions et concepts liés à la communication et à l'information.

D'abord, tout ce qui concerne la fonction de communication est décortiqué : définitions proposées, techniques utilisées, modes de communication suivis, buts attendus, éléments constituants ou entrant dans la communication, types de communication selon le nombre d'interlocuteurs impliqués et objectifs souhaités dans l'entreprise en favorisant la communication.

Ensuite, différentes notions liées à l'information sont présentées : définitions de l'information, supports utilisés pour sa transmission, ses caractéristiques et formes, ses différents types, et enfin ses rôles.

I Communication

I.1 Concept et définition

I.1.1 Définition et schéma de la communication

Étymologiquement[1], communiquer signifie **[1]**: « mettre en commun ». Cependant, le sens moderne donne la définition suivante : « Transmettre, donner connaissance, faire partager, être en relation ».Dans ce contexte, mettre en commun, exige d'avoir quelque chose à partager ou à communiquer.

[1]Étymologie : Branche de la linguistique qui étudie l'origine et la filiation des mots

Dans le cadre d'une communication, la chose qu'on communique ou qu'on transmet est le message. Cela nous pousse à retenir le sens suivant : communiquer veut dire « transmettre ou recevoir un message », ce sens nécessite d'être au moins deux pour pouvoir communiquer : un émetteur et un récepteur.

Pour communiquer, l'émetteur et le récepteur utilisent un moyen de communication dit canal et se fixent d'atteindre au travers de leur échange un but bien précis. Donc **[2]** : « La communication est le processus de transmission d'informations (envoi et de réception d'information) entre deux interlocuteurs (émetteur et récepteur). Cela signifie l'interaction et la coordination entre eux au sujet des renseignements, des opinions, de la direction ou du comportement ».

Nous pouvons ainsi schématiser la communication de la façon suivante **[1]:**

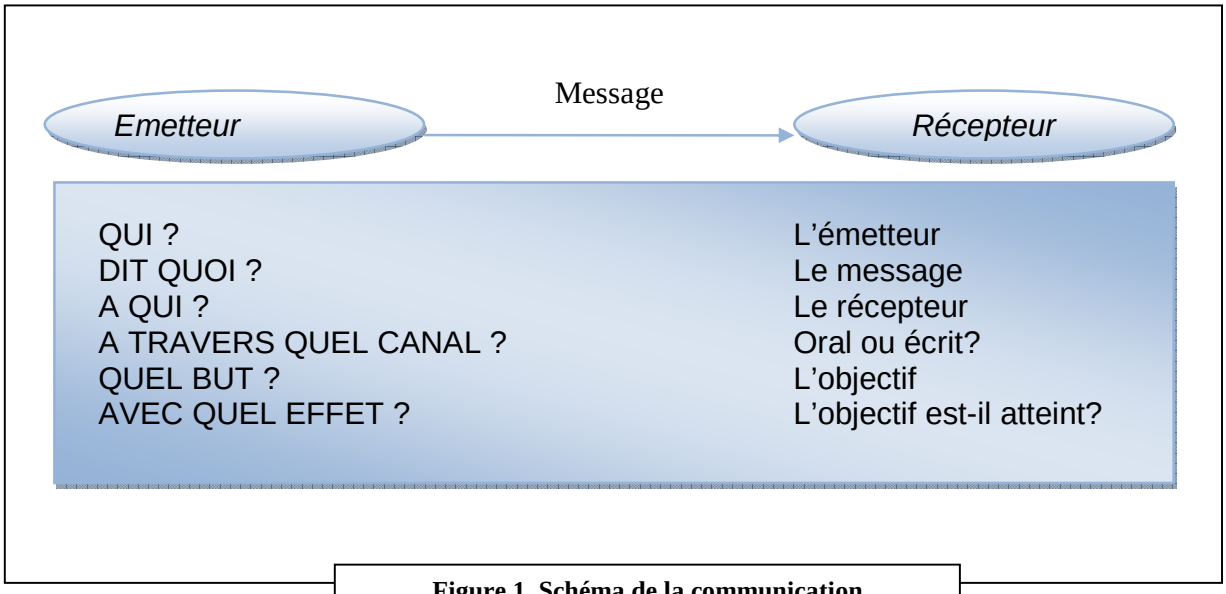

Figure 1. Schéma de la communication

I.1.2 Technique

La technique **[3]**: « ensemble des procédés et des méthodes que l'on utilise dans la pratique d'un métier, d'un art, d'une activité quelconque ». « Ensemble des procédés méthodiques, fondés sur la science, employés à la production ».

Une technique **[4]**, est une activité humaine ou un modèle d'efficacité de l'aide humaine.

I.1.3 Technique de communication

Les techniques de communication **[4]** : peuvent être définies comme un ensemble de méthodes de pointe qui sont utilisées pour la transmission de données et d'informations de l'expéditeur au destinataire en un minimum de temps, avec le moindre cout et avec la plus grande précision.

I.2 Modes de communication

La communication de l'entreprise peut être définie comme la circulation d'informations dans le milieu interne et vers l'environnement externe.On distingue habituellement **[5]**:

I.2.1 La communication interne

La mission quotidienne de la fonction communication interne est de participer au bon fonctionnement de l'organisation, en favorisant : la cohérence, l'unité, des relations sociales harmonieuses, la cohésion et la pluralité, et une culture commune.

La mission à long terme de la communication interne est de promouvoir la prise de risque, proposition de perspectives et de stratégies en vue de favoriser le développement de l'organisation.

La communication interne est une composante du système global de l'organisation et des flux d'information et des échanges, elle peut aider à changer la culture de l'organisation. Le gestionnaire des ressources humaines maitrise les mécanismes de diffusion (Email). L'administration connait les personnes impliquées dans la communication et les circuits d'échanges (workflow); elle apprécie la communication à l'aide de techniques pour élaborer un journal ou organiser une convention, etc.

I.2.2La communication externe

La mission quotidienne de la communication externe est de créer la rencontre de l'organisation avec les besoins et les demandes du marché : collecte des préférences des clients et faire la publicité pour promouvoir ses produits. Elle permet aussi de communiquer avec d'autres

cibles que les clients : les pouvoirs publics, les collectivités locales, l'opinion, les actionnaires, le marché financier, le marché du travail.

La mission à long terme de la communication externe est d'aider à la réussite de l'organisation, d'annoncer les stratégies et de faire connaitre ses progrès. Elle représente un facteur de compétitivité face à la concurrence qui est de plus en plus vive.

La communication devrait être fine et ciblée. Interne ou externe, la communication doit être de plus en plus professionnelle, pour participer efficacement à la stratégie de l'entreprise et se coupler parfaitement avec ses buts.

I.3 Les buts de la communication

La communication est un des besoins fondamentaux de l'homme: nous ne pourrions pas ne pas communiquer. Elle a bien des buts **[1]:**

- Pour découvrir qui nous sommes ;
- Pour apprendre à mieux connaître les autres ;
- Pour nous enrichir personnellement ;
- Pour connaître le monde ;
- Pour partager ce monde avec les autres ;
- Pour nous amuser et nous distraire ;
- Pour demander, convaincre, recevoir, donner...

I.4 Les Eléments de la communication

I.4.1 Les éléments principaux de la communication :

Lors d'une communication plusieurs éléments peuvent intervenir, à savoir **[6]:**

I.4.1.1 L'émetteur

Celui qui a l'initiative de la communication (compose et transmets le message) ;

I.4.1.2 Le message

L'ensemble des informations transmises (faire parvenir à autrui.) ;

I.4.1.3 Le canal

Le support, le mode de transmission du message (le papier, le son) ;

I.4.1.4 Le code

Le système de signes utilisé (la langue, les panneaux de la route) ;

I.4.1.5 Le récepteur

Celui qui reçoit le message transmis par l'émetteur.

I.4.1.6 Le référent

Le contexte (le lieu, le moment…), ainsi que l'ensemble des éléments auxquels fait référence le message (sujet ou objet de la communication.).

I.4.2 Les éléments complémentaires:

Quand on communiqué d'autres éléments complémentaires s'ajoutent à la communication, ces derniers peuvent soit aider les interlocuteurs à mieux se comprendre ou bien les perturber **[7] :**

I.4.2.1 Le feed back (effet de retour)

Désigne la perception par l'émetteur de l'effet du message qu'il a produit. L'émetteur est en même temps récepteur (il envoie le message puis reçoit et/ou aperçoit son effet).Le feed-back permet ainsi à l'émetteur de contrôler et/ou ajuster la forme du message émis selon l'effet qu'il désire voir.

I.4.2.2 Le bruit

Tout ce qui fait obstacle à la communication ou la parasite jusqu'à sa défiguration complète.

I.4.2.3 La redondance

Consiste à donner un élément d'information sous plusieurs formes ; le répéter.

I.5 Les types de communication

La science de la communication englobe un champ très vaste que l'on peut diviser en plusieurs niveaux **[8] :**

I.5.1 La communication intra-personnelle

C'est la communication qui s'effectue à l'intérieur de nous-mêmes, lorsque nous pensons, rêvons, ressentons... Ce sont ces échanges intérieurs qui régissent nos réactions, nos prises de décisions et donc nos actions.

I.5.2 La communication interpersonnelle

C'est la communication qui s'effectue lors des relations entre les individus. (Les collègues de travail, la famille, les amis). Entre humains, c'est la base de la vie en société. C'est là en général que la compréhension est la meilleure, mais le nombre de récepteurs est limité.

I.5.3 La communication de groupe

C'est la communication qui s'effectue entre plusieurs personnes en même temps.

I.5.4 La communication de masse

Dans la communication de masse, un émetteur s'adresse à tous les récepteurs disponibles. D'une façon générale, les médias (radio, presse écrite, télévision) et la micro-informatique (les bandes de données informatisées, le web, les messageries) représentent ce type de communication. Là, la compréhension est considérée comme la moins bonne, car le bruit est fort, mais nombre de récepteurs et bien plus important.

I.6 Objectifs de la communication dans l`entreprise

L'entreprise favorise la communication parmi les membres de son personnel pour plusieurs raisons **[9]** :

- ***Améliorer la productivité et l'efficacité au travail*** *:* Recevoir de l'information crée de la motivation et de la satisfaction chez les employés, ce qui les incite à fournir un meilleur rendement qui augmente l'efficacité générale de l'organisation
- ***Effectuer les changements*** *:* la communication contribue à orienter les efforts de la direction dans le sens souhaité.
- ***Prévoir et éviter les tensions trop fortes*** *:* le manque d'information ou encore une information insuffisante ….
- ***Répondre aux besoins des salaries et maintenir leur bon moral*** *: les* employés peuvent faire connaitre leurs besoins par le biais de la communication et les dirigeants peuvent mieux y répondre, ce qui contribue à soutenir les efforts des employés dans leurs travail
- ***Permettre a chacun de se situer dans l'organisation*** *:* les employés peuvent connaitre les attentes de la direction vis-à-vis d'eux, par exemple ils seront informés des critères sur lesquels ils seront évalués.
- Etc.

II L'information

II.1 Concept et définition

II.1.1 Définitions

Définition 1 :

L'information est un concept ayant plusieurs sens **[10],** il est étroitement lié aux notions de contrainte, communication, contrôle, donnée, formulaire, instruction, connaissance, signification, perception et représentation.

L'information désigne à la fois le message à communiquer et les symboles utilisés pour l'écrire, elle utilise un code de signes porteurs de sens tels qu'un alphabet de lettres, une base de chiffres, etc.

Définition 2 :

L'information est l'émission, réception, création, retransmission, de signaux groupés oraux ou écrits, sonores, visuels ou audiovisuels en vue de la diffusion et de la communication d'idées, de faits, de connaissances, d'analyses, de concepts, de thèses, de plans, d'objets, de projets, d'effets de toute sorte, dans tous les domaines, par un individu, par des groupes d'individus ou par un ou plusieurs organismes.

Définition 3 :

L'information peut se définir de manière objective. Il s'agit de tout ensemble de données susceptible à revêtir un sens particulier, pour un utilisateur **[11].**

Sens commun :

L'information est le produit destiné à la consommation et soumis au stockage, transfert et traitement. Elle est représentée par des données (information codée) utiles pour les actuelles ou futures actions ou décisions à prendre **[12].**

II.1.2 Technique de l'information

Les techniques de l'information représentent l'utilisation des outils et méthodes de la technique électronique pour la production, le stockage, le traitement, la transmission, la diffusion et la récupération de l'information par voie électronique **[13].**

II.2 Support de l'information

Le support d'information est l'objet matériel sur lequel sont représentées les informations ou les données. Il est la composante matérielle d'un document. On distingue différents supports d'information **[12]**:

- ✓ ***Support papier*** : Le support papier est constitué par les livres, fiches, affiches, documents administratifs (bons de commande, bons de livraison, factures,...).
- ✓ ***Support électronique*** *:* Le support électronique est constitué par les bases de données, les systèmes de gestion électronique des documents, les systèmes de gestion de contenu. Le

processus qui permet de faire passer des informations d'un support papier à un support électronique est souvent appelé numérisation.

- ✓ ***Autres supports :*** Il existe d'autres supports d'information :
  - ➢ Support photographique ;
  - ➢ Support magnétique ;
  - ➢ Support optique.

II.3 Les caractéristiques de l'information

Une information est caractérisée par **[14] :**

- Sa forme ;
- Son mode de présentation ;
- Ses qualités ;
- Son coût.

II.4 Les formes de l'information

Parmi les différentes formes que peut prendre une information, les plus courantes sont :

- Les informations **orales.**
- Les informations **écrites.**
- Les informations **visuelles**.

II.5 Les types d'information

On trouve différents type d'information **[15] :**

- ***Des informations fixes :*** Documents textes, images, vidéos, sons, des programmes.
- ***Des informations circulantes :*** Les messages échangés dans les News, Usenet, listes de diffusion, etc.
- ***Des bases de données :*** Elles sont publiées par des institutions internationales ou nationales (ministères, université, bibliothèques, musées), des sociétés commerciales, des associations et des particuliers,

II.6 Les principaux rôles de l'information

L'information est une source essentielle qui peut jouer plusieurs rôles dans l'entreprise. En effet, elle est considérée comme **[16] :**

- ***Un support des processus de gestion :*** Beaucoup de taches nécessitent suffisamment d'informations pour être menées à bien : Traitement des commandes, tenues d'une comptabilité, programmation d'une action, etc.
- ***Un instrument de communication :*** L'échange d'informations est nécessaire pour la réalisation de nombreuses activités.
- ***Un support de connaissance individuelle :*** Dans ce contexte l'information est utilisée pour garder l'expérience et préserver les connaissances des cadres et du personnel de l'entreprise : fiches techniques, règles d'administration, etc.
- ***Un instrument de liaison avec l'environnement :*** Sur ce plan, on ne peut nier l'intérêt de l'information. De même une information de qualité aura un effet positif sur le climat social au sein des organisations. L'information est facteur de motivation, d'intérêt, de cohésion sociale.

