Centre Africain d'Études Supérieures en Gestion

CESAG EXECUTIVE
(CEE)

Master Business Administration
En Audit Et Contrôle de Gestion

(MBA ACG)

Promotion 29
(2017-2018)

Mémoire de fin d'études

THEME :

ELABORATION D'UNE POLITIQUE DE SECURITE D'UN SYSTÈME D'INFORMATION : CAS DU RESEAU INFORMATIQUE DU CESAG

Présenté par :

Sylvère Gaël ALLOU

Dirigé par :

M. Baïdy T. SY
Directeur Général SAYTU SA,
Professeur associé au CESAG

OCTOBRE 2019

DEDICACE

Nous dédions ce mémoire à :

- ✓ L'Éternel tout puissant pour son amour et sa grâce toujours renouvelée ;
- ✓ Notre mère BLY Cécile épouse ALLOU et notre père Yapi Hubert ALLOU pour leur soutien affectif, spirituel et financier inestimable ;
- ✓ Nos frères et sœurs, pour leurs prières et toute la confiance placée en moi ;
- ✓ Nos amis pour leurs conseils avisés.

REMERCIEMENTS

«Ceux qui donnent ne doivent pas se rappeler, mais ceux qui reçoivent ne doivent jamais l'oublier." – Proverbe Africain à l'endroit de Monsieur Abdoul Karim TAHIROU*»*

Nous remercions :

- Pr Serge BAYALA, Directeur Général du CESAG d'avoir accepté que j'écrive sur son établissement;
- M Baidy SY, notre Directeur de mémoire pour son expertise apporté à notre travail mais aussi pour nous avoir donné une première expérience dans le domaine de l'audit;
- Abdoul Karim TAHIROU, Responsable du Service Informatique, mon Maître de stage, pour son dévouement, ses explications et sa disponibilité sans faille tout au long de mon stage et de ce travail.;
- L'ensemble du personnel du Service Informatique ;
- Et tous ceux, qui de près ou de loin, ont contribué à la réalisation de ce travail.

Qu'ils trouvent ici le fruit de la contribution qu'ils m'ont apporté.

LISTE DES SIGLES ET ABREVIATIONS

ANSSI	Agence nationale de la sécurité des systèmes d'information
ARS	Administrateur Réseaux et Systèmes
BCEAO	Banque Centrale des Etats de l'Afrique de l'Ouest
CAMES	Conseil Africain et Malgache pour l'Enseignement Supérieur
CEAO	Communauté Economique de l'Afrique de l'Ouest
CESAG	Centre Africain d'Etudes Supérieures en Gestion
COBIT	Control Objectives for Information and related Technology
DESS	Diplôme d'Etudes Supérieures Spécialisées
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
GSI	Gestion du Système d'Information
IFACI	Institut Français de l'Audit et du Contrôle Internes
ISACA	Information Systems Audit and Control Association
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
ITG	Information Technology Gouvernance Institute
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
LMD	Licence Master Doctorat
MEHARI	Méthode Harmonisée d'Analyse de Risques
MSSI	Management de la Sécurité des Systèmes d'Informations
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PCA	Plans de Continuité d'Activité
PME/PMI	Petites et Moyennes Entreprises/Petites et Moyennes Industries
PS	Politique de Sécurité
PSSI	Politique de Sécurité des Systèmes d'Informations
RSI	Responsable du Service Informatique

RT	Technicien Réseau
SEI	Software Engineering Institute
SI	Système d'Information
SMSI	Système de Management de la Sécurité Informatique
SSI	Sécurité des Systèmes d'Information
UEMOA	Union Economique et Monétaire Ouest Africaine
USA	United States of America

LISTE DES FIGURES ET TABLEAUX

Figure 1 : Critères de sécurité 14
Figure 2 : Schéma de pilotage de la sécurité des SI 17
Figure 3 : De la politique d'entreprise à la politique de sécurité 19
Figure 4 : Les 37 processus de COBIT 5 22
Figure 5 : Démarche de la méthode MEHARI 23
Figure 6 : Démarche globale de EBIOS 24
Figure 7 : Schéma de la démarche OCTAVE 25
Figure 8 : Démarche de l'élaboration de la PS 30
Figure 9 : Objectifs d'une PS 32
Figure 10 : Modèle d'analyse 38
Figure 12 : Architecture LAN du réseau 51

Tableau 1 : Rôle du Système d'Information 11
Tableau 2 : Risques généraux liés au SI 53
Tableau 3 : Risques liés au réseau 54
Tableau 4 : Résultat du diagnostique 57
Tableau 5 : Identification des acteurs avec leurs rôles et responsabilité 61
Tableau 6: Règles de sécurité 64

LISTE DES ANNEXES

Annexe 1 : Inventaire du matériel informatique 77
Annexe 2 : Inventaire des logiciels 78
Annexe 3: Identification des acteurs basé sur COBIT 5 78
Annexe 4: Organigramme fonctionnel du CESAG 79
Annexe 5 : Guide d'entretien 80
Annexe 6: Questionnaire d'entretien des rôles et responsabilités dans le MSSI 82
Annexe 7: Questionnaire d'entretien du contrôle interne des SI 83

SOMMAIRE

DEDICACE……ii
REMERCIEMENTS iii
LISTE DES SIGLES ET ABREVIATIONS iv
LISTE DES FIGURES ET TABLEAUX vi
LISTE DES ANNEXES vi
SOMMAIRE vii
INTRODUCTION GENERALE 1
PREMIERE PARTIE : 6
REVUE DE LITTERATURE ET METHODLOGIE DE L'ETUDE 6
CHAPITRE 1 : POLITIQUE DE SECURITE D'UN SYSTEME D'INFORMATION 8
1.1. Enjeux de la sécurité du système d'information au sein d'une entreprise 9
1.2. Politique de sécurité 18
1.3. Normes, méthodes et bonnes pratiques 19
CHAPITRE 2 : METHODOLOGIE ET CADRE DE L'ETUDE 26
2.1. Méthodologie de l'élaboration d'une PS 27
2.2. Présentation du CESAG 39
DEUXIEME PARTIE : 45
CADRE PRATIQUE DE L'ELABORATION DE LA POLITIQUE DE SECURITE 45
CHAPITRE 3 : DESCRIPTION DE L'EXISTANT 47
3.1. Description du réseau informatique 48
3.2. Administration du réseau informatique 52
3.3. Menaces liées à la sécurité 53
3.4. Gestion de la sécurité du réseau informatique 55
CHAPITRE 4 : ELABORATION DE LA PS 59
4.1. Objectif 60
4.2. Périmètre 60
4.3. Rôles et responsabilité 61
4.4. Règles générales de sécurité 62
4.5. Règles de sécurité 64
4.6. Revue de la politique 72
CONCLUSION GENERALE 74
ANNEXE 76
BIBLIOGRAPHIE 84
TABLE DES MATIERES 86

INTRODUCTION GENERALE

L'informatique est devenue pour l'entreprise un outil incontournable de gestion, d'organisation, de production et de communication. L'alignement du système d'information à la stratégie de l'organisation, l'obsolescence frénétique des systèmes d'information, la dépendance à l'informatique, la cybersécurité, plus spécifiquement la sécurité du réseau locale d'entreprise sont des sujets de plus en plus complexes à appréhender. Et posent donc de vrais problèmes pour les entreprises qui ne peuvent mobiliser que peu de ressources internes pour maintenir et protéger leur système d'information. Le vol ou la destruction de données, le déni de service, l'espionnage industriel, les dommages volontaires et involontaires causés par les acteurs internes à l'entreprise sont autant d'attaques et de dangers dont les entités sont victimes et dont les conséquences peuvent être dramatiques. Les attaques de ransomware paralysant une quarantaine d'hôpitaux britanniques en Mai 2017, suivi d'une vague d'attaque dans plusieurs pays du monde et plus récemment en Mars 2018 celles de la mairie d'Atlanta, du service des urgences de la ville de Baltimore et du géant Boeing de l'aéronautique aux USA en sont des exemples palpables. Il est donc impératif que les dirigeants ainsi que les utilisateurs comprennent les enjeux liés à la vulnérabilité de leur système informatique afin que les mesures de mitigations de ces risques soient beaucoup plus efficaces.

Ainsi, toutes les entreprises internationales comme nationale ne sont pas à l'abri de ce genre de menaces. Les entreprises africaines de façon générale et celles de l'espace UEMOA sont encore plus exposées du fait que, pour le commun du mortel, ces menaces ne concernent que les grands groupes. Aussi, force est de constater que, seules quelques entreprises disposent de procédures formelles et adaptées à la sécurité de leur système d'information.

Le CESAG comme beaucoup d'autres entreprises, qui se veut une institution aux standards internationaux se doit de disposer d'un système d'information performant. Celui-ci doit répondre aux normes de sécurité préconisées par les référentiels mondialement reconnus à l'image de COBIT 5ou encore la série des normes ISO/IEC 27000. Ainsi, selon ces standards, le management des risques lié au système informatique commence par la mise en place d'une politique de sécurité du système d'information. C'est pourquoi, dans la plupart des missions d'audit informatique basées sur la sécurité réseau informatique, la politique de sécurité ou la charte informatique fait partie des documents demandés par les auditeurs IT. Or, Il se trouve que ce document n'est pas encore disponible pour les acteurs du système d'information du CESAG.

Plusieurs causes peuvent être à la base de cette insuffisance dans la formalisation des processus de management des risques informatiques du CESAG, à savoir :

- la non-implication des différents acteurs dans la gestion leur système d'information ;
- la non-implication des dirigeants dans la gouvernance du système d'information ;
- l'absence de la culture de sécurité informatique ;
- l'absence d'audit IT pour révéler les risques auxquels est exposé le SI ;
- l'absence de cartographie des risques informatiques pour mesurer la criticité des risques encourus ;
- le sentiment de ne pas être concerné par les menaces liées à la cybersécurité.

De ces causes, nous pouvons avoir les conséquences suivantes :

- la perte ou divulgation des données pédagogique et administratives ;
- la perte financière ;
- la perte de crédibilité ;
- l'indisponibilité du réseau ;
- l'atteinte à l'image.

Pour pallier ces conséquences, nous proposons les solutions suivantes :

- recruter un IT manager au sein du service informatique ;
- former l'auditeur interne à l'audit des SI
- élaborer une cartographie des risques du SI ;
- diligenter des missions d'audit informatique axées sur la sécurité du réseau informatique ;
- rédiger une politique de sécurité pour piloter le management de la sécurité du SI

Bien que nous ayons une panoplie de solutions, il convient de retenir la solution la plus adaptée au contexte. Mieux encore, trouver la solution la plus urgente est essentiel pour l'atteinte des objectifs. En nous appuyant sur cette argumentation, il en ressort que la dernière solution, à savoir, rédiger une politique de la sécurité du SI est la solution que nous retenons. Pour nous, la rédaction d'une politique de la sécurité informatique permettra de mettre en œuvre des mécanismes de surveillance des accès. Cela permettra également de sensibiliser les utilisateurs du réseau aux bonnes pratiques de l'informatique. Ensuite les responsabiliser quant à

l'utilisation qu'ils font des outils mis à leur disposition ainsi que le partage d'éventuelles données sensibles sur des réseaux externes à celui du CESAG.

