Centre Africain d'Etudes Supérieures en Gestion

CESAG EXECUTIVE EDUCATION

(CEE)

MBA-Audit et Contrôle de Gestion

(MBA-ACG)

Promotion 25

(2013-2014)

Mémoire de fin d'étude

THEME

AUDIT DE LA SECURITE DU PARC INFORMATIQUE DE CONGO TELECOM

Présentée par :

Migi MPIKA RAZANDRY

Dirigé par :

M. Alain Sawadogo

Enseignant associé au CESAG

Avril 2015

DEDICACE

Nous dédions ce présent mémoire à :

- L'Eternel notre Dieu qui jusqu'ici nous a secouru ;
- Nos parents pour leur amour, leur affection, leur compréhension, leur confiance ainsi que leur soutien sans faille, tant matériel qu'émotionnel ;
- Nos deux grandes sœurs Tahiry et Gickelle pour leur amour, leur soutien et leur grande contribution dans nos vies ;
- Nos deux petites sœurs adorées, Nahomie et Yedidia.
- Nos chers amis qui ont toujours été là pour moi de loin comme de près à savoir Chancy, Gloria, Louison et Stève.

REMERCIEMENTS

Il est vrai qu'aucun travail humain ne s'accomplit dans la solitude. Plusieurs personnes ont contribué à l'aboutissement de ce travail et c'est pourquoi nous adressons nos sincères remerciements à :

- Monsieur AKOUALA, Administrateur Général de Congo Télécom ;
- Monsieur Jean Marie NGOUMBOLO, responsable des ressources humaines à Congo Télécom ;
- Monsieur Antoine NZILI, responsable de la formation ;
- Monsieur Crépin ITOUA, auditeur principal à Congo Télécom pour son encadrement ainsi que ses conseils;
- Monsieur Alphonse KOMBO, auditeur à Congo Télécom pour la disponibilité qu'il a montré à notre égard pendant toutes nos préoccupations;
- Monsieur Bruno KANGA responsable du service informatique pour son suivi et tout le temps qu'il nous a accordé malgré son indisponibilité, ainsi que son équipe ;
- Monsieur Alain SAWADOGO, notre professeur et directeur de mémoire pour son aide, ses remarques et directives ainsi que ses multiples encouragements. Puisse-t-il trouver ici l'expression de notre admiration et de notre profonde gratitude ;
- Monsieur Moussa YAZI, notre professeur d'audit interne et Directeur de la formation ;
- Monsieur Bertin CHABI, responsable du département CESAG EXECUTIVE EDUCATION ;
- Nos collègues de la 25ème promotion du MBA Audit et Contrôle de Gestion du CESAG ;
- Toute la communauté congolaise du CESAG ;

LISTE DES SIGLES ET ABREVIATIONS

ACK : Acknowledgment

ADSL : Asymmetric Digital Subscriber Line

AEF : Afrique Equatoriale Française

AFAQ : Association Française pour l'Assurance de la Qualité

AFNOR : Association Française de Normalisation

AG : Administrateur Général

ANSI : American National Standard Institute

ASTM: American Society for the Testing of Materials

BSI : British Standard Institute

CE : Communauté Européenne

CEI : Commission Électrotechnique Internationale

CEN : Comité Européen de Normalisation

CENELEC : Comité Européen de Normalisation pour l'Électrotechnique

CRF : Caisse de Retraite des Fonctionnaires

DAC : Direction d'Audit et Contrôle

DCNE : Direction de la Caisse Nationale d'Epargne

DGCA : Direction Générale de la Culture et de l'Art

DGGT : Direction Générale des Grands Travaux

DIN : Deutsche Industrie Normen

DMZ : Demilitarized Zone

ETSI : European Telecommunications Standard Institut

FRAP : Feuilles de Révélation et d'Analyse des Problèmes

OHADA : Organisation pour l'Harmonisation en Afrique du Droits des Affaires

IBN : Institut Belge de Normalisation

IDS : Intrusion Detection System

INTELCO : Office des Télécommunications Internationales du Congo

INRS : Institut National de Recherche et de Sécurité

IP : Internet Protocol

ISO : International Organization for Standardization

IUTA : Institut Universitaire de Technologie (point A)

MAC : Media Accès Control

NFS : Network File System

NTIC : Nouvelles Technologies de l'Informatique et de la Communication

OEPT : Office Equatoriale des Postes et Télécommunications

ONPT : Office Nationale des Postes et Télécommunications

PNC : Projet de Couverture National

QPC : Questionnaire de Prise de Connaissance

RSSI : Responsable de la Sécurité des Systèmes d'Information

SAU : Société Anonyme Unipersonnelle

SAV : Service Après-Vente

SGSI : Système de Gestion de la Sécurité de l'information

SI : Système d'Information

SMSI : Système de Management de la Sécurité de l'Information

SNMP : Simple Network Management Protocol

SNV: Schweizerischen Normen Vereinigung

SOTELCO : Société des Télécommunications du Congo

SOPECO : Société des Postes et de l'Epargne du Congo

SSC: Standards Council of Canada

SSI : Sécurité des Systèmes d'Information

SYN : Synchronize

TRS : Taux de Rendement Synthétique

TCP : Transmission Control Protocol

UIT : Union Internationale des Télécommunications

USB : Universal Serial Bus

UTE : Union Technique de l'Électricité

VPN : Virtual Private Network

WACS : West Africa Cable System

3G : Troisième génération

LISTE DES TABLEAUX & FIGURES

FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

AVANT-PROPOS

Le CESAG est une Institution postuniversitaire de formation, de perfectionnement, de consultation et de recherche en gestion. Il a été créé en application d'une décision prise par les Chefs d'Etat de la CEDEAO à la Conférence de Bamako en 1978.

L'objectif visé était de doter les pays membres d'une école communautaire capable de former des gestionnaires efficaces tout en tenant compte des réalités de l'environnement africain.

Entré en activité en 1985, le CESAG s'est imposé comme la principale grande école de formation en management en Afrique francophone au Sud du Sahara.

La mission du CESAG s'articule autour des points ci-après :

- former les cadres des entreprises privées et publiques, de l'administration et d'organisations diverses avec une vision régionale et africaine ;
- être une Institution postuniversitaire et complémentaire des Institutions existantes ;
- perfectionner et recycler les cadres en matière de gestion ;
- former des formateurs pour les Institutions de formation en gestion de la région.

Le CESAG assure différentes formations dont le MBA en audit et contrôle de gestion pour l'obtention du diplôme en audit et contrôle de gestion.

C'est dans le cadre de cette formation qu'un stage est prévu en fin d'études et conditionne l'obtention du diplôme en audit et contrôle de gestion. Ce stage devra permettre à l'étudiant d'avoir une première approche de la vie professionnelle et de mettre en pratique ses acquis théoriques, ainsi que de parfaire ses connaissances dans le cadre de sa formation.

C'est donc à cette fin que j'ai été amenée à effectuer mon stage au sein de Congo Télécom.

TABLE DES MATIERES

INTRODUCTION GENERALE

De nos jours, avec le progrès technique et l'évolution de l'informatique, toute entreprise voulant être dynamique, présente et efficace sur un marché quelconque doit nécessairement se doter d'outils informatiques. Depuis les années 70, l'intégration de l'informatique dans les processus de l'entreprise est devenue un levier de génération de croissance et un support pour la mise en œuvre de la stratégie. Cette intégration a généré au sein de l'entreprise, les risques informatiques qui sont relatifs aux choix des structures d'organisation, aux modes de fonctionnement et aux méthodes de surveillance des activités du système d'information.

Du fait du développement des Nouvelles Technologies de l'Informatique et de la Communication (NTIC), nous pouvons assister à une forte augmentation des risques dans le domaine de l'informatique ainsi que dans toutes les structures en activité. Chaque organisme doit établir un audit de sécurité informatique périodiquement afin d'identifier ses sources de menace et ses dégâts informationnels. En effet, tous les pays aspirent au développement de leurs organisations, qu'elles soient privées ou publiques, mais cela ne peut être atteint en l'absence de bonne gouvernance, d'une bonne sécurité de son parc informatique et d'une bonne maitrise de ses risques. L'expansion de toute organisation repose alors sur plusieurs éléments stratégiques tels que l'audit, le contrôle interne, l'organisation interne et l'information.

Les solutions informatiques sont actuellement indispensables aux activités de n'importe qu'elle structure, qu'elle se présente sous forme de sociétés ou d'un groupement de nature différente. Il faut souligner que cette nécessité d'emploi est essentiellement due à leur caractère multitâches et de ce fait, elles s'avèrent être des outils de travail primordiaux.

La sécurité du parc informatique comprenant l'ensemble des solutions informatiques dont dispose une organisation se doit de garantir :

- La disponibilité de l'information ;
- l'intégrité de l'information ;
- la confidentialité de l'information.

Il est en lui-même un processus complexe, souvent exposé à plusieurs zones de prédilection de risques apparents. Ce problème est encore tapageur dans les administrations publiques et nécessite une mise en place des solutions idoines pour le résoudre.

Cependant, Congo Télécom est une entreprise d'Etat qui ne procède pas régulièrement à l'audit de la sécurité de son parc informatique. L'absence d'une telle vigilance et d'un manque de contrôle permanent pourrait s'expliquer par :

- Un manque de volonté de dirigeants ;
- le nombre insignifiant des auditeurs en interne ;
- le manque d'organisation au sein du service ;
- l'absence de rigueur dans le travail ;
- le manque de motivation salarial auprès des employés.

Cela est susceptible d'entrainer plusieurs conséquences au sein de l'entité. Il s'agit notamment de :

- Possibilité d'usurpation d'identité ;
- malversations et fraudes ;
- dysfonctionnement du réseau informatique ;
- mécontentement des utilisateurs ;
- retard dans le traitement des données ;
- non atteinte des objectifs fixés ;
- non fiabilité de l'information comptable et financière ;
- difficulté de prévenir ou de détecter les risques ;
- absence d'une bonne gouvernance informatique.

Pour pallier cela, un audit sur la sécurité du parc informatique est nécessaire afin de détecter et prévenir le cas échéant les risques liés à la mauvaise gestion de la sécurité du parc informatique à Congo Télécom. C'est la famille des normes ISO 27000 qui traite de la problématique de la sécurité de l'information, ainsi la sécurité du parc informatique regroupant l'ensemble des actifs de l'entreprise (les matériels, les logiciels, les services, l'information, le personnel…) consistera à une mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) s'appuyant sur la norme ISO 27001 : 2005. Il est basé sur le principe du PDCA (Plan, Do, Check, Act).

Disposer d'une information fiable, actualisée et sécurisée est primordial pour le pilotage des entreprises. Le système d'information et de communication est un facteur clé de succès pour les stratégies du dirigeant, le développement des entreprises et l'évolution des organisations

participant à l'amélioration des performances administratives et commerciales de l'entité.

Dans le cadre de cette étude, nous retiendrons l'audit de la sécurité du parc informatique. Cette étude permettra d'améliorer la gestion de son parc et la maitrise de ses risques par les mesures correctives qu'elle peut suggérer. A ce titre, elle apportera des informations sur l'existence du risque et son ampleur afin de mettre en place des mesures de prévention pour une bonne maitrise de ses risques et une bonne gestion de son parc.

La question de recherche principale que nous nous posons pour circonscrire le champ de notre étude est de savoir dans quelle mesure la sécurité du parc informatique de Congo Télécom est-elle maitrisée ?

Il s'agit spécifiquement de savoir :

- Quels sont les critères d'évaluation du risque informatique ?
- Comment évaluer les contre-mesures ?
- Comment évaluer le contrôle interne du matériel informatique ?
- Quelles sont les démarches de sécurité du parc informatique pour Congo Télécom?
- Quelle est la typologie des risques rencontrés auxquels s'expose Congo Télécom?
- Comment améliorer l'efficacité de la gestion de la sécurité du parc?

Pour répondre à toutes ces questions, nous avons décidé d'étudier le thème suivant : « **Audit de la sécurité du parc informatique de Congo Télécom** ».

L'objectif principal de cette étude consiste à apprécier les dispositifs de sécurité relatifs à la gestion du parc informatique de Congo Télécom et de pouvoir cerner les risques qui en découlent.

Comme objectifs spécifiques, il s'agira de :

- Identifier, analyser et évaluer les risques liés au matériel informatique ;
- Définir les risques de patrimoine ;
- Définir les éléments pouvant contribuer à la réduction de l'impact du risque
- Calculer le poids du risque en fonction de la menace, vulnérabilité et la contre-mesure
- Renforcer la capacité du service d'audit.
- Présenter une approche de recommandations, permettant d'améliorer la sécurité du parc informatique.

Du fait de l'immensité du parc informatique, notre travail se délimitera à l'audit du parc par le serveur (stockage des données, authentification et contrôle d'accès, partage des fichiers, courrier électronique, accès aux informations world wide web …) conformément aux procédures de gestion du serveur informatique de Congo Télécom. Nous utiliserons essentiellement la norme de sécurité ISO 17799.

Cette étude présente plusieurs centres d'intérêts dont :

Pour l'entreprise :

Cette étude permettra à l'entreprise, d'une part, de rendre plus performante la gestion de son parc informatique, d'améliorer et de renforcer son dispositif de gestion des risques et d'autre part de contribuer à l'atteinte de ses objectifs tout en soignant son image.

Pour nous-mêmes :

De plus, elle sera, pour nous, l'occasion de mettre en pratique les connaissances acquises lors de notre formation et de nous familiariser avec les concepts d'audit et de management de risque.

Pour le lecteur

Ce mémoire sera, enfin, pour tout lecteur, un moyen d'avoir une compréhension de l'audit interne et des systèmes de sécurité d'information.

Ainsi, notre étude est structurée en deux grandes parties :

Première partie :

- Chapitre 1 Normes et Sécurité du Système d'information ;
- Chapitre 2 La sécurité informatique ;
- Chapitre 3 Méthodologie de la recherche.

Pour la deuxième partie :

- Chapitre 4 Description de Télécom CONGO ;
- Chapitre 5 Audit de la sécurité du matériel de Télécom Congo ;
- Chapitre 6 Recommandations et suggestion.

PARTIE I – CADRE THEORIQUE

Bien qu'il existait déjà, ce n'est qu'autour du 19èm siècle qu'est apparu l'audit sous la forme que nous connaissons aujourd'hui. En effet, la première forme de l'audit est celle de l'audit comptable et financier encore appelée commissariat aux comptes, qui a par le développement des organisations conduit au développement des pratiques de contrôle des comptes et ensuite entrainé une évolution des structures économiques et des grandes administrations administratives et commerciales.

C'est le système d'information qui coordonne, grâce à l'information, les activités de l'organisation et lui permet ainsi d'attendre ses objectifs. La dématérialisation des documents tend à augmenter la vulnérabilité du système d'information et conduit l'entreprise à ainsi maitriser de nouveaux risques. Un audit est alors nécessaire pour cerner les défaillances.

« L'audit interne est une activité indépendante et objective qui donne à une organisation une assurance sur le degré de maitrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management de risques, de contrôle et de gouvernement d'entreprise, et en faisant des propositions pour renforcer leur efficacité. » (IIA.IFACI).

Pour l'audit informatique, il est très important que l'auditeur puisse avoir un minimum de connaissances en ce qui concerne l'informatique, sans pour autant être un expert dans le domaine, mais il peut toutefois faire recours à un expert pour l'excellence de sa tâche. Dans notre étude, l'audit de la sécurité du parc informatique de Congo Télécom se délimitera au niveau de la gestion de son serveur.

Pour une meilleure assimilation de l'audit de la sécurité du parc informatique, nous avons consacré cette première partie à la revue de la littérature qui comporte trois chapitres :

- Chapitre 1 Normes et Sécurité du Système d'information ;
- Chapitre 2 La sécurité informatique ;
- Chapitre 3 Méthodologie de la recherche.

Chapitre 1 : NORMES ET SECURITE DU SYSTEME D'INFORMATION

Dans le but d'assurer un audit informatique efficace et efficient, plusieurs normes ont été établies dont chacune avec une spécificité précise afin d'assurer les relations de la sécurité des systèmes d'information.

Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises, et du mode de vie des citoyens.

Selon un éditorialiste sénégalais du journal le Soleil du 20 Janvier 2008, l'Etat a la responsabilité de :

- La sécurité de ses propres systèmes d'information ;
- la continuité de fonctionnement des institutions et des infrastructures vitales pour les activités socio-économiques du pays ;
- la protection des entreprises et des citoyens.

De leur côté, les entreprises doivent :

- Protéger de la concurrence et de la malveillance leur système d'information qui irrigue l'ensemble de leur patrimoine (propriété intellectuelle et savoir faire) et porte leur stratégie de développement.

Face à l'augmentation des menaces, cet éditorialiste propose 6 axes. Il ressort une préparation insuffisante des principaux acteurs pour assurer une sécurité convenable. Aussi, afin d'assurer la mise en œuvre opérationnelle des politiques et des décisions en matière de sécurité des systèmes d'information (SSI), nous proposons six axes de recommandations :

- Sensibiliser et former à la SSI ;
- Responsabiliser les acteurs ;
- Renforcer la politique de développement de technologies et de produits de SSI et définir une politique d'achat public en cohérence ;
- Rendre accessible la SSI à toutes les entreprises ;
- Accroître la mobilisation des moyens judiciaires ;
- Assurer la sécurité de l'Etat et des infrastructures vitales.

1.1. Les normes : Définitions

Selon l'encyclopédie Larousse il existe deux (2) types fondamentaux de normes :

- Les normes sociales ;
- Les normes techniques.

Exprimées ou tacites, les normes sociales sont indispensables à l'organisation et à la cohésion du groupe. Les normes techniques définissent les caractéristiques d'un produit ; de manière générale, elles garantissent la qualité du produit et peuvent même le protéger contre la concurrence.

Quelle est la signification de ces normes, et à quoi servent-elles exactement ? Comment sont-elles élaborées, et par qui sont-elles définies ?

Selon le Larousse 2005, une norme est une règle, principe, critère auquel se réfère tout jugement : Se fonder sur la norme admise dans une société. C'est aussi un ensemble des règles de conduite qui s'imposent à un groupe social.

- En Industrie c'est une Règle fixant les conditions de la réalisation d'une opération, de l'exécution d'un objet ou de l'élaboration d'un produit dont on veut unifier l'emploi ou assurer l'interchangeabilité. (Les travaux de normalisation internationale sont menés par l'Organisation internationale de normalisation *[International Organization for Standardization]*, conventionnellement appelée ISO, qui publie des normes internationales destinées à harmoniser entre elles les normes nationales. Il existe aussi un Comité européen de normalisation [CEN]) ;

- En Linguistique : c'est un Système d'instructions définissant ce qui doit être choisi parmi les usages d'une langue si on veut se conformer à un certain idéal esthétique ou socioculturel. (La norme se confond alors avec le « bon usage ».). Moyenne des divers usages d'une langue à une époque donnée. (La norme correspond alors à l'institution sociale que constitue la langue.) ;

Selon AFNOR 2003, une norme désigne un ensemble de spécifications décrivant un objet, un être ou une manière d'opérer. Il en résulte un principe servant de règle et de référence technique.

Une norme n'est pas obligatoire, son adhésion est un acte volontaire. Certaines sont rendues obligatoires par un texte réglementaire ou décret de loi.

Les normes sont élaborées par des organismes dont les plus connus sont :

- au niveau international
  - l'ISO (International Organization for Standardization) – 1947 ;
  - le CEI (Commission Électrotechnique Internationale) ;
  - l'UIT (Union Internationale des Télécommunications) ;
- au niveau européen
  - le CEN (Comité Européen de Normalisation) – 1961 ;
  - le CENELEC (Comité Européen de Normalisation pour l'Électrotechnique) ;
  - l'ETSI (European Telecommunications Standard Institut) ;
- au niveau français
  - l'AFNOR (Association Française de Normalisation) ;
  - l'UTE (Union Technique de l'Électricité) ;
- au niveau des pays étrangers
  - le SSC (Standards Council of Canada) ;
  - L'IBN (Institut Belge de Normalisation) ;
  - l'ASTM (American Society for the Testing of Materials) ;
  - LE SNV (Schweizerischen Normen Vereinigung) ;
  - le DIN (Deutsche Industrie Normen) ;
  - le BSI (British Standard Institute) ;
  - l'ANSI (American National Standard Institute) ;

Une norme homologuée française porte le label NF. Certaines normes en instance d'homologation sont dites expérimentales et portent l'inscription XP ; ce statut ne peut excéder 5 ans.