Conclusion

L'information et la communication jouent un rôle très important dans la vie quotidienne des personnes et des sociétés. Elles sont un facteur du succès de l'activité des entreprises, un signe de bonne santé de son système organisationnel et un révélateur de ses capacités compétitives.

L'échange d'informations et la communication entre personnes dans une société ou dans une entreprise sont devenus faciles grâce au développement des techniques et technologies de l'information et de la communication, qui seront exposées dans le chapitre suivant.

Chapitre 2 : technologies et technique de l'information et de la communication

Introduction

L'échange d'information et la communication se basent sur un certain nombre de techniques de transmission, eux-mêmes, dépendantes des technologies sur lesquelles elles sont utilisées. Aujourd'hui, avec l'émergence des technologies modernes ; il est devenu facile d'utiliser plusieurs techniques en même temps, ceci a rendu les techniques et les technologies de l'information et de la communication un instrument principal à la portée des personnes et des entreprises, un facteur primordial qui contribue à leur évolution et un signe fiable reflétant leur santé technologique. Historique

Historique

I Origine de Technologies de l'Information et de la Communication(Tics)

Les Technologies de l'Information et de la Communication (TIC) sont des techniques qui permettent le traitement et la transmission de l'information généralement dans les domaines de l'informatique, d'Internet et des télécommunications.

II Evolution des Tics

La transmission de l'information a débuté par le télégraphe pour ensuite évoluer vers le téléphone, la radiotéléphonie, la télévision, etc. Aujourd'hui, on est capable de transmettre en

même temps différents types d'informations : Internet et la télécommunication mobile ont associé aux textes les images et la parole. Cette évolution est due aux avancements technologiques qui ont permis de confectionner de miniatures composants électroniques servant à produire des appareils multifonctions à des prix abordables.

Les technologies de l'information et de la communication prennent de plus en plus de place dans la vie quotidienne des personnes, des sociétés et des entreprises. En effet, on les retrouve dans plusieurs domaines comme : la télémédecine, la bourse, les usages militaires et plus encore. Si la croissance des Tics continue à progresser, les prospectivistes prévoient que ces systèmes pourraient engendrer un nouveau paradigme civilisation el **[18].**

II.1 Appellation

Certaines ambigüités règnent dans la signification de l'abréviation TIC. En effet, la lettre « T : certains insinuent pour Techniques, tandis que d'autre insinuent pour technologies ». Concernant les deux initiales restantes « IC : tout le monde est d'accord pour Information et Communication ». Néanmoins, des propositions peuvent être données au préalable à ces termes **[19]** :

T : Techniques, méthodes ou opérations concrètes (fabriquer, adapter, modifier).

T : Technologie, matériel et outils utilisés (ordinateurs, logiciels, réseaux.)

I : Informations (transmission, partage, diffusion…).

C : Communication, transmission des informations entre récepteur et émetteur.

II.2 Définition des Tics

Les technologies de l'information et de communication regroupent l'ensemble des techniques qui contribuent à numériser l'information, la traiter, la stocker et la mettre à disposition d'un ou plusieurs utilisateurs **[20].**

Les Tics sont un atout irremplaçable pour accroitre la rapidité de la circulation de l'information, faciliter l'élaboration collective de plans d'action, permettre de nouvelles façons de faire et d'agir, assouplir la coordination de l'action, autoriser la mémorisation et la capitalisation

des expériences, rendre possible l'accès à des connaissances très diverses, ouvrir de nouveaux services à la clientèle, etc.

Cette contribution des **Tics** à la création de la valeur ajoutée prend aujourd'hui plusieurs formes : intranet, internet, messageries, forums, workflow, bases de données, édition multimédia, service à la clientèle, etc.

III Les outils des Tics

III.1 L'informatique

L'informatique (de : information et automatique) est la science (elle obéit à des lois et à des règles bien définies) du traitement rationnel (fondée sur la raison, conforme au bon sens, qualifié de logique) de l'information à l'aide de machines automatiques. Les machines automatiques dont traite la définition sont les ordinateurs.

III.2 Les Ordinateurs

Un ordinateur est une machine dotée d'une unité de traitement lui permettant d'exécuter des programmes enregistrés. C'est un ensemble de circuits électroniques permettant de manipuler des données sous forme binaire, ou bits. Cette machine permet de traiter automatiquement les données, ou informations, selon des séquences d'instructions prédéfinies appelées aussi programmes **[20].**

Elle interagit avec l'environnement grâce à des périphériques comme le moniteur, le clavier, le modem, le lecteur de CD, la carte graphique.

III.2.1 Composant d'un ordinateur :

III.2.1.1 Le matériel

On désigne par matériel toute la partie physique de l'ordinateur, constituée par l'ensemble de composants électroniques entrant dans son montage, et les différents périphériques qui lui sont connectés. Voici succinctement les composants essentiels d'un PC moderne :

Composant	Description
Carte mère	La carte mère constitue le cœur de tout PC. C'est en fait le PC lui-même. Tous les autres composants y sont connectés et c'est elle qui contrôle leur fonctionnement.
Processeur	Le processeur est souvent considéré comme le "moteur" de l'ordinateur. Il est également nommé CPU (Central Processing Unit, unité centrale de traitement).
Mémoire RAM	La mémoire système est généralement appelée RAM (Random Access Memory, mémoire à accès aléatoire). Il s'agit de la mémoire principale de l'ordinateur. Elle stocke tous les programmes et toutes les données dont le processeur se sert.
Boîtier	Le boîtier est le caisson externe qui abrite la carte mère, l'alimentation, les unités de disques, les adaptateurs ainsi que l'essentiel des composants physiques de l'ordinateur.
Alimentation	L'alimentation est le composant qui fournit aux différents composants du PC le courant électrique dont ils ont besoin pour fonctionner.
Lecteur de disquettes	Il s'agit d'un média amovible de stockage magnétique de faible capacité. Aujourd'hui, beaucoup de systèmes font plutôt appel à la mémoire flash à interface USB.
Disque dur	Le disque dur est le support de stockage de haute capacité le plus utilisé sur les ordinateurs.
Lecteur CD-ROM, ou DVD-ROM	Les lecteurs de CD (Compact Disc) et de DVD (Digital Versatile Disc) sont des lecteurs optiques à supports amovibles et d'une capacité relativement élevée. La plupart des systèmes récents intègrent des lecteurs ayant des possibilités de lecture/réécriture.

Clavier	Sur un PC, le clavier est le périphérique qui permet à l'utilisateur de contrôler l'ordinateur et de communiquer avec lui.
Souris	Il existe aujourd'hui sur le marché de nombreux périphériques de pointage, le premier et le plus utilisé étant la souris.
Carte vidéo	La carte vidéo (ou carte graphique) contrôle les informations affichées à l'écran.
Moniteur	Affiche sur son écran les images et textes générés par la carte vidéo
Carte son	Indispensables pour profiter des fonctions audio du PC.
Réseau/modem	Les PC assemblés sont généralement livrés avec une interface réseau et parfois un modem.

III.2.1.2 Les logiciels informatiques

Un logiciel est un ensemble d'information relatives a des traitements effectues automatiquement par un appareil informatique y sont inclus les instructions de traitement, regroupées sous forme de programmes, des données et de la documentation. Le tout est stocke sous forme d'un ensemble de fichiers dans une mémoire secondaire **[21].**

Les logiciels sont appelés sous différents noms. En plus du terme générique « logiciel », vous rencontrerez **[22] :**

Application : Cette catégorie de logiciels est utilisée pour des tâches productives ou pour créer des documents.

Programme : Ce sont des logiciels dont la finalité n'est pas de produire, mais plutôt de distraire ou à apprendre : Les jeux vidéo, les dictionnaires, etc.

Utilitaire ou Outil : ces programmes contribuent au bon fonctionnement de l'ordinateur ou de ses équipements. Ils servent par exemple à optimiser les performances du disque dur ou à compresser des données.

Système d'exploitation : il s'agit d'une interface entre la machine et l'utilisateur permettant à ce dernier d'exploiter le matériel dont il dispose et les logiciels installés dessus. Sans système d'exploitation, rien ne peut fonctionner : ni le matériel, ni les autres logiciels.

III.3 Télécommunications

Les télécommunications sont la transmission à distance, avec des moyens électroniques et informatiques, de l'information. Aujourd'hui, on utilise surtout des réseaux analogiques ou numériques comme le téléphone, la radio ou l'ordinateur.

Supprimant la notion d'espace et du temps les réseaux de télécommunication ont couvrit le monde par des réseaux filaires, fibres optiques,…etc.

III.4 Les réseaux informatiques

III.4.1 Infrastructure Réseau

Terme générique désignant un ensemble de composants physiques et logiciels assurant la connexion en réseau. L'infrastructure procure les bases de connexion, sécurité, routage, gestion et accès utilisateurs **[19].** On distingue :

L'infrastructure physique reprend la topologie, et les appareils mis en œuvre comme les commutateurs (hub, Switch, routeur, ...), les serveurs et clients, le câblage. Cette notion reprend également les modes de transmissions Ethernet, sans fils,…

L'infrastructure logicielle reprend les programmes nécessaires à cette connexion comme les DNS (Domain Name System), les protocoles réseaux (TCP/IP,...), la partie logicielle pour les clients et le système d'exploitation serveur.

III.4.2 Les protocoles et les services des réseaux informatiques

Les protocoles de communication orientent la manière dont les informations se transfèrent entre les équipements du réseau. Il existe des logiciels qui sont installés sur les équipements d'interconnexion (passerelles, routeurs, antennes GSM, etc.) qui permettent d'instaurer une communication inter-réseaux et inter-machines. Les services réseaux fournissent,

des protocoles de transfert de textes, de données, de communications vocales et/ou vidéo ainsi que des protocoles de diffusion **[18].**

III.4.3 Les catégories de réseaux informatiques

Un réseau informatique peut être catégorisé de plusieurs façons **[18]:**

- En termes d'étendue :
  - Personal Area Network (PAN): Réseau personnel.
  - Local Area Network (LAN): Réseau local.
  - Metropolitan Area Network (MAN) : Réseau métropolitain.
  - Wide Area Network (WAN): Réseau étendu.
- Par relation fonctionnelle :
  - Client-serveur
  - Architecture multi-tiers
  - Peer-to-Peer (P2P ou Poste à Poste)

III.4.4 Le réseau sans-fils

Le réseau sans fil permet de connecter plusieurs systèmes entre eux par ondes radio. Il peut aussi être utilisé dans le domaine des télécommunications afin de créer des interconnexions entre les nœuds. Wifi est la norme la plus utilisée parmi les réseaux sans fil. Ce type de réseau a été développé afin de répondre à un réseau interne, puisque les ondes sont limitées, donc propre à un bâtiment, soit pour usage corporatif ou personnel. Les réseaux sans fil ont été conçus comme une alternative aux réseaux câblés. Toutefois, puisqu'ils sont compatibles entre eux, le réseau sans fil peut donc être utilisé comme extension.

III.4.5 La sécurité

Qui dit technologie, dit risques **[18].**Nous avons simplement à penser à une panne ou un bris de composantes technologiques ou un vol, une destruction de données confidentielles par un partenaire, un employé ou un délinquant. Plusieurs mesures existent afin de limiter ces effets néfastes soit :

- Chiffrement de données
- Certificat numérique
- Pare-feu
- Logiciel anti-virus
- Logiciel de détection des intrusions
- Copie de sauvegarde de données sécurisées

IV Rôles des Tics

IV.1 Les avantages des Tics

Les technologies de l'information et de la communication peuvent créer de la valeur dans une entreprise si elles sont bien utilisées **[19].**

❖ Bénéfices au niveau du système d'information

- Hausse de la productivité du travail pour la saisie de l'information, donc baisse des coûts.
- Délocalisation de la production (ex : centre d'appels).
- Meilleure connaissance de l'environnement, réactivité plus forte face à cet environnement,
- Amélioration de l'efficacité de la prise de décision permise par une veille stratégique plus performante.

❖ Bénéfices de la structure de l'entreprise et de la gestion du personnel

- Moins hiérarchisée
- Partage d'information
- Meilleure gestion des ressources humaines (recrutement, gestion des carrières plus facile).

❖ Bénéfices au niveau commercial :

- Nouveau circuit de production grâce à l'extension du marché potentiel (commerce électronique).
- Une baisse des coûts d'approvisionnement.
- Développement des innovations en matière de services et réponses aux besoins des consommateurs.
- Amélioration de l'image de marque de l'entreprise (entreprise innovante).

IV.2 Les limites des Tics

L'investissement dans les dans une entreprise nécessité une grande volonté de changement, ceci est du aux problèmes de rentabilité **[21] :**

- Coût du matériel, du logiciel, de l'entretien et du renouvellement.
- Il est fréquent de voir apparaître un suréquipement par rapport aux besoins et donc une sous-utilisassions des logiciels.
- Coût de la formation du personnel, de sa résistance aux changements.
- Coût généré par la modification des structures, par la réorganisation du travail, par la surabondance des informations.
- Coût dû au rythme soutenu des innovations.
- Rentabilité difficilement quantifiable ou difficilement prévisible sur les nouveaux produits.

V Retour sur investissement des Tics

L'utilisation des technologies de l'information et de la communication peut être très bénéfique pour l'entreprise. Voici quelques exemples de retour sur investissement que cela peut rapporter **[19] :**

- Fidélisation de la clientèle
- Augmentation des ventes
- Amélioration de la communication de l'entreprise.

Il est bien important de considérer ces technologies comme un investissement à long terme plutôt que comme une dépense.

VI Les applications des Tics

VI.1 Les espaces de communication

VI.1.1 Internet

L'internet c'est une hiérarchie des réseaux interconnectés, ils sont liés par des artères à haut débit et Utilisent un protocole qui fonctionne selon la base de TCP/IP : ce couple de protocoles et mis pour faciliter la communication entre les machines, met à la disposition de ses utilisateurs un nombre important d'outils et de services pour mieux communiquer. Le multimédia et les possibilités interactives augmentent l'intérêt des clients dans les présentations. On peut les classer Comme Suite **[21]** :

- ***La Messagerie électronique :***

Elle sert à envoyer et recevoir toute sorte de documents **[23]**:Il est vrai simplifie sérieusement, l'envoi de messages à plusieurs destinataires internes ou externe ne doit pas faire oublier les règles élémentaires de sécurité, à chaque message émis, il est important de vérifier si tous les destinataires sont habilités de recevoir les informations ou pièces jointes transmises

Encore, on trouve des logiciels de messagerie permettent aux entreprises de créer "une signature»: c'est un petit texte ajouté à la fin de chaque message que l'entreprise expédie sur le réseau. Ces signatures permettent en fait de rappeler ses coordonnées sans avoir à les ressaisir à chaque fois, aussi, elles permettent de mieux se faire connaître La messagerie est devenue donc l'instrument de communication le plus utilisé dans les entreprises.