La politique de sécurité étant un document fondamental dans la gestion de la sécurité d'un réseau informatique, la question suivante retient notre attention : « quel contenu pouvons-nous donner à la politique de sécurité du SI du CESAG pouvant garantir raisonnablement la maitrise des risques auxquels son réseau informatique est exposé ? ». Cela nous emmène à répondre aux questions spécifiques suivantes :

- Comment est menée jusque-là, la politique de sécurité du réseau informatique ?
- Cette politique est-elle pilotée par la Direction Générale ?
- En quoi la mise en place d'une politique de sécurité du réseau informatique est-elle importante pour le service informatique ?
- Quelle est la structure d'une politique de sécurité ?
- Sur quel référentiel sera basée la politique de sécurité ?

« Elaboration d'une politique de sécurité d'un système d'information : cas du réseau informatique du CESAG » se justifie comme thème d'autant plus qu'il constituera le premier rideau de sécurité. Ainsi, la réponse à ces différentes questions permettra d'élaborer un manuel qui à son tour assurera une maitrise raisonnable des risques de sécurité.

Notre objectif principal est de doter le Service Informatique du CESAG d'un outil dont le contenu lui permettra d'assurer une maitrise raisonnable des risques auxquels son réseau informatique est exposé.

Outre cet objectif, nous avions des objectifs sous-jacents suivants :

- renforcer la formalisation des processus du Service Informatique ;
- faciliter la sensibilisation de l'ensemble des utilisateurs aux risques liés à la sécurité du réseau ;
- se conformer aux normes et réglementations en termes de sécurité du réseau ;
- mieux maitriser les risques de sécurité à travers l'implication de tous les acteurs ;
- proposer des axes d'amélioration du dispositif de gestion des risques de sécurité.

La rédaction de ce manuel se limitera principalement au réseau local du CESAG. Il s'agira ici d'élaborer un référentiel portant sur la politique de sécurité devant être adopté pour l'ensemble

des utilisateurs, des applications, les ordinateurs, des données et des interactions pilotées par le serveur central en :

- identifiant les besoins en termes de sécurité et les risques informatiques ;
- élaborant des règles et des démarches à mettre en œuvre par l'ensemble des usagers ;
- définissant des processus à déclencher et des personnes à contacter en cas de menace.

Cette étude revêt des intérêts à plusieurs niveaux. Pour le Service Informatique du CESAG, elle lui permettra de disposer d'un outil visant à formaliser son management des risques IT conformément aux normes applicables. Sur le plan académique, il constituera une base documentaire pour les étudiants qui travailleront sur les bonnes pratiques pour la sécurité d'un système informatique plus précisément celui d'un réseau informatique. Outre ces intérêts, cette étude permettra également de mettre en application les connaissances théoriques acquises en classe et de mettre ainsi en lumière notre savoir-être et notre savoir-faire.

Ce travail comporte deux parties. La première partie sera axée sur la revue de la littérature et la méthodologie de l'étude. La deuxième partie quant à elle sera consacrée au cadre pratique. Il sera question de faire la description de l'existant et de concevoir la politique de sécurité du réseau informatique du CESAG.

PREMIERE PARTIE :

REVUE DE LITTERATURE ET METHODLOGIE DE L'ETUDE

Introduction de la première partie

L'adoption de bonnes pratiques dans le domaine de la sécurité des systèmes d'informations (SI) passe par un système de management de la sécurité des systèmes d'informations (SMSSI) qui inclut une politique de sécurité du système d'information (PSSI). La mise en œuvre de ces bonnes pratiques augmente la fiabilité du SI et la confiance essentielle des parties prenantes de l'organisation. Pour se faire, une gestion quotidienne de la sécurité du SI s'impose. L'administration de la sécurité au quotidien est la traduction de la politique de sécurité du SI en politiques opérationnelles spécifiques aux différents composants du SI (Vidal et al., 2009). Pour mieux cerner la notion de politique de sécurité (PS), nous jugeons essentiel d'aborder les différents aspects auxquels la PS fait appel.

Ainsi, dans cette première partie constituée de deux chapitres, nous aborderons dans le chapitre 1 les enjeux de la sécurité des SI, les objectifs d'une politique de sécurité et les normes, méthodes et bonnes pratiques. Dans le deuxième chapitre, nous nous consacrerons à la méthodologie et au cadre de l'étude. Il s'agira ici de nous appesantir sur la démarche de l'élaboration d'une PSSI en général. De façon spécifique, nous aborderons également la démarche de l'élaboration une politique de sécurité d'un réseau informatique. Outre cela, nous présenterons l'entité dans laquelle nous avions effectué notre stage, objet de cette étude.

CHAPITRE 1 : POLITIQUE DE SECURITE D'UN SYSTEME D'INFORMATION

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien. La politique de sécurité est de facto le premier élément du management de la sécurité des systèmes d'information (MSSI) au sein d'une organisation. Elle garantit une approche globale, homogène et hiérarchisée de la sécurité du SI. L'idée dans ce chapitre est de nous interroger sur les enjeux de la sécurité du SI au sein d'une entreprise. Pour ce faire, nous procéderons dans un premier temps à la définition du SI, puis à celle de la sécurité informatique. Nous répondrons ensuite aux questions ci-dessous :

- pourquoi la sécurité des SI ?
- comment doit être mené le management de la sécurité des SI ?

Nous poursuivrons avec les objectifs d'une politique de sécurité d'un SI et finirons par les normes, les méthodes et bonnes pratiques.

1.1. Enjeux de la sécurité du système d'information au sein d'une entreprise

Le système d'information d'une entreprise est un patrimoine essentiel qu'il convient de protéger. La sécurité ne doit pas être perçue comme une contrainte car elle donne de la cohérence à la gestion et permet d'adopter vis-à-vis des risques et des menaces une attitude préventive et proactive, et pas seulement réactive.

1.1.1. Définition du système d'information

R. REIX (Systèmes d'information et management des organisations, 1998, p409) définit un système d'information comme étant « un ensemble organisé de ressources : matériel, logiciel, personnel, données, procédures permettant d'acquérir, de traiter, stocker, communiquer des informations (sous forme de données, textes, images, sons, etc.) dans des organisations ». Cette définition nous permet de considérer qu'un système d'information est un ensemble finalisé, construit à partir de différentes ressources et susceptibles d'être défini à différents niveaux.

R. REIX & F. ROWE (Faire la recherche en système d'information : de l'histoire au concept, 2002, p366) affirment qu' « un système d'information est un système d'acteurs sociaux qui mémorise et transforme des représentations via des technologies de l'information et des modes opératoires ». Dans cette définition, le système d'information aide l'acteur à former des représentations et qu'en fait le système ne peut le faire sans l'acteur, le système interface-acteur est le véritable générateur de l'information.

Jacques THEVENOT (Master Systèmes d'Informations, 2011, p536) : un système d'information est un « Ensemble des moyens, des modèles et des méthodes, destinés à assurer dans une organisation, le stockage, le traitement et la circulation des données, informations et connaissances dans le but d'aider à prendre des décisions ». Il ressort de cette définition que le SI un est outil de pilotage des activités de l'entreprise et d'aide à la prise de décisions.

Marc BIDAN (Le système d'information de gestion en question, 2013, p144) affirme qu'un SI est un réseau complexe de relations structurées où interviennent hommes, machines et procédures qui a pour but d'engendrer des flux ordonnés d'informations pertinentes provenant de différentes sources et destinées à servir de base aux décisions.

Jacques SORNET, Hengoat OONA, Nathalie LE GALLO (DCG 8, Systèmes d'information de gestion - Manuel et applications, 2016, p456) : Le système d'information peut se définir par son objectif, qui est d'assurer la saisie, la conservation, le traitement et la circulation des informations, de façon que chacun, dans l'organisation, puisse disposer au bon moment des données dont il a besoin pour remplir sa tâche. Pour eux, le système d'information répond aux besoins courants, aide aux prises de décision et à la préparation de l'avenir (veille informationnelle, gestion des connaissances).

De toutes ces définitions, nous retenons que le SI est un ensemble complexe de relations structurées où interviennent hommes (personnel), machines (ordinateurs), logiciels et procédures dans le but de faciliter les activités de l'entreprises et de fournir des informations pertinentes d'aide à la prise de décisions.

1.1.2. Rôle du système d'information

Le tableau ci-dessous résume l'importance du SI au sein d'une organisation :

Tableau 1 : Rôle du Système d'Information

	Rôle du Système d'Information	Exemple d'application
Système d'information opérationnel	Collecter, mémoriser, traiter les données nécessaires à la conduite de l'activité Automatiser, fluidifier et optimiser les processus	Achats, stocks, logistique Gestion de production, gestion des données techniques Comptabilité générale et analytique Trésorerie, suivi des investissements Gestion des commandes, suivi des ventes Paie et gestion des ressources humaines Service après-vente, maintenance Workflow
Système d'information d'aide à la décision	Fournir des indicateurs pertinents sur l'activité Connaître les clients, offrir des outils d'analyse et de simulation Gérer la connaissance	Budget, tableau de bord des activités reporting, simulation Analyse du profil client ; datamining logiciels experts (scoring) et statistiques (segmentation) Bases de données de connaissance communautés virtuelles
Système d'information de communication	Communiquer les informations en interne Echanger avec les partenaires (clients, fournisseurs etc.) Gérer des Systèmes d'informations à l'échelle mondiale	Messagerie, réseau d'échange interne (workflow, intranet, groupware, portails d'entreprises, gestion de la connaissance). Echanges normalisés (EDI) : réseaux d'échanges avec les clients et les fournisseurs (supply chain, extranet. plateformes de commerce électronique). sites Web Systèmes opérationnels distribués, disponibles 7j/7, 24 h/24 Pratique de l'offshore développements et maintenance délocalisée Business Process Outsourcing

1.1.3. Sécurité des systèmes des systèmes d'information : qu'est-ce que c'est ?

MENTHONNEX (1995 :74) la sécurité d'un SI est l'ensemble des moyens techniques ou non, de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des équipements et /ou des données traitées ou transmises et des services connexes offerts ou rendus accessibles par le système. : L'on déduit de cette définition qu'il s'agit d'un ensemble de facteurs, qui assurent pour le système d'information, une assurance de Disponibilité, d'Intégrité et de Confidentialité.

Pour Rodolphe ORTALO dans sa Thèse (Évaluation quantitative de la sécurité des systèmes d'information, 1988, p193) : Assurer la sécurité d'un système consiste à garantir le maintien d'un certain nombre de propriétés de sécurité définissant les caractéristiques de confidentialité, d'intégrité et de disponibilité qui doivent être maintenues dans le système. Ceci implique d'empêcher la réalisation d'opérations illégitimes contribuant à mettre à défaut ces propriétés, mais aussi de garantir la possibilité de réaliser des opérations légitimes dans le système.

ISO 27002 (2005 : 14) : 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 une entreprises pour préserver : la confidentialité, l'intégrité et la disponibilité de l'information que détient l'entreprise quel que soit le support (papiers, électronique etc…). Il ressort de cette définition que la sécurité de l'information est l'ensemble des mesures prises pour faire face aux risques auxquels le système est confronté.

Jacques THEVENOT (Master Systèmes d'Informations, 2011, p536) : la sécurité d'un système d'information peut être définie comme l'ensemble des moyens techniques, organisationnels, juridiques et humains à mettre en œuvre pour protéger le SI contre les menaces auxquelles il est soumis. Pour l'auteur, la sécurité du SI doit-être abordée selon une approche globale sur la maitrise des risques, l'implication du personnel et des partenaires sur le périmètre des activités de l'organisation.