Selon « *Management du risque. Approche globale*. AFNOR. 2002. (ISBN 2-12-169211-8) », une **norme**, du latin *norma* « équerre, règle », désigne un état habituellement répandu, moyen, considéré le plus souvent comme une règle à suivre. Ce terme générique désigne un ensemble de caractéristiques décrivant un objet, un être, qui peut être virtuel ou non. Tout ce qui entre dans une norme est considéré comme « normal », alors que ce qui en sort est « anormal ». Ces termes peuvent sous-entendre ou non des jugements de valeur.

Selon la Norme (ISO, 2005), « La *norme* est un document, établi par *consensus* et approuvé par un organisme reconnu, qui fournit pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leur résultats, garantissant un niveau d'ordre optimal dans un contexte donné » (extrait de la norme NF EN 45020 de 2007 « vocabulaire de la normalisation ». La norme doit être distinguée des documents normatifs à caractère informatif (guide d'application, fascicule de documentation) ou faisant état d'accords spécifiques à un groupe ou à un métier (accord, référentiel de bonnes pratiques).

1.2. Norme ISO

L'ISO (ce n'est pas un acronyme, ISO vient du grec « isos » signifiant égal) a son siège à Genève en Suisse. C'est une organisation internationale créée en 1947 et composée de représentants des organismes nationaux de plus de 150 pays. Le CEN siège à Bruxelles en Belgique avec un statut d'association. Il n'y a pas de catalogue général des normes CEN, il faut aller sur les sites de chaque pays membre ou de chaque pays affilié.

La norme ISO 17799 est issue de la norme anglaise BS7799 créée en 1995 et révisée en 1999. Cette norme constitue un code de bonnes pratiques pour la gestion de la sécurité de l'information. Elle fait l'objet en Grande Bretagne d'un schéma de certification (C:Cure). C'est-à-dire qu'un client qui opère avec cette entreprise a la garantie que ses informations sont gérées de manière plus ou moins sécurisée car un certain nombre de mesures techniques ou non techniques ont été mises en place.

Le contenu de l'ISO 17799 est à la fois un ensemble de mesures techniques et organisationnelles qu'il faudrait mettre en place pour gérer de manière sécurisée les informations. La norme propose plus d'une centaine de mesures possibles réparties en 10 chapitres:

- **Politique de sécurité** (nécessité pour l'entreprise de disposer d'une politique de sécurité et d'un processus de validation et de révision de cette politique) ;
- **Organisation de la sécurité**

    - Une partie traite de la nécessite de disposer au sein de l'entreprise d'une organisation dédiée à la mise en place et au contrôle des mesures de sécurité.

        - l'implication de la hiérarchie,
        - la désignation de propriétaires responsables de la classification de l'information,
        - processus pour la mise en place de tout nouveau moyen de traitement de l'information.

        - Une seconde partie traite des accès aux informations de l'entreprise par une tierce partie. (accès encadrés par un contrat qui stipule les conditions d'accès et les recours en cas de problèmes.)
        - Une troisième partie indique comment traiter du cas où la gestion de la sécurité est externalisée (outsourcing).

- **Classification des informations** (nécessité de répertorier et de déterminer la classification de l'ensemble des informations) ;

- **Sécurité du personnel**
    - lors du recrutement de personnel, il est tout aussi important de mentionner dans les contrats d'embauche des clauses spécifiques à la sécurité comme une clause de confidentialité.
    - une sensibilisation à la sécurité doit être proposée à toute personne accédant à des informations sensibles (nouvel arrivant, tierce partie)
    - l'ensemble du personnel doit être informé de l'existence et du mode d'emploi d'un processus de remontée d'incidents.
- **Sécurité de l'environnement et des biens physiques** (mesures classiques pour protéger les bâtiments et les équipements)
    - délimitation de zone de sécurité pour l'accès aux bâtiments
    - mise en place de sécurité physique comme la lutte contre l'incendie ou le dégât des eaux

- mise en place de locaux de sécurité avec contrôle d'accès et alarmes, notamment pour les salles machines
- mise en place de procédures de contrôle pour limiter les vols ou les compromissions
- mise en place de procédures pour la gestion des documents dans les bureaux

- **Administration**

  - rédiger et mettre à jour l'ensemble des procédures d'exploitation réseau, système ou sécurité de l'entreprise ;
  - rédiger et mettre à jour les critères d'acceptation de tout nouveau système ;
  - prévoir un planning pour l'achat de composants ou matériels pour éviter toute interruption de service ;
  - mettre en place un certain nombre de politique organisationnelle et technique (anti-virus, messagerie, diffusion de document électronique en interne ou vers l'extérieur, sauvegarde et restauration, etc.)

- **Contrôle d'accès**

  - qui a droit à quoi, comment y accéder, révision de ces droits ;
  - la responsabilité des utilisateurs face à l'accès au SI ;
  - mise en place d'un système de contrôle de la sécurité et de tableaux de bord ;

- **Développement et maintenance**

  - nécessité d'intégrer les besoins de sécurité dans les spécifications fonctionnelles d'un système ;
  - intégration de services de sécurité comme le chiffrement, la signature électronique, la non-répudiation ;

- **Plan de continuité** (nécessité pour l'entreprise de disposer de plans de continuité)
- **Conformité légale et audit de contrôle**

- la nécessité de disposer de l'ensemble des lois et règlements qui s'appliquent aux informations manipulées et des procédures associées ;
- procédures pour le déroulement d'audit de contrôle.

1.3. La norme AFNOR

AFNOR Certification est une société qui opère dans le domaine volontaire comme dans le domaine réglementaire. Au niveau européen, AFNOR Certification est notifiée pour plusieurs directives européennes afin de délivrer le marquage CE, qui atteste la conformité des produits aux exigences réglementaires européennes. AFNOR Certification est née dans la continuité de la fusion, en 2004, entre l'Association française pour l'assurance de la qualité (AFAQ) et l'Association française de normalisation au sein du groupe AFNOR.

La certification s'adresse avant tout au client final, qu'il soit consommateur ou utilisateur. Elle est la preuve objective que le produit ou le service acheté ou fourni dispose des caractéristiques définies dans une norme ou un référentiel, et qu'il fait régulièrement l'objet de contrôles. Acheter, utiliser ou consommer un service ou un produit certifié est une garantie de qualité au sens large.
La certification est un des tout premiers critères quand il s'agit de choisir parmi plusieurs offres existantes. Sa crédibilité repose sur la compétence d'un organisme certificateur comme AFNOR Certification, mais aussi sur son impartialité. À noter que les organismes certificateurs sont eux-mêmes contrôlés par des organismes d'accréditation indépendants, le Comité français d'accréditation en France.
La certification est délivrée après une évaluation des systèmes, des services, des produits ou encore des compétences professionnelles, objets de la demande. Cette évaluation consiste à en mesurer les caractéristiques. Si celles-ci correspondent en tous points à celles fixées dans le référentiel, la certification est délivrée. Malheureusement après avoir reçu cette certification, les divers entrepreneurs français ne prennent pas toujours compte de la réglementation européenne, notamment en ce qui concerne les garanties européennes des produits (produits défectueux, SAV) qui est de 2 ans minimum dans toute l'Europe.

La norme Afnor E60-182 défini les indicateurs de productivité usuels. Le plus connu est le TRS (Taux de Rendement Synthétique) qui synthétise en 1 chiffre tous les aspects de votre productivité.

1.4. Sécurité Système d'Information

1.4.1. Définition Sécurité SI

Selon (ISO 2005), la sécurité de l'information est l'état de protection face aux risques identifiés et résultant de l'ensemble des mesures de sécurité prises par votre entreprise pour préserver :

- La confidentialité ;
- l'intégrité ;
- la disponibilité de l'information que vous détenez, quel que soit son support (papier, électronique, etc.).

La sécurité de l'information englobe l'ensemble des :

- Sous systèmes d'exploitation ;
- réseaux de telecommunication ;
- logiciels ;
- applications ;
- documents ;
- de même que la sécurité physique des lieux et des équipements ;
- ainsi que la sécurité logique des applications et des données.

1.4.2. Contexte de la Sécurité du SI

Pour mettre en place de bonnes pratiques de gestion de l'information et implanter une politique de sécurité de l'information, les normes ISO 17799:2005 et ISO 27001:2005 peuvent vous servir de guide et de référence. La norme ISO 17799:2005 indique quoi protéger et la norme ISO 27001:2005 indique comment assurer la sécurité de l'information.

Selon la Norme (ISO 17799, 2005), pour réduire les risques, il faut définir ses objectifs de sécurité. Ceux-ci consistent :

- à identifier les menaces,
- à déterminer les vulnérabilités et à procéder à l'analyse des risques identifiés en tenant compte des paramètres suivants :

- sensibilité des actifs informationnels de l'entreprise ;
- impact économique des sinistres potentiels ;
- probabilité de leur survenance et coût des mesures proposées.

La norme ISO 27001:2005 indique les conditions à remplir pour :

- Implanter ;
- maintenir ;
- améliorer le système de gestion de la sécurité de l'information (SGSI).

Le modèle suggéré par la norme ISO 17799, est d'utiliser une démarche d'amélioration continue qui comprend quatre étapes récurrentes :

- **Planifier :** définir le périmètre du SGSI, bâtir la politique de la sécurité de l'information, procéder à l'évaluation des risques, préparer le plan d'action de la sécurité.
- **Réaliser :** mettre en place le plan d'action de la sécurité, sensibiliser et former le personnel.
- **Vérifier :** s'assurer que les mesures de sécurité mises en place sont efficaces en effectuant le contrôle des procédures, et en évaluant la fiabilité des données, réaliser périodiquement des audits du SGSI.
- **Agir :** mettre en place des mesures correctives et de prévention appropriées, implanter les améliorations du SGSI qui ont été identifiées.

1.4.3. Organisation de la sécurité

Selon la norme (ISO 2005), l'organisation de la sécurité de l'information consiste à:

- Préciser les rôles et responsabilités des gestionnaires, utilisateurs, contractuels, fournisseurs de services et propriétaires d'actifs informationnels ;
- assurer la protection de vos actifs ;
- mettre en place des mécanismes de sécurité pour assurer la sécurisation de l'accès des tiers aux informations et ressources de votre entreprise.

L'organisation de la sécurité est une bonne pratique qui permet de clarifier les rôles et responsabilités des acteurs en sécurité de l'information au sein de votre entreprise et d'assurer la gestion de vos actifs. Pour mettre en place une sécurité adéquate, il est indispensable d'implanter des règles de conduite et de partager les responsabilités entre les différents intervenants de votre entreprise.

Les responsabilités à l'égard de la sécurité des actifs informationnels de votre entreprise reposent sur :

- Les gestionnaires qui en assurent la gestion ;
- les utilisateurs des actifs informationnels;
- les tiers, fournisseurs de services et contractuels.

Le dirigeant de votre entreprise a comme responsabilités de :

- Désigner un responsable de la sécurité des systèmes d'information (RSSI);
- approuver la politique globale de sécurité, les orientations et les directives.

Le comité de la sécurité de l'information doit :

- Recommander les orientations et les directives au dirigeant de l'entreprise;
- approuver les standards, les pratiques et le plan d'action de la sécurité de l'entreprise;
- assurer le suivi du plan d'action de sécurité.

Le responsable de la sécurité agit comme responsable désigné pour coordonner la sécurité de l'information de l'entreprise. À cet effet, il a la responsabilité de :

- Elaborer et assurer le suivi et la mise à jour périodique du plan d'action;
- communiquer au personnel, aux clients et partenaires de l'entreprise les orientations de sécurité de l'information;
- veiller au respect de la politique de sécurité de l'information ainsi qu'à la protection des renseignements personnels et sensibles;
- informer périodiquement le comité de l'état d'avancement des dossiers.

Le responsable de la sécurité agit comme responsable désigné pour coordonner la sécurité de l'information de l'entreprise. À cet effet, il a la responsabilité de :

- Elaborer et assurer le suivi et la mise à jour périodique du plan d'action;
- communiquer au personnel, aux clients et partenaires de l'entreprise les orientations de sécurité de l'information;
- veiller au respect de la politique de sécurité de l'information ainsi qu'à la protection des renseignements personnels et sensibles;
- informer périodiquement le comité de l'état d'avancement des dossiers.

1.4.4. Bâtir une Politique de Sécurité

Selon (ISO 2005), une politique de sécurité de l'information est un ensemble de documents émanant de la direction de votre entreprise et indiquant les directives, procédures, lignes de conduite et règles organisationnelles et techniques à suivre relativement à la sécurité de l'information et à sa gestion. Une telle politique constitue un engagement et une prise de position claire et ferme de la direction de protéger ses actifs informationnels.

Il faut protéger les informations et ressources considérées comme vitales ou importantes pour votre entreprise, soit des :

- Systèmes d'information (application, logiciel, etc.) ;
- éléments de l'infrastructure technologique (serveur, réseau de télécommunications, réseau téléphonique, etc.) ;
- types de documents (contrat, procédure, plan, procédé de fabrication, etc.) ;
- installations (immeuble, local, groupes, ascenseurs etc.).

La politique de sécurité devra contenir les éléments suivants :

- Confirmer l'engagement de la direction;
- désigner une personne responsable de la sécurité de l'information;
- identifier ce qui doit être protégé;
- identifier contre qui et quoi vous devez être protégé;
- inclure des considérations de protection de l'information;
- encadrer l'utilisation des actifs informationnels;

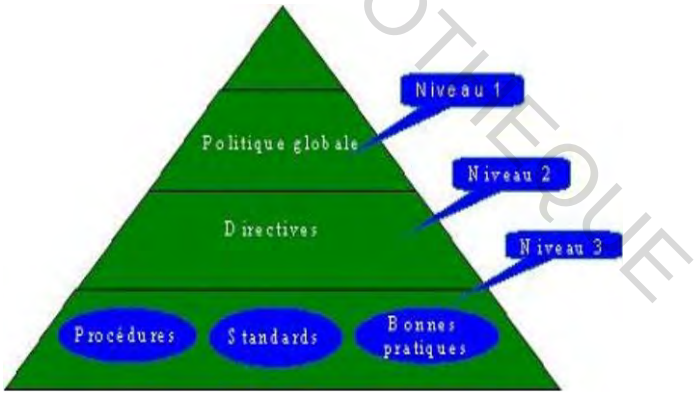
- tenir compte de la conservation, de l'archivage et de la destruction de l'information;
- tenir compte de la propriété intellectuelle;
- prévoir la réponse aux incidents et préparer une enquête, s'il y a lieu;
- informer vos utilisateurs que les actes illégaux sur les informations et ressources de l'entreprise sont interdits.

Le cadre d'élaboration de la politique de sécurité est constitué des lois, règlements, politiques, directives, normes, procédures, guides et standards dont l'entreprise doit tenir compte lors de l'élaboration d'une politique de sécurité de l'information.

La pratique recommandée pour l'élaboration d'une politique de sécurité repose sur les éléments suivants :

- Une politique globale;
- des directives;
- des procédures, standards et bonnes pratiques.

Figure 1 : Bâtir une Politique de sécurité



Source : ISO 2005

Niveau 1 : Politique globale

La politique globale de sécurité des actifs informationnels est un engagement et une prise de position ferme et claire de la direction de l'entreprise quant à la protection à accorder aux actifs informationnels.

Niveau 2 : Directives

Les directives déterminent, par des mesures concrètes, la façon de procéder en vue d'assurer la sécurité des actifs informationnels. Elles peuvent porter, par exemple, sur l'utilisation d'internet, du courrier électronique ou des écrans de veille.

Niveau 3 : Procédures, standards et bonnes pratiques

- **Procédures** : les procédures mises en place par votre entreprise décrivent en détail toutes les étapes d'un processus humain ou technologique d'implantation ou d'opération d'une mesure de sécurité.
- **Standards** : les standards sont des normes non entérinées par un organisme officiel de normalisation, mais qui se sont imposés par la force des choses parce qu'ils font consensus auprès des utilisateurs qui les adoptent.
- **Bonnes pratiques** : les bonnes pratiques de sécurité mises en place par votre entreprise assurent que les contrôles de sécurité ainsi que les processus de soutien nécessaires sont implantés de façon constante et adéquate à travers l'entreprise.

1.4.5. La Gestion des risques de sécurité

Selon (ISO 2005), la gestion des risques (accidents, erreurs, défaillances, malveillances) de sécurité consiste à protéger les biens de votre entreprise contre les menaces pouvant survenir.
L'évaluation des risques est la première étape à réaliser lors d'une démarche de sécurité. Il revient au responsable de la sécurité de votre entreprise d'organiser et de superviser l'évaluation des risques.
Il faut débuter l'évaluation des risques en déterminant les actifs informationnels vitaux et importants de votre entreprise. On les évalue lors de la démarche de Gérer les actifs informationnels) selon des critères de

- Disponibilité ;
- d'intégrité ;
- de confidentialité, afin de déterminer lesquels sont essentiels à votre entreprise pour atteindre ses objectifs.

L'évaluation des risques doit combiner :

- La probabilité de la menace ;
- le degré de vulnérabilité ;
- le niveau de gravité de son impact.

L'analyse des menaces (écoute clandestine, destruction de fichiers, inondation, erreur d'acheminement, virus, incendie, etc.) vous permet d'en faire une liste exhaustive et de déterminer les vulnérabilités qu'elles pourraient exploiter.

On entend par vulnérabilité toute faiblesse des actifs informationnels qui peut être exploitée par des menaces :

- Manque de contrôle de l'accès aux locaux ;
- mauvaise gestion des supports de sauvegarde ;
- complexité des règles d'accès sur les coupe-feux et les routeurs ;
- manque d'information des utilisateurs sur les procédures de sécurité, mots de passe inadéquats.

L'impact est la conséquence d'une menace, causée soit de façon délibérée, soit accidentellement, qui porte atteinte à vos actifs informationnels. Les conséquences peuvent être la destruction ou des dommages à certains actifs informationnels et une perte de confidentialité, d'intégrité et de disponibilité.

Les conséquences indirectes comprennent:

- Les pertes financières ;
- de parts de marché ;
- de bénéfices ou d'image ;
- l'évaluation des impacts permet de comparer les conséquences d'une menace et l'investissement requis pour se protéger de cette menace potentielle.

1.4.6. Gestion des actifs informationnels

Selon (ISO 2005) la gestion des actifs informationnels consiste à faire leur inventaire, à leur déterminer un propriétaire, à les catégoriser, à déterminer leur niveau de protection et à établir les mesures de sécurité à mettre en place selon leur contexte d'utilisation.

Le responsable de la sécurité doit s'assurer de maintenir une protection adéquate des actifs informationnels de votre entreprise. Il doit s'assurer, selon une démarche d'amélioration continue, que les mécanismes de sécurité appropriés sont élaborés, mis en place et appliqués.

Il faut élaborer un inventaire des ressources informationnelles de votre entreprise. Ces ressources sont constituées des actifs informationnels ainsi que des ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Cet inventaire doit s'appliquer aux trois catégories d'actifs informationnels suivantes :

- Ceux appartenant à votre entreprise et exploités par elle-même;
- ceux appartenant à votre entreprise et exploités ou détenus par un fournisseur de services ou un tiers;
- ceux appartenant à un fournisseur de services ou un tiers et exploités par lui au profit de votre entreprise.

Il faut élaborer un registre d'autorité de la sécurité de l'information. Ce registre contient :

- La description des actifs informationnels qui doivent être protégés;
- la désignation et les attributions des propriétaires d'actifs;
- la désignation et les attributions du responsable de la sécurité;
- les attributions de tout autre intervenant en sécurité.