- ***Forum (newsgroup) :***

Les forums sont des lieux d'échanges thématiques fonctionnant en mode asynchrone. Une fois connectés, les utilisateurs lisent les messages existants, répandent s'ils le souhaitent ou posent à leur tour une question. La vie d'un forum est totalement dépendante de ses animateurs pour lancer ou recentrer les Débats.

- ***Chat ou IRC (Internet Relay Chat) :***

C'est un protocole de communication qui offre la possibilité à plusieurs personnes de créer des salons virtuels et temporaire afin de communiquer par écrit et en temps réel .C'est une des fonctions de base des outils de conférence à distance. Pour mieux exprimer la personnalité, l'utilisateur peut se définir un personnage et utiliser des sons et des couleurs .Il peut aussi sélectionner un mode de conversation privée avec un seul interlocuteur.

VI.1.2 Intranet

L'intranet **[21]** : est un réseau informatique utilisé à l'intérieur d'une entreprise ou de toute autre entité organisationnelle utilisant les technique de communication d'internet (IP, serveur, HTTP).C'est un système de communication sécurisé car seul les membres autorisés peuvent y accéder. Il joue un rôle très important comme composant intégral des systèmes d'information et cela pour plusieurs raisons: des déploiements plus simples, une conception objet permettant de réduire les coûts de développement, une ergonomie simple tendant à diminuer les coûts de formation.

VI.1.3 Extranet

L'extranet **[21]** : est un réseau informatique qui permet un accès contrôlé de l'extérieur pour les affaires spécifiques ou éducatives. Extranets sont des extensions, ou des segments de

réseaux intranet privés qui ont été construits dans de nombreuses entreprises pour le partage de l'information et de commerce électronique.

VI.2 Multimédia

VI.2.1 Définition

Le multimédia est l'intégration de textes, du son et/ou d'images comme moyen de représentation de l'information. Le multimédia propose aussi l'interactivité en permettant à l'utilisateur de naviguer d'une information à l'autre. C'est aussi une technologie qui permet d'enregistrer, de restituer ou de transmettre un mélange de sons, images, textes et vidéo **[18].**

VI.2.2 Apprentissage du multimédia

Pour avoir un environnement d'apprentissage multimédia, il faut mettre sur un même support (page web ou une interface graphique) un mélange de : Textes, sons, images fixes et/ou animées et vidéos. Le logiciel propose ensuite un certain niveau d'interactivité (recherche d'informations, aide en ligne, navigation) entre l'utilisateur et les différents éléments.

VI.2.3 L'audioconférence

C'est un mode de communication utilisant le principe de la voix sur IP, il est très avantageux dans la mesure où il permet de téléphoner de PC à PC en limitant l'infrastructure à un seul type de câble celui du réseau d'ordinateur de l'entreprise.

Avec le système audioconférence, l'internaute peut entrer en contact directement depuis son site avec un opérateur en ligne. Il peut ainsi obtenir rapidement les informations complémentaires sur un point précis ou simplement des garanties orales mais rassurantes sur des inquiétudes bien naturelles.

VI.2.4 La visioconférence

L'enjeu de la visioconférence réside dans la multiplication des échanges entre des individus éloignés géographiquement par des outils de communication transportant de la voix et de l'image.

La visioconférence par exemple, en abolissant les distances dans le travail collectif et en permettant une communication en temps réel, compenserait certains inconvénients des structures en réseaux notamment l'éloignement géographique des individus.

L'équipement nécessaire pour organiser une visioconférence est relativement simple à installer: chaque participant doit disposer d'un ordinateur avec carte son, d'un logiciel client (intégré sous Windows), d'une caméra (webcams), d'un micro-casque et d'une ligne haut débit **[24]**.

La visioconférence permet aussi le partage des documents en direct ainsi que tout les outils utilisables sur Internet, intranet et extranet.

VI.2.5 Les Echanges de Données Informatisées (EDI)

L'EDI (Electronic Data Interchange) définit un ensemble de normes et outils pour échanger des documents commerciaux structurés entre les applications informatiques distantes reliées par un réseau. L'ensemble de partenaires que ce soit : clients, fournisseurs, organismes bancaires ou administrations échangent ainsi des documents papier **[25]**.

VI.2.6 Les Echanges de Données Informatisées Pour le Commerce Administratif et le Transport (EDIFACT)

Cette norme définit un langage normalisé d'échanges. Chaque entreprise définit son propre format pour ses documents comme les factures, les bons de commande. Pour faciliter les échanges et l'automatisation de la gestion, des travaux de normalisation ont été entrepris depuis déjà pas mal d'années avec cette norme qui définit précisément le format et les verbes pour chaque type d'échanges. À partir de cette définition, chaque domaine professionnel peut affiner le langage et les procédures de communication spécifique à ses propres échanges.

VI.3 Le commerce électronique

VI.3.1 Définition :

Le commerce électronique représente l'échange, surtout sur le web, de biens et de services entre deux entités **[19]**.

VI.3.2 La vente à distance :

Le commerce électronique est une forme de vente à distance au bénéfice des particuliers et des entreprises. Plusieurs produit et services y sont échangés chaque jour **[18]**.

- Principaux biens et services vendus par Internet aux particuliers :
  - Les biens culturels : Livres, CD et DVD
  - Appareils électroniques : ordinateurs, téléphones portables, etc.
  - Tourisme et voyages : Billet de train, d'avion, etc.
  - Supermarché en ligne.
- Produits vendus exclusivement pour les professionnels :
  - Traceurs, copieuse de plan, photocopieur
  - Matériel BTP (Bâtiments de travaux publics)
  - Véhicules utilitaires
- Système de vente conçu pour le web :
  - Développement de photos numériques
  - Téléchargement de musique
  - Vente aux enchères (EBAY)
  - Vidéo à la demande
- Service en ligne :
  - Banque en ligne
  - Assurance en ligne
  - Presse en ligne

VI.4 Les puces intelligentes :

Afin de protéger les données, les entreprises et les consommateurs utilisent à présent des cartes à puces intelligentes dans plusieurs applications, à titre d'exemple les opérations bancaires, accès aux messageries électroniques, démarrage de l'ordinateur, consultation des messages téléphoniques.

Si le niveau de sécurité requis est plus élevé, une carte à puce intelligente est probablement le meilleur choix. Une empreinte digitale peut facilement être sauvegardée dans la mémoire de la puce, ce qui permettra une validation plus élaborée grâce à un lecteur avec biométrie. Lorsque l'employé présente sa carte au lecteur, il est aussi invité à présenter sa référence biométrique (empreinte digitale). Cette façon de faire permet de s'assurer que la personne qui présente la carte est bien la personne pour qui la carte a été émise. Selon le cas, l'accès sera approuvé ou refusé.

Conclusion

Dans ce chapitre nous avons présenté les notions et concepts de base concernant les Tics. Ces derniers évoluent constamment et prennent de plus en plus de place dans la vie quotidienne des personnes, des sociétés et des entreprises. Leur évolution les rend un instrument efficace à la portée des personnes et des entreprises ouvrant de nouvelles perspectives dans tous les domaines.

Le domaine de la sécurité est l'un des domaines où les Tics peuvent jouer un rôle primordial. Les contextes d'utilisation sont multiples (sécurité des biens, des personnes, des entreprises, des réseaux informatiques, etc.) et les choix sont nombreux (les techniques et technologies utilisées varient selon les circonstances de sécurité).

Le chapitre suivant présente les concepts et principes de base de l'utilisation des Tics dans la sécurité et illustre les principaux outils et techniques utilisées dans ce contexte.

Chapitre 3 : utilisation des Tics dans la sécurité

Introduction

Le progrès des technologies de l'information et de la communication n'est pas sans risques. Des failles de sécurité se multiplient et engendrent de nouvelles vulnérabilités, des menaces pernicieuses et inédites. Les sociétés perdent des sommes considérables, en raison des dysfonctionnements induits par les questions de sécurité. Ce dernier est affaire de balance entre les risques et les bénéfices. Le choix d'une solution de sécurité ne doit pas seulement réduire les risques mais aussi favoriser la probabilité du succès d'une mission.

I La sécurité

I.1 Concept et définition

La sécurité, d'une manière générale, est l'état d'une situation présentant le moindre risque, ou l'état d'esprit d'une personne qui se sent tranquille et confiante. Pour un individu ou un groupe, c'est le sentiment (bien ou mal fondé) d'être à l'abri de tout danger et risque **[26]**.

La sécurité informatique consiste à assurer que les ressources du système d'information (matérielles et/ou logicielles) d'une organisation sont uniquement utilisées dans le cadre où il est prévu qu'elles le soient **[27]**.

I.2 Fondamentaux de la sécurité

La sécurité informatique vise à se protéger contre les risques liés à l'informatique qui sont dus à plusieurs éléments, à savoir :

- Les menaces qui pèsent sur les actifs à protéger ;
- Les vulnérabilités de ces actifs ;

- Le manque de sensibilité de ceux-ci.

Si l'un des éléments est nul, le risque n'existe pas. C'est pourquoi, l'équation est généralement représentée par **[26]** :

Risque = Menaces * Vulnérabilités * Manque de Sensibilité.

Les menaces : Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

Les vulnérabilités : Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.

Le manque de sensibilité : C'est l'ignorance de l'existence de ces menaces et de ces vulnérabilités et le manque de conscience chez les responsables sur la sécurité du système.

Le risque : C'est l'association d'une menace aux vulnérabilités qui permettent sa réalisation.

Les solutions de sécurité doivent contribuer à satisfaire les critères de base de la sécurité qui sont :

I.2.1 La disponibilité des données

C'est-à-dire le fait que les données soient effectivement à disposition des ayants droit en temps voulu. L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources en temps bien précis **[27]**.

I.2.2 L'intégrité des données

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle). L'objectif c'est d'assurer que la donnée arrive à la destination en bon état.

I.2.3 Confidentialité des données

Consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction. L'objectif c'est d'assurer que la donnée ne circule qu'entre les bonnes mains.

I.2.4 L'authentification

L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

I.2.5 Non répudiation

La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction ou l'exécution d'une action.

I.3 Les Principales menaces de la sécurité Informatique

I.3.1 Les Utilisateurs :

L'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur (par insouciance ou malveillance) **[26]**.

I.3.2 Les programmes malveillants :

Un logiciel destiné à nuire ou à abuser des ressources du système est installé (par mégarde ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données.

I.3.3 L'intrusion :

Une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès.

I.3.4 Un sinistre : (vol, incendies, inondations) :

Une mauvaise manipulation, une malveillance ou des aléas naturels entraînant une perte de matériel et/ou de données.

I.4 La sécurité par la conception globale :

La sécurité d'un système peut être comparée à une chaîne de maillons plus ou moins résistants. Elle est alors caractérisée par le niveau de sécurité du maillon le plus faible. Ainsi, la sécurité doit être abordée dans un contexte global :

- La sensibilisation des utilisateurs aux problèmes de sécurité.
- La sécurité logique, c'est-à-dire la sécurité au niveau des données.
- La sécurité des réseaux.
- La sécurité des systèmes.
- La sécurité des télécommunications.
- La sécurité des applications.
- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles.

I.5 Aspects de la sécurité informatique

I.5.1 Objectifs

Les objectifs de la sécurité informatique sont **[28]** :

- Réduire les risques technologiques.
- Réduire les risques informationnels dans l'utilisation des systèmes d'information.

I.5.2 Domaines de la sécurité

Il existe plusieurs domaines de sécurité :

I.5.2.1 Sécurité physique :

La sécurité physique représente le contrôle le plus fondamental et le plus courant des systèmes informatiques. C'est la première objective à assurer avant toute autre objective de sécurité. Elle couvre plusieurs aspects :

- Aspects liés aux systèmes matériels.
- Aspects liés à l'environnement : locaux, alimentation électrique, climatisation, etc.
- Mesures : Respect de normes de sécurité, protections diverses, traçabilité des entrées, gestion des accès, redondance physique, marquage de matériels, etc.

I.5.2.2 Sécurité logique

Les virus informatique sont des programmes informatiques conçus pour causer des dégâts dans les ordinateurs cibles, ces derniers constituent les menaces logiques qui guettent les ordinateurs. Plusieurs mécanismes pour remédier ces menaces logiques existent, à savoir :

- Mécanismes logiciels de sécurité : firewall, antivirus, etc.
- Contrôle d'accès logique : identification, authentification, autorisation.
- Protection des données : cryptage, anti-virus, sauvegarde.

I.5.2.3 Sécurité applicative

L'objectif est d'éviter les « bugs » :

- Méthodologie de développement.
- Contrôles et tests.
- Plans de migration des applications.

I.5.2.4 Sécurité de l'exploitation

Elle vise le bon fonctionnement des systèmes

- Procédures de maintenance, de test, de diagnostic, de mise à jour.
- Plan de sauvegarde.

- Plan de secours.

I.5.2.5 Sécurité des télécommunications

Elle exige une infrastructure réseau sécurisée :

- Au niveau des accès.
- Au niveau des protocoles.
- Au niveau des systèmes d'exploitation.
- Au niveau des équipements.

II Utilisation des techniques d'information et de communication dans la sécurité

II.1 Sécurité du système d'information

II.1.1 Les composants du système d'information

Le système d'information comprend **[29]** :

- Le ou les serveurs réseau et les postes de travail informatique (fixes et nomades) ;
- Les applications (systèmes d'exploitation, suites bureautiques, logiciels métiers, etc.) ;
- Les infrastructures de communication et de télécommunication (réseaux locaux, liaisons intersites, réseau téléphonique, accès Internet, liaison radio, etc.) ;
- Les informations sensibles détenues par l'entreprise.

Les risques pesant sur le système d'information peuvent être : vols, destruction de données ou de matériels, interception d'informations, indisponibilité de services, etc. avec une origine qui peut être externe mais souvent interne (malveillance ou négligence).

II.1.2 Procédures de sécurisation du système d'information :

II.1.2.1 Authentification :

- Déterminer des droits d'accès au système d'information différenciés selon les responsabilités des salariés et les statuts des autres personnes pouvant avoir accès au système d'information (stagiaires, personnels temporaires, prestataires extérieurs) : qui a le droit de faire quoi ? de savoir quoi ?
- Gestion des codes d'accès et des mots de passe (attribuer des mots de passe suffisamment sécurisés (agrégat de caractères alphabétiques et numériques), les renouveler régulièrement (tous les 3 mois par exemple), les supprimer lors du départ des individus).
- Configuration des postes par le responsable de la sécurité du système d'information.

II.1.2.2 Sécuriser les informations et le système :

- Utilisation de logiciels et de matériels de sécurité (antivirus, anti-spyware, pare-feu, anti-spam, etc.) pour les serveurs et postes informatiques (fixes et nomades) ;
- Sécurisation des échanges (Internet - extranet – Wifi, etc.) par le chiffrement des données les plus sensibles ;
- Pour les données très sensibles, utilisation de matériel non connecté au réseau ;
- Application des mises à jour et correctifs des logiciels ;
- Contrôler régulièrement la configuration des pare-feu ;
- Veille sur les nouveaux virus, logiciels espions, etc.