Solange GHERNAOUTI (Cybersécurité, Sécurité informatique et réseaux, 2016, p384) : La notion de sécurité fait référence à la propriété d'un système, qui s'exprime généralement en termes de disponibilité (D), d'intégrité (I) et de confidentialité (C). Ces critères de base (dits critères DIC) sont des objectifs de sécurité que la mise en œuvre de fonctions de sécurité permet d'atteindre.

De l'ensemble de ces définitions, nous pouvons ajouter que la sécurité du SI est l'ensemble de mesures (techniques, procédures, juridiques et humains) prises pour garantir la Disponibilité, l'Intégrité et la Confidentialité du SI.

Ainsi, la sécurité d'un SI peut être vue comme sa non-vulnérabilité aux menaces auxquelles il est soumis, c'est-à-dire l'impossibilité que des attaques induisent des conséquences graves sur l'état du SI ou sur son fonctionnement. Pour ce faire, trois principaux critères ont été définis qui sont aussi, depuis plus de vingt ans les piliers de la sécurité de l'information (McLeod et Schell, 2008) : il s'agit de la confidentialité, l'intégrité et la disponibilité. Ces critères connus sous l'acronyme anglais de CIA pour Confidentiality Integrity Availability (en français DIC pour Disponibilité Intégrité et Confidentialité) sont d'ailleurs formellement définis par la norme ISO/IEC 13335-1.

Nous définissons ces critères de base comme suit :

- Confidentialité (confidentiality) : l'information ne doit être divulguée à toute personne, entité ou processus non autorisé. En d'autres termes, la confidentialité garantit qu'une donnée n'est accessible qu'aux seuls utilisateurs autorisés ;

- Intégrité (integrity) : le caractère correct et complet des actifs doit être préservé. En d'autres termes, l'intégrité garantit qu'une donnée n'a subi aucune altération ou destruction, volontaire ou accidentelle, depuis sa création et conserve un format permettant son utilisation. L'intégrité des données comprend généralement quatre aspects l'intégralité, la précision, l'exactitude, l'authenticité et la validité.

- Disponibilité (availability) : l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. En d'autres termes, la disponibilité garantit qu'une ressource du SI est accessible aux utilisateurs autorisés au moment voulu.

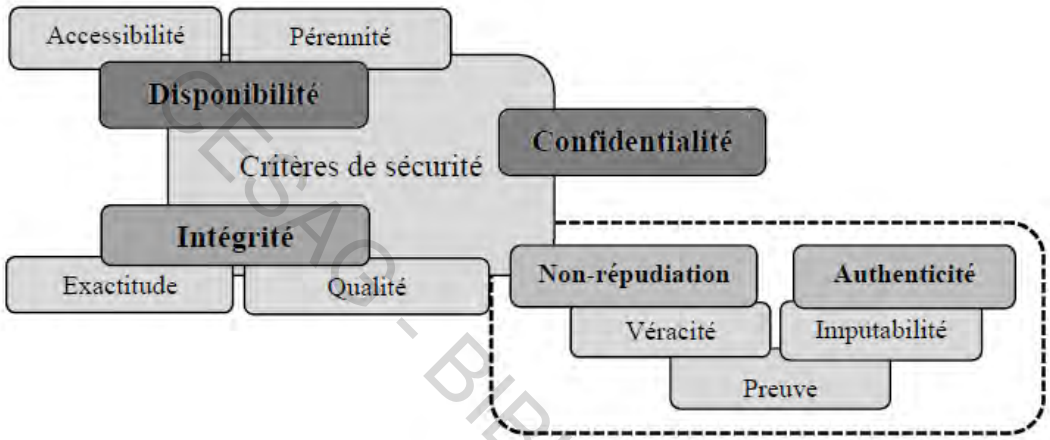
A ces trois critères de sécurité de base, nous pouvons ajouter les objectifs ou critères complémentaires suivants :

- Authentification (authentification) : elle consiste à vérifier l'identité d'une entité (utilisateur ou machine) afin d'autoriser son accès à une ressource (système, réseau, application) ;

- Non-répudiation (non repudiation) : elle assure qu'un échange électronique ne peut être remis en cause par l'une des parties, notamment par l'utilisation du certificat numérique ;

- Imputabilité (accountability) conjuguant authentification et non-répudiation, elle permet de faire porter la responsabilité d'une action à un utilisateur. Ce critère prend une place grandissante avec l'expansion du commerce électronique, notamment avec la signature électronique ;
- Traçabilité (traceability) : elle garantit que les accès et tentatives d'accès aux ressources du SI sont tracés, que ces traces sont conservées et exploitables.

Figure 1 : Critères de sécurité



Source : GHERNAOUTI (2013 : 2)

1.1.4. Pourquoi la sécurité des SI ?

Intrusions, vols d'informations, déni de service, attaque virale, chantage au cryptage de données… la liste des cybermenaces semble s'allonger sans fin ces dernières années. Ainsi, pour une entreprise connectée à internet, le problème n'est pas de savoir si on va se faire attaquer mais quand cela va arriver.

En plus de ces raisons, d'autres raisons peuvent inciter une gestion accrue de la sécurité du SI telles que :

1.1.4.1. Enjeux stratégiques

On dit le plus souvent que l'information c'est le pouvoir. On ne peut décider sans avoir l'information à temps. Pour une entreprise, les dirigeants doivent s'appuyer sur un certain nombre d'indicateurs issus du système d'information pour les analyser (la finesse et la pertinence de ces indicateurs est primordiale), examiner les solutions possibles aux problèmes identifiés, choisir en envisageant les conséquences de chaque solution, et enfin décider d'une

solution. Pour se faire, le SI doit répondre aux critères de sécurité évoqués plus haut. Pour une meilleure gouvernance des risques, il est essentiel que la sécurité du SI s'aligne sur la stratégie générale de l'entreprise, au même titre que le marketing, la finance ou encore la R&D. Outre cela, ce qui a toujours permis aux entreprises les plus compétitives de nos jours d'atteindre leurs objectifs et ainsi de l'emporter sur leurs rivales (avantage concurrentiel) est bien leur SI qui devient dès lors un outil précieux, irremplaçable, en un mot vital.

Ainsi, la direction générale et le conseil d'administration doivent s'imprégner puis accompagner le pilotage des risques informatiques, la mise en place de la politique sécurité du système d'information et les plans d'actions associés, du management de la sécurité de leur SI dans sa globalité.

1.1.4.2. Enjeux organisationnels

Pour une entreprise comme Air France, le système de réservation Amadeus est considéré comme l'actif le plus crucial de l'organisation, bien plus que les avions. C'est ce qu'explique Michel Volle dans son livre e-commerce paru en 2000 aux éditions Economica. A travers cet exemple, l'on comprend combien de fois le système est incontournable pour l'animation des activités. Par conséquent, pour la compétitivité et la survie d'une entreprise.

1.1.5. Le management de la sécurité d'un SI

Le management de la sécurité s'intègre généralement dans un dispositif de gouvernance de la sécurité. Piloté par l'organe en charge de la sécurité. Ce facteur rend obligatoire une pluridisciplinarité de cet organe :

- la formalisation et le suivi de la mise en application de la Politique de Sécurité
- les relations avec les acteurs métiers, l'analyse de leurs risques et l'assistance sécurité pour leurs projets de SI
- la gestion du PCA (Plan de Continuité d'Activité)
- les opérations de sensibilisation et de communication
- le pilotages stratégique et budgétaire des plans d'actions sécurité
- la mise en conformité avec les exigences légales

Mettre en place une organisation de gestion de la sécurité permet de structurer une démarche méthodologique de maintien du niveau de sécurité souvent laissée jusqu'alors à l'état d'ébauche.

Le management de la sécurité s'organise autour de quatre missions majeures :

- Etudes et standards de sécurité

L'objectif principal ici, consiste à rédiger la politique de sécurité ou le Plan de Continuité d'Activité (PCA), puis à les décliner dans les processus opérationnels. Cela permet de transformer les concepts et les directives en réalisations concrètes sur le système d'information. Cette fonction couvre à la fois les impératifs de prévention et défense.

- Contrôle de la sécurité

Il regroupe l'ensemble des actions permettant de mesurer le niveau de sécurité de tout ou partie du système d'information : identifications objective et exhaustive des menaces, évaluation de l'efficacité des mesures de protection, suivi des procédures correctrices (mise en conformité). Il répond ainsi à l'objectif de maitrise des risques.

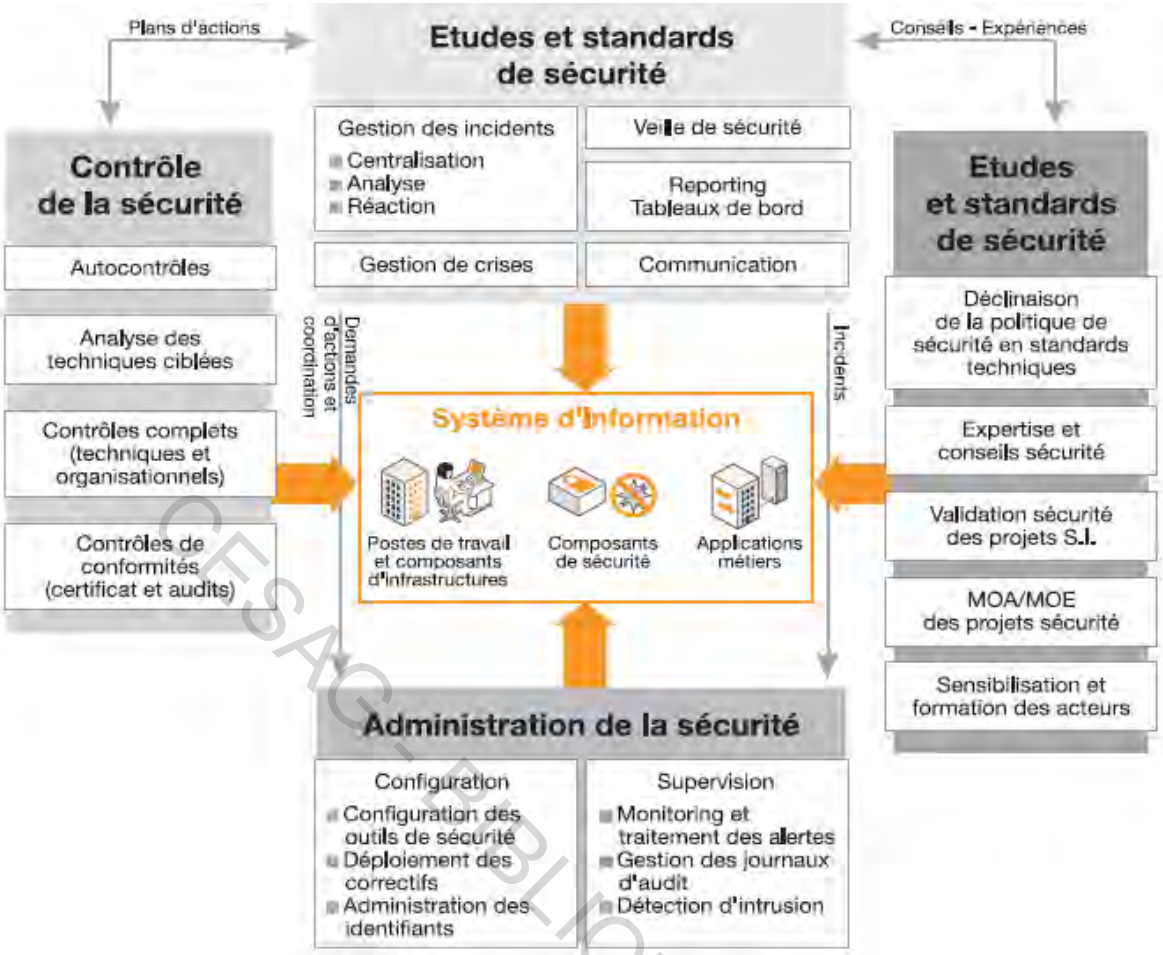
- Administration de la sécurité

Cette fonction englobe des actions qui visent la mise en œuvre, la surveillance et l'application des règles de sécurité aux systèmes d'information. Elle couvre les aspects techniques des objectifs de prévention, de défense et de détection. Ainsi les actions de configuration permettent de maintenir les composants du système d'information à un niveau optimal de sécurité. Les actions de supervision permettent quant à elles de détecter tout événement anormal identifié et d'initier les actions correctrices.