Protection des actifs informationnels

La protection des actifs informationnels est une méthode de gestion comprenant trois étapes qui doit être appliquée :

Étape 1 : Déterminer les actifs informationnels à catégoriser

Un inventaire des actifs informationnels est réalisé et ceux-ci sont regroupés par :

- Système d'information;
- élément de l'infrastructure technologique (serveur, réseau de télécommunication, réseau téléphonique, etc.);
- type de document (contrat, procédure, plan, etc.) ;
- environnement physique (immeuble, local…).

Chaque actif informationnel doit se voir attribuer un propriétaire, une indication de catégorisation et une valeur.

Étape 2 : Catégoriser les actifs informationnels

À cette étape, une évaluation est faite pour donner des valeurs aux attributs disponibilité (D), intégrité (I) et confidentialité (C) selon le contexte d'utilisation des actifs informationnels de l'entreprise.

Les valeurs sont : élevée, moyenne ou basse. Les contextes d'utilisation retenus sont : les postes autonomes ou mobiles, le réseau fermé et le réseau ouvert.

Il est recommandé d'effectuer après cette étape une évaluation et une analyse des risques.

Étape 3 : Déterminer les mesures de sécurité à appliquer pour protéger les actifs informationnels

À partir du contexte d'utilisation de chaque actif défini dans l'étape précédente, il faut indiquer les mesures de sécurité qui devront être appliquées. Cette étape est répétée autant de fois qu'i l y a d'actifs à catégoriser.

1.4.7. Assurer la sécurité des ressources humaines

La sécurité des ressources humaines consiste à indiquer au personnel les bonnes pratiques à utiliser pour protéger les renseignements confidentiels et nominatifs, faire enfin un bon usage de leur équipement informatique selon les normes et les règles et mettre en place un

programme de sensibilisation à la sécurité de l'information de même qu'une procédure d'accueil des nouveaux employés.

Formation et sensibilisation

La formation et la sensibilisation à la sécurité de l'information sont des moyens pour soutenir la vigilance des employés de votre entreprise. Elles permettent de responsabiliser ces derniers pour qu'ils voient les conséquences de leurs actes dans l'utilisation des informations et des ressources de l'entreprise.

Il faut informer le personnel des consignes suivantes :

- Chaque nouvel employé ou contractuel doit lire et signer un engagement de respect de la sécurité (ou lors de l'implantation de la politique de sécurité).
- Les employés et les contractuels qui traitent de l'information sensible doivent être soumis à une habilitation sécuritaire et signer une entente de confidentialité.
- Chaque utilisateur du réseau de votre entreprise doit respecter les contraintes suivantes. Il ne peut :

    - Télécharger et/ou installer des jeux ou des logiciels non autorisés et sans droit de licence, de même que des films et des pièces musicales;
    - empêcher le fonctionnement des outils de protection (antivirus, écran de veille, etc.);
    - accéder par Internet à des sites interdits;
    - installer des programmes ou fichiers reçus par courriels et ne concernant pas son travail.

- Chaque utilisateur doit assurer la protection de la vie privée des personnes et le respect des renseignements personnels. À cet effet, il doit :

    - Utiliser des données fictives lors des tests de systèmes;
    - assurer l'intégrité de l'information lors de sa collecte, de son traitement et de sa conservation;
    - assurer la conservation de l'information à l'abri des indiscrétions;
    - procéder à la conservation d'informations confidentielles ou sensibles de l'entreprise sur un support amovible;

- surveiller l'impression ou la photocopie d'informations confidentielles;
- assurer la destruction sécuritaire des supports informatiques.

o Chaque utilisateur doit informer son supérieur immédiat et le responsable de la sécurité de l'information de tout incident ou disfonctionnement de sécurité qu'il constate ou détecte par un outil de surveillance ou tout autre moyen.

Le processus d'accueil lors de l'entrée en fonction d'un nouvel employé ou d'un contractuel est une bonne occasion de le sensibiliser à la sécurité de l'information.

La séance d'accueil doit inclure, pour le volet sécurité, les éléments suivants :

- o les politiques et procédures;
- o le registre d'autorité sur les responsabilités des intervenants en sécurité (qui fait quoi);
- o l'identifiant et le mot de passe:

  - Composition et longueur minimale du mot de passe;
  - confidentialité du mot de passe;
  - responsabilités des actions effectuées avec son identifiant;
  - la prise de copie;
  - l'éthique et le droit d'auteur;
  - l'usage judicieux des équipements et logiciels incluant Internet.

Procédure de départ

Vous devez veiller à ce que les droits d'accès de tout employé contractuel ou tiers aux actifs informationnels de votre entreprise prennent fin immédiatement lors d'un départ, d'une fin de contrat ou d'une entente. Une procédure à cet effet doit être mise en place.

1.4.8. Vérifier la conformité

La vérification de la conformité consiste à s'assurer :

1. du respect des lois et des réglementations;
2. de la conformité des procédures de sécurité en place en relation avec la politique de sécurité émise par votre entreprise;

3. de l'efficacité des dispositifs de suivi des fichiers journaux d'activités, des enregistrements de transactions, des procédures et des registres de suivi.

Le responsable de la sécurité de l'information doit s'assurer, auprès des différents responsables des actifs informationnels, du respect des lois et des réglementations et de l'application de la politique de sécurité de l'information.

Le non-respect de la législation dans le domaine des technologies de l'information et des communications peut mettre votre entreprise dans une situation précaire par rapport à votre clientèle et avoir des conséquences financières ou pénales.

Un audit, interne ou externe, doit être fait périodiquement pour assurer :

- La vérification de la conformité des mécanismes de sécurité physique et logique;
- la vérification des contrôles de sécurité effectués sur les actifs informationnels vitaux et importants de l'entreprise;
- la validation de l'efficacité des mesures de sécurité mises en place;
- la validation des processus d'alertes et de réaction aux incidents ou disfonctionnements de sécurité;
- La vérification des mécanismes de contrôle d'accès par des tests d'intrusion;
- l'évaluation du plan de continuité et de relève;
- la conformité aux lois et règlements;
- la sensibilisation de la direction et des utilisateurs aux risques potentiels.

1.4.9. Assurer la sécurité physique et environnementale

La sécurité physique et environnementale est une mesure de sécurité primordiale à mettre en œuvre. Il faut empêcher l'accès non autorisé ainsi que les dommages et perturbations pouvant affecter les activités quotidiennes et les actifs informationnels installés dans les locaux de l'entreprise.

Tous les actifs informationnels identifiés comme vitaux ou importants doivent être installés dans des locaux sûrs qui constituent le périmètre de sécurité. Des procédures de supervision des actifs à protéger et des contrôles d'accès physiques au périmètre de sécurité doivent être mises en place.

Protection des équipements et des locaux

Tout équipement réseau ou lié au réseau doit être situé dans un local dédié, réservé au personnel habilité (muni de carte d'accès, clé, etc.). Une climatisation adéquate doit être installée dans le local de même qu'un système d'extinction en cas d'incendie. Ce local ne doit pas être utilisé à d'autres usages (stockage de papiers et de cartons, rangement de matériaux divers, etc.). Il peut être équipé de caméras de surveillance, d'un système d'alarme et, idéalement, ne doit pas être situé au rez-de-chaussée d'un immeuble.

Il faut porter attention à l'emplacement et à la mise au rebut du matériel et des documents et protéger et sécuriser les infrastructures d'alimentation électrique et de câblage.

Il faut anticiper ou prévoir toute action de maintenance sur les installations électriques.

Les alimentations électriques des équipements considérés comme vitaux ou importants doivent être sécurisées par :

- Une unité non interruptible qui garantit l'alimentation (UPS);
- une génératrice de secours.

La détection d'incendie doit prévoir la coupure automatique de l'alimentation électrique du périmètre de sécurité. Ces dispositifs doivent être testés et vérifiés périodiquement.

Il faut faire respecter les consignes suivantes :

- Tout équipement qui est mis au rebut ou réutilisé par un autre utilisateur doit être vidé de son contenu et les disques doivent être reformatés. Si des données sensibles avaient été emmagasinées, la destruction physique des disques est à faire ;
- Les papiers, documents et supports informatiques amovibles (disquettes, cd-rom) ne doivent pas être placés à vue sur les bureaux. Les supports et documents importants sont stockés sous clé et ceux identifiés comme vitaux sont stockés dans un coffre-fort. Une déchiqueteuse doit être utilisée pour éliminer les documents confidentiels ou sensibles ;
- Les équipements informatiques utilisés en dehors des locaux de l'entreprise (chez un client, à la maison, etc.) sont soumis aux mêmes procédures de sécurité.

Protection reliée à l'environnement

Selon l'environnement, vous devez prévoir ou ajouter des mesures spécifiques de protection contre les inondations, les explosifs, la fumée, la poussière, les vibrations, les tremblements de terre, les produits chimiques et les interférences avec l'alimentation électrique.

1.4.10. Contrôle des accès

Le contrôle des accès consiste à gérer et contrôler les accès logiques et physiques aux informations et ressources de l'entreprise; détecter les activités non autorisées et préciser les règles à observer concernant l'identifiant et le mot de passe, de même que les autorisations d'accès.

L'accès aux actifs informationnels catégorisés comme vitaux ou importants est réservé aux seules personnes autorisées. Le droit d'accès et le type d'accès (lecture seule, modification, droit d'effacement ou d'écriture) sont accordés par le propriétaire de chaque actif.

Rôle du responsable de la sécurité

Le responsable de la sécurité doit veiller à mettre en place une directive pour contrôler l'attribution des droits d'accès aux informations et ressources de l'entreprise.

Cette directive doit couvrir tous les stades du cycle de vie des accès d'un utilisateur, de son enregistrement initial (arrivée) à son annulation (départ).

Une attention particulière doit être accordée pour limiter les droits d'accès privilégiés (par exemple : administrateur d'un système d'exploitation) qui permettent d'outrepasser des mesures de contrôle.

Les accès aux informations et ressources de l'entreprise se faisant selon un profil d'accès, le responsable doit attribuer un identifiant et un mot de passe, de même que les autorisations reliées au profil d'accès de chaque utilisateur.

Le responsable doit s'assurer que les systèmes d'applications peuvent :

- Contrôler l'accès des utilisateurs à l'information et aux fonctions des systèmes d'applications, conformément à une procédure définie de contrôle des accès;

- fournir une protection contre l'accès non autorisé à tout programme utilitaire et à tout logiciel de système d'exploitation capable d'outrepasser les commandes du système ou des applications;
- ne pas porter atteinte à la sécurité des autres systèmes avec lesquels les ressources d'information sont partagées;
- être capables de fournir l'accès aux informations uniquement au propriétaire, à d'autres individus autorisés ou à des groupes définis d'utilisateurs.

Le responsable doit recourir à des dispositifs de sécurité pour chaque système d'exploitation utilisé afin de limiter l'accès aux ressources contrôlées ou exploitées par ce système. Ces dispositifs doivent remplir les fonctions suivantes :

- L'identification et la vérification de l'identité et, si requis, du poste de travail ou du site de chacun des utilisateurs autorisés;
- l'enregistrement des accès au système, qu'ils soient réussis ou non;
- la prévision d'un moyen d'authentification approprié; si un système de gestion des mots de passe est utilisé, il doit assurer la qualité des mots de passe;
- la restriction des heures de connexion des utilisateurs, si le besoin est requis.

Le responsable doit contrôler l'accès aux services internes et externes sur le réseau. Pour ce faire, il doit assurer :

- La présence d'interfaces appropriées entre le réseau de l'entreprise et les réseaux appartenant à d'autres organisations;
- la présence de mécanismes d'authentification appropriés pour les utilisateurs et le matériel à distance;
- le contrôle de l'accès utilisateur aux services d'information.

La connexion à Internet ou à des réseaux externes peut se faire selon certaines balises :

1. La connexion se fait à partir de postes de travail spécifiques, qui ne sont pas connectés au réseau de l'entreprise et qui ne contiennent aucune donnée critique. Les postes sont protégés par un coupe-feu personnel et un antivirus; ils communiquent via un modem ou un modem câble.
2. Des postes de travail spécifiques sont autorisés à se connecter directement. Ils sont protégés par un coupe-feu personnel et par un antivirus. Le coupe-feu est configuré de

façon à limiter les connexions sortantes permises. Les postes communiquent via un modem ou un modem câble.

3. Des postes de travail spécifiques sont autorisés à se connecter via la passerelle de sécurité (équipée d'un coupe-feu) où passent toutes les connexions sortantes. Toute autre façon de se connecter est interdite. Les postes communiquent via un modem câble ou une connexion à haut débit.

Responsabilités de l'utilisateur

L'utilisateur détient un droit d'accès personnel et unique à son environnement de travail qui comprend des :

- Outils de communication (courrier électronique, Internet, intranet);
- systèmes d'exploitation, logiciels, applications, progiciels et de l'information personnelle ou partagée.

Il est interdit à l'utilisateur de :

- Divulguer de l'information confidentielle;
- chercher à obtenir de l'information non reliée à sa tâche;
- abuser de son droit d'accès par curiosité ou pour autre motif.

Le mot de passe est l'une des principales façons de garantir la sécurité d'accès aux systèmes et à l'information de l'entreprise.

En conséquence, l'utilisateur doit :

- Garder secret son mot de passe;
- éviter de l'afficher ou de l'écrire sur un papier à la vue d'autres personnes;
- changer le mot de passe lorsque le système le demande;
- utiliser un mot de passe d'au moins 8 caractères, composé de lettres, chiffres, caractères spéciaux, minuscules et majuscules et facile à retenir;
- ne pas permettre à un tiers d'ouvrir une session de travail sous l'identifiant de l'utilisateur;

- utiliser, s'il y a lieu, l'écran de veille avec mot de passe imposé par l'entreprise qui permet de verrouiller le poste de travail lorsqu'il est hors d'usage pendant une période déterminée;
- être responsable des actions effectuées avec son identifiant et son mot de passe.

L'informatique mobile, le télétravail et les réseaux sans fil

La directive concernant l'utilisation de l'informatique mobile (accès à distance au réseau de l'entreprise via un micro-ordinateur portable, un agenda électronique, un cellulaire, …) doit inclure des spécifications concernant :

- La sécurité physique;
- le contrôle des accès;
- les mesures de chiffrement;
- les procédures de sauvegarde;
- la protection contre les virus.

Les facteurs à considérer sont :

- La sécurité physique du lieu de télétravail;
- les heures de travail, la catégorisation des informations à rendre disponibles, les services et applications accessibles;
- La sécurité des moyens de télécommunication utilisés;
- l'accès à l'information par des personnes non autorisées;
- les procédures de sauvegarde;
- la disponibilité d'une assurance;
- le soutien technique et la maintenance;
- l'audit et la surveillance.

Le VPN (*Virtual Private Network*) peut être utilisé pour sécuriser les connexions à distance des utilisateurs mobiles et des télétravailleurs. Le VPN permet d'établir une connexion sécurisée privée à travers l'Internet grâce à des techniques de cryptage et d'authentification.

Les informations importantes et vitales de votre entreprise ne doivent pas être disponibles via un réseau sans fil.

1.4.11. Gestion des communications et les opérations

Le réseau de télécommunications étant une composante critique du système d'information, il doit faire l'objet de mesures de sécurité et de contrôle qui tiennent compte de tous les besoins d'accès des clients, des partenaires et du personnel de l'entreprise (accès à distance, communication avec des tiers, commerce et transactions électroniques, etc.).

Le responsable de la sécurité doit s'assurer de la fiabilité, de l'intégrité et de la disponibilité du réseau de télécommunications :

- En mettant en place des procédures de contrôle et des mécanismes de sécurité;
- en installant des moyens de protection adéquats pour sécuriser les systèmes d'exploitation et les applications.

Gestion des opérations

Toutes les opérations concernant le traitement des informations doivent être documentées. Dans ce contexte, il faut établir les responsabilités et les procédures de gestion et d'utilisation de toutes les infrastructures technologiques.

Les activités de développement d'applications et de tests ne doivent pas être réalisées sur les mêmes environnements que ceux en cours de production. Cette séparation vise à éliminer la possibilité de confondre les données de tests avec les données réelles.

Gestion des communications

Les risques d'altération et de divulgation d'informations confidentielles et sensibles sont maintenant de plus en plus élevés. Les causes de ces risques sont :

- Les logiciels pernicieux (vers, usurpation d'identité, logiciels espions, etc.);
- les intrusions et les écoutes à travers les réseaux;
- la disponibilité de réseaux sans fil;
- les nouvelles technologies de stockage (clé USB, disque amovible, etc.);
- les erreurs humaines et la possibilité d'actes malveillants effectués par le personnel de l'entreprise.

Pour se protéger d'actes malveillants ou des attaques de pirates informatiques, plusieurs moyens de protection sont disponibles :

- **Le coupe-feu** : il permet de protéger le réseau contre les intrusions et empêche le trafic non autorisé de l'intérieur vers l'extérieur. Un coupe-feu personnel peut également être installé sur les micro-ordinateurs, afin de les protéger des attaques provenant du réseau;
- **Le logiciel antivirus** : il permet de rechercher et d'éliminer les virus informatiques et autres logiciels pernicieux. L'antivirus doit être installé sur différents points névralgiques sur :
  - Chaque micro-ordinateur du parc informatique de l'entreprise;
  - le serveur de messagerie;
  - la passerelle d'accès Internet.

Il est recommandé, pour chaque point névralgique retenu, d'utiliser des fournisseurs distincts afin d'augmenter les chances de détection.

- **La mise à jour des logiciels** : la mise à jour de tous les logiciels utilisés par l'entreprise permet d'éliminer les vulnérabilités connues et de profiter des améliorations apportées à la sécurité. Un service de mise à jour automatique (Windows Update) est disponible sous Windows 2000 et Windows XP.
- **L'analyse de l'infrastructure technologique** : l'analyse des vulnérabilités de l'infrastructure technologique (serveurs, routeurs, pare-feux …) permet de vérifier si des vulnérabilités pourraient être exploitées par des personnes malveillantes. Le scanner de vulnérabilités est un logiciel automatisé conçu pour analyser les équipements du parc informatique et pour détecter les vulnérabilités et les faiblesses du réseau de communication.

Le responsable de la sécurité doit faire respecter les consignes suivantes, en informant les intervenants concernés :

- La sauvegarde des données personnelles des utilisateurs, des fichiers de production, des applications et des logiciels d'exploitation représente une activité essentielle et primordiale pour l'entreprise. S'il survient un sinistre (incendie, inondation) ou un problème de matériel (disque défectueux, serveur endommagé), il faut être en mesure de

récupérer les informations et ressources dans des délais raisonnables et les rendre accessibles.

- Si l'on doit transporter ou expédier des supports contenant de l'information de l'entreprise, on doit prendre des mesures appropriées pour assurer la sécurité du transport (emballage spécial, mallette à ouverture par code, livraison selon un processus sécuritaire, cryptage de l'information).

Le courrier électronique sur Internet ne peut être considéré comme un moyen sûr de communication. Dans le cas où l'on a à transmettre des informations confidentielles ou sensibles, on doit utiliser un mécanisme de chiffrement convenu avec son correspondant

1.4.12. Gestion de l'acquisition, le développement et l'entretien des systèmes

La sécurité des systèmes comprend : les systèmes d'exploitation, les infrastructures technologiques, les applications d'affaires, les progiciels et les applications développés par les utilisateurs.

La sécurité de l'information doit être une préoccupation constante dans les développements de systèmes, leur implantation, leur entretien de même que lors des évolutions logicielles et matérielles. Pour ce faire, le responsable de la sécurité doit prendre en considération les éléments suivants :

- L'identification des exigences de sécurité des systèmes;
- les contrôles dans le traitement de l'information;
- les mesures de chiffrement de l'information;
- la sécurité des fichiers des systèmes d'information;
- la sécurité des environnements de développement et de soutien;
- la gestion des vulnérabilités techniques.