II.1.2.3 Sauvegarde :

- Définir le type de données à sauvegarder, selon quelle périodicité, pour quelle durée (obligations légales pour certaines données) – Revoir périodiquement le périmètre de sauvegarde.
- Dupliquer les sauvegardes.
- Répartir les informations confidentielles sur plusieurs supports.

- Sécurisation des lieux de sauvegardes, conservation des supports mensuels et annuels en dehors de l'entreprise.
- Contrôle du bon fonctionnement des sauvegardes.

II.1.2.4 Gestion des incidents :

- Détection des vulnérabilités et anomalies le plus tôt possible.
- Prévoir des solutions de secours en cas d'indisponibilité du système informatique (assistance dépannage – mise à disposition de matériel de secours, etc.).

II.2 La sécurité des ordinateurs:

II.2.1 Le cas général des ordinateurs personnels

Internet regorge d'ordinateurs personnels que peut un pirate contrôlé à distance en quelques minutes. Il suffit de peu de choses pour ne plus être importuné, à savoir **[30]** :

1- Mettre à jour son ordinateur

Appliquez les correctifs, La quasi-totalité des incidents, et notamment les dernières grandes épidémies de vers qui ont circulé sur l'internet, utilisent une faille de sécurité connue pour laquelle existe déjà une rustine.

Pour les ordinateurs équipés de Windows, la solution la plus simple pour rester à jour est d'activer le service de mise à jour, Windows Update, depuis le Menu Démarrer ou se connecter directement sur le site consacré. Certains programmes disposent néanmoins de leur propre fonction de mise à jour automatique, qu'il convient d'activer spécifiquement.

2- Choix de bons outils de navigation

Internet Explorer est un bon navigateur, s'il est tenu à jour, cependant d'autres alternatives sont réputées statiquement plus sûres (Firefox par exemple).L'avantage de ces applications réside dans le fait qu'elles n'exploitent pas, par exemple, la

technologie ActiveX de Microsoft qui est largement détournée pour piéger des pages web.

3- Utilisation d'un pare-feu

L'utilisation d'un pare-feu est nécessaire en réseau, Windows intègre un pare-feu, cependant, l'utilisation d'un autre comme Zone Alarme ou Norton Firewall est fortement conseillée. Ces produits offrent une plus grande souplesse de configuration, des interfaces plus agréables à utiliser et permettent de contrôler les applications qui peuvent se connecter à l'internet.

4- Utilisation d'un Antivirus

L'installation d'un antivirus est plus qu'obligatoire, car, des codes malicieux peuvent être intégrer dans les pages web ou même dans les documents office. De plus, les programmes amusants (jeux, Screen-Saver, etc.) peuvent contenir des chevaux de Troie ou des Key-Loger. L'antivirus est là pour les déloger.

L'antivirus doit être capable non seulement d'analyser les fichiers du disque dur, mais aussi d'analyser les fichiers reçus par courriers électroniques, et ceux reçus par les logiciels des messageries instantanées telles MSN ou Yahoo. Messenger.

De plus, une fois l'antivirus installé, il est indispensable d'activer la mise à jour automatique de sa base virale.

5- Utilisation d'un Antispyware

Les spywares sont des logiciels espions permettant de collecter des données confidentielles concernant l'ordinateur cible et de les transmettre aux pirates qui les ont installés. Eux aussi sont intégrés dans des pages web malicieuses ou dans des utilitaires téléchargés du web.

Les adwares sont des logiciels clandestins qui s'installent avec des applications (souvent gratuites) téléchargée d'internet, voire pendant la navigation. Leur rôle peut être d'afficher de la publicité ou d'étudier les habitudes de navigation. Leur objectif est alors de servir les sociétés de marketing qui les installent (faire de la publicité et/ou collecte de renseignements).

Il ne faut pas toujours compter sur l'antivirus pour se débarrasser des spywares puisque les éditeurs d'antivirus n'ont jamais pris la peine de lutter contre ce type de parasites. Ils commencent tout juste à s'y intéresser. Deux logiciels gratuits s'en chargent de ces parasites très bien : Spybot Search & Destroy et Ad-aware de Lava-soft.

6- Utilisation de compte non privilégié

Tout programme qui s'exécute sur un système (Windows à titre d'exemple) possède les droits de l'utilisateur qui l'a lancé. Si cet utilisateur dispose les droits d'administrateur, les programmes qu'il exécute auront également tous ces droits sur le système. Dans ce contexte, si l'administrateur exécute par mégarde un virus ou un cheval de Troie : le parasite aura alors tous les droits pour modifier le système. Donc, il est nécessaire d'utiliser un compte non privilégié pour le travail quotidien et de faire recours au compte administrateur dans les circonstances de première nécessité.

7- Faire attention aux cliques

La clique sur les pièces jointes exécutables reçues par e-mail peut déclencher l'exécution d'un virus ou d'un cheval de Troie. En outre, les liens reçus peuvent être déguisés pour mener vers une destination autre que celle affichée. Par exemple, le lien indique le site de téléchargement d'un utilitaire d'un éditeur connu, tandis qu'il conduit vers un site pirate qui distribue des versions piégées de cet utilitaire.

Plus dangereux encore, un message peut être déguisé pour paraitre comme celui de notre banque en ligne, contenant un lien qui mène au site de ce dernier, alors qu'il conduit réellement vers une copie falsifiée de celui-ci. Bien évidemment, on ne se rend compte de ça qu'après que le compte soit complètement dévalisé.

8- Faire attention à tout type de programmes

Les programmes "traditionnels" ne sont pas les seuls qui peuvent être piégés et causer des dégâts au système ; Les auteurs de virus utilisent souvent d'autres types de fichiers pour diffuser leurs parasites. C'est le cas par exemple des économiseurs d'écran (fichiers .scr), des raccourcis de programmes DOS (.pif), des scripts (.vbs,

.wsh) et même des fichiers de commandes de Windows (.bat), etc. donc, il faut être vigilent.

9- Tests de sécurité

Plusieurs services en ligne, souvent gratuits, permettent de détecter si l'ordinateur est accessible depuis l'internet. Ils testent en réalité le pare-feu en essayant de déterminer les ports ouverts. Certains vont plus loin et tentent de repérer d'éventuels virus et/ou chevaux de Troie dissimulés dans le système (Symantec Security check par exemple).

De nombreux éditeurs d'antivirus proposent également une analyse gratuite du disque dur directement depuis le réseau mondial.

II.2.2 Le cas particulier des ordinateurs portables et des équipements mobiles

La sécurisation des ordinateurs portables qui se connectent à un réseau à partir de n'importe quel endroit (gare, aéroport, avion, café, hôtel, centre de conférence, etc.) constitue un problème bien spécifique. Cette sécurisation doit faire l'objet d'une attention particulière pour plusieurs raisons **[31]**:

- Les utilisateurs prennent rarement la précaution de protéger ces terminaux par un mot de passe ;
- Quand le mot de passe existe, il est souvent devinable ;
- L'utilisateur détient le plus souvent des droits d'administrateur ;
- Les ordinateurs portables sont souvent visés parles voleurs ;
- Les ordinateurs portables regorgent souvent d'informations confidentielles de l'entreprise ou de l'administration. Ces ordinateurs sont souvent la cible de professionnels qui ont intérêt à voler ces informations (physiquement ou virtuellement) pour agir à l'encontre de l'organisation concernée ou rendre publique ces informations confidentielles.
- etc.

Ces ordinateurs personnels doivent être munis de firewalls, d'antivirus et d'antispyware afin de les protéger contre le vol virtuel. Concernant le vol physique, il faut être vigilent et prendre toujours ses précautions.

II.3 Sécurité des télécommunications

II.3.1 Sécurité et secret des télécommunications

En matière de télécommunications, l'obligation de sécurité et de confidentialité est une exigence essentielle dont le non respect peut entraîner des sanctions pénales. L'opérateur doit prendre toutes les dispositions nécessaires pour assurer la sécurité des communications empruntant son réseau, et doit informer ses clients des services existants permettant le cas échéant de renforcer la sécurité des communications **[32]**.

II.3.1.1 Les garanties opérateurs

Le secret des correspondances étant un prolongement du respect de la vie privée, le code des postes et télécommunications prévoit expressément la protection de la vie privée des consommateurs.

II.3.1.2 Utilisation de la cryptologie

La cryptologie constitue aujourd'hui pour les entreprises la solution technique incontournable pour protéger leurs échanges sur le réseau contre d'éventuelles violations de correspondance. La cryptologie est un moyen de préservation de l'intimité de la vie privée.

II.3.2 Sécurité et patrimoines informatiques :

Le patrimoine informatique comprend non seulement les biens matériels, mais également les œuvres et créations issues de ces matériels. Il s'agit d'œuvres et de créations audiovisuelles, multimédias, ou cinématographiques ; mais il peut également s'agir d'un logiciel, d'une marque, d'un brevet, d'une base de données, ou d'un jeu vidéo, etc.

II.3.2.1 Sécurité des œuvres immatérielles

Les œuvres de l'esprit considérées comme originales sont protégées par le droit de la propriété intellectuelle. En violation totale des droits d'auteur, ces œuvres circulent parfois de façon illégale sur le web.

II.3.2.2 Sécurité des systèmes informatiques

Il s'agit ici de la protection contre les fraudes informatiques, notamment la violation des secrets de l'entreprise.

II.3.3 Sécurité et commerce électronique

Le commerce électronique exige des garanties en matière de sécurité, de confidentialité et de preuve des transactions. Ces garanties sont essentielles tant pour la protection du consommateur que pour celle du commerçant qui offre des produits et services au grand public.

II.3.3.1 Risques relatifs au manque de sécurité dans les outils de télécommunications

II.3.3.1.1 **Menace au niveau de la transmission des données**

Une personne non autorisée peut intercepter des données transférées entre deux sites sur le web. Elle peut lire les données et les altérer. L'intégrité des données du commerce électronique telles que les demandes d'achats doit être assurée. La sécurité reposerait donc sur la confidentialité.

II.3.3.1.2 **Menace au niveau de l'authenticité**

Dans une transaction électronique, il n'est pas toujours aisé d'identifier l'acheteur et le vendeur. L'une des deux parties peut utiliser une fausse identité. Ici, la fonction de sécurité consiste à certifier que l'offre ou la commande provient bien de leur véritable auteur.

II.3.3.1.3 **Menace pour les paiements**

La vente de produits ou de services sans la conclusion d'un paiement est un risque commercial réel. Des exemples de non-paiements sont des achats réalisés avec

une fausse identité, l'utilisation d'un compte bancaire non valide et le paiement avec des numéros de cartes de crédits illégitimes.

D'un point de vue légal, il est essentiel de pouvoir prouver devant un tribunal qu'un client a acheté le produit. Pour cela, l'utilisation d'une signature électronique fiable permet de réduire une grande partie des menaces visées.

II.3.3.2 La signature électronique

La signature électronique permet, à l'aide d'un procédé cryptographique, de garantir l'intégrité du document signé et l'identité du signataire.

II.3.3.3 Sécurité des paiements en ligne

Le développement du commerce électronique exige des garanties de sécurité des réseaux. La cryptologie, et tout particulièrement le chiffrement, constituent aujourd'hui le moyen de sécurisation de paiement en ligne le plus généralisé. En général, lors de l'utilisation d'une carte bancaire de paiement en ligne, l'utilisateur est redirigé vers le site Internet de la banque du cybercommerçant pour payer la facture d'achat selon les contraintes de sécurité mises en place par la banque.

II.4 La sécurité des réseaux informatique

II.4.1 Sécurisation au niveau réseau :

Firewall :

La sécurisation des systèmes informatiques d'une entreprise ou d'une administration commence avec la sécurisation au niveau réseau. Le firewall est à ce sujet un outil indispensable.

Le rôle du firewall est d'assurer un périmètre de protection entre le réseau interne à l'entreprise et le monde extérieur. Basé sur des technologies d'analyse des paquets à l'entrée du périmètre protégé, le firewall permet ou interdit l'accès de et vers ce périmètre.

Composé d'équipements matériels et/ou logiciels, le firewall va réaliser les tâches suivantes **[31]** :

- Bloquer l'accès à des services non autorisés ;
- Interdire l'accès à des systèmes ;
- etc.

Les firewalls peuvent intégrer des techniques de détection d'intrusions et peuvent envoyer des alertes afin de prévenir les équipes de surveillance technique. Ces équipements prennent en compte un ensemble de règles qui doivent être définies en fonction des besoins d'une entreprise ou d'une administration.

Les meilleurs firewalls incluent des modules pour:

- Le scan antivirus ;
- Les proxys de messagerie instantanée ;

II.4.2 La Sécurité des réseaux sans fil

II.4.2.1 Définition

Le réseau sans fil est le réseau qui utilise des ondes radios comme support de transmission, il présente par rapports les réseaux filaires les intérêts suivants :

- ✓ Mobilité des usagers
- ✓ Simplicité et souplesse de déploiement
- ✓ Faible coût d'installation et de maintenance en comparaison avec les réseaux filaires

II.4.2.2 Les types des réseaux sans fil

Il existe deux types de réseaux sans fil :

Les réseaux en clair : aucun chiffrement, directement accessible.

Les réseaux chiffrés (WEP **:** Wired Equivalent Privacy), (WPAWi-fiProtected Access, WPA2).

II.4.2.3 Wardriving

Le Wardriving **[33]** : consiste à rechercher des réseaux sans fil (Wireless). Cette recherche se fait généralement en voiture, d'où son nom, mais aussi en train, en autobus, à pied, etc. La personne qui fait du Wardriving est un Wardriver.

Pour cela, il faut une carte réseau Wireless, un ordinateur portable ou un PDA, une antenne (généralement couplée à la carte réseau, mais il est aussi possible de monter une antenne externe pour plus de réceptivité), et un logiciel de sniffer (renifleur) Wireless.

Il existe de plus en plus de Wardrivers pour les raisons suivantes :

Pas cher : Il suffit une carte sans fil couplée à un ordinateur portable pour être un Wardriver.

Méthode difficilement détectable.

Figure 2 : Exemple de Wardriving

II.4.2.4 Les moyens de sécurisation d'un réseau sans fil

Pour sécuriser un réseau sans fil, il faut procéder au **[31]:**

- Changement des paramètres de configuration par défaut fournis par les constructeurs (mot de passe administrateur, etc.);
- Configuration de l'PA (Point d'Accès) de telle manière qu'il passe inaperçu.
- Utilisation des méthodes d'identification et de filtrage pour les stations clientes autorisées à utiliser le réseau sans fil. La manière la plus simple est de définir une liste des clients autorisés lesquels sont identifiés par l'adresse MAC MAC (Media Access Control) Adresse qui est associée à une interface qui se situe au niveau de la couche liaison de données, comme le protocole Ethernet. Cette adresse identifie univoquement l'interface au sein d'un réseau local. Cette liste sera mise à jour par un administrateur réseau.
- Utilisation de standards ou de protocoles ouverts tels que:

- **WEP (Wired Equivalent Privacy):** Technique développée pour renforcer la protection des réseaux sans fil avec un encryptage des paquets basé sur une clé connue seulement par les clients autorisés.
- **WPA (Wi-fi Protected Access):** nouveau concept développé par Wi-Fi Alliance pour répondre aux limitations du WEP.