- Pilotage de la sécurité

Cette fonction couvre tous les objectifs de sécurité et joue un rôle central dans le dispositif de management de la sécurité. Elle représente la tour de contrôle en termes de coordination et d'homogénéité des actions de sécurité au quotidien, de manière proactive et réactive (veille de sécurité, solutions réactives). Elle permet de suivre le niveau de sécurité interne et externe (reporting, tableaux de bords) et d'apporter des réponses efficaces aux nouvelles menaces (gestion de crises).

Figure 2 : Schéma de pilotage de la sécurité des SI



Source : Orange Business Services, 2007

Ces différentes fonctions s'exercent sur l'ensemble des composantes du SI et chacune d'elle a un rôle crucial dans la gestion de la sécurité du SI. Cependant, nous analyserons de plus près la première fonction qui consiste à définir une politique de sécurité.

1.2. Politique de sécurité

On ne peut concevoir de sécurité durable sans s'être doté d'un guide de gouvernance et de gestion efficace de la sécurité de son SI.

1.2.1. Définitions

La première étape de sécurisation des systèmes d'information consiste à définir une politique de sécurité comme illustrée ci-dessus. Celle-ci est constituée de règles permettant de s'assurer que des propriétés de sécurité s'appliquent sur les données du système étudié.
Dans les Critères d'évaluation de la sécurité des systèmes informatiques (ITSEC, 1991, p166), la politique de sécurité "est l'ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique".

Jacques SORNET, Hengoat OONA, Nathalie LE GALLO (DCG 8, Systèmes d'information de gestion - Manuel et applications, 2016, p456) : Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Une politique de sécurité concrétise une stratégie sécuritaire et est un outil indispensable à la gouvernance de la sécurité. Elle spécifie les moyens (ressources, procédures, outils, etc.) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité. La politique de sécurité fait le lien entre la stratégie de sécurité de l'entreprise et la réalisation opérationnelle de la sécurité. L'on déduit qu'une politique de sécurité est une vision stratégique de la maitrise des risques.
La politique de sécurité des systèmes d'information (PSSI) est un plan d'actions définies pour maintenir un certain niveau de sécurité. Elle reflète la vision stratégique de la direction de l'organisme (PME/PMI, industrie, administration, État, unions d'États…) en matière de sécurité des systèmes d'information (SSI).
Au regard de ces définitions, il ressort qu'une politique de sécurité est le premier maillon de sécurisation du SI. C'est pourquoi, la direction doit s'approprier et s'impliquer dans l'élaboration de ce manuel.

1.2.2. Objectifs

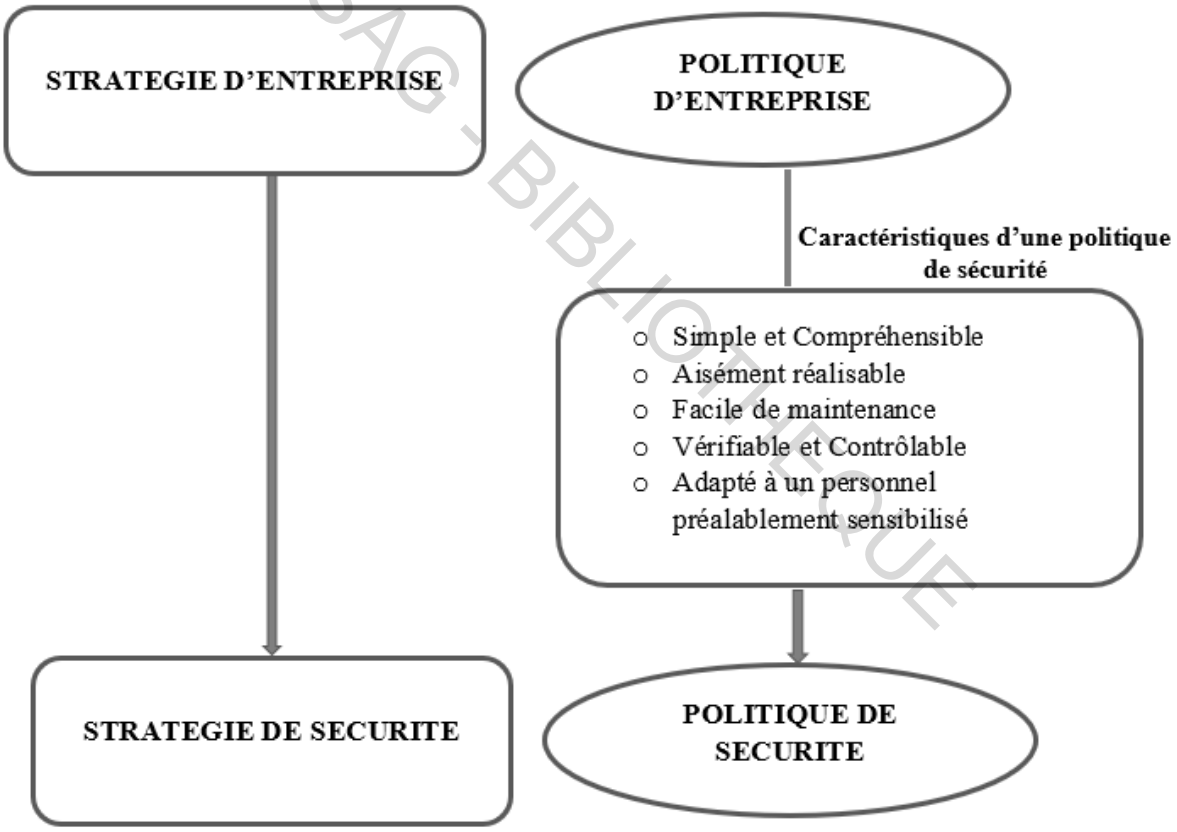
La Politique de Sécurité exprime la stratégie de l'entreprise en matière de sécurité de l'information. Elle constitue la référence en matière de protection des Systèmes d'Information et traduit les exigences de sécurité en règles pragmatiques. Celles-ci permettront de choisir les

dispositifs de protection adaptés. Ainsi, la mise en œuvre d'une politique de sécurité permettra principalement de :

- adopter une politique de gestion de risques et de sécurité ;
- créer une structure en charge d'organiser et de piloter la gestion de la sécurité des SI
- installer un cadre organisationnel et juridique nécessaire à la responsabilisation collective et individuelle des utilisateurs du SI
- inventorier et classifier les ressources. Cette démarche doit permettre d'optimiser les processus de sécurisation en insistant sur ses composants les plus critiques

Ces objectifs sont en corrélation avec les autres fonctions du management de la sécurité.

Figure 3 : De la politique d'entreprise à la politique de sécurité



Source : Nous même

1.3. Normes, méthodes et bonnes pratiques

Il existe plusieurs normes et référentiels de bonnes pratiques qui permettent aux organisations de disposer d'un ensemble de procédures et de règles afin d'assurer une meilleure sécurité de leur actif informationnel. Ils constituent donc, des guides méthodologiques, des moyens pour

la gestion efficace de la sécurité. Ils servent également d'arsenal pour les professionnels de la sécurité des SI.

1.3.1. ISO/IEC 27001

La norme ISO/IEC 27001 publié en novembre 2005, puis révisée en 2013 décrit la politique du management de la sécurité du système d'information au sein d'une organisation. Elle comprend quatre domaines de processus dont :

- définir une politique de la sécurité des informations ;
- gérer les risques identifiés ;
- choisir et mettre en œuvre les contrôles ;
- préparer un SOA (Statement Of Applicability).

Elle spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte propre d'une organisation. Elle comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation.

1.3.2. ISO/IEC 27002

La norme ISO/CEI 27002 est composée de onze sections principales, qui couvrent le management de la sécurité aussi bien dans ses aspects stratégiques que dans ses aspects opérationnels. Chaque section constitue un chapitre de la norme :

- Chapitre 1 : Politique de sécurité ;
- Chapitre 2 : Organisation de la sécurité de l'information ;
- Chapitre 3 : Gestion des biens ;
- Chapitre 4 : Sécurité liée aux ressources humaines ;
- Chapitre 5 : Sécurité physique et environnementale ;
- Chapitre 6 : Gestion des communications et de l'exploitation ;
- Chapitre 7 : Contrôle d'accès ;
- Chapitre 8 : Acquisition, développement et maintenance des systèmes d'information ;
- Chapitre 9 : Gestion des incidents liés à la sécurité de l'information ;

- Chapitre 10 : Gestion de la continuité d'activité
- Chapitre 11 : Conformité légale et réglementaire.