Identification des exigences de sécurité des systèmes

Tous les contrôles et mesures de sécurité requis, manuels ou automatisés, doivent être spécifiés et décrits lors de la définition des besoins, pendant la réalisation de la phase d'analyse préliminaire de développement ou d'entretien des systèmes d'information. La catégorisation de ce nouvel actif (effectuée au début du cycle de développement du nouveau système) permet de baliser les contrôles et mesures à mettre en place.

Contrôles dans le traitement de l'information

Les données d'entrée des systèmes d'information doivent être validées. Pour ce faire, les activités suivantes doivent être réalisées :

- Vérification des éléments de données (valeurs acceptées, limites inférieures et supérieures, etc.);
- examen des fichiers afin de vérifier leur intégrité et validité;
- vérification d'autorisation des changements aux données selon la procédure établie;
- définition des responsabilités du personnel affecté au traitement des données d'entrée;
- création d'un journal de transactions enregistrant tous les changements apportés aux données d'entrée.

La validation des données de sortie des systèmes d'information implique de réaliser les activités suivantes :

- Vérifications permettant d'assurer la validité des données;
- mise en place d'une procédure de contrôle permettant de vérifier le traitement complet de tous les enregistrements d'un fichier;
- définition des responsabilités du personnel affecté au traitement des données de sortie;
- création d'un journal de transactions enregistrant tous les changements apportés aux données de sortie.

Contrôles par des mesures de chiffrement de l'information

Pour protéger la confidentialité, l'authenticité et l'intégrité de l'information, des mesures de chiffrement peuvent être implantées. Le chiffrement de l'information permet de rendre illisibles à un tiers non autorisé des informations, notamment l'accès à des courriels et à des fichiers lors du transfert d'informations sensibles ou confidentielles.

Sécurité des fichiers des systèmes d'information

L'accès aux fichiers et aux bibliothèques de programmes sources des systèmes d'information doit être contrôlé. De plus, des mesures de sécurité doivent être prises pour protéger les données sensibles dans les environnements de tests. L'utilisation de bases de données contenant des renseignements personnels et sensibles comme des données de tests doit être prohibée.

Sécurité des environnements de développement et de soutien

La sécurité des environnements de développement et de soutien de systèmes implique :

- La mise en place de procédures de contrôle des changements apportés aux systèmes;
- une révision technique de toutes les modifications apportées à un système d'exploitation;
- des restrictions sur les modifications à apporter aux progiciels (limiter à l'essentiel les modifications à ces produits);
- la sous-traitance du développement de logiciels doit être supervisée par le personnel de l'entreprise en précisant les modalités d'exécution (droits de licence, propriété du code source, droits d'accès pour vérifier la qualité et la sécurité au niveau des fonctionnalités, etc.).

Gestion des vulnérabilités techniques

Pour diminuer les risques reliés à la publication et à l'exploitation des vulnérabilités connues, une procédure doit être mise en place pour appliquer rapidement les correctifs identifiés et en assurer l'efficacité.

1.4.13. Gestion des incidents de sécurité

Un incident de sécurité est une atteinte à la sécurité qui menace la confidentialité, l'intégrité ou la disponibilité des actifs informationnels et met en péril, selon sa gravité, le déroulement des activités de votre entreprise.

Lorsqu'un événement est détecté, il faut :

- Détailler les faits (date, heure, description de l'incident, nom des personnes impliquées, identification du poste de travail s'il y a lieu, etc.);
- informer rapidement son supérieur immédiat et le responsable de la sécurité de l'information en transmettant les détails de l'événement.

La déclaration rapide des incidents ou dysfonctionnements de sécurité permet de limiter les dégâts.

Le processus de gestion des incidents est constitué de cinq activités :

- **la prévention des incidents,** qui consiste à réaliser des tests d'intrusion, sensibiliser et former les utilisateurs, et réaliser une analyse de risques;
- **la détection,** qui consiste à mettre en place des moyens de détection (antivirus, système de prévention et de détection d'intrusions, serveurs pièges) et de déclaration de surveillance;
- **la réaction aux incidents,** qui vise à mettre en place des mécanismes appropriés permettant de réduire les impacts;
- **l'activation de mesures de rétablissement ou de retour à la normale** dans les meilleurs délais;
- **la rétroaction**, basée sur l'analyse de l'incident afin d'améliorer, s'il y a lieu, le processus de gestion et de traitement des incidents ou de mettre en place de nouvelles mesures de sécurité.

1.4.14. Prévision de la continuité des activités

La gestion de la continuité des activités de votre entreprise vise à mettre en place des mesures permettant d'identifier et de réduire les risques, limiter les conséquences des incidents et permettre le rétablissement dans un délai raisonnable des activités essentielles de l'entreprise.

Plan de continuité et de relève

Le plan de continuité et de relève indique :

- Les procédures à suivre;
- l'ordre des priorités pour les actifs informationnels à relever;
- le temps de restauration de chaque actif informationnel vital ou important.

Le plan de continuité et de relève doit être testé périodiquement, afin de s'assurer de son bon fonctionnement.

Plan de sauvegarde

La sauvegarde des données personnelles des utilisateurs, des fichiers de production, des applications et des logiciels d'exploitation représente une activité essentielle pour l'entreprise. S'il survenait un sinistre (incendie, inondation) ou un problème de matériel (disque défectueux, serveur endommagé), il faudrait être en mesure de récupérer les informations et les ressources dans des délais raisonnables et les rendre accessibles.

Ce plan doit être défini en fonction :

- Du volume de données à sauvegarder;
- de la périodicité des prises de copie pour la sauvegarde;
- de la durée légale de la conservation des données (s'il y a lieu, en fonction du type de données).

Le plan de sauvegarde doit être testé de façon continue (2 fois par année) afin de s'assurer de son bon fonctionnement. La procédure de vérification doit inclure le contrôle régulier d'un journal des activités de sauvegarde.

Plan de communication

Le plan de communication doit permettre de préciser vos objectifs ainsi que les publics que vous devez atteindre. Vous devez aussi établir vos stratégies et le programme des activités qui se réaliseront sur une période déterminée et respecteront les contraintes et la culture de votre entreprise. Le choix des outils et des activités qui auront le meilleur impact dépend souvent de la qualité et de la rigueur de votre effort de planification.

Conclusion chapitre 1

Dans ce chapitre nous avons décrit de façon théorique les normes et sécurité système d'information qui nous ont permis de mieux cerner les différentes normes et aussi comment élaborer si non bâtir une politique de sécurité. Pour mieux appréhender la notion de sécurité

du système d'information, nous avons défini la sécurité de l'information et souligné l'ensemble des mesures de sécurité prises par l'entreprise pour préserver sa disponibilité, son intégrité et sa confidentialité. La sécurité du parc informatique doit être auditée dans le but de prévenir, gérer, améliorer les défaillances au système et aussi pour garantir l'atteinte des objectifs. Le chapitre suivant traitera de la sécurité informatique.

Chapitre 2 : LA SECURITE INFORMATIQUE

La sécurité informatique est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informatiques. D'une manière générale, la sécurité informatique consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants :

- La disponibilité ;
- l'intégrité ;
- la confidentialité.

Ces objectifs peuvent être compris comme étant des critères de base auxquels s'ajoute des fonctions de sécurité qui contribue à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'**authentification**) et, d'autre part, l'existence d'une action (notion de **non-répudiation** d'une transaction, voire d'**imputabilité.**

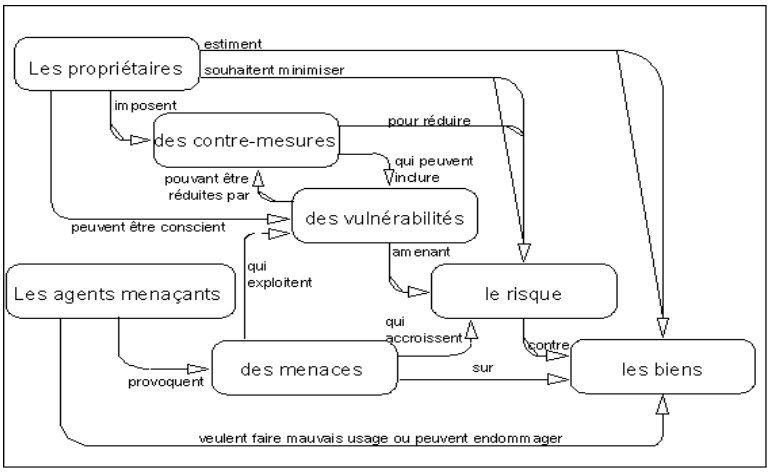
La réalisation de fonctions de sécurité, telles que celles de gestion des identités, du contrôle d'accès, de détection d'intrusion par exemple, contribuent, via des mécanismes de sécurité comme le chiffrement par exemple, à satisfaire les exigences de sécurité exprimées en termes de disponibilité, d'intégrité, de confidentialité. Elles concourent à la protection des contenus et des infrastructures numériques et sont supportées par des solutions techniques. Celles-ci sont à intégrer dans le système à sécuriser, en fonction du cycle de vie de ce dernier, par des approches complémentaires d'ingénierie et de gestion de la sécurité informatique.

2.1. Définition système informatique

Selon (MEHARI 2001), un **système informatique** est un ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures…) permettant d'acquérir, de stocker, de communiquer des informations sous forme de données, textes, images, sons… dans des organisations.

Alors qu'un **système d'information** est un ensemble de moyens techniques, administratifs, et humains qui servent à la collecte, au classement et à la transmission d'informations entre les membres d'une organisation (institution, entreprise, association,..)

Figure 2 : Concept et relation de la sécurité informatique



Source ISO 2002

Au titre de la sécurité informatique, nous distinguons :

- La sécurité physique
- La sécurité personnelle
- La sécurité procédurale
- La sécurité des systèmes d'exploitation
- La sécurité des communications
- La sécurité logique

Selon (ISO 2005), la sécurité est donc un concept relatif, car dit-on : « On est plus ou moins en sécurité qu'avant, plus ou moins qu'ailleurs, mais on ne peut jamais être sûrs d'être parfaitement en sécurité. »

2.2. Objectifs principaux sécurité informatique

Nous distinguons 5 objectifs parmi lesquels :

- Accessibilité (continuité du service)
- Confidentialité;
- Authenticité;
- Irrépudiabilité;
- Intégrité ;
- Disponibilité

2.2.1. Confidentialité des données

Selon la norme (ISO 2005), c'est un concept permettant de s'assurer que l'information ne peut être lue que par les personnes autorisées :

- Solution dans le monde réel :
- Utilisation d'enveloppes scellées ;
- Verrouillage avec clés ;
- Mesures de Sécurité physique ;
- Utilisation de l'encre invisible.

Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- Limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;
- les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

Le chiffrement des données (ou cryptographie) contribue à assurer la confidentialité des données et à augmenter la sécurité des données lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement sont relativement peu mises en œuvre par les internautes de manière courante.

2.2.2. Authentification

C'est un concept permettant de s'assurer que l'identité de l'interlocuteur et bien celle qu'il prétend. On distingue les techniques traditionnelles suivantes :

- Some Thing you Know : mot de passe
- Some Thing you Have : carte à puce
- Some Thing you Are : empreinte digitale.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associées aux personnes. Cela exclut l'usage anonyme des ressources. C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

L'authentification, suite à une identification donne lieu à un « accord » ou un « refus » après un contrôle d'accès.

2.2.3. Non répudiation

C'est un ensemble de moyens techniques permettant de prouver la participation d'une entité dans un échange de données. La Technique traditionnelle utilisée est la signature légalisée.

Elle permet de garantir qu'une transaction ne peut être niée. La **non-répudiation** est alors le fait de ne pouvoir nier ou rejeter qu'un événement (action, transaction) a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité.

2.2.4. Intégrité des données

C'est un ensemble de moyens et techniques permettant de restreindre la modification des données aux personnes autorisées.

En effet, il convient de se prémunir contre l'altération des données en ayant la certitude qu'elles n'ont pas été modifiées lors de leur stockage, de leur traitement ou de leur transfert. Les critères de disponibilité et d'intégrité sont à satisfaire par des mesures appropriées afin de pouvoir atteindre un certain niveau de confiance dans les contenus et le fonctionnement des infrastructures informatiques et télécoms. Si en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques

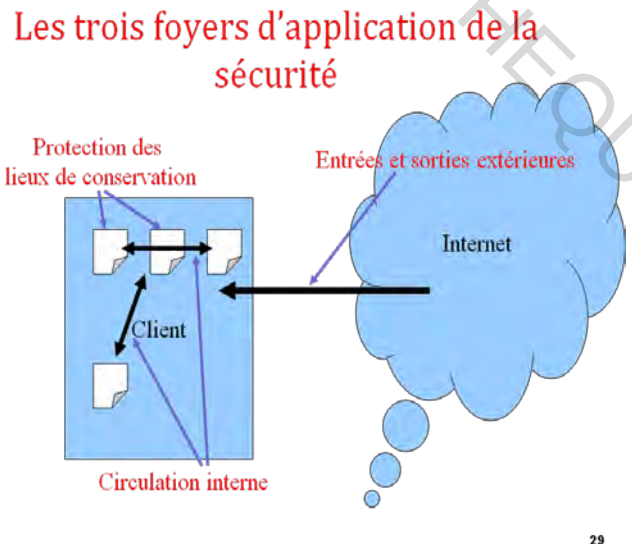
de traitement de l'information (logiciels d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données).

2.2.5. La disponibilité

Permettant de maintenir le bon fonctionnement du système d'information, la disponibilité d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée (serveur ou réseau par exemple).

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit (notion d'accessibilité). La disponibilité des services, systèmes et données est obtenue par un dimensionnement approprié et une certaine redondance des infrastructures ainsi que par une gestion opérationnelle et une maintenance efficaces des infrastructures, ressources et services.

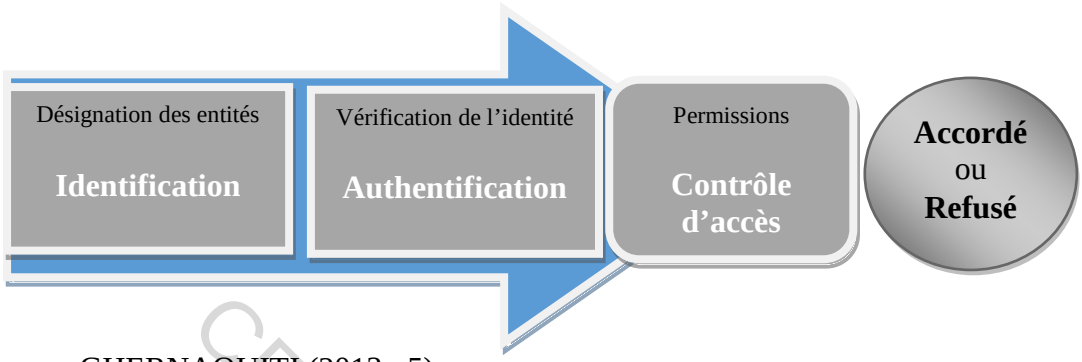
Figure 3 : Les foyers d'application de la sécurité informatique



Source ISO 2005

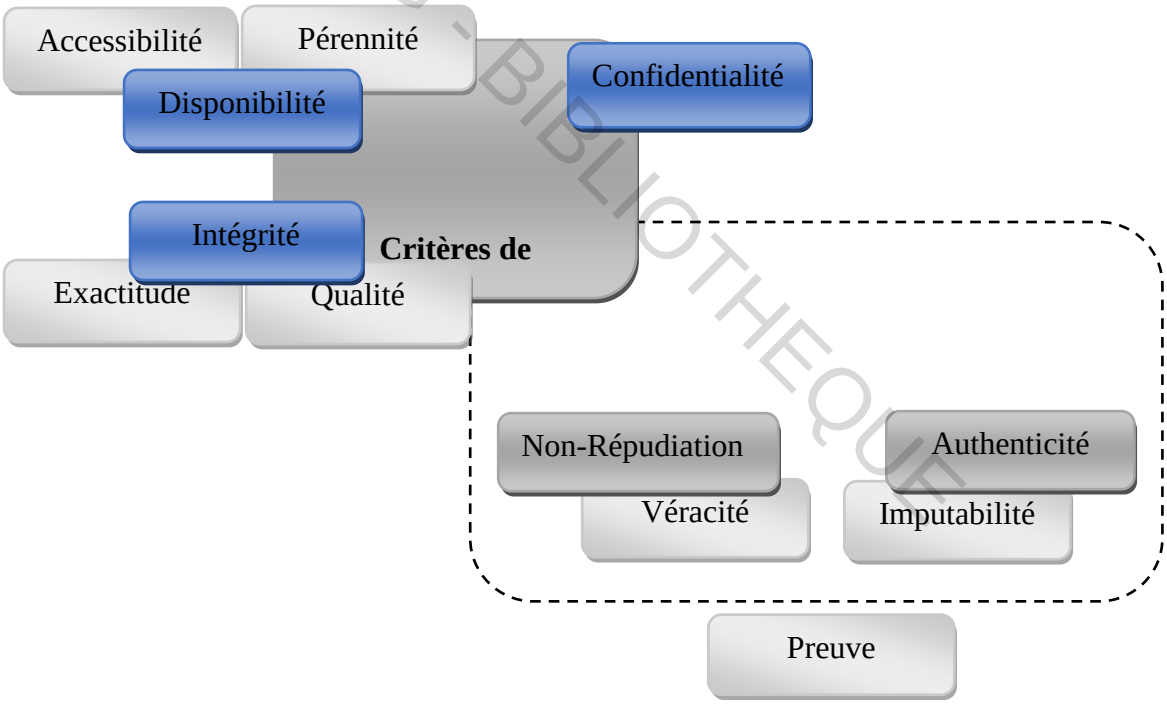
Le schéma que suit un « Accord » ou un « Refus » peut être élaboré de la manière suivante :

Figure 4 : Identification et authentification



Source : GHERNAOUITI (2013 : 5)

Figure 5 : Critères de sécurité



Source : GHERNAOUITI (2013 : 2)

2.3. La Politique de Sécurité

C'est l'expression de ces objectifs cités ci-dessus.

Elle indique l'ensemble des mesures à prendre, des structures à définir et l'organisation à mettre en place afin :

- D'empêcher (ou tout au moins freiner) la détérioration, l'utilisation anormale ou la pénétration des systèmes et réseaux ;
- de détecter toute atteinte, malveillante ou non, à l'intégrité, la disponibilité et la confidentialité des informations ;
- d'intervenir afin d'en limiter les conséquences et, le cas échéant, poursuivre l'auteur du délit.

Il est indiqué dans toute entreprise de développer une politique de sécurité adaptée aux risques et identifier les points sensibles. Il s'agira alors :

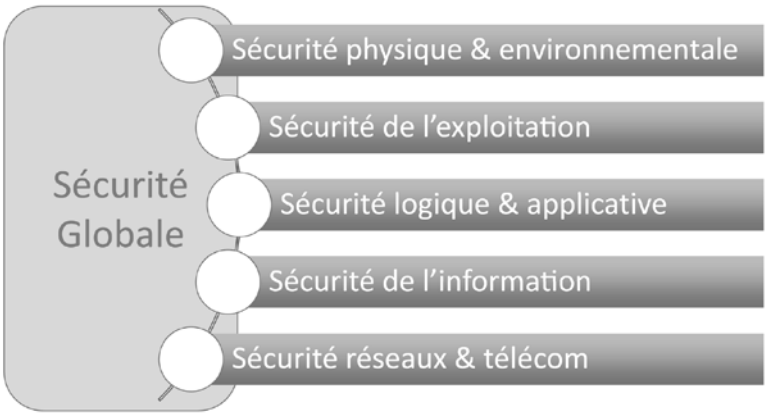
- Identifier les actifs de l'entreprise et auditer chaque système correctement
- Analyser correctement le système dans son ensemble et le sécuriser
- Cloisonner l'Intranet et garder une vue d'ensemble de la problématique.