II.5 Les réseaux privés virtuels (VPN)

Le VPN (Virtual Private Network) **[31] :** permet d'établir des connexions sécurisées privées (un réseau privé) au travers d'un réseau public comme l'Internet. IL est utilisé pour:

- Réaliser des interconnexions LAN to LAN.
- Réaliser des connexions à distance pour des utilisateurs mobiles ou télétravailleurs.
- Contrôler l'accès dans un intranet.

II.5.1 Avantage des VPNs :

Les VPN présentent essentiellement deux avantages:

- Les économies sur les budgets alloués à la connectivité : Ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet.
- La flexibilité : Dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN de l'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.

II.5.2 Inconvénient des VPNs:

Parmi les désavantages des VPN, on peut citer:

- La disponibilité et les performances des VPN dépendent largement des fournisseurs de service. L'entreprise ou l'administration utilisant un VPN ne contrôle en effet pas tous les paramètres nécessaires;
- Les standards ne sont pas toujours respectés et les technologies VPN restent dépendantes des équipements utilisés**.** On conseille d'utiliser les équipements du même constructeur pour assurer le bon fonctionnement du VPN d'entreprise.
- La mise en route d'un VPN réclame une forte expertise, et notamment une bonne compréhension de la sécurité informatique et des technologies VPN spécifiques.

II.6 La sécurité des téléphones portables

Il ya quelques précautions simples que les propriétaires de ces appareils peuvent prendre pour réduire les risques associés à ces dispositifs. Ils comprennent **[34]** :

- Les mots de passe ou des codes PIN pour empêcher les autres à accéder aux informations et données si l'appareil est perdu ou volé.
- Etre vigilent, de la même façon avec le courrier électronique régulier et la sécurité web, les messages et/ou sites tente de tromper l'utilisateur pour l'acheminer vers un contenu malveillant. As with a regular computer, "Think Before You Click".
- Désactivation des services tels que le Wi-Fi et Bluetooth quand ils ne sont pas utilisés.
- Téléchargement d'applications provenant de sources fiables. Les sources non crédibles peuvent intégrer des contenus malveillants dans leurs applications.
- Etre sûr de posséder toujours la dernière mise à jour du système d'exploitation et des applications installées. Ils sont mis à jour pour une

raison et c'est habituellement pour fournir plus de sécurité ou réparer des bugs.

- Exploitation au maximum possible des options de sécurité disponibles sur l'appareil.
- Utilisation de l'option "Remote essuyage" en cas de vol ou de perte du téléphone, elle permet de supprimer toutes ses données à distance.

II.7 La sécurité des données informatiques :

Les données sont à la fois la base de travail et l'historique de l'entreprise. Il existe différents types de risques qui peuvent toucher aux données d'une entreprise, les principaux sont **[35] :**

- Les virus et programmes malveillants ;
- Les Emails frauduleux ;
- Le piratage ;
- L'espionnage industriel ;
- La malversation ;
- La perte d'informations confidentielles ;
- L'erreur de manipulation.

Les principales actions à mener pour sécuriser les données informatiques sont :

- Protection de l'accès à internet ;
- Protection du réseau informatique ;
- Sauvegarde des données informatiques ;
- Filtrage des courriers électroniques ;
- Sensibilisation des utilisateurs ;
- Anticipation des incidents et minimisation de leurs impacts.

III Les technologies de prévention

Les technologies préventives sont couramment utilisées et sont généralement très efficaces. Elles peuvent être **[37]** :

- La télésurveillance ;

- Le contrôle d'accès ;
- Les alarmes et les détecteurs.
- La sécurité par Biométrie

III.1 La télésurveillance

La télésurveillance permet de superviser plusieurs lieux différents et d'enregistrer automatiquement les incidents et les anomalies. Quand de nombreuses caméras de surveillance sont installées dans divers endroits, un seul surveillant posté dans une centrale peut voir autant que quelques gardes.

III.1.1 Le but de la sécurité par télésurveillance

Les caméras visibles ont pour but ;

- De faire reculer les individus qui tentent de violer la loi. Elle produit donc un effet de dissuasion situationnelle.
- De guider une intervention rapide sur les lieux d'un incident. Constatant une intrusion, une agression ou toute autre anomalie, le préposé d'une centrale de surveillance peut demander l'intervention des personnes habilitées.
- D'enregistrer les incidents et donc reconnaitre les coupables.

III.1.2 Les éléments de la sécurité par télésurveillance

Un système de télésurveillance est formé de trois éléments ;

- **Les caméras** visibles ou invisibles ; équipées ou non de zoom et de téléobjectif; pouvant ou non être contrôlées à distance et être déclenchées par un mouvement inhabituel; pouvant ou non suivre automatiquement un individu dans ses déplacements, etc.
- **Les moyens de retransmission** de l'image captée par la caméra vers un moniteur.
- **Une centrale de surveillance** munie de moniteurs, magnétoscopes, voyants et autres avertisseurs.

Un système de télésurveillance peut être combiné à des détecteurs de mouvement, à un système d'alarme, à un appareil qui localise les sons et même à un appareil à rayons X pouvant détecter des armes dissimulées sous des vêtements, etc.

III.2 Le contrôle d'accès

Il a trois fonctions

1. Filtrer les personnes qui veulent entrer ou sortir d'un lieu ou encore les objets que l'on voudrait, soit introduire, soit faire sortir. Un système de contrôle d'accès laisse entrer les gens autorisés et interdire l'accès aux autres (suspects, bagarreurs connus, intrus, etc.). Il peut aussi empêcher que l'entrée à un établissement avec des armes ou des explosifs.

2. Empêcher la fuite des individus qui auraient commis un délit dans un lieu fermé. Un dispositif pour empêcher les gens d'entrer peut aussi être utilisé pour les empêcher de sortir. Il est possible, dans les banques, de bloquer la fuite d'un braqueur en l'enfermant entre deux portes fonctionnant comme un sas. Dans un magasin, les voleurs à l'étalage sont interceptés par des systèmes de détection des étiquettes électroniques ou magnétiques dissimulées dans les produits mis en vente.

3. Diriger l'enquête ; Quand un dispositif de contrôle d'accès par carte s'accompagne d'un enregistrement des entrées et des sorties, il permet de reconnaitre les personnes se trouvant dans un endroit au moment d'un incident ce qui aide à retracer les circonstances de l'incident.

Il est utile de distinguer deux éléments dans un système de contrôle d'accès.

1. L'identification permet de discriminer entre les individus qui sont autorisés à entrer ou à sortir et les autres.

2. L'autorisation ou l'interdiction d'entrer ou de sortir selon le résultat de l'identification.

III.3 Alarmes et détecteurs

L'alarme est le signal annonçant le danger ou attirant l'attention sur une anomalie. Elle permet de déclencher l'intervention qui s'impose.

Il est possible de distinguer dans un système d'alarme trois éléments.

1. Des détecteurs ou capteurs utilisent des systèmes électromagnétiques, des microondes, des rayons X, des cellules photo électriques, des ultrasons, etc. pour détecter les mouvements, les ouvertures de portes ou de fenêtres, les chocs, les vibrations, les bruits, des variations dans l'intensité lumineuse, la fumée, des explosifs, les perturbations d'un champ électrostatique, etc. On protège un périmètre par des capteurs installés aux portes, aux fenêtres, sur les murs, sur les clôtures, sous le sol, sur les toits et sur un objet, etc. Les capteurs peuvent balayer un espace pour y détecter les mouvements.

2. Le système de contrôle d'alarme : Dans les entreprises possédant un système d'alarme élaboré, le poste de contrôle a pour fonctions de recevoir les signaux émis par les capteurs, de traiter l'information, d'effectuer les discriminations nécessaires et d'envoyer des instructions. Les systèmes modernes possèdent généralement des algorithmes de détection qui empêchent le déclenchement d'alarmes intempestives.

3. Un signal : L'alerte est donnée par une sonnette, une sirène, des lumières ou un voyant lumineux, etc.

III.4 La sécurité par Biométrie

La biométrie **[38]** est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

III.4.1 Caractéristiques physiques :

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu, et il existe également pour chacune d'entre elles plusieurs façons de les mesurer.

Empreintes Digitales (finger-scan):la donnée de base dans le cas des empreintes digitales est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu.

Figure 3. Empreinte digitale

Les techniques utilisées pour la mesure sont diverses : Capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de température, etc. Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt) : mesure de la constante diélectrique relative du l'échantillon, sa conductivité, les battements de cœur, la pression sanguine, etc.

III.4.1.1 Géométrie de la main / du doigt (hand-scan):

Ce type de mesure biométrique est l'un des plus répandus, notamment aux Etats Unis. Cela consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) tel que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter-articulations, etc. La technologie associée à cela est principalement de l'imagerie infrarouge; d'une façon générale. Le système présente des FAR (False Acceptation Rate) assez élevés, surtout entre personnes de la même famille ou bien encore des jumeaux.

III.4.1.2 Iris (Iris-scan):

Ce dessin nous permet de distinguer entre l'iris et la rétine :

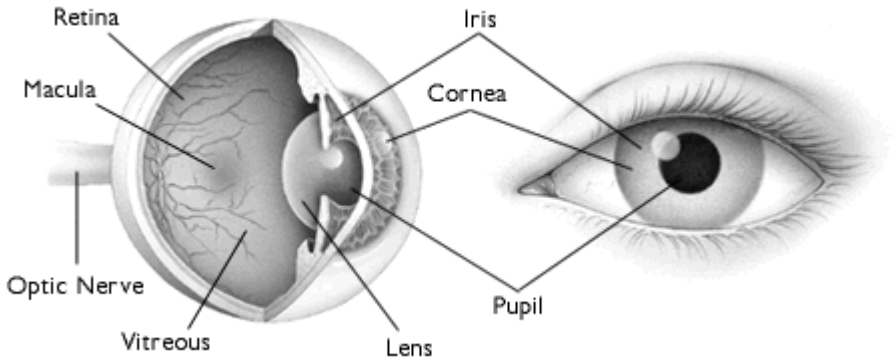

Figure 4 : Vue frontale et latérale d'un œil

Autrement dit, l'étude de l'iris porte sur la partie de l'œil visible ci-dessous :

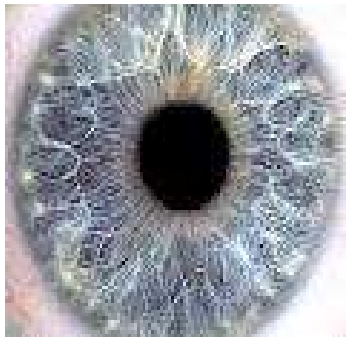

Figure 5 : L'iris de l'œil

En ce qui concerne l'iris, l'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. Celui-ci représente quelque chose de très intéressant pour la biométrie, car il est à la fois toujours différent (même entre jumeaux, entre l'œil gauche et le droit, etc.), indépendant du code génétique de l'individu, et très difficilement falsifiable. En effet, l'iris présente une quasi-infinité de points caractéristiques, qui ne varient pratiquement pas pendant la vie d'une personne contrairement à la couleur de l'iris qui, elle, peut changer. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc.

III.4.1.3 Rétine (retina-scan):

Cette mesure biométrique se base sur le fait que le schéma formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'œil) est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne.

III.4.1.4 Visage (facial-scan):

Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc. Il existe plusieurs variantes de la technologie de reconnaissance du visage.

III.4.1.5 Système et configuration des veines (vein pattern-scan):

Cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. Il s'agit ici d'analyser le dessin formé par le réseau des veines sur une partie du corps d'un individu (la main) pour en garder quelques points caractéristiques.

III.4.2 Caractéristiques comportementales

Outre les caractéristiques physiques, un individu possède également plusieurs éléments liés à son comportement qui lui sont propres :

III.4.2.1 Dynamique des frappes au clavier (keystroke-scan):

Selon le texte qu'on tape on aura tendance à modifier notre comportement de taper au clavier. C'est d'ailleurs un des moyens utilisés par certaines attaques (Timing-Attacks) pour inférer des mots de passe. Les mesures à faire sont : les durées entre frappes, la fréquence des erreurs, durée de la frappe elle-même, etc.

III.4.2.2 Reconnaissance vocale (Voice-scan):

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. Ils ne sont en général pas imitables.

III.4.2.3 Dynamique des signatures (signature-scan):

Ce type de biométrie est à l'heure actuelle peu utilisé mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents

électroniques, rapports, contrats, etc.). Le procédé est habituellement combiné à une palette graphique munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc. Bref, tout ce qui permet d'identifier une personne de la façon la plus sure possible quand on utilise une donnée aussi changeante que la signature.

Conclusion

Dans ce chapitre nous avons essayé de se mettre dans les différents coins ou les technologies de l'information et de la communication sont utilisées pour assurer la sécurité et d'évoquer leurs utilité. Dans ce contexte, nous avons constaté que les outils et technologies de l'information et de la communication sont à la fois, d'une part, cause de l'insécurité et d'autre part, un facteur pesant pour se sentir en sécurité. Certes, nous n'avons pas évoqué tous les domaines ou les Tics sont utilisés dans la sécurité, mais la liste présentée prouve une dépendance humaine vis-à-vis des Tics (on ne peut s'en séparés) et la confiance qu'on les porte pour notre sécurité.

Dans le chapitre suivant, nous présentons une étude de cas concernant l'utilisation des Tics dans la sécurité qui s'est déroulé au niveau de l'université 8 mai 1945 de Guelma.

Chapitre 4 : Méthodologie et présentation d'étude réalisée

Introduction

Ce chapitre concrétise les résultats obtenus pendant notre stage, on commence dans un premier temps par présenter la structure du questionnaire proposé pour faire la collecte d'informations nécessaires au sujet étudié. Ensuite, on enchaine par présenter l'analyse des résultats obtenus en essayant de justifier chaque résultat à part. Enfin, nous terminons par une conclusion dans laquelle nous valorisons les résultats obtenus.

I. Structure du questionnaire

Le questionnaire est un formulaire ou un processus d'interrogation qui couvre une série de questions servant à réunir d'une manière exhaustive les informations nécessaires au sujet étudié.

Notre questionnaire est divisé en deux parties, la première composée de 7 questions et intitulée «Informations générales». Cependant, La deuxième partie regroupe une série de 19 questions et intitulée « Questions relatives à l'utilisation des Tics dans la sécurité ».

Les réponses ont été fournies par un échantillon composé de 50 agents de sécurité travaillant à l'université 08 Mai 1945 de Guelma.