De façon schématique, la démarche de sécurisation du système d'information selon la norme ISO/CEI 27002 passe par quatre étapes à savoir :

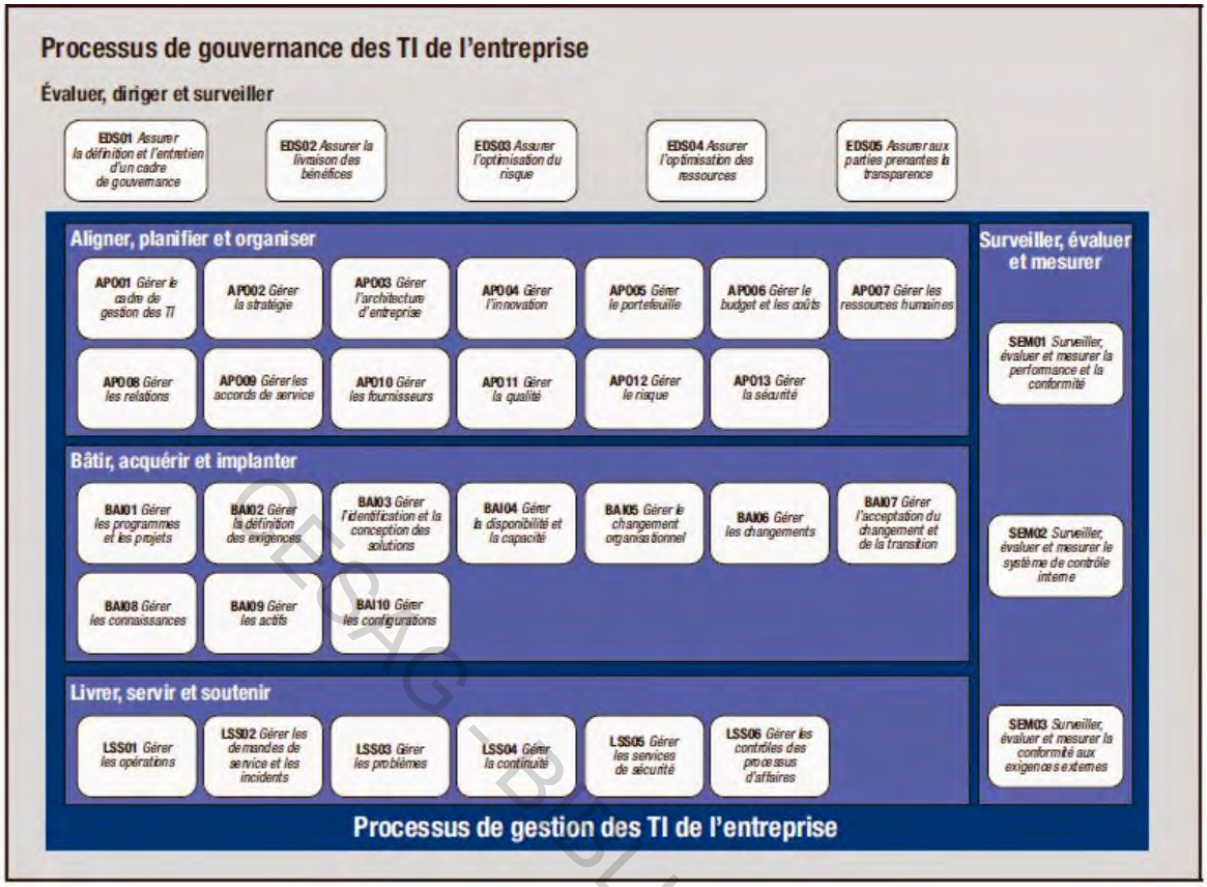
- la définition du périmètre à protéger (liste des biens sensibles) ;
- l'identification de la nature des menaces ;
- l'évaluation de leur impact sur le système d'information ;
- la détection de mesures de protection à mettre en place pour réduire les impacts.

Elle comporte ainsi 39 catégories de contrôle et 133 points de vérification répartis en 11 domaines.

1.3.3. COBIT

Le référentiel COBIT (Control Objectives for Information and relatead Technology ou Objectifs de contrôle de l'information et des technologies associées) publié en avril 1996, il a été développé par l'ISACA dont l'AFAI est le correspondant en France. Il couvre 37 processus pour sa version 5 (COBIT 5) dont cinq processus de gouvernance des TI intitulés EDS (évaluer diriger et surveiller) et 32 processus de gestion répartis en quatre grands domaines qui sont : APO (Aligner, Planifier et Organiser; BAI (Bâtir, acquérir et implanter) LSS (Livrer, servir et soutenir) et SEM (Surveiller, évaluer et mesurer).

Figure 4 : Les 37 processus de COBIT 5



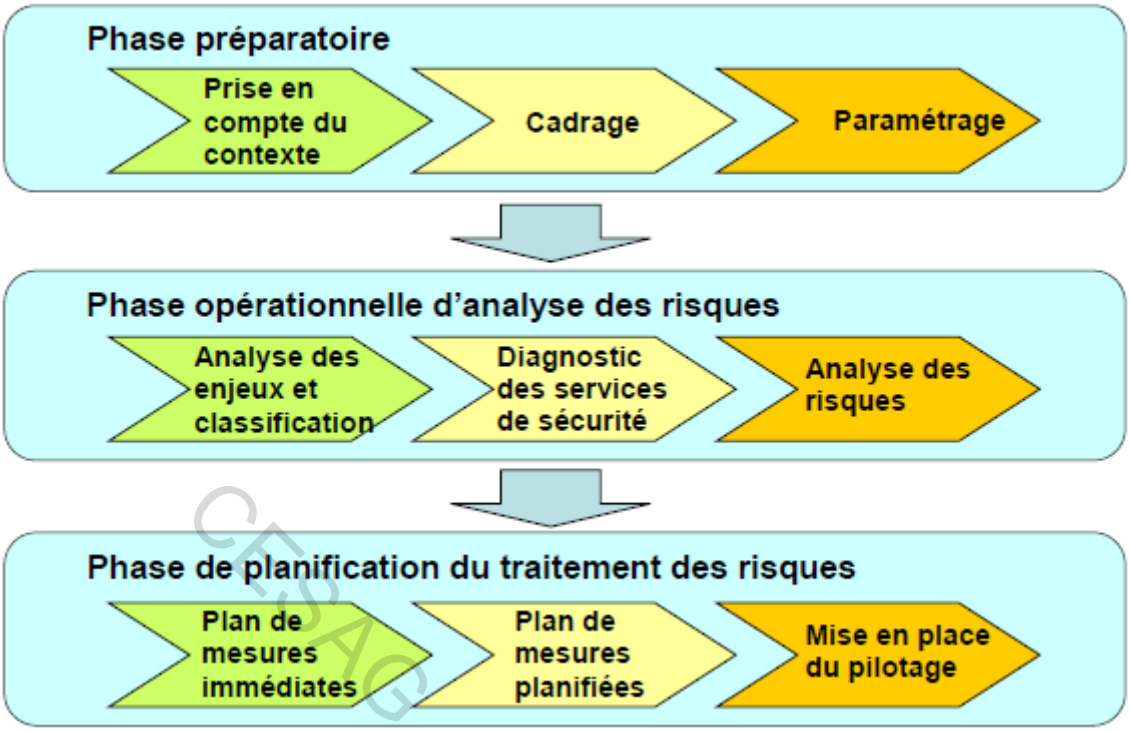
COBIT est un ensemble complet de ressources contenant toutes les informations dont les entreprises ont besoin pour adopter un cadre de contrôle et de gouvernance des systèmes d'information. COBIT propose de bonnes pratiques à travers un cadre de référence par domaine et par processus, dans une structure logique facile à appréhender.

1.3.4. MEHARI

MEHARI (Méthode Harmonisée d'Analyse de Risques) est issue de la fusion de deux méthodes que sont MELISA (Méthode d'évaluation de la vulnérabilité résiduelle des SI) et MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) (MENTHONNEX, 1995 : 361).

Elle est la propriété de CLUSIF. Cette méthode apporte des conseils, fait référence à un cadre méthodologique cohérent et fournit un ensemble d'outils et de bases de connaissance sur des domaines spécifiques tels que l'analyses des enjeux, l'étude des vulnérabilités, les scénarii de risques, le pilotage de la sécurité de l'information (CLUSIF, 2010).

Figure 5 : Démarche de la méthode MEHARI



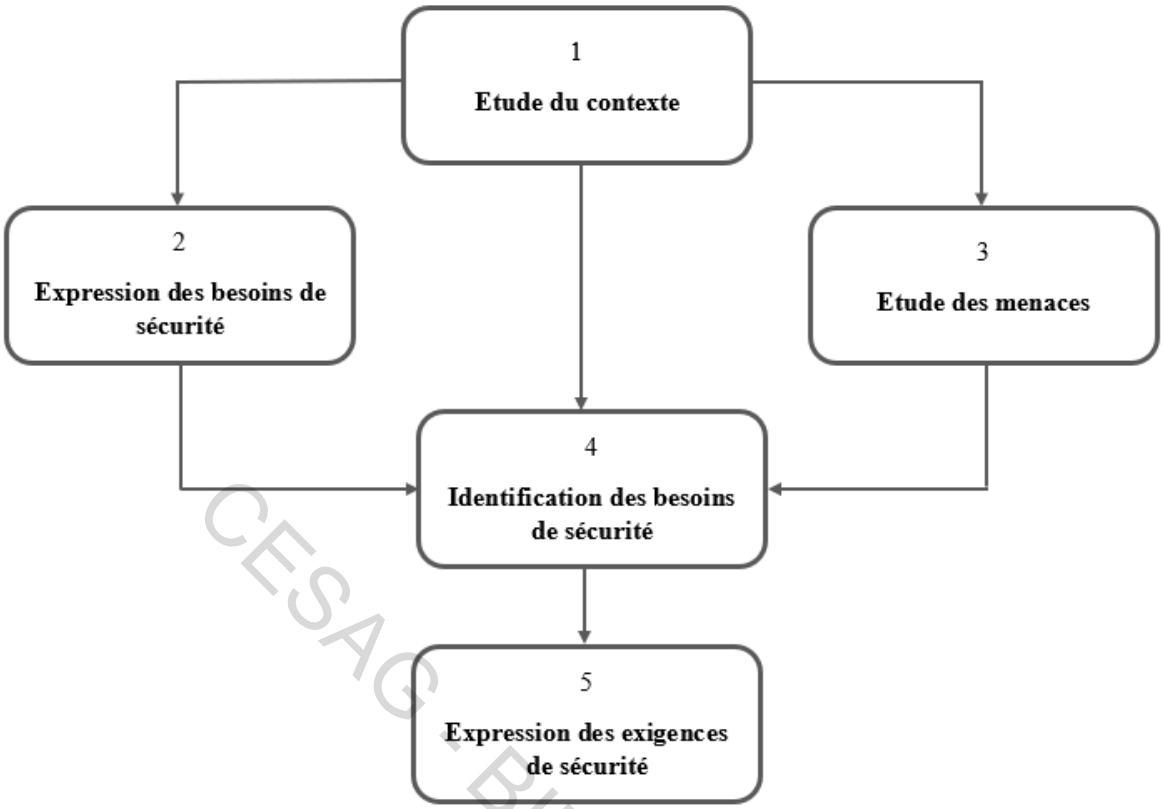
Source : CLUSIF

1.3.5. EBIOS

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), est également l'une des méthodes d'analyse des risques SI. Elle est d'origine française. L'agence nationale de la sécurité des systèmes d'information (ANSSI) qui en est l'auteur, la présente sous forme de document et de logiciel gratuit. Pour reprendre BLOCH & al. (2011 : 23), EBIOS permet d'apprécier et de traiter les risques relatifs à la SSI et de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques de SSI.

Cette méthode apporte toute l'aide nécessaire et indispensable pour juger des mesures de sécurité fonctionnelles et techniques qu'il faudra mettre en place autour du système d'information dans sa démarche de gestion des risques en cinq étapes. Elle est aussi un recueil de bonnes pratiques pour élaboration du schéma directeur de la SSI.

Figure 6 : Démarche globale de EBIOS



Source : ANSSI (2010 : 13)

La phase principale concerne la méthode d'analyse de l'existant (contexte). Après avoir mené ces différentes analyses, des actions appropriées doivent être mises en œuvre afin de réduire les risques à un niveau acceptable.