2.4. Domaine d'application de la sécurité informatique

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information. En fonction de son domaine d'application la sécurité informatique se décline en :

- Sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité logique, sécurité applicative et sécurité de l'information **;**
- sécurité des infrastructures informatique et de télécommunication (sécurité des réseaux, sécurité Internet et cyber sécurité)**.**

Figure 6 : Sécurité Globale



Source : GHERNAOUITI (2013 : 7)

2.5. Causes des vulnérabilités des réseaux

Selon la norme ISO 17799, les causes essentielles sont :

- La multiplication des serveurs ;
- La désinformation et l'obsolescence ;
- L'accès Internet et les applications extranet ;
- L'encapsulage des protocoles ;
- La diffusion de codes mobiles incontrôlables (ActiveX,) ;
- Utilisation de formats propriétaires mal conçus ;
  - transmission accrue de virus (macro)
- Protocoles non-documentés, protocoles propriétaires ;
- Systèmes d'exploitation et applications inadaptées à la sécurité ;
- Soumission passive au monopole ou Inconscience.

Figure 7 : Les menaces sur le système informatique

Source : Isabelle, 2008

Ce schéma montre tout simplement les différentes menaces que nous pouvons rencontrer sur un système d'information. Nous remarquons trois têtes de personne, présentes dans un réseau inter-relié où nous voyons une entreprise et un utilisateur individuel reliés à un serveur web. Ces trois personnes représentent ici des pirates ou des personnes de mauvaise foi dont l'un procède par une attaque en interne par usurpation de mots de passe pouvant lui conduire à entrer dans le système de l'entreprise ou de l »utilisateur individuel. Un autre attaque par l'émission des virus en émettant des virus dans le réseau informatique et un dernier par l'usurpation d'identité et par des accès non autorisés tout en utilisant des virus, des modifications de fichiers et de programmes, etc.

Comme menace nous remarquons aussi les accidents pouvant survenir, comme des incendies, des dommages électriques, etc.

Les risques liés au système informatique sont classés en trois catégories liées à la causalité :

- Accidents ;
- Erreurs ;
- Malveillance.

et en deux familles :

- **Risques Physiques ou risques matériels** : (incendies, explosions, dommages électriques, tempêtes, bris de machines, vols ;
- **Risques Logiques ou risques immatériels** : Accidents : endommageant ou perturbant les supports d'information ;

  - Erreurs **humaines** : (programmation, exploitation, manipulation...) ;
  - Malveillance : interne ou externe ;
  - Risques Juridiques : responsabilité civile ou pénale vis à vis d'autrui, clients, autorités

2.6. Les différents types de risques pour une structure

Figure 8 : Risques pour l'organisation

Risques pour l'organisation (1/3)

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
Authentification : détermination de l'identité de l'interlocuteur	Le serveur est-il réellement celui qu'il dit être?	L'utilisateur est-il bien celui qu'il prétend être?	Usurpation d'identité
Intégrité l'assurance que l'information stockée ou transmise n'est pas altérée	L'information reçue est-elle identique à celle émise? Mes fichiers sont-ils corrompus? L'information est-elle fiable?		odification accidentelle ou intentionnelle de l'information hébergée ou des transactions électroniquesM
Confidentialité la connaissance de l'information par un groupe restreint de personnes ou de systèmes	L'information n'est-elle connue que de l'émetteur et du récepteur? L'information stockée est-elle accessible uniquement aux personnes autorisées?		Détournement de l'information, appropriation non autorisée d'informations

Risques pour l'organisation (2/3)

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
Autorisation la permission de faire ou d'accéder à quelque chose	Qui peut accéder à mon ordinateur pendant mon absence?	L'utilisateur distant accède-t-il uniquement aux services et informations pour lesquels il a obtenu une autorisation?	Accès non autorisé à des ressources ou informations
Non répudiation protection contre la négation d'une action accomplie	Le fournisseur de services peut-il faussement prétendre qu'il n'a pas reçu ou effectué la transaction?	L'utilisateur peut-il faussement prétendre qu'il n'a pas effectué une transaction?	Nier avoir passé une commande électronique ou avoir effectué un achat
Traçabilité garder un historique des événements	Qui a fait quoi, utilisé quoi et quand et comment?		Impossibilité de reconstituer les étapes qui ont conduit à un incident

Risques pour l'organisation (3/3)

Domaines	Exemples de question de la part		Problèmes potentiels
	de l'utilisateur externe	du fournisseur de services et d'informations	
Intrusion accès non autorisé	Comment protéger mon système personnel?	Comment détecter les intrus? Comment protéger le serveur?	Accès non autorisés et actions malveillantes (introduction de virus ou de mouchards, modification de contenu, blocage des accès, etc.), accès non souhaités (spams)
Protection physique protection contre les accidents ou sabotage	Garder l'intégrité des informations en cas de panne de courant, dégâts des eaux, incendie, etc.		Interruption non prévue de l'opérationnel et impossibilité de redémarrage rapide, dégâts irréversibles du matériel, de données
Gestion des procédures, des ressources humaines et machines		Que doit-on faire? Qui fait quoi, qui est responsable de quoi, qui met à jour quoi? Qui peut entrer en salle machine?	Pas de contrôle, manque de rigueur dans la gestion des mots de passe, des mises à jour des fichiers d'autorisation d'accès, des fichiers d'audit, de la configuration des routeurs et firewalls, etc.

Source : Norme ISO 2005

2.7. Les divers types de vulnérabilités réseaux

Au titre des vulnérabilités réseaux qui ne sont pas exhaustives, nous avons :

- Le système de fichiers en réseau
  - Partage de fichiers (NFS, dossiers partagés)
- Le social engineering
  - Technique d'intrusion sur un système qui repose sur les points faibles des personnes qui sont en relation avec un système informatique plutôt que sur le logiciel. Le but est de piéger les gens en leur faisant révéler leur mot de passe ou toute autre information qui pourrait compromettre la sécurité du système informatique
- « crackage » de mot de passe
  - Dans ce genre d'attaque, on utilise un dictionnaire de mots et de noms propres, et on les essaie un à un pour vérifier si le mot de passe est valide. Bien évidemment, ces attaques ne se font pas « à la main », mais avec des programmes qui peuvent deviner des centaines voire des milliers de mots de passe à la seconde
- « sniffing » des mots de passe et des paquets
  - La plupart des réseaux utilisent la technologie de « broadcasting » ce qui signifie que chaque message (ou paquet) qu'un ordinateur transmet sur un réseau peut être lu par n'importe quel ordinateur situé sur le réseau. En pratique, tous les ordinateurs sauf le destinataire du message vont s'apercevoir que le message ne leur est pas destiné et vont donc l'ignorer. Mais par contre, beaucoup d'ordinateurs peuvent être programmés pour regarder chaque message qui traverse le réseau
- L'IP spoofing
  - Récupération de numéro IP
  - Messagerie électronique
  - Services basés sur le protocole IP
- Les chevaux de Troie
  - Un cheval de Troie est un programme qui se cache lui-même dans un autre programme apparemment au-dessus de tout soupçon. Quand la victime (l'utilisateur normal) lance ce programme, elle lance par la même le cheval de

Troie caché.

- Les vers
  - Un ver est un agent autonome capable de se propager sans l'utilisation d'un programme quelconque ni d'une action par une personne
- Les trappes
  - Une trappe est un point d'entrée dans un système informatique qui passe au-dessus des mesures de sécurité normales. C'est généralement un programme caché ou un composant électronique qui permet au système de protection d'être inefficace. De plus, la trappe est souvent activée par un évènement ou une action « normale
- TCP-SYN flooding (déni de service)
  - Le système client commence par envoyer un message SYN (pour synchronisation) au serveur. Le serveur renvoie alors un accusé de réception du SYN: SYN-ACK (pour synchronisation-aknowledgment) au client.
  - Le client doit alors établir la connexion en répondant par un ACK dans le cas d'une connexion normale.
  - En cas de déni de service, le client ne renvoie pas ACK et la connexion reste ouverte jusqu'au TIME-OUT Système.

2.8. Les actions préventives

Les actions préventives contre les menaces types informatiques sont :

- Définition d'architectures réseau sécurisées ;
- Protection des accès internet et intranet ;
- Installation des anti-virus ;
- Définition des procédures d'identification des utilisateurs ;
- Mise en place de solutions firewall ;
- Sécurisation des serveurs sensibles et des applicatifs ;
- Audits sécurité ;
- Externalisation des sauvegardes informatiques ;
- Sécurisation du transport des données (cryptologie, certificats électroniques, VPN).

Conclusion chapitre 2

Ce chapitre nous a permis d'identifier et classer les différents types de risque, de se prévenir contre les menaces informatiques et évaluer les procédures nécessaire liés à la sécurité informatique. Il nous a également permis de comprendre la démarche d'une politique de sécurité.

Vu l'importance de l'audit interne et ses enjeux dans le développement des activités d'une structure, nous estimons qu'il est nécessaire pour toute entreprise de mettre en place une politique de sécurité adaptée aux risques et ainsi identifier les points sensibles. La bonne santé de l'entreprise passe toujours par un contrôle sérieux du fonctionnement de ses activités.

Dans le but d'approfondir notre second chapitre, notre étude se poursuivra avec un troisième qui portera sur la méthodologie de l'étude. Il s'agit pour nous de déterminer quelle approche allons-nous adopter pour la phase pratique de l'étude.

Chapitre 3 : METHODOLIGIE DE LA RECHERCHE

La revue de littérature nous a permis de dresser le cadre théorique de notre étude ainsi que d'avoir une vue d'ensemble des concepts liés à la sécurité des systèmes d'information. Ce cadre théorique ainsi élaboré servira pour nous de levier dans l'élaboration de la méthodologie à suivre pour atteindre les objectifs de notre recherche. Ce chapitre consistera à présenter la méthodologie que nous utiliserons et les outils de collecte de données nécessaires pour la réalisation de l'étude.

3.1 Modèle d'analyse

Il s'agit d'une représentation graphique qui récapitule les différentes phases, étapes et outils qui seront appliqués lors de la réalisation de notre étude.

Le modèle suivant représente notre modèle d'analyse.

Tableau 1 : Modèle d'analyse

Phases		Etapes		Outils
Phase de planification	⇒	Prise de connaissance	⇒	Entretien Entretien Analyse documentaire Observation participative QPC
⇓				
Phase d'accomplissement	⇒	Test de conformité Test de permanence Evaluation du système	⇒	Code du droit du travail Flow-charts L'arbre des causes, le comptage thématique, l'analyse de contenu Tableau de répartition des responsabilités
⇓				
Phase de conclusion	⇒	Evaluation du contrôle interne Analyses recommandations	⇒	FRAP Points de contrôle

Source : Nous-mêmes

3.2. Outils de collecte et d'analyse des données

Nous distinguerons les outils de collectes des outils d'analyses des données.

3.2.1. Les outils de collecte des données

Les outils de collecte de l'information portent sur le « comment » dans la démarche de l'audit social. Les outils choisis doivent être pertinents par rapport à la taille de l'échantillon (le qui), au temps disponible pour mener l'audit social (le quand) et au type d'information à recueillir (le pourquoi). Compte tenu du contexte et du climat dans lequel nous évoluions, nous avons décidé d'adopter l'analyse documentaire, l'entretien individuel et l'observation, le questionnaire de prise de connaissance (QPC), le flow-chart ou diagramme de circulation des documents et la FRAP (Feuille de Révélation et d'Analyse de Problème). Pris individuellement ils ne seraient pas pertinents mais ensemble ils permettent de combler les manquements qui auraient pu être décelés compte tenu de leur caractéristique propre.

3.2.1.1. L'analyse documentaire

Elle consiste à consulter et à exploiter les documents que Congo Télécom nous aura fournis. Selon Sylvie Guerrero (2008 : 24), l'analyse documentaire présente l'avantage d'être rapide, de permettre une collecte facile et systématique de l'information et de permettre de traiter beaucoup de dossiers de salariés. Toutefois, elle ajoute que cet instrument doit être utilisé en complément d'autres outils de collecte pour une meilleure efficacité.

L'utilisation donc de la revue documentaire à Congo Télécom nous permettra d'avoir une vue d'ensemble sur Congo Télécom et sur le fonctionnement de ses différents services. Elle permettra également avec l'aide de l'entretien d'effectuer le test de conformité et les tests de permanence.

3.2.1.2. Questionnaire de prise de connaissance (QPC)

Le Questionnaire de Prise de Connaissance intervenant lors de la phase de préparation, permettra de prendre connaissance de l'application du code de travail, du système de contrôle interne. La prise de connaissance portera également sur la gestion du personnel et du climat dans lequel il évolue.

La prise de connaissance du domaine ou de l'activité à auditer ne doit pas se faire dans le désordre, c'est pourquoi l'auditeur va utiliser un questionnaire dénommé « Questionnaire de Prise de Connaissance » récapitulant les questions importantes dont la réponse doit être connue si on veut avoir une bonne compréhension du domaine à auditer. C'est un moyen efficace pour organiser la réflexion et les recherches et surtout pour :

- bien définir le champ d'application de sa mission,
- prévoir en conséquence l'organisation du travail et en particulier en mesurer l'importance,
- préparer l'élaboration des Questionnaires de **Contrôle** Interne.

De surcroît, chaque auditeur construit son QPC en fonction de ses acquis, de ses expériences, de ce qu'il sait et de ce qu'il a besoin d'apprendre. Quelles que soient ses dimensions, il est indispensable à la compréhension du sujet par l'auditeur.

Un QPC complet doit comprendre trois parties, allant du général au particulier, sachant que le général ne doit pas déjà être connu et/ou inventorié.

La structure globale du QPC est la suivante :

- Connaissance du contexte socio-économique :
  - taille et activité du secteur audité
  - situation budgétaire
  - situation commerciale
  - effectifs et environnement de travail.
- Connaissance du contexte organisationnel de l'unité :
  - organisation générale et structure
  - organigrammes et relations de pouvoir
  - environnement informatique.
- Connaissance du fonctionnement de l'entité auditée :
  - méthodes et procédures
  - informations réglementaires

- organisation spécifique de l'entité
- système d'information
- problèmes passés ou en cours
- réformes en cours ou prévues.

L'auditeur attachera une importance toute particulière à ces deux dernières rubriques car elles signalent des zones à risques :

- Ou bien on est en présence d'une activité « à problèmes », donc une attention toute particulière va être nécessaire.
- Ou bien on est en présence d'une activité où se préparent d'importantes réformes.
- C'est alors que l'attention se relâche. La situation est identique si des réformes viennent d'être mises en place et que la période de rodage n'est pas achevée.

Donc nécessité absolue pour l'auditeur de faire l'inventaire complet de ces situations d'exception.

3.2.1.3. L'entretien individuel

Il s'agit d'une discussion entre l'auditeur et un salarié de l'entreprise. L'auditeur aborde les thèmes et les points qui lui permettront de compléter ses recherches débutés avec la revue documentaire. Cette méthode bien qu'elle soit longue, permet d'obtenir des informations riches et détaillés de la part du salarié. Cependant, lors d'un entretien certains salariés pourraient être réticents à donner des informations surtout lorsque le thème abordé est sensible.

Afin d'éviter les pertes de temps et d'informations, nous ne passerons les entretiens qu'à un échantillon du personnel de Congo Télécom. Son but étant de faire un rapprochement en termes d'observation avec les pratiques de l'entreprise.

3.2.1.4. L'observation

L'observation et plus particulièrement l'observation participante permet à une personne de se substituer au salarié et de vivre son travail à sa place. Elle est généralement limitée à des activités qui sont visibles de l'extérieur et prend énormément de temps. Cette approche permet de recueillir des informations sur le travail, l'ambiance, le comportement,…. sans

que ceux-ci ne soit biaisés par les autres acteurs. Elle s'utilise également lorsque l'on pense qu'il y aura des réticences avec les autres outils (questionnaires,…).

Son application au sein de notre entreprise d'études (Congo Télécom) nous permettra de mieux apprécier l'environnement de travail des salariés.

3.2.1.5. Le Flow-chart ou diagramme de circulation des documents

Le flow-chart permet de prendre connaissance des processus de l'entreprise au travers d'un graphique. C'est-à-dire qu'il permet d'indiquer l'origine des documents, leur destination et de donner une vision complète du cheminement des informations et de leurs supports.

Cette description graphique s'opère au moyen d'une description narrative et chronologique des opérations constituant la procédure, d'une représentation simplifiée des documents créés ou utilisés, de lignes de flux retraçant le cheminement des documents.

3.2.1.6. Les FRAP (Feuilles de Révélation et d'Analyse de Problèmes)

La FRAP est un document normalisé qui s'utilise durant la phase de terrain. Celui-ci aide l'auditeur à conduire et à structurer son raisonnement de façon logique et chronologique. Ainsi, chaque fois que l'auditeur constate un problème ou un dysfonctionnement, il rédige une FRAP.

La finalité de la FRAP est de formuler des recommandations et sert également de base pour la rédaction du rapport.

3.2.2. Les outils d'analyse des données

Les outils de collecte des données tiennent compte du « qui », du « comment » et du « pourquoi » pour permettre à l'auditeur social de présenter les résultats de sa mission. L'importance de ces outils ne doit pas être négligée car seule une bonne analyse garantit la solidité des résultats. Comme outils d'analyses, nous utiliserons l'analyse de contenu et l'arbre des causes.

3.2.2.1. L'arbre des causes

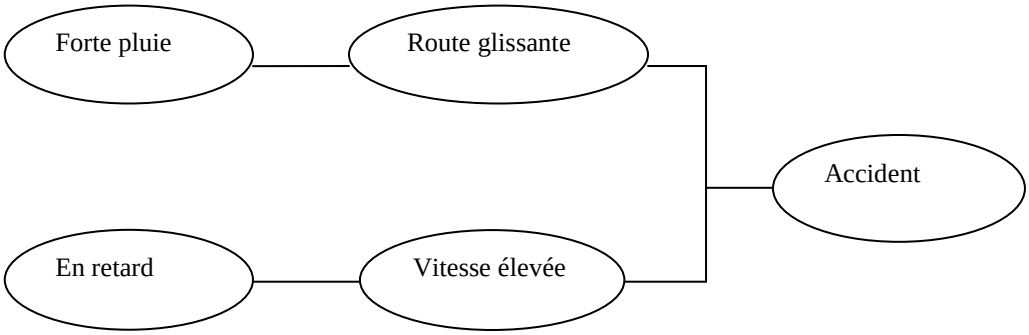
Il s'agit d'une technique d'analyse qui permet de synthétiser toutes les informations dont dispose l'auditeur. Dans cette optique il s'agit de repérer l'ensemble des causes d'un phénomène, telles qu'elles apparaissent à la lumière des informations collectées.

Selon Jean-Pierre Heckmann (D'après un document de l'IUTA de l'université de Bordeaux : 1-8) l'arbre des causes a été élaborée par l'INRS en se fondant sur des travaux initiés par la Communauté Européenne du Charbon et de l'Acier. Sa première expérience pratique remonte à 1970 dans les mines de fer de Lorraine. Et à partir de 1976, il est utilisé par un grand nombre d'entreprises et d'organismes comme technique d'investigation et de recherche de facteurs d'incidents / accidents.

Pour Jean-Pierre Heckmann, réaliser un arbre des causes consiste à lister tous les faits recueillis et de les résumer en de simples mots. Ces mots sont ensuite organisés sous forme de diagramme en partant de la droite vers la gauche. Pour cela, on doit toujours se poser certaines questions relatives à l'ensemble des faits antécédents ayant engendré l'accident. Il s'agit de :

- Qu'a-t-il fallu pour que ce fait se produise ?
- ce fait a-t-il été nécessaire ?
- ce fait a-t-il été suffisant ?