Dans les paragraphes qui suivent, nous étalerons les résultats obtenus :

Analyse des résultats obtenus

I.1 Distribution d'âge de l'échantillon étudié

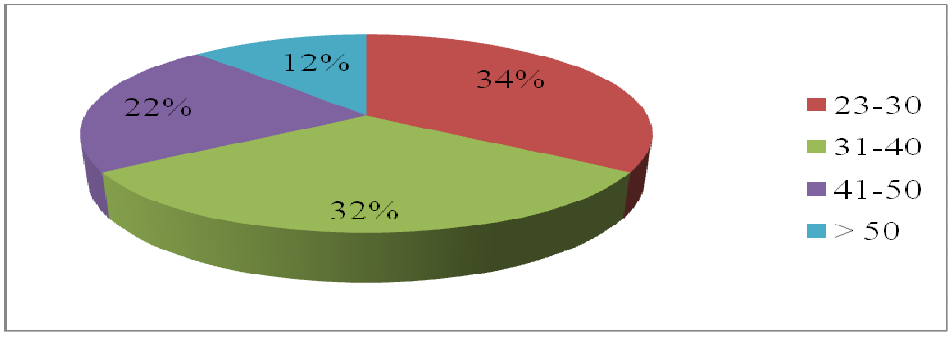

Figure 6. Distribution d'age de l'échantillon interrogé

On remarque que les agents de sécurité sont pour la majorité entre 23 et 40 ans (66% du totale des agents interrogés) parce c'est un métier qui demande de la concentration et une vigilance totale pendant les horaires de travail. L'autre tranche d'âge est surtout pour apporter de l'expérience et du savoir-faire.

I.2 Niveau éducatif selon la distribution d'age de l'échantillon étudié :

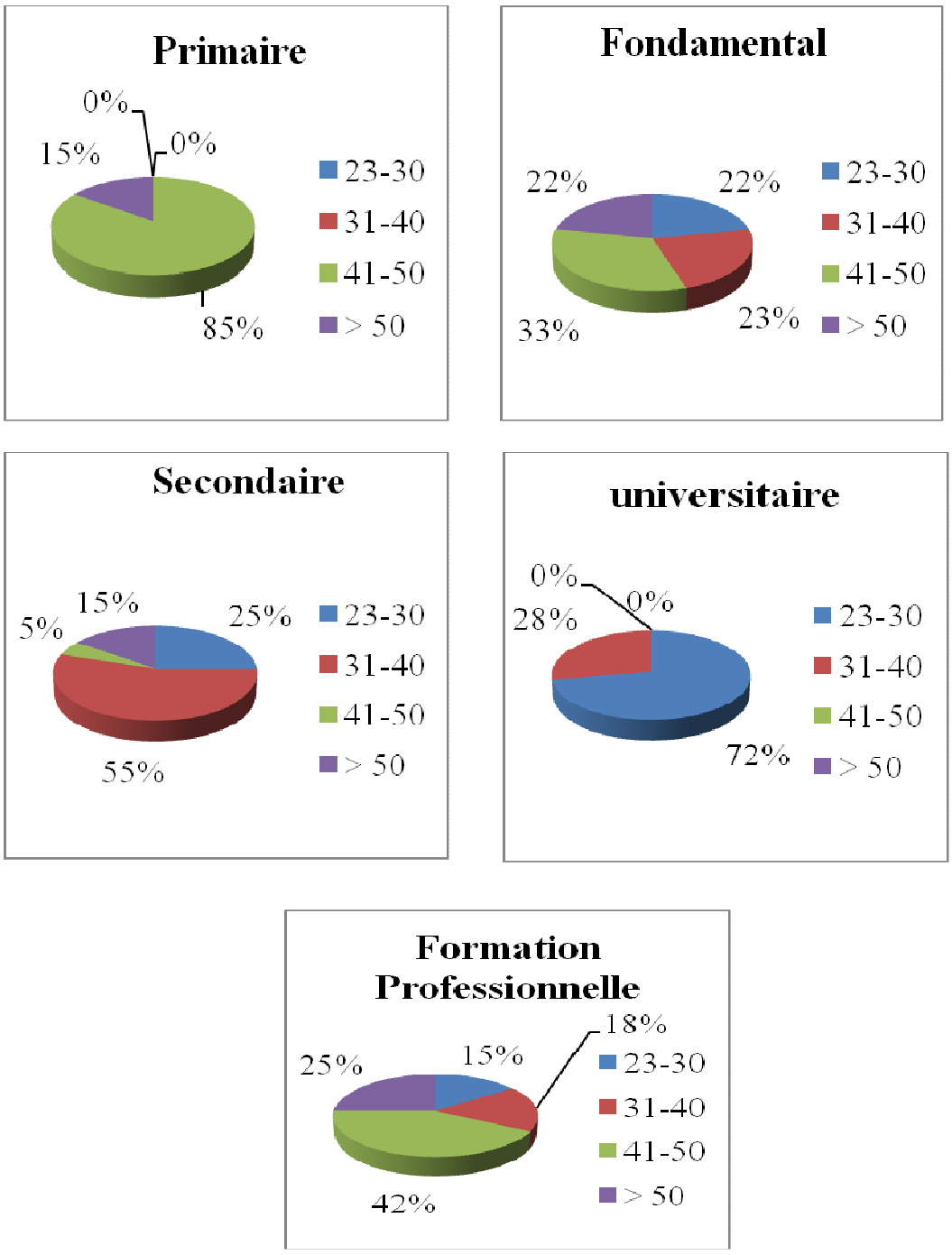

Figure 7. Niveau éducatif de l'échantillon interrogé

La majorité des jeunes agents ont un niveau d'étude universitaire ou secondaire alors que les plus âgés ont généralement passé par des formations professionnelles, cela est dû au faite que l'éducation et les études sont aujourd'hui plus accessibles qu'auparavant.

Le niveau d'étude élevé des jeunes leur procure une meilleure adaptation aux Tics et les aide à assimiler plus facilement leur fonctionnement, cela justifie plus tard beaucoup d'autres réponses.

I.3 Les Tics exploités par l'échantillon interrogé

La question posée était : « Quelles sont les Tics que vous avez exploités ? ». Les réponses des personnes interrogées sont présentées dans le schéma suivant :

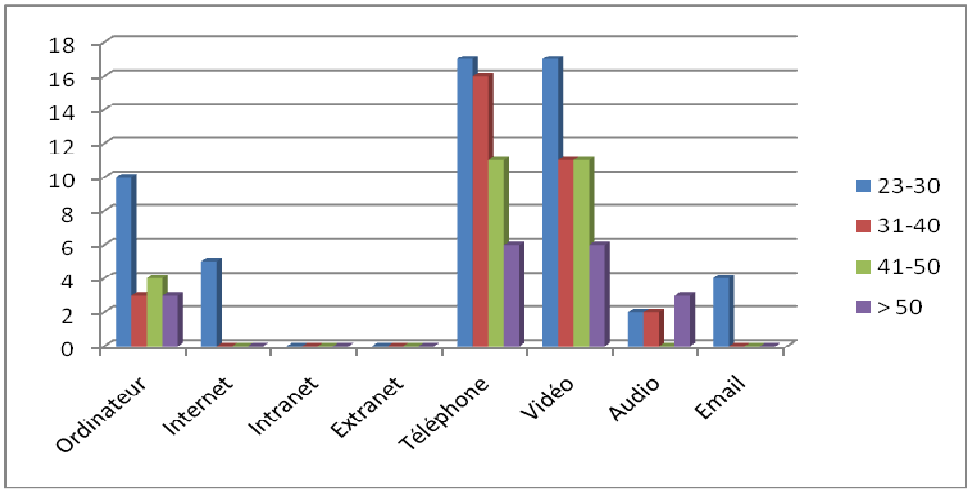

Figure 8 : Les Tics utilisés par l'échantillon interrogé

Les Tics sont généralement exploitées par la partie jeune de l'ensemble des agents de sécurité puisque ce sont eux qui ont les compétences, la curiosité, la volonté d'apprendre ces technologies et de suivre leur évolution.

Le téléphone mobile fait l'entente de tout l'échantillon interrogé, il est facile à utiliser et permet de se débarrasser des contraintes géographiques et de communiquer à faible coût. Les agents de sécurité l'utilisent pour communiquer et à des fins sécuritaires notamment les jeunes qui approuvent la simplicité et la fiabilité dans son utilisation. Cependant, cela diminue chez les plus âgés à cause du manque de maitrise de cet outil.

Assurer la sécurité par la vidéo est assez simple qu'avec ses propres yeux, cet outil est très souhaitable dans l'opération de sécurisation surtout pour les jeunes de plus en plus

dépendant des Tics, et à cause du confort à l'intérieur de la salle de contrôle et aussi son rendement effectif dans la sécurité.

Extranet et Intranet n'ont jamais été exploités par l'échantillon interrogé car ils sont utilisables dans un contexte d'échange de données et d'informations dans les réseaux d'entreprises. L'université dispose son propre réseau local, mais les agents ne sont pas dotés pour accéder à ce réseau.

Internet et le service E-mail sont à usage publique. L'utilisation de ces derniers est pratiquement monopolisée par la partie jeune de l'échantillon interrogé comme outils de communication et recherche d'informations.

L'ordinateur reste l'outil à usage multiple, qui facilite pas mal de tâches, comme les autres outils il est plus exploité par la partie jeune de l'échantillon interrogé.

I.4 But d'utilisation des Tics d'après l'échantillon interrogé

La question posée était : « Pourquoi vous utilisez les Tics ? ». Les réponses des personnes interrogées sont présentées dans le schéma suivant :

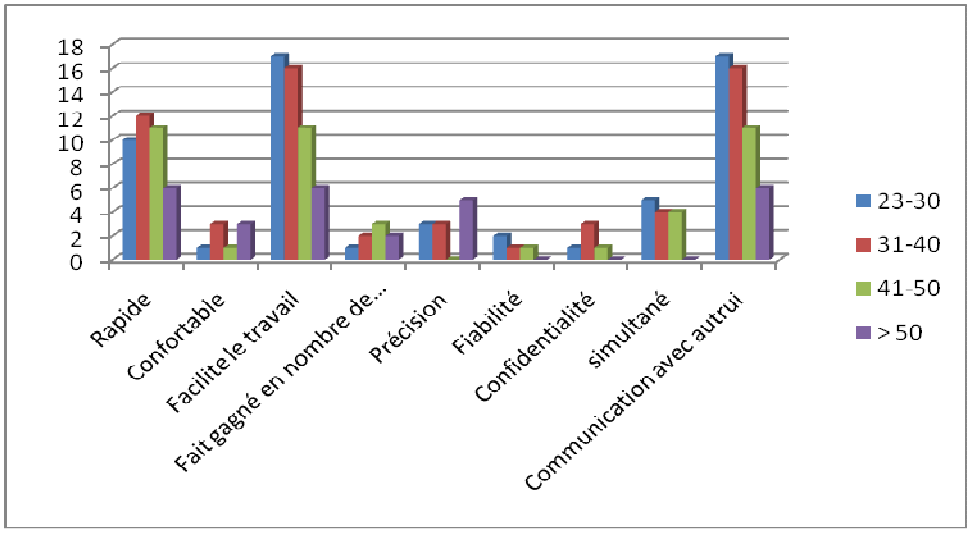

Figure 9. But d'utilisation des Tics d'après l'échantillon interrogé

On remarque que la facilité du travail est l'avantage des Tics le plus approuver par l'échantillon interrogé parce qu'ils permettent d'automatiser des tâches qui était pénibles et exige un certain nombre de personne pour les faire, comme la vidéosurveillance qui permet de surveiller seul un site sans avoir à être présent sur lieu, etc.

D'un autre coté la communication est intéressante vu que les agents de sécurité sont sensés travailler ensemble. Dans ce contexte, la communication est cruciale pour partager les informations au bon moment. Les agents utilisent le poste radio pour communiquer n'importe où (dans l'université bien sûr) et sans les moindres frais.

On voit aussi que la rapidité pousse les agents à utiliser les Tics. Car, aujourd'hui, le temps est très important et on est de plus en plus exigent en terme de temps de réponse et les Tics apportent un gain considérable en terme de rapidité, par exemple l'utilisation de l'E-mail pour transmettre très rapidement des données comme l'envoi d'un rapport.

I.5 Efficacité des Tics dans la sécurité

La question était la suivante : « Les Tics aident elles à assurer la sécurité ? ». Les résultats obtenus sont les suivants :

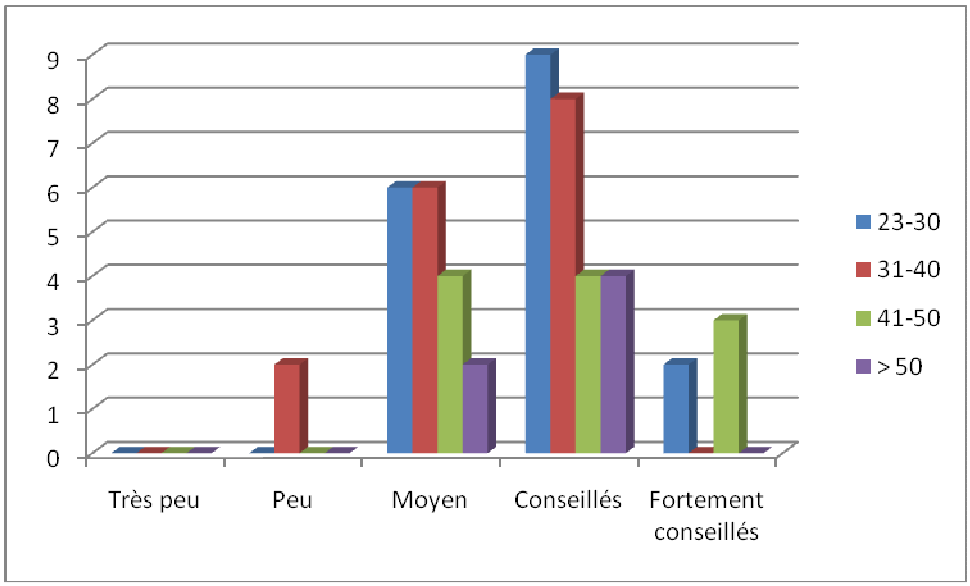

Figure 10. Efficacité des Tics dans la sécurité selon l'échantillon

Les Tics peuvent aider à garantir la sécurité, et la majorité des agents pensent que les Tics apportent un réel plus et une amélioration indéniable à leur travail.