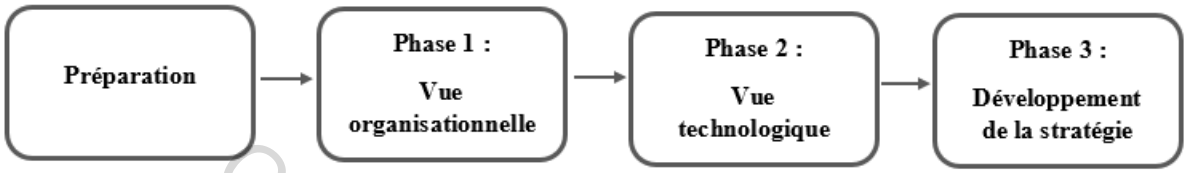
1.3.6. OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) est une méthode d'évaluation publiée par le SEI (Software Engineering Institute) de la Carnegie Mellon University de Pittsburgh aux États-Unis, université très reconnue dans le domaine de la sécurité. En se basant sur les travaux du CERT11 Américain, l'équipe du SEM (Survivable Enterprise Management) a développé cette méthode d'évaluation des vulnérabilités, des menaces, et des actifs opérationnels critiques. L'ensemble de la méthode est public et maintenu par l'université. La méthode OCTAVE se compose en trois phases :

- vue organisationnelle ;
- vue technique ;
- développement de la stratégie de sécurité.

Elle est centrée sur la protection des actifs de l'entreprise et le management du personnel. Elle couvre l'ensemble des processus métiers de l'entreprise aux niveaux organisationnel et technique. Cette méthode suppose la constitution d'une équipe pluridisciplinaire comprenant des membres de tous les services de l'entreprise. Elle leur permettra d'améliorer leur connaissance de leur entreprise et de mutualiser les bonnes pratiques de sécurité.

Figure 7 : Schéma de la démarche OCTAVE



Source : Nous même à partir de AMAN VLADIMIR GNUAN (Concevoir la sécurité Informatique en entreprise, 43)

Conclusion du premier chapitre

L'étude des notions liées au SI, à leur sécurité et à la PS a permis de comprendre les concepts clés de notre étude. Aussi, elle a approfondi notre connaissance de l'environnement normatif en ce qui concerne la sécurité des systèmes d'information. Le chapitre suivant nous permettra de présenter une méthodologie accompagnée des outils qui serviront de guide lors de l'étude de notre deuxième partie.

CHAPITRE 2 : METHODOLOGIE ET CADRE DE L'ETUDE

Dans la plupart des projets de mise en place d'une PS, il n'y a pas de démarche standard à appliquer ou encore de formule magique. Il revient cependant à chaque professionnel ou à l'équipe de professionnels de tenir compte du contexte de l'entité pour formuler une démarche. Afin de proposer une PS appropriée, répondant aux besoins des parties prenantes et à la hauteur des enjeux évoqués dans le chapitre 1, une démarche méthodique et adaptée s'impose dans l'élaboration de notre PS.

C'est pourquoi dans ce chapitre, nous commencerons dans un premier temps par définir le contexte dans lequel notre PSSI sera élaborée. Nous procéderons ensuite au recensement des moyens du SI. Il s'agira ici de faire un inventaire des différentes composantes du réseau informatique. Plus loin, nous qualifierons des principaux risques liés à la sécurité du réseau en les identifiant et en proposant une stratégie de traitement pour chacun des risques identifiés. Nous finirons par le choix des mesures de sécurité qui constitueront les règles de base du management de la sécurité de notre réseau informatique.

En second lieu, nous présenterons l'entité qui fait l'objet de notre étude en évoquant notamment son historique, sa mission et sa vocation. Nous présenterons un aperçu des activités qu'elle propose à ses clients et nous montrerons comment est régie son organisation interne. Nous finirons par la présentation du Service Informatique, service au sein duquel nous avions effectué notre stage.

2.1. Méthodologie de l'élaboration d'une PS

La méthodologie est la partie de l'étude qui fait suite à la propédeutique et qui rend possible la systématisation des méthodes, des techniques et outils nécessaires pour mener à bien cette étude.

2.1.1. Les outils de collecte et d'analyse de données

Pour une analyse pertinente, nous disposons d'un ensemble d'outils et de moyens de collecte de données.

2.1.1.1. L'observation physique

L'observation physique est une expérience de sélection et de recueil d'informations sur un phénomène, un objet d'étude en vue de dégager des hypothèses ou de vérifier celles découlant d'observations antérieures. Elle est l'action de suivi attentif des phénomènes, sans volonté de les modifier, à l'aide de moyens d'enquêtes et d'études appropriées.

Il existe plusieurs types d'observation mais nous opterons, dans le cadre de notre étude, pour l'observation participative. En effet, c'est une technique de collecte de données qui consiste à aller vivre avec les personnes concernées afin de pouvoir observer et partager les multiples aspects de leur quotidien.

2.1.1.2. L'entretien

L'entretien sera mené auprès des employés sur la base d'un canevas de questions préalablement construit. Il se déroule en face à face dans un lieu choisi d'un commun accord. Les données recueillies sont essentiellement des opinions, des motivations c'est-à-dire des informations qualitatives.

Nous rechercherons auprès des entretenus des explications et ce qu'ils pensent du système du management de la sécurité réseau ou du SI dans son ensemble.

Plusieurs types d'entretiens existent mais nous nous intéresserons à l'entretien semi directif. C'est l'entretien qui est le plus utilisé sur le terrain car, contrairement à l'entretien non directif où l'on pose comme principe l'acceptation de l'autre donc de ce qu'il dit ou ne dit pas, on va chercher à obtenir des informations sur des thèmes préalablement définis.

L'entretien semi directif est une technique qualitative fréquemment utilisée. Il permet de cerner le discours des personnes interrogées autour de différents thèmes définis au préalable par les enquêteurs et consignés dans un guide d'entretien. Il peut venir compléter et approfondir des domaines de connaissances spécifiques liés à l'entretien non directif qui se déroule très librement à partir d'une question.

Les entretiens seront ensuite retranscrits et feront dans un second temps l'objet d'une analyse qualitative qui examinera le contenu des propos recueillis.

2.1.1.3. L'analyse documentaire

L'analyse des documents nous permettra de connaitre d'avantage l'entité à travers ses objectifs, ses missions et ses différents organes. Ces documents seront essentiellement : l'organigramme de l'entité, les fiches de postes, l'architecture réseau, le manuel de procédure du Service Informatique, etc.

L'analyse documentaire sera essentiellement basée sur une recherche quantitative et qualitative.

2.1.1.4. La cartographie des risques

La cartographie des risques se définit comme la démarche d'identification, d'évaluation, de hiérarchisation et de gestion des risques inhérents aux activités d'une organisation. La

cartographie des risques est un levier indispensable au pilotage des risques et constitue le socle de la stratégie de gestion des risques.

La cartographie des risques permet d'appréhender l'ensemble des facteurs susceptibles d'affecter les activités et leur performance. L'objectif est de mettre alors en place les actions nécessaires afin de se prémunir au maximum des conséquences juridiques, humaines, économiques et financières que représentent les risques identifiés.

La cartographie des risques implique d'investiguer de façon approfondie sur l'ensemble des processus managériaux, opérationnels et supports que les activités nécessitent de mettre en œuvre. Elle nécessite également d'identifier les rôles et responsabilités de chaque acteur, à chaque étape des processus.

Pour être efficace, la cartographie des risques doit respecter trois conditions :

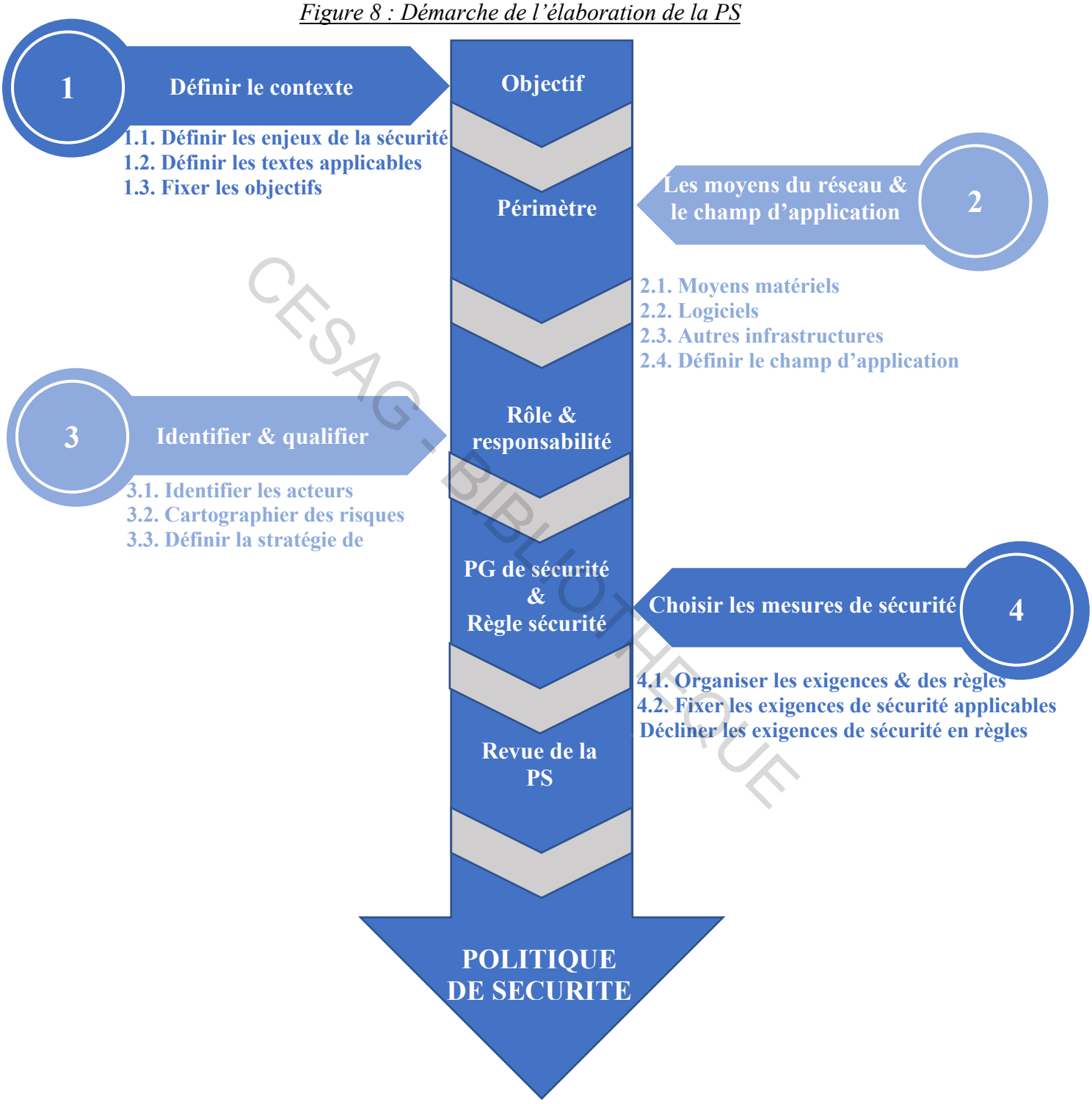
- être exhaustive et précise ;
- être formalisée et accessible ;
- être évolutive.

Dans le cadre de notre étude, nous utiliserons la cartographie des risques pour identifier les risques auxquels fait face notre réseau afin d'apporter une réponse adéquate en ce qui concerne les mesures de sécurité à mettre en place dans la PS.

2.1.2. Démarche de l'élaboration d'une PSSI

Notre démarche se présente comme suit :

Figure 8 : Démarche de l'élaboration de la PS



Source : nous-même

2.1.2.1. Le Contexte

La première étape dans notre démarche a pour objet de fixer le périmètre du SI auquel doit s'appliquer la PSSI, d'expliciter les enjeux associés à ce périmètre, et de vérifier que les conditions requises pour la définition et la mise en œuvre d'une PSSI sur ce périmètre sont réunies.