Figure 9 : L'arbre des causes de l'analyse d'un incident / accident



Source : *Jean-Pierre HECKMANN (D'après un document de l'IUTA de l'université de Bordeaux : 6)*

Selon Sylvie Guerrero (2008 : 28), l'arbre des causes présente des avantages. En effet, il permet de faire une synthèse des causes et met en perspective les données recueillies quel que soit l'outil de collecte utilisé. Nonobstant, son inconvénient est qu'il n'apporte pas de garantie statistique contrairement aux tests. Toutefois cet auteur dénote une pertinence dans son utilisation du fait qu'il est généralement utilisé pour ordonner, trier l'information, pour représenter les causes et conséquences d'un problème dans un schéma.

3.2.2.2. L'analyse de contenu

Née aux Etats Unies, l'analyse de contenu s'est développée du fait de la deuxième guerre mondiale. Au début penchée sur l'analyse de la presse écrite, elle s'est ensuite tournée vers l'analyse du discours politique. L'une des premières définitions est celle de Berelson qui a été reprise par Yves Evrad & al (2000 : 116) qui dit que : *« l'analyse de contenu est une technique de recherche pour la description objective, systématique, et quantitative du contenu manifeste des communications ayant pour but de les interpréter »*. Passée par une période d'abandon et de désintérêt elle retrouve une nouvelle jeunesse dans les années 60-70 grâce à l'arrivée de trois éléments déterminants que sont l'ordinateur, l'intérêt pour les études concernant la communication non verbale et l'épanouissement de la sémiologie et en dernier la précision enviable des travaux linguistiques. Tout ceci fait qu'aujourd'hui Laurence Bardin (2009 : 13) définit l'analyse de contenu comme *« un ensemble d'instruments méthodologiques de plus en plus raffinés et en constante amélioration s'appliquant à des discours (contenus et contenants) extrêmement diversifiés »*. En somme,

l'on constate quel que soit son évolution, son analyse porte sur les communications et consiste à étudier en détail le contenu des discours et des propos prononcés.

Selon Sylvie Guerrero (2008 : 28), l'analyse de contenu présente des avantages. Celui de permettre de comprendre une situation et d'avoir des analyses précises et détaillées. Toutefois il n'a pas que des avantages. Son inconvénient est qu'il est très long et demande beaucoup de rigueur. Cette dernière note également une pertinence dans l'utilisation de cet outil dès lors que l'on a procède à des entretiens ou à de l'observation.

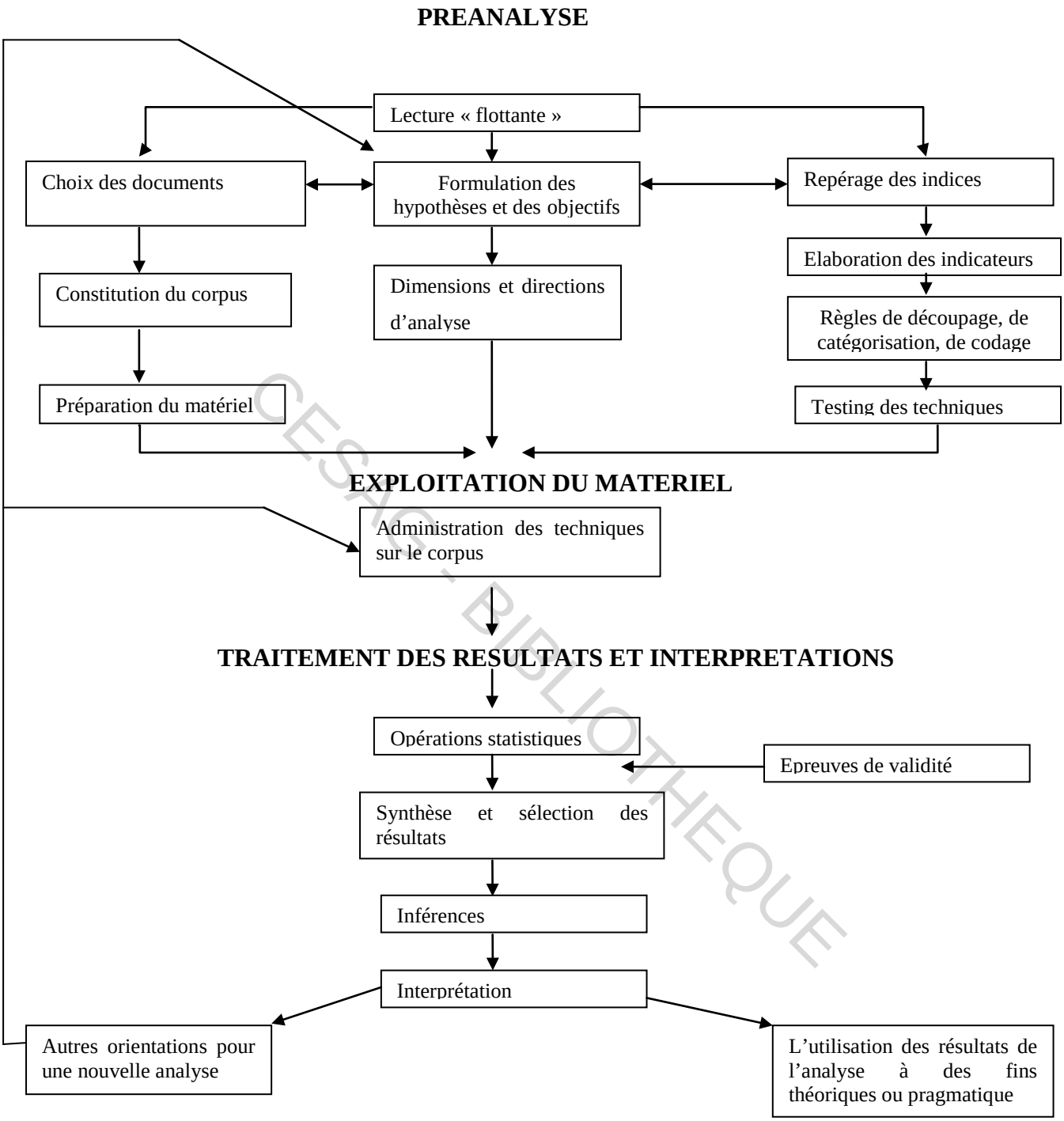
Selon L. Bardin (2009 : 125-133), l'analyse de contenu comporte trois phases : la pré-analyse, l'exploitation du matériel, le traitement des résultats, l'inférence et l'interprétation.

La pré-analyse est la phase d'organisation et comprend trois missions très liées l'une à l'autre. Il s'agit du choix des documents, la formulation des hypothèses et celle des objectifs. Pour la réalisation de ces missions, il faut réaliser certaines activités telles que la lecture « flottante » qui consiste en une lecture des documents et en l'émission d'hypothèses. Le choix des documents où il faut constituer un corpus. Le corpus étant « l'ensemble des documents pris en compte pour être soumis aux procédures analytiques ». La constitution de ce corpus est soumis à des choix, des sélections et à des règles (exhaustivité, représentativité, homogénéité, pertinence,…). Ensuite vient la formulation des hypothèses et des objectifs qu'il faudra confirmer ou infirmer.

L'exploitation du matériel consiste en la mise en œuvre de la procédure décrite dans la pré-analyse (découpage, regroupement, codage, décompte ou énumération en fonction des consignes préalablement formulées). Elle peut se faire manuellement ou par ordinateur.

La figure suivante récapitule le déroulement d'une analyse de contenu.

Figure 10 : Déroulement d'une analyse de contenu



Source : *Laurence BARDIN, (2009 : 133)*

Ce chapitre qui porte sur la méthodologie de l'étude nous a permis d'illustrer notre modèle d'analyse. De ce fait, les outils de collectes et d'analyses devraient nous permettre d'apprécier les procédures de Congo Télécom en matière de réalisation d'une mission d'audit informatique.

Conclusion de la première partie

L'évolution des théories des organisations à travers le temps ont contribués à la création de l'audit informatique. Cet audit par la force de ses auteurs s'est fait connaître à travers le monde. Elle s'est ainsi règlementé et a créé des certifications. Tous ces travaux montrent qu'elle est agrée par les entreprises et les particuliers. Ce qui nous laisse croire que cette dernière n'a pas fini son évolution.

L'audit informatique possède une démarche et des outils auxquelles nous allons recourir pour effectuer une mission d'audit du matériel informatique de Congo Télécom. Il s'agira d'un audit de conformité basé sur des référentiels qui aura pour but de connaitre le fonctionnement de cette entité, mais aussi de faire des analyses et de formuler des recommandations.

Cette première partie que nous venons d'achever nous a permis de faire une revue de littérature globale par rapport à notre thème.

Dans la seconde partie de notre travail, nous allons dans un premier temps présenter Congo Télécom ainsi que son mode de fonctionnement au travers de ses procédures. Pour terminer, nous ferons une analyse de ses procédures puis nous proposerons des recommandations.

Pour la deuxième partie :

- Chapitre 4 Description de Télécom CONGO ;
- Chapitre 5 Audit de la sécurité du matériel de Télécom Congo ;
- Chapitre 6 Recommandations et suggestion.

PARTIE II – CADRE PRATIQUE DE L'ETUDE

Introduction partie 2

Après une connaissance théorique sur les risques, la sécurité du parc informatique, ses normes et sécurité système d'information, nous allons procéder dans une seconde partie à la mise en œuvre pratique de ces aspects tout en abordant la présentation de Congo Télécom. En effet, les décisions qui étaient par le passé plus ou moins faciles à prendre dans un environnement simple et stable, présentent actuellement plus de difficultés dans un environnement risqué. Pour une décision de qualité, il est indispensable de disposer d'une très bonne qualité d'informations. La garantie de la qualité de ces informations dépend de l'opinion d'un professionnel.

L'auditeur doit donner son opinion sur le système de contrôle interne de l'entreprise dans le souci d'apporter une aide et pour permettre une réduction de l'étendue des travaux traditionnels d'audit.

Ainsi, cette partie se subdivise en trois chapitres :

- Chapitre 4 Description de Télécom CONGO ;
- Chapitre 5 Audit de la sécurité du matériel de Télécom Congo ;
- Chapitre 6 Recommandations et suggestion.

Chapitre 4 : DESCRIPTION DE CONGO TELECOM

Ce chapitre a pour objectif de mettre en exergue la présentation de Congo Télécom, son historique, ses missions, ses activités, ses directions et services ainsi que son organigramme afin de mieux appréhender la gestion de la sécurité de son parc informatique.

4.1. Historique Congo Télécom

L'historique de Congo Télécom remonte de la fin de la colonisation, entre 1958 et 1960, les années de l'indépendance de plusieurs pays africains, dont le Congo Brazzaville fait partie. A cette époque, les services des postes et télécommunications de la sous-région équatoriale ou de l'Afrique Equatoriale Française (AEF) étaient au compte de l'Office Equatoriale des Postes et Télécommunications (OEPT) qui va survire jusque dans les années 1963 et 1965.

En 1963, après la conséquence de l'indépendance en 1960 à travers les colonies de l'AEF, l'OEPT s'éclate avec la décolonisation des colonies qui vont devenir des Etats : Cameroun, Congo, Gabon, Guinée Equatoriale, République Centrafricaine et Tchad ; qui formaient cette entreprise équatoriale. Chaque colonie devenant un pays indépendant profite de la souveraineté pour gérer les services des postes et télécommunications en toute indépendance ; ainsi, sera créée une société paraétatique appelée : Office Nationale des Postes et Télécommunications (ONPT).

L'ONPT a subi des conséquences de la gestion de l'Etat qui est l'actionnaire principal et cela s'est traduit par un échec, trois décennies plus tard, suite à plusieurs difficultés financières et autres afin d'arriver à la création de la SOTELCO (Société des Télécommunications du Congo) pour devenir Congo Télécom tel que nous allons découvrir dans la suite de l'historique.

Le 19 Août 2009, Congo Télécom est née des ruines de l'ancienne appellation SOTELCO (Société des Télécommunications du Congo).

En 1960, lors de l'accession de la République du Congo à l'Indépendance, l'Office Equatorial des Postes et Télécommunications (l'OEPT) se disloque pour voir se créer à la place quatre ans plus tard, trois structures dont les deux premières fusionneront en 1979:

- L'Office des Télécommunications Internationales du Congo (INTELCO) ;
- l'Office National des Postes et Télécommunications (ONPT) ;
- la Direction de la Caisse Nationale d'Epargne (DCNE).

L'ordonnance n° 08-2001 du 1 juillet 2001 dissout l'ONPT et donne naissance à deux autres entités :

- La Société des Postes et de l'Epargne du Congo (SOPECO) par ordonnance n°10-2001 du 1 juillet 2001 ;
- la Société des Télécommunications du Congo (SOTELCO) par ordonnance n°11-2001 ;

Deux ans plus tard, le décret présidentiel du 28 février 2003 appliqué le 03 mars 2003 fait de la SOTELCO une société anonyme unipersonnelle (SAU) au capital de 5 200 000 000 FCFA avec à sa tête un Administrateur Général.

CONGO TELECOM voit le jour le 18 aout 2009 pour pallier toutes les difficultés qui freinent son développement.

4.2. Présentation de Congo Télécom

Situé au cœur du centre-ville de Brazzaville, Congo Télécom se place au numéro 67 du boulevard Dénis SASSOU NGUESSO (ex avenue Emery Patrice LUMUMBA) dans l'arrondissement 3 Poto-poto Brazzaville. Elle a au nord, la Délégation Générale des Grands Travaux (DGGT), au sud la Caisse de Retraite des Fonctionnaires (CRF), la Direction Générale de la Culture de de l'Art (DGCA) et la papeterie centrale plus les éditions HARMATTAN, à l'Est l'avenue Sergent MALAMINE et à l'Ouest le boulevard Dénis SASSOU NGUESSO.

Le siège de l'administration générale a trois bâtiments construits successivement montrant une forme en « U » et un bâtiment annexe. Une société anonyme unipersonnelle (SAU) avec un Administrateur Général, représentant de l'Etat qui est le principal actionnaire, le capital de l'entreprise est de cinq milliards deux cent millions de francs CFA (5 200 000 000 F CFA) hors projet de couverture nationale en infrastructures de télécommunications en sigle PCN/West Africa Cable System (WACS). Congo Télécom est une société qui gère la téléphonie (fixe et mobile) ainsi que l'internet à côté des

sociétés comme : Airtel, MTN, Warid et Azur qui ne gèrent que la téléphonie mobile et l'internet. On peut aussi ajouter d'autres sociétés qui gèrent les autres services de la communication en fournissant aussi l'internet ou les accessoires des NTIC.

4.3. Missions

Selon l'article 2 des statuts, Congo Télécom a pour missions de :

- Assurer dans le respect de l'équilibre de la gestion financière, le service public des télécommunications nationales et internationales sur toute l'étendue du territoire national ;
- offrir la fourniture des services ou des produits existants, ou nouveaux se rattachant directement ou indirectement en favorisant le développement ;
- conclure les contrats dans le respect de la législation et de la réglementation sectorielle ou générale du cahier de charges de l'opérateur et des dispositions de ses statuts ;
- établir et exploiter tous les types de réseaux de télécommunication, fournir et commercialiser tous les services s'y rapportant ;
- participer au capital de toute société créée ou à créer, ayant un objet similaire ou connexe à celui de la présente société, notamment par voie de création de nouvelles sociétés d'apport, de fusion, d'association en participation.

Sa mission principale est d'ordre public face à l'actionnaire unique. Tout en assurant une rentabilité sur les investissements, Congo Télécom développe des technologies, des infrastructures et des réseaux de télécommunication pour permettre à tous les citoyens et aux entreprises de bénéficier de produits et services au moindre coût.

Du point de vue juridique, Congo Télécom étant une société née des cendres de la SOTELCO retrouve son cadre juridique d'un acte de notarié du 04 Mars 2003, comme une société anonyme unipersonnelle (SAU) avec un Administrateur Général. Elle est régie par l'acte uniforme issu du traité portant le nom Organisation pour l'Harmonisation en Afrique du Droits des Affaires (OHADA).

4.4. Activités Congo Télécom

Comme son nom l'indique, Congo Télécom a ses activités dans le domaine de la télécommunication et en particulier dans celui de la téléphonie. Elle développe et commercialise trois grandes familles de services :

- Les services de communication résidentiels dont la téléphonie fixe, l'internet bas débit par modem, l'internet haut débit par ADSL et très haut débit par fibre optique ;
- les services de communication personnels, c'est-à-dire mobiles ;
- les services de communication d'entreprise.

Avec pour slogan « **le bonheur d'être chez vous !**», Congo Télécom souhaite répandre ses produits dans toutes les habitations du pays. Pour cela, elle a créé divers types de produits et a décidé de créer la marque « Bisengo », chargée de commercialiser des produits et des services fixes et mobiles, destinés au plus grand nombre et au meilleur coût.

Sa gamme de produits est constituée de téléphones fixes, de mobiles, de smartphones, de tablettes, de clés 3G, de modems ADSL et fibre, et d'une offre triple Play (TV + internet + téléphone), pour les particuliers et les professionnels. Cette gamme étendue regroupe des produits d'entrée de gamme jusqu'aux dernières innovations.

4.5. Les structures

Le management de Congo Télécom est dirigé par sept (7) directions coordonnées par un administrateur général et un administrateur général adjoint qui assurent tous la gestion de l'entreprise.

4.5.1. L'administrateur général (AG)

Encore appelé directeur général dans d'autre entreprise, Congo Télécom est représenté par un administrateur général. Il est nommé par décret présidentiel. Il assure la direction générale de la société et représente celle-ci dans ses rapports avec les tiers.

4.5.2. L'administrateur général adjoint

Il assure l'intérim de l'administrateur général et la direction finances et comptabilité, services grands publics.

4.5.3. Direction des ressources humaines

La direction des ressources humaines est chargée de la gestion prévisionnelle et de la gestion administrative centralisée des ressources humaines. Elle est responsable de l'élaboration de la stratégie de formation, élabore puis exécute les plans de formation.

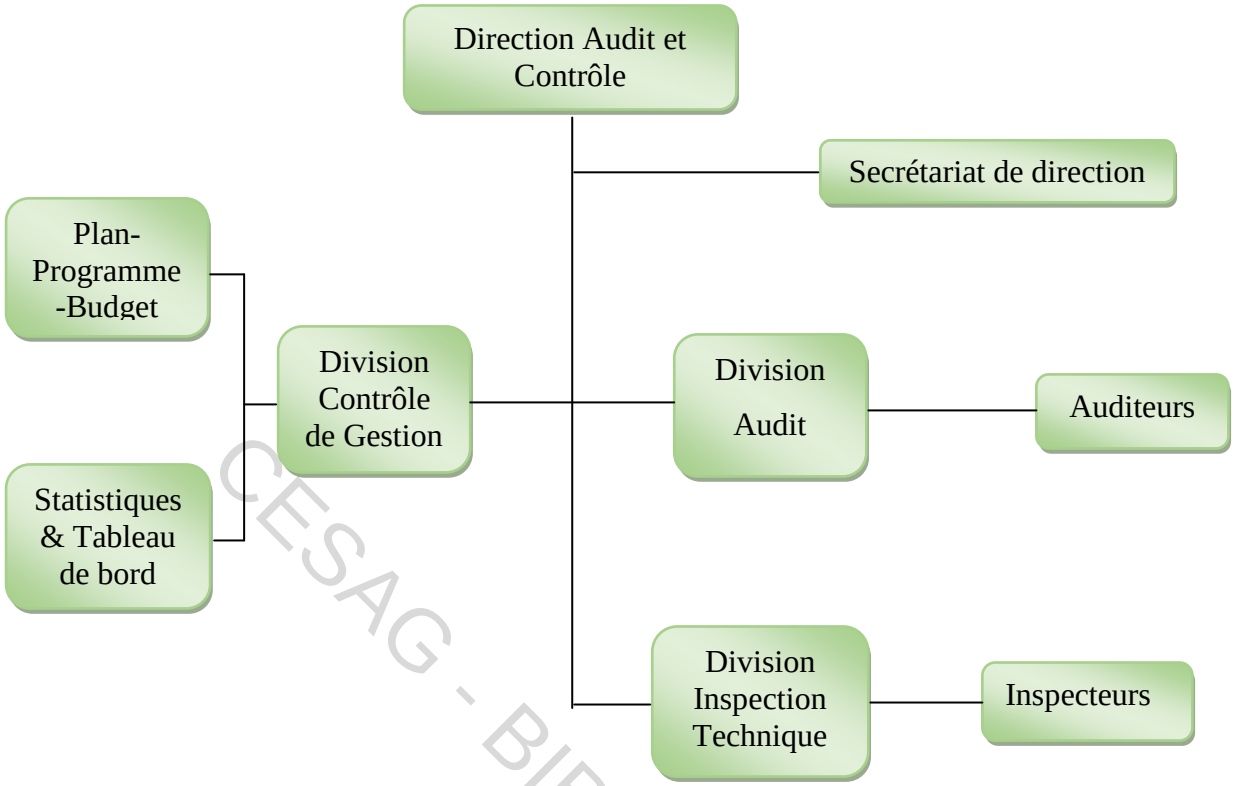
4.5.4. Direction finance et comptabilité

La direction financière et comptable de Congo Télécom est responsable de l'enregistrement exact, exhaustif et traçable de toutes transactions comptables et financières de l'entreprise, de l'établissement et de la présentation à la bonne date selon les règles de l'art des états financiers de synthèse approuvés par les auditeurs externes.