I.6 Les Tics les mieux adaptés pour la tâche de sécurité

La question posée était la suivante : « Quelles sont les Tics qui conviennent mieux pour assurer la sécurité ? ». Les résultats obtenus sont présentés sur le schéma suivant :

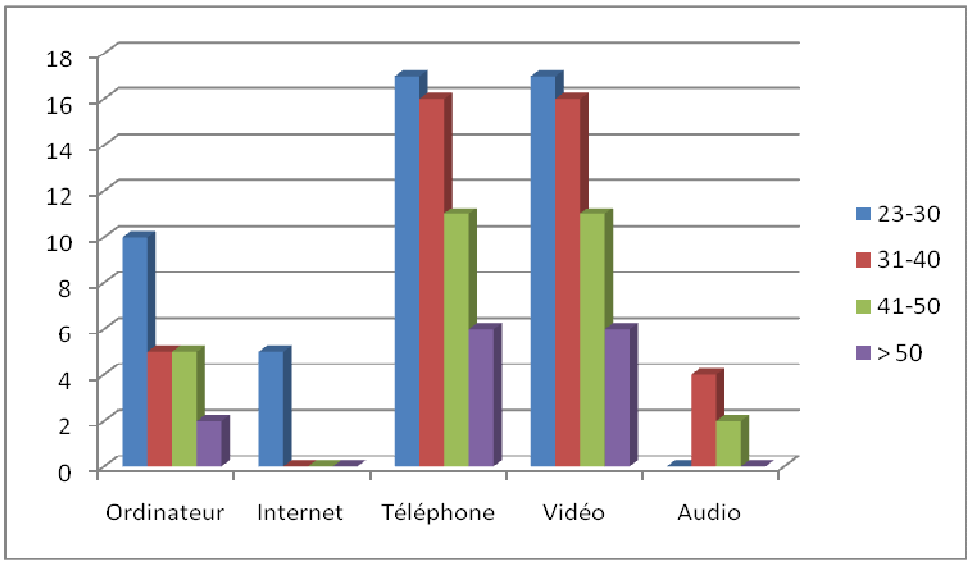

Figure 11 : Les Tics les mieux adapté pour la sécurité selon l'échantillon interrogé

D'après les personnes interrogées, les Tics qui apportent une véritable aide dans la tâche de sécurité sont : La vidéo et le téléphone et l'ordinateur.

Concernant la vidéo, elle apportent un réel plus à la sécurité parce qu'elle permet de surveiller plusieurs point géographiquement éloignés sur un petit écran et par un nombre réduit de personnes. De plus, avec les nouvelles technologies on peut intégrer des intelligences vidéo comme la détection de mouvement ou même si l'agent n'a pas remarqué, le logiciel peut notifier à l'aide d'une alarme l'agent pour qu'il puisse intervenir si nécessaire, donc la vidéo intéresse vraiment le personnel de sécurité parce qu'elle apporte des gains illimité en terme d'efficacité.

Pour le téléphone qui est un moyen de communication très pratique permettant de transmettre un message sans avoir à se déplacer vers son interlocuteur ce qui fait gagner beaucoup de temps aux agents de sécurité. En plus de ça, le téléphone est très répondu et utilisé par tout le monde ce qui le rend encore plus efficace.

L'ordinateur est souvent une interface pour l'utilisation des autres Tics comme la vidéosurveillance, les Emails, etc. En plus, l'ordinateur automatise des taches difficiles comme l'écriture des rapports, etc.

Les autre Tics et vu qu'elles sont un peu plus technique comme l'internet ou l'audio leurs utilité n'est pas directement perçu par les agents de sécurité et aussi elles chevauchent avec d'autre Tics comme les E-mails qui utilise l'internet, donc les agents ne remarquent que les Tics qui sont directement utilisées.

I.7 L'apport des Tics dans le travail de sécurité

La question posée était la suivante : « Les Tics apportent-elles une valeur ajoutée réelle dans votre travail ? », les résultats obtenus sont les suivants :

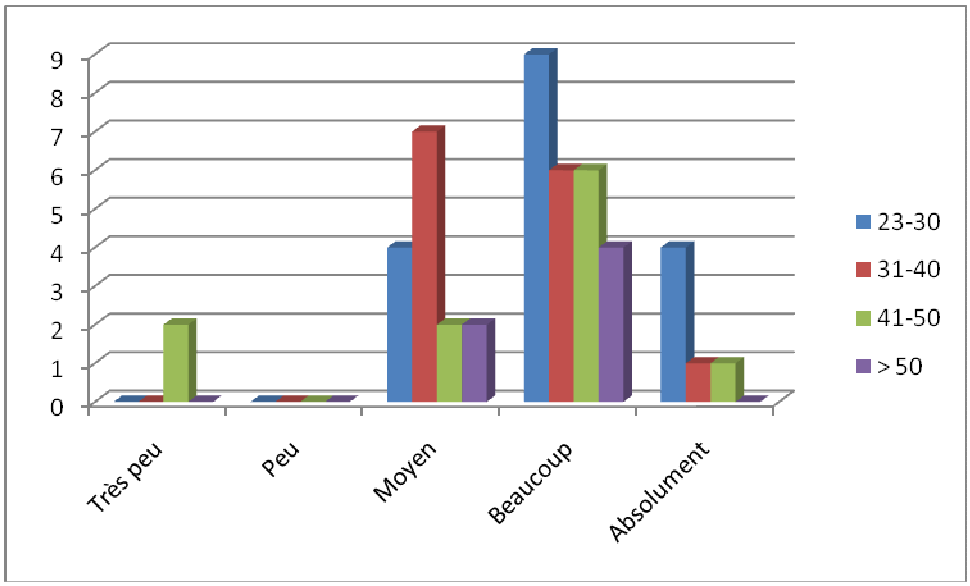

Figure 12. Apport des Tics dans la sécurité selon l'échantillon interrogé

Les personnes interrogées pensent que les Tics apportent une valeur ajoutée non négligeable à leur travail parce que ça leur permettra de faire leur travail avec moins d'effort. Si on prend a titre d'exemple le poste radio qui facilitera la communication qui est un point important et crucial dans le domaine de la sécurité ou bien la vidéosurveillance qui apporte un plus réel et de façon direct à la sécurisation des sites. La vidéosurveillance permet d'éviter de trop se déplacer et de surveiller plusieurs endroits en même temps et a distance. Donc, c'est évidant que les Tics apportent une valeur ajoutée significatif au travail des agents de sécurité.

I.8 Répercutions des Tics sur les méthodes de surveillance

La question posée était la suivante : « L'utilisation des Tics aura-t-elle des répercutions sur les méthodes de surveillance ? ». Les résultats obtenus sont présentés sur le schéma suivant :

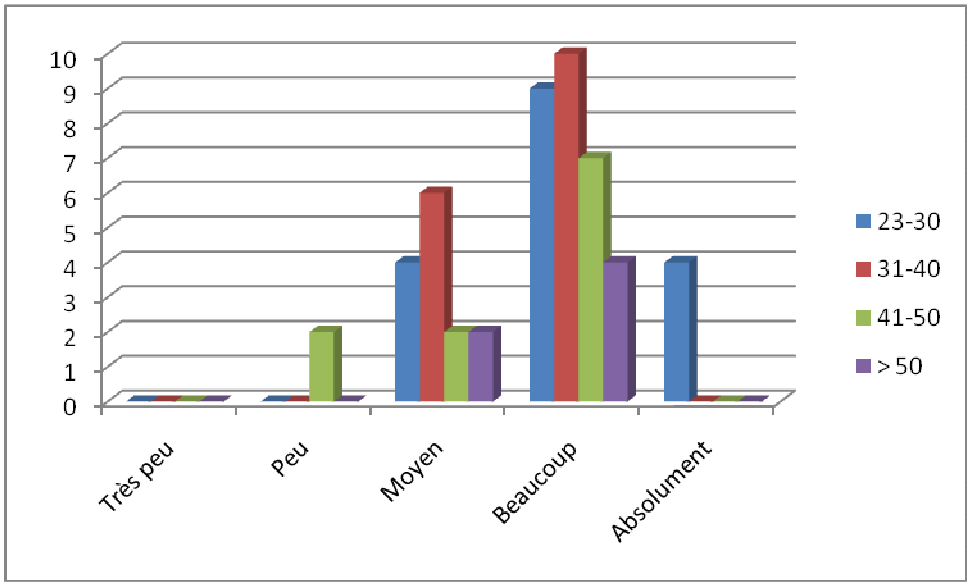

Figure 13. Répercutions des Tics sur les méthodes de surveillance

L'introduction des Tics n'améliore pas seulement le travail des agents de sécurité, mais elles apportent des changements dans les méthodes de travail, par exemple la vidéosurveillance va changer la façon de contrôler les lieux de l'université. Au lieu de faire une patrouille à chaque fois, l'agent peu vérifier les lieux sans se déplacer. Aussi, l'envoi des rapports par E-mail au lieu de les remettre manuellement. Un autre exemple, le responsable de sécurité peut recueillir par téléphone ou par poste radio les informations de différents agents sans avoir à se déplacer.

I.9 Les Tics actuellement utilisés

La question posée était la suivante : « Quelles sont les Tics actuellement utilisés pour assurer la sécurité dans l'université ? ». Les résultats obtenus sont présentés sur le schéma suivant :

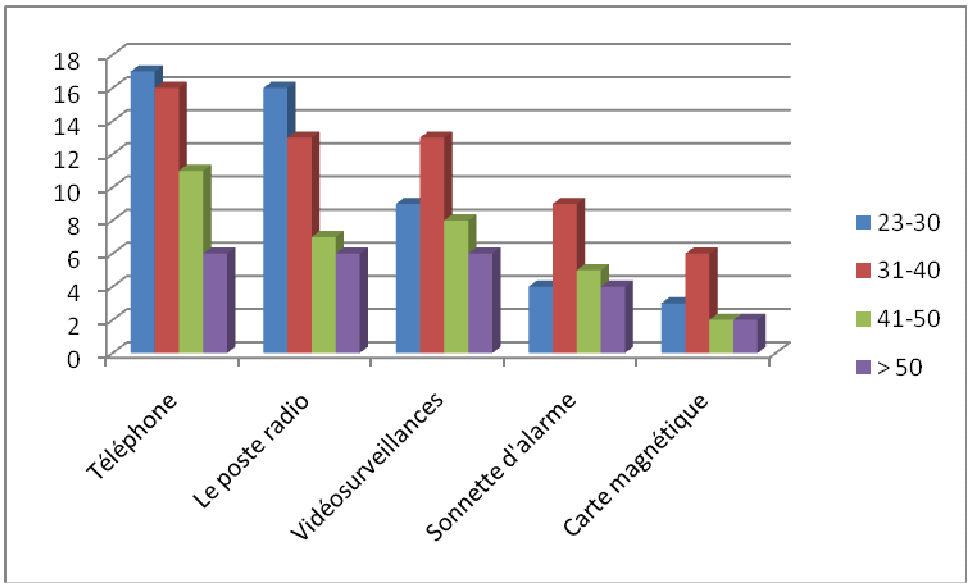

Figure 14. Les Tics utilisés dans l'université de Guelma

On remarque que le téléphone et le poste radio sont les plus utilisés avec un peu moins la vidéosurveillance.

L'utilisation du téléphone chevauche entre travail professionnel et vie personnel, donc il est tout le temps utiliser et tout le monde devient dépendant.

Le poste radio est le moyen de communication officiel utilisé par les agents de sécurité dans l'université de Guelma.

L'utilisation de la vidéosurveillance est entrain de s'accroitre considérablement : sécurisation des accès et des points névralgiques comme les directions par exemple.

L'université est dotée d'un système d'alarme, mais il est plutôt réservé au cas d'urgence extrême.

Et les cartes magnétiques sont utilisées pour contrôler l'accès aux restaurants universitaire.

I.10 Contrôle de l'accès à l'université

La question posée était la suivante : « Comment vous autoriser l'accès à l'université?». Les résultats obtenus sont présentés sur le schéma suivant :

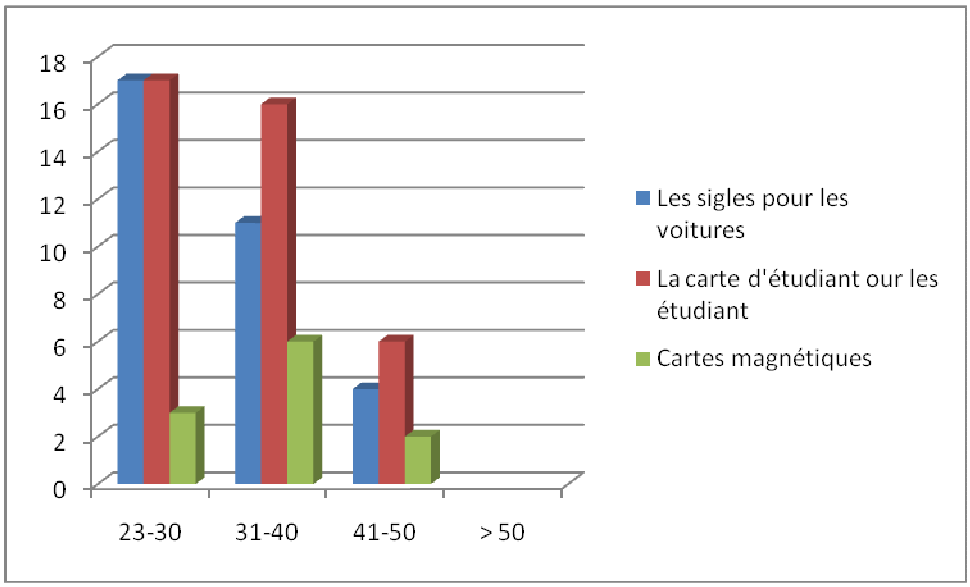

Figure15. Contrôle d'accès à l'université de Guelma

Les agents de sécurité se basent sur les normes de sécurités les plus simples et les plus sûres. La carte étudiant est l'outil traditionnel pour identifier si les personnes sont autorisées et qu'ils ne sont pas des intruses.

L'université a conçu un sigle d'authentification qui sera le mot de passe pour les personnes véhiculées pour entrer à l'université. Les agents de sécurité se basent sur ce concept de sigle pour permettre l'entrée légale.

Quant à la technologie de cartes magnétique, son utilisation est limitée à la restauration.

I.11 Tics utilisés, pour détecter un évènement suspect :

La question posée était la suivante : « Si un évènement suspectes produit, quel sont les Tics qui vous permettent de le détecter ?». Les résultats obtenus sont présentés sur le schéma suivant :

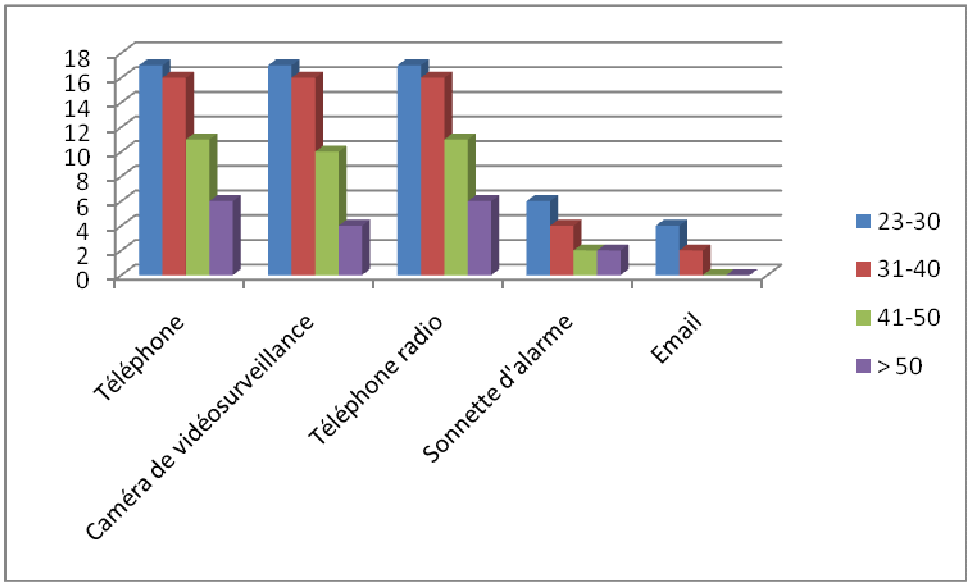

Figure16: Les Tics utilisés, pour détecter un évènement suspect

Quand un évènement suspect se produit, les agents de sécurité auront connaissance de l'arrivée de cet évènement soit directement en le voyant par leur propres yeux, ou sur l'écran du centrale de contrôle, comme ils peuvent le connaitre par un collègue qui leur communique l'information par téléphone ou poste radio.