Les différentes activités à mener au cours de cette étape sont :

- préciser les enjeux de sécurité ;
- identifier les textes applicables.
- Fixer les objectifs

2.1.2.1.1. Préciser les enjeux de sécurité

L'objet de cette activité est d'expliciter en quoi la sécurité du SI est importante pour la bonne réalisation des activités retenues pour le périmètre de la PSSI.

L'expression de ces enjeux fait typiquement ressortir l'importance du SI dans la réalisation des missions du CESAG et, de fait, les exigences qui pèsent sur le SI pour que ces activités puissent être réalisées conformément aux attentes. Les contraintes liées au contexte, aux obligations, à l'environnement, peuvent également être mentionnées ici si elles sont susceptibles de conditionner les attentes en termes de SSI.

Le périmètre métier et support retenu conditionne notamment les enjeux de sécurité, les moyens du SI pris en compte et les risques liés au SI.

2.1.2.1.2. Identifier les textes applicables

Il s'agira ici d'identifier les principaux textes qui imposent des contraintes quant à l'usage du SI. Il ne s'agira pas pour nous de lister ces contraintes, mais d'identifier les textes de bonnes pratiques qui fixent ces contraintes, afin que la Direction, les Responsables d'applications, le Responsable du Service Informatique puissent les prendre en compte et s'y reporter quand nécessaire.

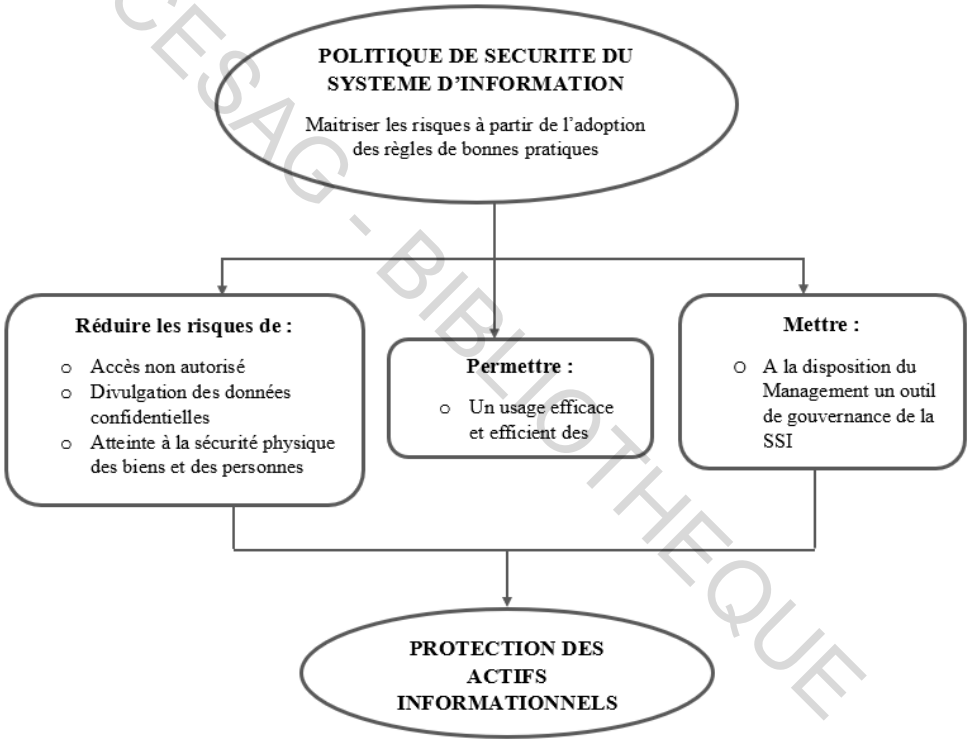
2.1.2.1.3. Fixer les objectifs de la PSSI

La PSSI a pour objectif de permettre à une entité de se doter d'un ensemble de règles organisationnelles, techniques, de codes de conduite et de bonnes pratiques visant à protéger ses biens (infrastructures et actifs critiques). Elle se veut être un document dans lequel la

Direction Générale et toute l'entité manifestent leur engagement clair et ferme en matière de gestion de la sécurité. En d'autres termes, elle permettra de :

- définir la cible en termes de gestion de la sécurité des systèmes d'information
- organiser la sécurité
- fédérer tous les organes de l'entité autour du thème 'sécurité'
- savoir mesurer la sécurité
- améliorer la sécurité au quotidien

Figure 9 : Objectifs d'une PS



Source : nous-même

2.1.2.2. Définir les moyens du réseau et le champ d'application

La définition des moyens du réseau et le champ d'application permettront de définir le périmètre de la PS.

2.1.2.2.1. Recenser les moyens du réseau

Les moyens sur lesquels s'appuie le SI, également appelés « biens supports » dans le cadre d'une analyse de risques, constituent le patrimoine matériel et organisationnel que les règles de la PSSI vont contribuer à protéger pour permettre le bon déroulement des activités.

Pour que ces règles soient définies de manière pertinente, il est nécessaire de connaître d'une part la nature de l'ensemble des éléments auxquels elles vont s'appliquer et d'autre part, qui aura en charge de mettre ces règles en application. A cette fin, un inventaire des catégories de biens supports du SI doit être réalisé.

Il ne s'agira pas ici de dresser un inventaire détaillé qui recenserait chaque composant du SI comme on le ferait pour une gestion de parc par exemple, mais d'identifier des groupes de biens supports homogènes.

A cette fin, nous procéderons par l'observation physique dans le but de nous assurer de l'exhaustivité de l'ensemble des moyens existants.

2.1.2.2.2. Champ d'application de la PSSI

Le champ d'application de la PSSI se définit :

- du point de vue des activités métiers et des activités support d'une part ;
- du point de vue des moyens du SI d'autre part.

Cette activité a pour objet de traiter le premier aspect, à savoir le périmètre auquel doit s'appliquer la PSSI du point de vue des activités. Le second aspect est traité au cours de l'étape «recenser les moyens du SI ».

Il s'agit ici de dresser une brève description des activités qu'on souhaite inclure dans le périmètre et de préciser celles qu'on souhaite exclure du périmètre le cas échéant (par exemple, de façon temporaire, pour une première mise en œuvre de la PSSI uniquement).

Les activités supports qui sont nécessaires aux activités métiers doivent également être indiquées. La description nécessite le niveau de détail juste suffisant à garantir que le périmètre pris en compte est clair pour l'ensemble des utilisateurs.

Pour ce faire, nous procéderons à l'observation physique. Selon IFACI (2013), c'est le moyen le plus fiable pour obtenir une preuve directe d'une situation.

2.1.2.3. Identifier les acteurs et qualifier les principaux risques du SI

L'identification des acteurs et qualification des principaux risques aboutiront à l'établissement des rôles et des responsabilités.

2.1.2.3.1. Identification des acteurs

Dans le projet d'élaboration de la PSSI ou de sa mise en œuvre, différents acteurs sont susceptibles d'être mobilisés. Outre les travaux opérationnels autour de la PSSI, il est essentiel que les acteurs qui participent à l'animation de la SSI soient concernés par la PSSI.

Afin de répondre à cette exigence, différents acteurs peuvent être identifiés. Il s'agira pour nous d'identifier l'ensemble des acteurs pouvant être impliqués dans l'élaboration et la mise en œuvre de la PSSI. Il sera question également de situer brièvement les responsabilités de chacun des acteurs identifiés. Pour ce faire, nous allons nous appuyer sur le tableau RACI (Responsable Approuve Consulté et Informé) de COBIT 5. C'est un tableau permettant de situer un niveau de responsabilité à chaque acteur en fonction des activités de GSSI.

(Tableau d'identification des acteurs basé sur COBIT 5 : voir annexe)

2.1.2.3.2. Identifier les principaux risques liés au SI

Il est important de comprendre les principaux risques auquel est exposé le SI afin de nous assurer que les exigences et les règles de sécurité proposées sont adaptées au contexte.

Il s'agira pour nous d'établir ou de mettre à jour la cartographie des risques. La finalité de cette cartographie est de lister les principaux risques qui pèsent sur le SI, les hiérarchiser par niveau de risque, afin de pouvoir définir les priorités de mise en œuvre des règles de sécurité. L'analyse de risque doit-être minutieusement menée en vue de déterminer si des exigences de sécurité supplémentaires sont nécessaires, et de définir dans ce cas les règles de sécurité qui permettent d'y répondre.

2.1.2.3.3. Préciser la stratégie de traitement des risques

Une fois les principaux risques identifiés, il reste à confirmer la manière dont ils doivent être traités. C'est l'objet de cette étape.

Pour chaque risque, il s'offre quatre options de traitement. Les deux premières sont le plus souvent adoptées :

- réduire le risque : mettre en œuvre des mesures de sécurité pour diminuer la vraisemblance du risque ou son impact (ou les deux), pour que le risque se limite à un niveau acceptable ;
- transférer ou partager le risque : partager les pertes avec d'autres acteurs en cas de sinistre (par exemple avec une compagnie d'assurance), faire assumer la responsabilité par un tiers…

Les deux dernières peuvent être retenues vis-à-vis de certains risques, dans des situations particulières :

- éviter (ou refuser) le risque : modifier des éléments du contexte du SI afin qu'il n'existe plus d'exposition à ce risque. Par exemple, pour une application, l'autoriser qu'au personnel interne authentifié au lieu de la laisser en libre accès à toute personne interne comme initialement souhaité, ou encore renoncer complètement à une application car le coût des mesures nécessaires pour la sécuriser n'est pas acceptable au regard des services attendus de cette application ;
- prendre (ou « maintenir ») le risque : accepter le risque tel quel et assumer ses conséquences sans prendre de mesure de sécurité supplémentaire ;

Il est possible de choisir plusieurs options pour un même risque, par exemple réduire partiellement le risque par des mesures de sécurité et recourir à une assurance pour couvrir les frais en cas de réalisation du risque résiduel.
Bon nombre de méthodes de management des risques existent et nous seront forts utiles dans notre démarche.

2.1.2.4. Choisir les mesures de sécurité

A ce stade de la démarche, les éléments constitutifs du SI ont été identifiés, les risques qui peuvent y être associés ont été cartographiés et la stratégie de traitement de chaque risque a été fixée.
L'activité suivante consistera, pour chaque risque qu'il a été décidé de réduire à un niveau acceptable, à déterminer les exigences de sécurité qui doivent être imposées au SI pour atteindre cet objectif.
Ces exigences de sécurité peuvent être de nature à éviter la survenance du risque (il s'agit alors de prévention) ou à en limiter les impacts lorsqu'ils donnent lieu à des incidents (il s'agit alors de réaction à l'incident). Elles sont généralement exprimées sous une forme fonctionnelle,

générique et peu technique. C'est sur la base de ces exigences que seront élaborées, les mesures opérationnelles concrètes qui répondront à ces exigences.

Le choix des mesures de sécurité permettra de définir la politique générale de sécurité et les règles de sécurité.