4.5.5. Direction audit et contrôle (DAC)

Elle inclut la division contrôle de gestion, la division audit interne et la division inspection technique. Elle est chargée de l'audit technique, financier, comptable, et social des procédures et règles de gestion des unités. Elle conçoit les procédures pour assurer la transparence des opérations et l'exactitude des transactions. Elle apporte à l'administrateur général, à travers un système d'informations fiables les éléments essentiels pour le managent de l'entreprise. Elle est chargée du reporting, le l'analyse des résultats de l'entreprise pour l'administrateur général, de l'élaboration du budget général et du suivi de son exécution. Elle contrôle aussi le respect des normes techniques de réalisation des ouvrages d'exploitation et de maintenance.

Figure 11 : Organigramme DAC



Source : Nous-mêmes

4.5.6. Direction des services grand public

Cette direction est chargée de définir la politique commerciale grand publique et de la mettre en œuvre, ainsi que de s'assurer de la mise en œuvre de l'ensemble des actions, méthodes et outils permettant le fonctionnement des divers processus commerciaux. Elle gère les abonnés, en particulier les petits clients.

4.5.7. Direction multimédia WHOLESALE et solutions d'entreprise

Cette direction est chargée de concevoir, développer et mettre sur le marché de nouvelles offres de services. Cette direction a déjà conçu le « triple play» qui est un pack comportant les chaines de télévision, l'internet et le téléphone. Elle assure l'adéquation entre les offres et les attentes et besoins des gros clients.

4.5.8. Direction des réseaux et systèmes fixes

La direction des réseaux et systèmes fixes s'occupe de tout ce qui est installation et gestion des appareils fixes. Elle garantit la qualité de fonctionnement des équipements et assure la continuité du service fourni aux clients. Elle assure le développement, l'exploitation et la maintenance des réseaux fixes.

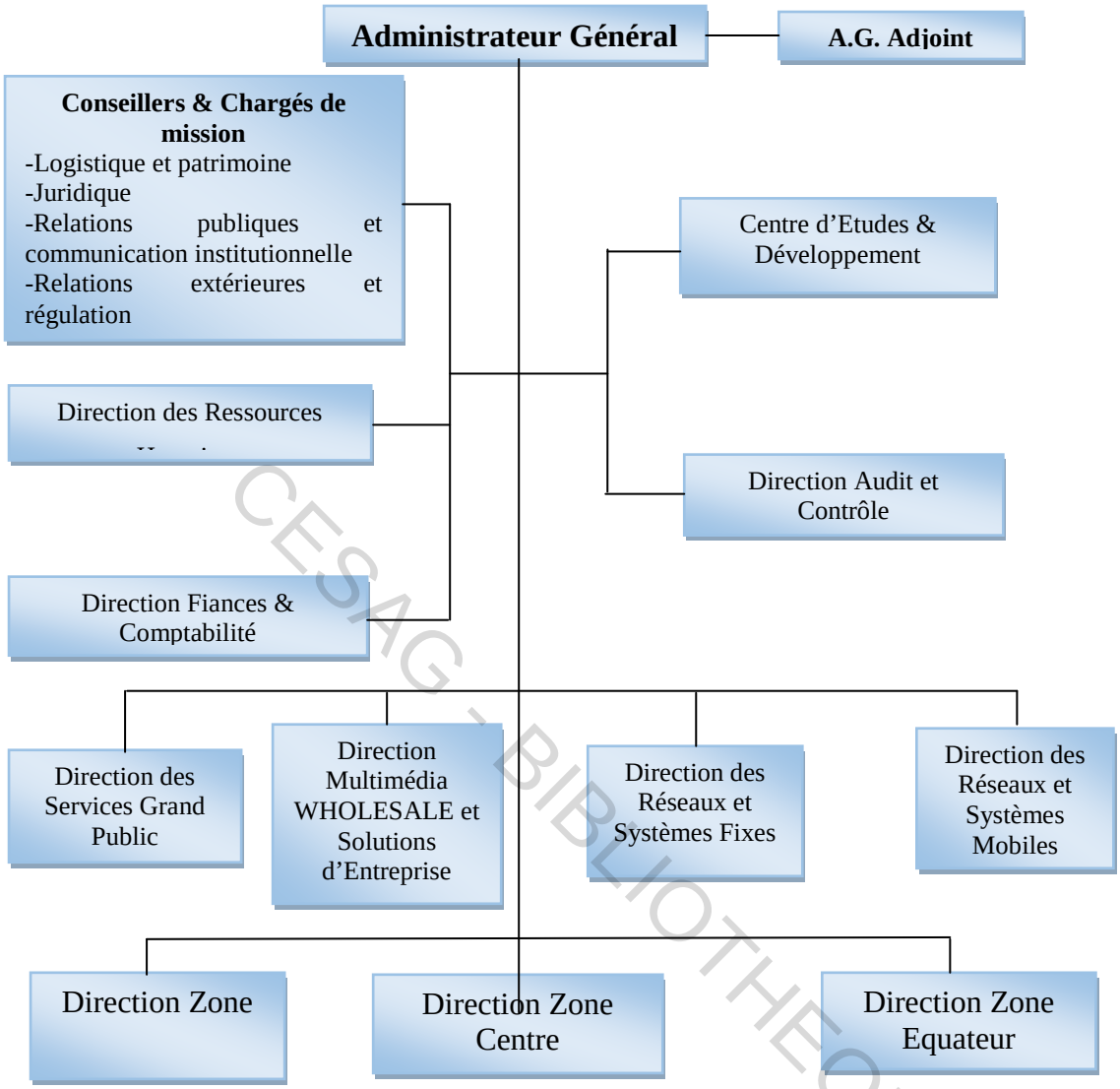
4.5.9. Direction des réseaux et systèmes mobiles

Cette direction par contre n'assure que le développement, l'exploitation et la maintenance des réseaux mobiles. Comme la précédente, elle garantit aussi la qualité de fonctionnement des équipements et des réseaux, mais des réseaux sans fils.

4.5.10. Organigramme de Congo Télécom

Congo Télécom est organisée comme l'indique la figure qui suit :

Figure 12 : Organigramme Général



Source : Nous-mêmes

Conclusion Chapitre 4

Ce chapitre nous a permis après un bref aperçu d'avoir une vue d'ensemble des grandes lignes sur le secteur des télécommunications. Il nous a permis de présenter Congo Télécom, ses activités et d'avoir un aperçu sur son organisation. Cette présentation nous permettra d'appréhender son fonctionnement afin de pouvoir analyser la sécurité de son parc informatique.

Chapitre 5 : AUDIT DE LA SECURITE DU MATERIEL DE CONGO TELECOM

Après avoir présenté Congo Télécom, l'heure est à l'analyse de la sécurité de son matériel informatique.

Du fait de l'immensité du parc informatique, notre travail se limitera à l'audit du parc par le serveur (stockage des données, authentification et contrôle d'accès, partage des fichiers, courrier électronique, accès aux informations world wide web …) conformément aux procédures de gestion du serveur informatique de Congo Télécom. Nous utiliserons essentiellement la norme de sécurité ISO 17799.

5.1. Description du processus de conduite de la mission

Plusieurs documents et outils vont nous permettre de faire la description du processus de conduite de notre mission. Nous pouvons souligner les différentes interviews et les descriptions narratives que nous avons eues auprès des directions réseaux systèmes notamment auprès du service informatique. Dans l'accomplissement de notre mission, une phase de planification a été établie, suivie d'une phase d'accomplissement et enfin une phase de conclusion.

5.1.1. La conduite de la mission

La conduite des missions d'audit au sein de Congo Télécom se résume principalement en trois (3) grandes phases : la phase de planification qui permet la préparation les contrôles, la phase d'accomplissement qui est la phase de conduite des travaux de contrôle ainsi que la phase de conclusion qui est celle de la rédaction du rapport. Après cela, une phase de suivi des recommandations est essentielle afin de suivre la mise en œuvre des plans d'actions.

5.1.1.1. La phase de planification

Cette phase comporte trois étapes dont l'établissement de l'ordre de mission, la prise de connaissance préalable de la structure contrôlée et l'adaptation des guides d'audit.

5.1.1.1.1. L'ordre de mission

Il est rédigé à chaque mission de vérification. L'ordre de mission est établi par l'administrateur général lui-même, conférant les pouvoirs à l'équipe d'audit afin de

poursuivre à bien leur mission. Dans cet ordre de mission sont précisés l'objet, le champ, l'équipe devant conduire la mission, la structure à contrôler ainsi que la durée de la mission.

Toutefois, il existe un programme d'audit et ce programme d'audit constitue par lui-même un ordre de mission collectif. Le service d'audit ne doit donc pas attendre de recevoir d'ordre de mission spécifique pour débuter une mission qui est prévue dans le programme d'audit. Il arrive que, la DAC rédige de sa propre initiative un ordre de mission selon un modèle préétabli et le soumet à la signature de l'AG pour une mission non programmée.

Un ordre de mission additif ou complémentaire peut être joint à l'ordre de mission initialement établi dans le but de couvrir un aspect non prévu.

5.1.1.1.2. La prise de connaissance de la structure contrôlée

Une fois avisée de l'objet de la mission, l'équipe des auditeurs se familiarise avec la structure contrôlée. Après réception de l'ordre de mission et avant de commencer le travail dans le service, l'équipe rencontre les responsables du service informatique pour se familiariser avec la structure, notamment par la lecture des rapports ou notes afin de relever les contrôles qui devraient être faits, de connaitre les points de vue et l'étendue des investigations qui ont été menées. La prise de connaissance se fait également par la lecture des textes de base relatifs au service tel que les lois, les décrets, les circulaires et les notes.

Cette phase permet d'organiser et réaliser la prise de connaissance préalable de l'entité et celle du sujet, de décomposer le sujet de la mission en objets auditables, d'élaborer le référentiel d'audit, de préparer le rapport d'orientation de la mission et de préparer ou actualiser les dossiers.

Plusieurs outils sont utilisés pour acquérir des connaissances au sein des services. Nous pouvons citer : les entretiens, l'analyse documentaire, l'observation physique et les QPC.

Quant à la phase d'adaptation des guides d'audit, elle permet de préparer les documents de travail.

5.1.1.2. Phase d'accomplissement

Cette phase se focalise sur le matériel informatique de Congo Télécom, notamment les serveurs. Elle débute par une réunion d'ouverture, et cette réunion est présidée par le responsable du service d'audit. Après cela, un programme de vérification est établi avant de commencer le travail sur le terrain.

La conduite de la mission se déroule en dehors des locaux de la direction du service d'audit et contrôle. L'équipe d'audit est alors composée d'un chef de mission qui est l'auditeur principal, des auditeurs internes et parfois des contrôleurs et des inspecteurs techniques par rapport à la nature de la mission. Le chef de mission répartit les tâches à effectuer entre les membres de l'équipe.

Les questionnaires de contrôle établis sont administrés au responsable et aux agents du service contrôlé. Au cours de cette intervention, l'audité suspend son activité en cours et se met à la disposition des auditeurs. Chaque auditeur fait une prise de note avec un carnet et les feuilles de travail spécialisées pour la collecte des informations nécessaires à la rédaction du rapport. Après présentation de l'ordre de mission auprès du service, la première personne à être interrogée est le responsable. Il est interrogé sur les missions et les objectifs dévolus à la structure, la gestion des activités du service ainsi que les contraintes et les limites auxquelles ils peuvent être confrontés. Après, le responsable du service nous laisse avec les autres membres du service pour la suite de la mission. Les autres membres du service mettent à notre disposition toutes les informations et tous les documents demandés. La consultation des documents se fait sur place et les faits constatés sont relevés sur les blocs note, par chaque auditeur.

Une fois ouverte, la phase d'accomplissement se poursuit par des tests de conformité, un test de permanence et enfin l'évaluation du système.

5.1.1.2.1. Tests de conformité

Ils ont pour objet de confirmer que la description des procédures correspond bien aux procédures appliquées dans l'entreprise. Ils permettent alors à l'auditeur de s'assurer de la réalité de l'existence du système ayant fait l'objet de description. Nous avons pu constater que les procédures existent belles et bien, mais elles ne sont pas toujours appliquées de la même

manière que celle décrite dans la documentation de Congo Télécom. Nous avons réalisé quelques tests selon différentes modalités telles que :

- Par des observations directes, comme le décrit la procédure, nous avons regardé si la salle des serveurs et fermée à clé après chaque journée de travail terminée, en regardant aussi si les mises à jours des systèmes et anti-virus sont faites de manière régulière, si toutes les machines sont branchées à des onduleurs, si les machines obsolètes sont belles et bien rangées dans la salle « OMEGA » etc.
- par des confirmations verbales du déroulement des procédures, vérifiées par les personnes qui les mettent en œuvre ;
- et aussi par la vérification de l'existence des matériels et logiciels utilisés.

5.1.1.2.2. Test de permanence

Ce test nous a permis de nous assurer et de voir à quel niveau les opérations sont traitées dans la réalité conformément à ce qui nous a été décrit lors des différents entretiens. Le test de permanence permet de vérifier que les procédures de sécurité telles que décrites dans le manuel de procédures sont effectivement celles qui font l'objet d'une application permanente dans l'entreprise. En d'autres termes, nous pouvons dire que les tests de permanence consistent à s'assurer de l'application permanente de conformité des procédures par les opérationnels.

A cette étape de contrôle interne, il faut chercher les preuves que les contrôles décrits dans le diagramme et les questionnaires de contrôle interne sont réellement appliqués pour l'ensemble de la structure.

5.1.1.2.3. Evaluation du système

L'évaluation du système se fait d'une part par un audit organisationnel et physique et d'autre part par un audit technique.

Dans le 1er cas, il s'agit pour nous de nous intéresser à l'aspect physique et organisationnel de notre organe cible à auditer à savoir le service informatique. Nous nous sommes alors intéressés aux aspects de gestion et d'organisation de la sécurité sur les plans organisationnels, humains et physiques. Il était pour nous question d'avoir une vue globale de l'état de la sécurité et d'identifier les risques potentiels sur le plan organisationnel. Dans la

réalisation de cette étape d'audit, il s'agissait pour nous de suivre une approche méthodologique s'appuyant sur un ensemble de questions. Dans le second cas, une analyse est tirée et elle fait apparaitre les failles et les risques, les conséquences d'intrusions ou de manipulations illicites de données. C'est dans cette phase que s'apprécie l'écart avec les réponses obtenues lors des entretiens ainsi que la robustesse de sécurité, sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

Nous avons remarqué que l'accès aux informations du world wide web a été comme limité dans le fait où les agents ne peuvent se connecter qu'à certains site internet. Par contre, les informaticiens eux ont accès à tout car ce sont eux qui détiennent la clé pour sortir de ce cercle restreint. Les courriers électroniques : c'est ce service de transmission de messages écrits et de documents envoyés électroniquement via internet. Il est géré et dispatché par les serveurs qui eux sont sous la disposition des informaticiens. En cas de non réception d'un mail par un agent, le service informatique s'en charge pour le rétablissement. Pour ce qui est des bases de données, elles sont stockées si non localisées dans un même lieu à savoir les serveurs. Cela constitue pour l'entreprise une faiblesse car en cas de préjudice ces données risqueront d'être perdues. Ce sont elles qui sont au centre des dispositifs informatiques de collecte, mise en forme, stockage, et utilisation des informations. Pour les authentifications et contrôle d'accès, étant donné que chaque poste de travail dispose d'un « login » avec mot de passe, ce sont aussi les serveurs qui gèrent ces informations. L'authentification permet de valider l'authenticité de l'entité en question. Quant aux contrôles d'accès, c'est pour vérifier si une entité (une personne, un ordinateur,…) demandant à accéder à une ressource a les droits nécessaires pour le faire. Congo Télécom ne dispose pas pour ses agents d'éléments biométriques ou de carte autorisant l'accès à une ressource quelconque. Cela constitue une faiblesse pour la sécurité car l'accès est surveillé de manière informelle.

Dans le département de la ville de Brazzaville, Congo Télécom comporte au sein de son service informatique sept (7) agents, dont trois (3) femmes et cinq (4) hommes. L'organisation de la sécurité est ici gérée par le RSSI qui est le responsable de la sécurité en matière de système d'information. Cela constitue ici une force car l'entreprise dispose d'un coordonnateur en matière de sécurité. Dans le plan organisationnel, humain et physique, plusieurs risques sont du fait que les informaticiens manquent de vigilances aigues dans leurs tâches, le nombre d'agents n'étant pas suffisant avec un travail qui s'avère volumineux, les règles et les procédures de travail n'étant pas totalement respectées, et aussi du fait causés par

les utilisateurs. Pour ce qui est des serveurs, seuls les informaticiens ‘’porteront le chapeau’’ en cas d’incident car ils sont les seuls à avoir accès à la salle des serveurs. Comme en toute activité, les humains commettent des erreurs, il peut s’avérer qu’un informaticien arrive donc plus ou moins fréquemment d’exécuter un traitement non souhaité ou d’effacer involontairement des données ou des programmes : c’est ce que l’on appelle le risque de maladresse. D’autres peuvent volontairement mettre en danger le système d’information en introduisant dans les serveurs des virus, ou en introduisant de mauvaises informations dans une base de données. C’est par là qu’on remarque le risque de malveillance. Ce risque peut être représenté comme étant un sabotage, chose qui est heureusement un cas très rare à constater.

Après une série de questions, nous nous sommes rendu compte que les risques rencontrés pouvaient être d’ordre technique ou d’ordre humain. Les serveurs peuvent être attaqués par des programmes malveillants, qui sont des logiciels développés dans le but de nuire aux systèmes informatiques, et on y rencontre principalement des « virus », des « vers » et des « Cheval de Troie ». Nous avons remarqué que les postes de travail de Congo Télécom donnent accès aux clés USB lorsqu’elles sont branchées. Cela constitue une faiblesse pour l’entreprise car il n’y a pas de barrière contre les disques amovibles venant de l’extérieur et cela peut constituer un obstacle à la sécurité de Congo Télécom. Les accidents peuvent aussi être rencontrés, tels que les pannes, les incendies, les dégâts des eaux, etc. le fait que les serveurs se situent au premier niveau réduit la probabilité d’être affecté par ce dernier. Parmi les risques les plus rencontrés y figurent en premier lieu, les erreurs. C’est pourquoi il est interdit à tout agent de consommer de l’alcool pendant les heures de travail afin de réduire ce risque. Que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation des données ou de leurs supports, l’erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisés des données. Comme risque, il existe aussi les techniques d’attaques par messagerie tels que le pourriel encore appelé « Spam » qui sont des messages indésirés, mais aussi l’hameçonnage afin d’obtenir des renseignements personnels dans le but de perpétrer une usurpation d’identité ; les attaques sur le réseau comme le « sniffing » qui est une technique qui consiste à récupérer toutes les informations sur le réseau généralement les mots de passe des applications qui ne chiffrent pas leurs communications, ainsi que la mystification ou « spoofing » qui est une technique qui consiste à prendre l’identité d’une personne ou d’une machine. Un autre point à souligner ici est sur ce qui concerne les attaques sur les mots de passe. Chaque machine avant utilisation

est munie d'un compte avec mot de passe, et les attaques sur les mots de passe sont ces attaques qui consistent à faire des tentatives ou de nombreux essais jusqu'à trouver le bon mot de passe. Les mots de passe peuvent constituer une force lorsqu'ils sont non seulement alpha numérique mais aussi constitués des lettres majuscules avec des caractères allant jusqu'à plus de 8 (huit) lettres. Afin d'imprimer un document depuis un poste quelconque, il y a une gestion d'imprimante qui se fait par le serveur, c'est le partage d'imprimante. Ce partage se fait en réseau interconnecté afin d'imprimer depuis son poste de travail.