I.12 Les Tics utilisés pour informer un évènement suspect

La question posée était la suivante : « Si un évènement suspect se produit, quels sont les Tics que vous utilisez pour informer de cet évènement ? ». Les résultats obtenus sont présentés sur le schéma suivant :

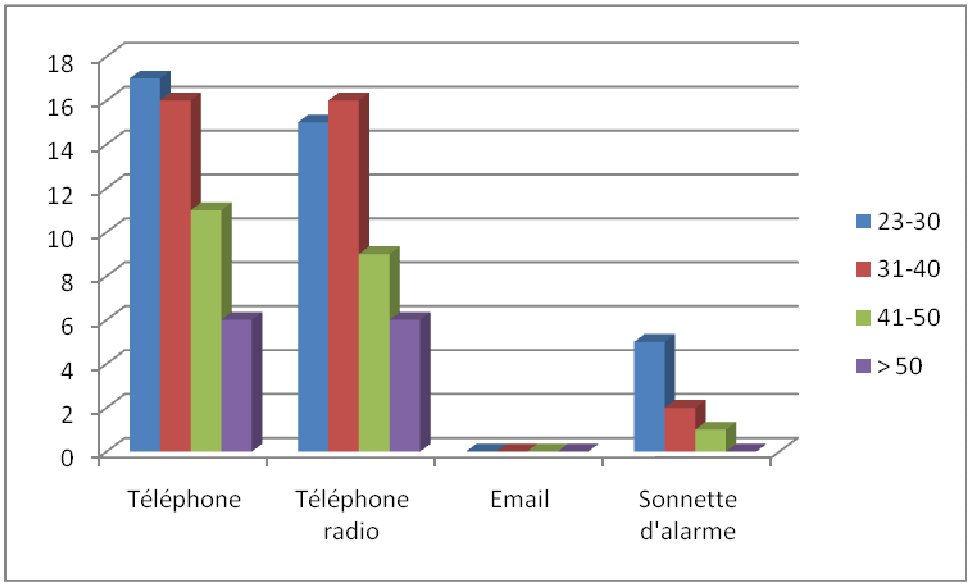

Figure 17. Les Tics utilisés dans les cas d'urgence

Pour assurer la fonction de sécurité dans l'entreprise, la vigilance doit être présente tout le temps. Si un évènement suspect aura lieu, les agents de sécurité doivent réagir très rapidement pour gérer le problème. Le téléphone Fixe, le téléphone Mobile ou le poste radio représente le moyen le plus efficace en termes de rapidité à réagir et le moyen le plus disponible qui permet de communiquer et passer le message (information) aux responsables le plus vite possible.

Informer cet évènement par le moyen téléphonique est plus discret qu'avec la sonnette d'alarme qui pourra engendrer de l'anarchie et la perturbation au niveau de l'université.

L'E-mail n'est pas utilisé car il n'est pas opérationnel pour les évènements qui exigent la rapidité de transmission de l'information et l'intervention sur place.

Conclusion

Dans ce chapitre, nous présenté les résultats obtenus suite à un stage effectué au niveau de l'université 8 mai 1945 de Guelma. Les résultats nous ont permet de reconnaitre les moyens disponibles et les mesures mises en place pour assurer la sécurité au niveau de l'université.

On a pu dans un premier lieu reconnaitre la distribution d'âge et le niveau éducatif des agents de sécurité de l'université. Pour ensuite se rendre compte de leur expérience dans l'utilisation des différents outils et techniques des Tics ainsi que les buts pour lesquels ils les utilisent.

Aussi, on a pu reconnaitre l'avis des agents de sécurité sur l'efficacité de l'utilisation des Tics pour garantir la sécurité, ceux les mieux adapté pour ce travail et leur apport dans le déroulement des différentes tâches ainsi que leurs répercussions sur les méthodes de surveillance.

De plus, on a pu reconnaitre les Tics actuellement utilisés dans l'université de Guelma et les moyens utilisés pour contrôler l'accès à l'université et ceux permettant de détecter et d'informer le déroulement d'un incident.

L'efficacité de la sécurité au niveau de l'université est assurée par la qualification des agents et leurs capacité d'adaptations aux Tics, parce qu'au final c'est le facteur humain qui est le plus important.

Conclusion générale

Pour se sentir en sécurité il faut investir et de prendre des précautions et des mesures pour pallier aux différents risques et menaces qui guettent les personnes, les sociétés et les entreprises. L'utilisation des Tics pour maintenir la sécurité est un choix primordial pour toute personne, société ou entreprise voulant garantir sa sécurité.

Dans ce mémoire nous avons traité ce sujet, à savoir : l'utilisation des Tics dans la sécurité. On a commencé par présenter les différentes notions et concepts liée à la représentation de l'information et la communication pour enchainer par la présentation des différents techniques et technologies permettant la communication, l'échange et la transmission de l'informations, ces techniques et technologies sont multiples et chacune convient mieux pour certains types de communication et de partage d'informations que d'autres. Ensuite, nous avons présenté des différents outils et techniques des Tics utilisés dans la sécurité. Pour finir ce mémoire, une présentation d'une étude réalisée au niveau de l'université 8 mai 1945 de Guelma portant sur le sujet de l'utilisation des Tics dans la sécurité a été faite.

Cette étude nous a permet de se rendre compte que l'université fait de plus en plus recours aux Tics pour garantir sa sécurité, surtout dans les points névralgiques où la vidéosurveillance est utilisée, nous avons constaté que les agents de sécurité les plus jeunes sont plus aptes à opter pour l'utilisation et l'apprentissage de nouveaux outils de sécurité.

Enfin, nous avons conclu que le facteur humain est plus important que les Tics utilisés, car, c'est le personnel qualifié qui est capable de maitriser et d'interagir avec le système mis en place (techniques et technologies des Tics utilisés dans la sécurité).

La bibliographie

[1] http://ICM_c_Elements de communication_V1.pdf.

[2] http://Communication-Définition- Encyclopédie en ligne/www.techno-science.net/?... définition.2010.

[3] TheFreeDictionary: http://fr.thefreedictionary.com/technique

[4] oumeddour youcef, benabda rafik, impact des NTIC sur les techniques d'information et de communication dans l'enseignement supérieur en Algérie, Encadré par .Mr.Kelaiaia Abdesslem, Département de gestion, Guelma, Juin, 2010

[5] http:// Principaux types de communication.fr.wikipedia.org/wiki/Communication

[6] http:// Les Six Eléments De La Communication/www.nairaland.co.m/nigeria/topic- Block all nairaland.com results.2009.

[7] http://(Univ, 2009) …/gc/gomari/…/introduction1567.pdf. www.univ-tlemcen.dz/2009.

[8] http:// Les types de communication.users.skynet.be/intelligence/com./types.htm- Block all skynet.be results.2001.

[9] Jean-Paul la France ; Thibault-laulan ; Anne marie « place et rôle de la communication dans le développement international» Québec ; 2006 ; p59.

[10] http://www.olats.org/schoffer/definfo.html

[11] http://www.les-infostrateges.com/article/031264/definition-objective-de-l'information

[12] http://www.phpeasydata.com/annuaire/documentation/les-differents-types-d'information fr.html

[13] Gabriel Gallezot ; techniques de l'information : usage de l'I.S.T ; France ; 2000.

[14] http://www.maxicours.com/soutien-scolaire/information-et-gestion/1re stg/184320.html

[15] http:// document ; accès à l'information : la recherche documentaire /www.pedagene.creteil.iufm.fr/internet/recherc.htm.2008.

[16] http://fr.wikipedia.org/wiki/Information

[17] Michel Barrot. Information et entreprise.pdf

[18] http://www.guidepme.com

[19] www.wikipédia.com

[20] Yannick Chatelain et loick Roche « cyber gagnant » Maxima Paris ,2000.

-Scott Mueller, Le PC Architecture, maintenance et mise à niveau,Pearson, 2009.

[21] Communication-Définition-Encyclopédie scientifique en ligne ; www.techno-scienc.net/onglet…..3982.2010

[22] Extrait de « Le Guide Complet » 06/2009 – Jérôme Souc.

[23] http://europa.eu/legislation_summaries/information_society/index_fr.htm

[24] Alain Fernandel « le bon usage des technologies expliqué au manager »Edition d'Organisation 2001.

[25] Marie Héleine Hélpher « Communicator »Dunod Paris, 1998.

[26]http:/ /www.securiteinf.com.

[27] http://www.commentcamarche.net/contents/secu/secuintro.php3

[28] Gérard-Michel Cochard« Les dangers qui guettent les SI -Les aspects de la sécurité informatique- » Pearson, 2010.

www.securite-informatique.gouv.fr

[30] www.cnetfrance.fr/.../dix-conseils-pour-securiser-votre-pc-39197790.htm

[31] www.awt.be/web/sec/index.aspx.

[32] www.murielle-cahen.com/.../p_telecom.asp

[33] http://www.securiteinfo.com.

[34] http://www.ballarat.edu.au/is/ict/security.

[35] http://www.securiteinfo.com.

[36]www.murielle-cahen.com.

[37] Maurice Cusson« la cyber-sécurité pour les pays en développement » ITU ; Union internationale des telecommunications,CIMICHELLA Sandro,2006.

[38] http://capirossi.org/info/Securite/Securite.pdf

Liste des figures

Acronymes

TIC : technologies de l'information et de la communication

CPU : Central Processing Unit, unité centrale de traitement.

RAM : Random Access Memory, mémoire à accès aléatoire.

CD : Compact Disc

DVD : Digital Versatile Disc

DNS: Domain Name System

PAN: Personal Area Network

LAN: Local Area Network

MAN: Metropolitan Area Network

WAN : Wide Area Network

IRC : Internet Relay Chat

EDI : Echanges de Données Informatisées ; Electronic Data Interchange

EDIFACT : Echanges de Données Informatisées Pour le Commerce Administratif et le Transport

BTP : Bâtiments de travaux publics

AP : Accès Poin

WEP : Wired Equivalent Privacy

WPA: Wi- fi Protected Access

VPN: Virtual Private Network

VPN IPSec: Virtual Private Network Internet Protocol Security

ISO: International Organization for Standardization

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 8 mais 1945 -Guelma-

Faculté des sciences économiques, commerciale et sciences de gestion

Département de sciences de gestion

Questionnaire de Master

Madame/Monsieur,

Par le présent questionnaire, nous sollicitons votre participation à une étude effectuée dans le cadre de préparation d'un mémoire de Master.

Nous vous prions de répondre à ce questionnaire dans le but d'élargir le champ de la connaissance scientifique et nous permettre d'avoir une vision plus claire du sujet étudié.

Il est important, pour la qualité de notre travail, que vos réponses soient précises et reflétant réellement vos avis et connaissances.

Informations générales

1. **Age :** ……..
2. **Le sexe :**

   ☐ Homme ☐ Femme

3. **Fonction occupée :**

   ☐ Agent de sécurité
   ☐ gardien
   ☐ Chef service
   ☐ Autre. Préciser : ……..

4. **Niveau éducatif :**

   ☐ Primaire
   ☐ Fondamental
   ☐ Secondaire
   ☐ Formation professionnelle
   ☐ Universitaire

5. **Nombre totale d'employé dans votre poste :** ……..

6. **Quelles sont les Tics[1] que vous avez exploités ?**

- ☐ Ordinateur
- ☐ Internet
- ☐ Intranet
- ☐ Extranet
- ☐ Téléphone
- ☐ Vidéo
- ☐ Audio
- ☐ Email
- ☐ autre. Préciser : ……..

7. **Pourquoi vous utilisez les Tics ?**

- ☐ Rapide
- ☐ Confortable
- ☐ Facilite le travail
- ☐ Fait gagné en nombre de personnel
- ☐ Précision
- ☐ Fiabilité
- ☐ Confidentialité
- ☐ Simultané
- ☐ Communication avec autrui

8. **Les Tics aident elles à assurer la sécurité ?**

- ☐ Très peu
- ☐ Peu
- ☐ Moyen
- ☐ conseillés
- ☐ Fortement conseillés

[1] Technologies de l'information et de la communication

9. Quelles sont ceux qui conviennent mieux pour assurer la sécurité ?

- ☐ Ordinateur
- ☐ Internet
- ☐ Téléphone
- ☐ Vidéo
- ☐ Audio
- ☐ autre. Préciser : …….

10. Les Tics donnent-elles une valeur ajoutée réelle dans votre travail ?

- ☐ Très peu
- ☐ Peu
- ☐ Moyen
- ☐ Beaucoup
- ☐ Absolument

11. L'utilisation des Tics aura-t-elle des répercutions sur les méthodes surveillance ?

- ☐ Très peu
- ☐ Peu
- ☐ Moyen
- ☐ Beaucoup
- ☐ Absolument

12. Quelles sont les Tics actuellement utilisés pour assurer la sécurité dans l'université ?

- ☐ Téléphone
- ☐ Le poste Radio
- ☐ Vidéosurveillances
- ☐ Sonnette d'alarme
- ☐ Carte magnétique
- ☐ Autres. Préciser : …….

13. Comment vous autoriser l’accès à l’université ?

- ☐ Les sigles pour les voitures
- ☐ La carte d’étudiant pour les étudiants
- ☐ Cartes magnétiques
- ☐ Autres. Préciser : …….

14. Comment vous vous comporte avec une personne étrangère qui veut accéder à l’université ?

- ☐ Véhiculé : ……
- ☐ piétant : …….

15. Si un évènement suspectes produit, quel sont les Tics qui vous permettent de le détecter ?

- ☐ Caméras de vidéosurveillance
- ☐ Téléphone radio
- ☐ Téléphone
- ☐ Sonnette d’alarme
- ☐ Email
- ☐ Autre. Préciser : ……

16. Si un évènement suspect se produit, quel sont les Tics que vous utilisez pour informer decet évènement ?

- ☐ Téléphone radio
- ☐ Téléphone
- ☐ Email
- ☐ Alarme
- ☐ Radio phonie
- ☐ Autre. Préciser : ……