Parmi les risques rencontrés, nous pouvons les classer en types de menaces pour l'entreprise. Nous avons :

- Les accidents physiques ;
- la malveillance physique ;
- la carence du personnel ;
- les pannes ;
- les interruptions de fonctionnement réseau ;
- les erreurs de saisie ;
- les erreurs de conception et développement ;
- les copies illicites des logiciels ;
- l'indiscrétion et détournement d'informations ;
- les attaques logiques du réseau :
- les erreurs de transmissions ;

5.1.1.3. Phase de conclusion

Dans cette dernière étape, nous avons remarqué que notre travail d'audit a mis en évidence des faiblesses qui peuvent rendre fragile la sécurité de Congo Télécom. Entre autres, nous avons constaté qu'il y a une absence de stratégie claire de protection contre les attaques virales (anti spam par exemple), venant des messageries électroniques depuis les ordinateurs qui ont un accès à internet. Il existe une absence de politique pour la mise à jour pour l'antivirus et des correctifs de Windows et de plus les machines sont sur Windows XP qui est une version non récente de Microsoft. Nous avons aussi constaté que la porte de la salle des serveurs n'est pas munie d'une sécurité d'authentification automatique mais d'une simple serrure à clé. Les stockages des données se font entièrement dans les serveurs de l'entreprise. Congo Télécom ne stocke pas ses données en ligne à l'étranger comme le font certaines

entreprises. Cela peut aussi constituer une faiblesse dans le cas où tout le bâtiment subissait un coup, la perte des données serait totale.

Nous devons savoir qu'en matière de sécurité, la norme 17799 souligne trois (3) objectifs à savoir la confidentialité, l'intégrité et la disponibilité. Ces objectifs sont regroupés au travers les dix grandes thématiques suivantes :

- La politique de sécurité, pour exprimer l'orientation de la direction à la sécurité de l'information ;
- l'organisation de la sécurité, pour définir les responsabilités du management de la sécurité de l'information au sein de l'entité ;
- la sécurité et les ressources humaines, pour réduire les risques d'origine humaine, de vol ou d'utilisation abusive des infrastructures, notamment par la formation des utilisateurs ;
- la sécurité physique, pour prévenir les accès non autorisés aux locaux ;
- la gestion des opérations et des communications, pour assurer le fonctionnement correct des infrastructures de traitement de l'information, et minimiser les risques portant sur les communications ;
- les contrôles d'accès, pour maitriser les accès au patrimoine informationnel ;
- l'acquisition, le développement et la maintenance des systèmes, pour que la sécurité soit une part intégrante du développement et de la maintenance des systèmes d'information ;
- la gestion des incidents, pour s'assurer d'une bonne gestion des événements liés à la sécurité de l'information ;
- la gestion de la continuité d'activité, pour parer aux interruptions des activités de l'entité et permettre aux processus cruciaux de l'entité de continuer malgré des défaillances majeures ;
- la conformité à la réglementation interne et externe, pour éviter les infractions de nature légale, réglementaire ou contractuelle «pour vérifier la bonne application de la politique de sécurité».

Après constatation des risques, quelques recommandations pour améliorations du système ont été soulignées et proposées. Il s'agissait en premier lieu de l'augmentation du salaire des agents, ainsi qu'avec des primes pour les motiver dans le travail, de renforcer le nombre de personnel et de former les agents pour une meilleur approche en sécurité, de renforcer aussi

la sécurité en ce qui concerne l'accès au sein du service informatique en mettant une porte magnétique qui autorisera l'accès par le biais d'une carte électronique, de disposer et de suivre des fiches techniques ou des manuels de politique de norme et de procédures servant à la planification, à l'organisation au contrôle et à l'évaluation de la direction informatique, etc. Nous remarquons que ces faiblesses sont pour Congo Télécom des générateurs de risques et sont susceptibles de faire perdre à l'entreprise sa qualité de travail, sa rentabilité, la satisfaction de sa clientèle, son positionnement, sa part sur le marché, etc.

Conclusion chapitre 5

Ce chapitre nous a permis de connaitre les différents risques rencontrés au sein de Congo Télécom, d'en connaitre les causes et d'avoir un nouveau regard sur l'audit informatique. Suite à cela, nous proposerons des recommandations et des suggestions pour une meilleure approche que nous allons retrouver dans le chapitre suivant.

Chapitre 6 : RECOMMANDATIONS ET SUGGESTIONS

Après l'analyse de son parc et ayant identifié des insuffisances dans la gestion de la sécurité de Congo Télécom, nous allons formuler à présent des recommandations et des suggestions dans le but de l'améliorer et de la rendre plus efficace.

6.1. Recommandations et suggestions relatives au système d'organisation de l'entreprise

Nous voulons premièrement nous appuyer sur l'organisation de l'entreprise du fait que si l'entreprise possède une organisation excellente, toute la gestion du parc informatique aura une influence positive. Une bonne organisation nécessite un bon management, alors nous suggérons :

- L'établissement des fiches de postes pour tous les agents ;
- que la direction puisse mettre à jour le manuel de procédures qui couvre toutes les branches d'activités, en le diffusant et aussi en le vulgarisant ;
- de veiller aussi à leur documentation correcte, à leur disponibilité et leur mise à jour :
- un recrutement afin de renforcer le personnel particulièrement au service d'audit et contrôle mais aussi au service informatique pour toutes les tâches à accomplir au sein de l'entreprise ;
- que Congo Télécom rende opérationnel son service de la formation afin de disposer d'un personnel de qualité et compétent. Ce service permettra de renforcer les capacités des agents dans le but d'améliorer la qualité de leur prestation. Pour cela, l'entreprise doit affecter à ce service un budget conséquent ;
- la formation à la sécurité puisse être régulière ;
- une nouvelle conception et organisation du service audit et contrôle qui permettra d'améliorer l'efficacité du contrôle afin d'aider et accompagner le personnel dans l'assimilation et le respect des procédures.

Afin d'identifier, d'évaluer, de maitriser, de sensibiliser et de communiquer sur les risques, nous recommandons qu'il soit créé au sein de Congo Télécom la fonction de « Risk manager » car le gestionnaire de risque occupe aujourd'hui une place très importante si non de premier plan auprès des entreprises.

6.2. Recommandations et suggestions relatives au système d'information

Au sein d'une organisation, les systèmes d'information occupent une place très importante. Dans le but d'améliorer son système d'information, nous recommandons à Congo Télécom :

- De sauvegarder leurs données sur la toile auprès des hébergeurs étrangers pour une meilleure sécurité et conservations des informations ;
- mettre au point les outils nécessaires et améliorer le partage des responsabilités pour la politique de sécurité de l'information afin de pouvoir mieux répondre aux exigences de disponibilité et d'intégrité ;
- rappeler si non renforcer l'implication des agents dans les activités de gestion de risque.

6.3. Recommandations et suggestions relatives à la gestion des risques

Nous pensons qu'il est primordial de développer une certaine culture en matière de management des risques afin de mieux appréhender et de mieux cerner les risques liés à la sécurité du parc informatique de Congo Télécom. Pour cela nous suggérons :

- Que les responsables puissent premièrement soutenir cette culture non seulement à travers des discours mais aussi dans des actions quotidiennes ;
- mettre en place une solution de gestion centralisée des mises à jours afin de réduire, minimiser les bugs et les failles de la sécurité et de vérifier que les mises à jours sont bien installées ;
- remplacer les serrures des portes par des serrures automatisées donnant accès au service informatique par une carte d'accès ;
- désactiver ou fermer les services réseaux inutiles et surtout SNMP (Simple Network management Protocol) sur les serveurs ;
- prévoir des matériels de remplacement en cas de panne d'un composant essentiel ;
- assurer un contrôle de la saisie des données où les données sensibles seront autocontrôlées pour assurer la vérification des données saisies ;
- assurer l'intégration d'un outil de vérification d'intégrité pour protéger les données contre les erreurs de manipulations des utilisateurs ;
- se munir d'équipements logiciels spéciaux (IDS) qui permettront de mettre en place des mécanismes de détection d'intrusion ;

- mise en place d'un système de détection d'incendie et vérifier si les extincteurs existants sont toujours utilisables ;
- contrôler les accès et mettre en place des systèmes de détection intrusion pour limiter les actions malveillantes ;
- mise en place de processus cohérents de détection des défauts ;
- mise en place d'une solution Firewall applicatif, Firewall Statefull inspection et Firewall à filtrage de paquets afin de protéger en premier lieu des tentatives d'intrusion interne, en deuxième lieu, l'utilisation d'un firewall applicatif permet de contrôler les connexions depuis et vers ces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants. On peut citer par exemple un Firewall : Mod_security et Mod_Proxy ; afin de contrôler les couches applicatives, sans nécessité de proxy applicatif pour chaque service, en cherchant une session correspondante pour les paquets analysés ; et aussi afin de permettre de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC (Media Accès Control) ;
- bloquer tout accès aux clés USB et autres disques amovibles souvent source de virus afin de réduire le nombre de risque d'infection des machines ;
- installer des caméras dans tout le service informatique pour pouvoir mieux contrôler tout ce qui se passe ;
- un audit régulier en interne par un organisme extérieur agréé.

Conclusion chapitre 6

Au terme de notre étude, portant sur l'audit de la sécurité du parc informatique de Congo Télécom, nous avons fait ressortir des forces et des faiblesses concernant la gestion de sa sécurité et à partir desquelles nous avons pu émettre des suggestions et recommandations visant à réduire les risques qu'ils comportent. Cette étude devrait permettre à l'entreprise d'améliorer les pratiques en matière de sécurité et d'en obtenir une bonne gestion.

Conclusion de la deuxième partie

Au terme de cette deuxième partie de notre travail, nous pouvons dire qu'elle nous a permis de présenter de manière générale la société de téléphonie de l'Etat qui n'est autre que Congo Télécom. Grâce aux informations que nous avons reçues, nous avons identifié les risques liés à la gestion du parc informatique de l'entreprise, et nous nous sommes fait une opinion concernant l'organisation de celle-ci.

Nous avons dégagé quelques forces et faiblesses, analysé les risques puis tiré des recommandations et suggestions. Le cadre pratique de notre étude nous a permis la mise en application de l'approche méthodologique adoptée. Ceci nous a facilité la collecte des données grâce à des outils préalablement définis.

La prise en compte et la mise en œuvre de ces recommandations nécessite l'implication du département informatique ainsi que les organes de direction en vue d'avoir des dispositifs de sécurité rigide.

CONCLUSION GENERALE

Notre travail qui se proposait comme objectif principal d'analyser si non d'évaluer la gestion du parc informatique de Congo Télécom a été atteint. Il a été fait à travers une revue de la littérature que contient une première partie qui nous a permis d'avoir un gros plan sur la sécurité, et de dérouler ses objectifs. La deuxième partie concerne le cadre pratique de notre étude où la réalisation de l'analyse proprement dite a permis de détecter les risques si non failles du système de sécurité de Congo Télécom concernant on parc informatique.

Ainsi, au terme de notre étude, nous pensons atteindre également les objectifs spécifiques assignés à savoir :

- Identifier, analyser et évaluer les risques liés au matériel informatique ;
- définir les risques de patrimoine ;
- définir les éléments pouvant contribuer à la réduction de l'impact du risque ;
- renforcer la capacité du service d'audit ;
- présenter une approche de recommandations, permettant d'améliorer la sécurité du parc informatique.

Le but de cette étude se veut d'apporter des améliorations par rapport à la gestion de la sécurité informatique. L'analyse du dispositif nous a permis de souligner quelques points forts et faibles du système où les points forts constitueront une amélioration continue et les points faibles une attention particulière en tenant compte des recommandations. Ces recommandations sont d'ordre objectif, elles veulent amener les managers à asseoir des outils de travail performants, pour faire preuve de professionnalisme et d'éthique.

ANNEXES

Annexe 1 : **Interview (guide d'entretien)**

Guide d'entretien	
Questions principales	Questions subsidiaires
Comment s'effectue la sécurité des serveurs de Congo Télécom ?	Quelles sont les différentes étapes de la sécurité des serveurs?
	Qui sont les différents intervenants dans le processus?
	Quelles en sont leurs tâches ?
	Quels sont les agents qui ont accès à la salle des serveurs?
	Quelles sont les dispositions prises en cas perte des données?

Source : Nous-même

Annexe 2 : Questionnaire de contrôle interne

QUESTIONNAIRE DE CONTROLE INTERNE	Entité audité : Auditeur : Date : Rubrique : Sécurité	Folio 1/4 Exercice

Objectifs de contrôle :

A. S'assurer que la salle des serveurs est protégée contre les dégâts des eaux.

Questions	N/A	OUI	NON	Commentaires	Réf
1. Existe-t-il un dispositif contre fuites d'eau de pluies ?			X	Les serveurs se trouvant au 1er étage, il ne peut avoir de fuite de pluie	
2. Les tuyaux d'eau sont ils en bon état pour éviter les fuites d'eau ?			X		
3. Existe des mécanismes de coupure automatique en cas de fuite ?			X	Pas encore constaté de fuite au sein du service où se trouvent les serveurs.	

QUESTIONNAIRE DE CONTROLE INTERNE	Entité audité : Auditeur : Date : Rubrique : Sécurité	Folio 2/4 Exercice

Objectifs de contrôle :

B. S'assurer que la salle des serveurs est protégée contre les incendies et les explosions.

Questions	N/A	OUI	NON	Commentaires	Réf
4. Existe-t-il des extincteurs dans le service ?		X			
5. Ces extincteurs sont-ils encore opérationnels ? Fonctionnent-ils ?	X			Ils n'ont pas encore été utilisés depuis leur installation.	
6. Avez-vous des dispositifs contre les baisses et les hausses de tension ?		X			
7. Le stockage des matières inflammables se fait-il avec sûreté et loin du service informatique ?		X			
8. Existe-t-il une mise en place et maintenance de systèmes de détection et d'extinction d'incendie ?			X		

QUESTIONNAIRE DE CONTROLE INTERNE	Entité audité : Auditeur : Date : Rubrique : Sécurité	Folio 3/4 Exercice

Objectifs de contrôle :

C. S'assurer que l'électricité n'est pas une source de danger pour les serveurs

Questions	N/A	OUI	NON	Commentaires	Réf
9. Toutes les machines sont-elles branchées à des onduleurs ?		X			
10. Disposez-vous d'un paratonnerre en cas de foudre ?		X			
11. La qualité des câblages et des connexions est-elle en bon état ?		X			
12. Disposez-vous d'un groupe électrogène automatique en cas de coupure d'électricité ?		X			

QUESTIONNAIRE DE CONTROLE INTERNE	Entité audité : Auditeur : Date : Rubrique : Sécurité	Folio 4/4 Exercice

Objectifs de contrôle :

D. S'assurer que la salle des serveurs est protégée contre les intrusions et la malveillance interne.

Questions	N/A	OUI	NON	Commentaires	Réf
13. L'entrée à la salle des serveurs est-elle conditionnée d'une carte biométrique magnétique ?			X	La porte se ferme avec une serrure à double clé.	
14. Existe-t-il une détection anti-intrusion par des caméras, des alarmes, des détections de coupure de circuit, etc. ?			X		
15. Existe-t-il un contrôle d'accès rigoureux à l'entrée de l'entreprise par le gardiennage ?		X			
16. Existe-t-il un système d'identification des visiteurs à l'entrée ?		X			

BIBLIOGRAPHIE

Ouvrages et articles

1. ANGOT Hugues, FISCHER Christian, THEUNISSEN Baudouin (2004), Audit comptable, Audit informatique, Boeck université, 3ème édition, P.279
2. A.T.H. (1986), JOCELYN Michel, Audit opérationnel : Guide pour l'audit opérationnel et des systèmes d'informations, édition Clet, P.273
3. BARTHELEMY Bernard, COURREGES Philippe (2004), Gestion des risques : méthodes d'optimisation globale, 2ème édition, Edition d'organisation, P. 266
4. BERRADA Moshsin (2012), L'audit interne tout simplement, éditions Afrique challenge, P.139
5. BERTIN Elisabeth (2007), Audit interne : enjeux et pratique à l'international, édition Eyrolles, P.320
6. DERRIEN Yann (1992), Les techniques de l'audit informatique, édition Dunod, Paris, P.238
7. FAUTRAT Michel (2000), De l'audit interne au … management de la maitrise des risques, Revue française de l'audit interne, n°148, pages 24-25
8. FERNANDEZ – TORO Alexandre (2009), Management de la sécurité de l'information Implémentation ISO 27001 : Mise en place d'un SMSI et audit de certification, 2ème édition Eyrolles, P. 101
9. GHERNAOUTI Solange (2008), Sécurité Informatique et Réseaux, 2ème édition, Dunod, Paris, P.341
10. GHERNAOUTI Solange (2013), Sécurité Informatique et Réseaux, 4ème édition, Dunod, Paris, P. 2-7
11. IFACI (1993), Audit et contrôle des systèmes d'informations, module 1 : Management de l'audit et du contrôle interne, IFACI, P.110
12. IFACI (1993), Audit et contrôle des systèmes d'informations, module 2 : Les outils informatiques de l'audit, IFACI, P.129
13. IFACI (1993), Audit et contrôle des systèmes d'informations, module 8 : Sécurité, IFACI, P.126
14. IFACI (2011), Manuel d'audit interne : Améliorer l'efficacité de la gouvernance, du contrôle interne et du management des risques
15. IFACI (2013), Les outils de l'audit interne, Eyrolles éditions, 103 pages

16. LEMANT Olivier (1995), La conduite d'une mission d'audit, Dunod, Paris, 261 pages
17. RAFFEGEAU J. & RITZ A. (1993), Audit et informatique, 2ème édition, Presse de France, Paris
18. RENARD Jacques & CHAPLAIN Jean Michel (2006), Théorie et pratique de l'audit interne, 6ème édition organisation, Paris, 479 pages
19. RENARD Jacques (2009), Théorie et pratique de l'audit interne, 7ème édition, Eyrolles, P.244
20. RENARD Jacques (2009), Théorie et pratique de l'audit interne, 7ème édition, Eyrolles, P.463
21. THORIN Marc (2000), l'audit informatique, édition HERMES Sciences, P.184

WEBOGRAPHIE

22. Club de la sécurité informatique français (2009), Sécurité des salles des serveurs, www.clusif.aso.fr
23. Management de la sécurité de l'information (2013), ISO 27001, http://www.iso.org/iso/fr/home/standards/management-standards/iso27001.htm
24. La sécurité de l'information pour tous (2013), Risques protection traitement, www.cases.lu
25. Communauté d'apprentissage des standards du web (2013), Sécurisation du serveur (SSH, Firewall iptable, fail2ban, etc.), http://www.alsacreations.com/
26. KEMP Tom, Gestion informatique : Faire l'audit des serveurs Windows, https://technet.microsoft.com/fr-fr/magazine/hh848746.aspx (2008)
27. L'association française de l'audit et du conseil informatique (2009), COBIT V4 et Val IT, www.afai.asso.fr
28. Congo Télécom (2015), Nos produits, www.congotelecom.cg