2.1.2.4.1. Organisation des exigences et des règles

Les exigences et les règles sont organisées en 7 thématiques :

- Thématique 1 : Répondre aux obligations légales
- Thématique 2 : Promouvoir et organiser la sécurité
- Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI
- Thématique 4 : Protéger les infrastructures informatiques
- Thématique 5 : Maîtriser les accès aux informations
- Thématique 6 : Acquérir des équipements, logiciels et services
- Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité

Cette structuration en 7 thématiques s'est appuyée sur les thèmes utilisés par l'ISO 27002. Certains de ces thèmes ont cependant été regroupés pour être adaptés à notre cas. Cet aménagement a pour finalité de nous permettre d'identifier plus aisément les contextes sur lesquels portent les exigences afin d'en apporter une déclinaison adaptée aux personnes qui doivent les mettre en œuvre.

2.1.2.4.2. Fixer les exigences de sécurité applicables

Il s'agira ici de proposer des mesures conformément au cadre légal et à la stratégie de traitement des risques adoptée, afin de :

- réduire les risques génériques identifiés dans le tableau de la cartographie des risques ;
- répondre aux principales obligations légales en matière de sécurité des SI.

Ces mesures sont issues de l'ensemble des référentiels techniques et des bonnes pratiques en sécurité des SI (norme ISO/ IEC 27001 — Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences, norme ISO/IEC 27002 – Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences, guides ANSSI).

2.1.2.4.3. Décliner les exigences de sécurité en règles

Une fois les exigences de sécurité établies, il convient de déterminer les mesures de sécurité qui permettront de satisfaire chacune d'elles.

Ces mesures sont présentées sous forme de règles, de consignes à mettre en œuvre par les utilisateurs du SI. La norme ISO/ IEC 27001 propose un ensemble de mesures qui permettront de répondre aux exigences que nous aurons prédéfinies.

A cette fin, les opérations à mener au cours de cette tâche sont, pour chaque mesure proposée :

- vérifier que la mesure s'applique à des catégories de composants de SI effectivement présentes dans le SI ;
- si la mesure est applicable à au moins un composant du SI, la contextualiser pour notre SI ;

2.1.2.5. Revue de la politique de sécurité

La revue de la politique de sécurité constitue un support à la mise en place d'un cycle d'amélioration continue. Ce cycle permettra d'améliorer continuellement la sécurité afin d'atteindre un objectif de sécurisation conforme à la PSSI et adapté aux enjeux.

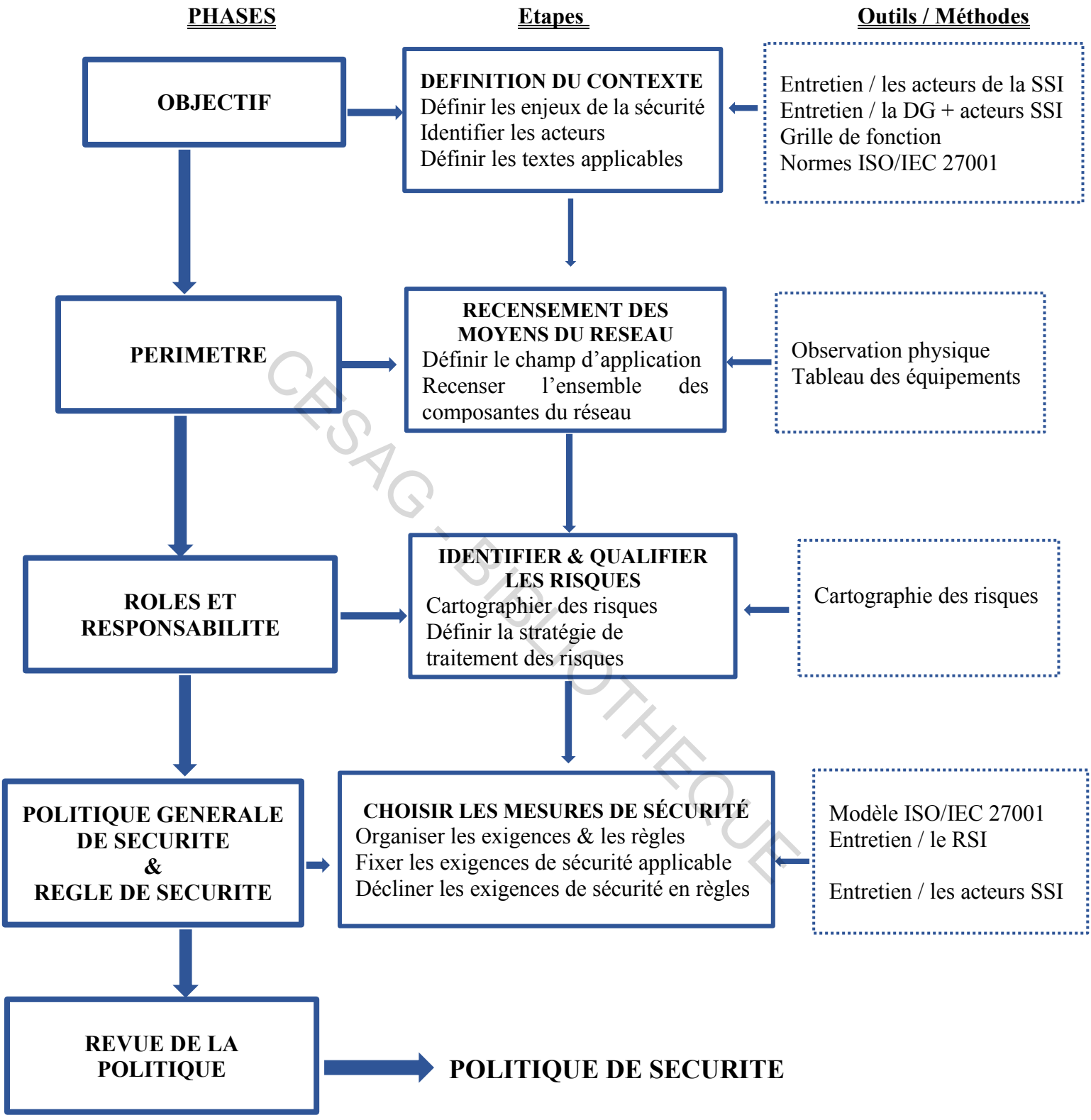
Pour ce fait, il est proposé une liste des mesures essentielles propres à constituer cette première marche.

2.1.3. Modèle d'analyse

Le modèle d'analyse nous permettra de fournir une approche conceptuelle de notre méthodologie. Le but de ce modèle est de définir une structure robuste et extensible qui nous servira de base pour la construction de notre PS.

Ainsi, après avoir exposé nos outils de collecte et d'analyse de données et présenté notre démarche, nous pouvons résumer notre méthodologie à travers le modèle d'analyse schématisé ci-dessous :

Figure 10 : Modèle d'analyse



Sources : nous-même

2.2. Présentation du CESAG

Nous avons effectué un stage de sept (07) mois au Centre Africain d'Etudes Supérieures en Gestion (CESAG). Le CESAG est une institution sous régionale spécialisée en matière de formation, de recherche et de consultation dans le domaine du management.

2.2.1. Historique, Mission et Vocation

Bien plus qu'une école, le CESAG est un patrimoine sous régional.

2.2.1.1. Historique

Entré en activité en 1985, le CESAG s'est rapidement établi un rayonnement régional en s'imposant comme la principale grande école de formation au management en Afrique francophone au Sud du Sahara. Les principaux diplômes qu'il délivre sont reconnus par le Conseil Africain et Malgache pour l'Enseignement Supérieur (CAMES).

A la suite de la liquidation de la Communauté Economique de l'Afrique de l'Ouest (CEAO), organisme de tutelle du CESAG jusqu'en 1995, la Banque Centrale des Etats de l'Afrique de l'Ouest (BCEAO), sollicitée par les Etats membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA), soucieux de conserver les acquis de la CEAO en matière d'intégration régionale, a repris le CESAG et l'a doté d'une large autonomie de gestion pour lui permettre de poursuivre sa mission avec plus d'efficacité.

2.2.1.2. Mission

Le CESAG a pour mission de contribuer, par la formation, la recherche et le conseil, au renforcement des capacités de gestion dans la sous-région.

A cet effet, un objectif important du CESAG est d'accompagner le processus d'intégration régionale en Afrique de l'Ouest par le renforcement des capacités humaines et institutionnelles en vue d'assurer le succès des importants projets sectoriels d'intégration (le Système Comptable Ouest Africain (SYSCOA), l'Organisation pour l'Harmonisation du Droit des Affaires en Afrique (OHADA), la Centrale des Bilans, le Marché Financier Régional, l'Union Douanière). Ainsi, en partenariat avec les entreprises, les Administrations et organisations de la région, le CESAG met au point et conduit des programmes et des actions de formation qui contribuent de manière déterminante à renforcer l'efficacité des hommes et des structures et donc à accroître la productivité.

2.2.1.3. Vocation

Les participants aux programmes du CESAG proviennent de l'ensemble du continent africain : pays de l'UEMOA, Burundi, Cameroun, Congo, Gabon, Ghana, Guinée, Madagascar, Mauritanie, Tchad et Djibouti.

Des ressortissants de la République Centrafricaine, du Cap-Vert, du Rwanda, d'Algérie, d'Haïti, des Philippines, de Tunisie, du Maroc, et de France ont également eu à s'inscrire aux programmes longs et courts du Centre par le passé

2.2.2. Portefeuille d'activités

Le portefeuille d'activités du CESAG comporte des activités de formation, de consultation et de recherche.

La formation

Elle comprend la formation diplômante (DESS, Master et Licence), fortement marquée par une restructuration intervenue en 2001-2002, puis par la réforme Licence, Master, Doctorat (LMD) en cours, et la formation qualifiante (séminaires) l'évolution des effectifs est la suivante depuis 1998.

La formation diplômante

Les programmes de MBA et de Master

Une dizaine de MBA ouverts aux candidats titulaires d'un diplôme de niveau Bac + 4, trois Masters en Sciences de Gestion, en Audit et Contrôle de Gestion et en Techniques Comptables et Financières, créés dans le cadre de la réforme LMD.

Les programmes de Licence

Deux programmes de Licence en Sciences de Gestion et en Techniques Comptables et Financières créés dans le cadre de la réforme LMD.

Formation qualifiante

En plus des programmes diplômants, le CESAG offre, chaque année, un grand nombre de séminaires de recyclage et de perfectionnement de courte durée (quelques jours à quelques semaines). Certains de ces séminaires sont coorganisés avec des partenaires internationaux tels que la Banque Mondiale, l'Organisation Mondiale de la Santé, l'USAID, l'UNFPA, etc.

Ils peuvent être offerts sous forme intra-entreprise ou inter-entreprises. Le CESAG peut également répondre à des besoins spécifiques par des formations sur mesure.

La recherche et la consultation

Parallèlement aux activités d'enseignement, les enseignants permanents mènent des activités de recherche et de consultation.

Le plan stratégique en cours a inscrit, parmi ses objectifs principaux, de donner une nouvelle impulsion à la recherche par la mobilisation et la mise à la disposition des chercheurs des ressources nécessaires et par diverses mesures incitatives.

2.2.3. Gouvernance et Organisation

Comme toute entité de grande taille, le CESAG dispose en son sein d'un système de gouvernance et d'organisation bien articulé.

2.2.3.1. Gouvernance

Le CESAG est un Établissement Public International régi par un ensemble de textes réglementaires et statutaires :

- le Statut du Centre ;
- le Statut du personnel ;
- le Protocole d'accord du 6 septembre 1995 entre la CEAO et la BCEAO concernant les modalités et conditions de transfert du patrimoine du CESAG à la BCEAO ;
- l'avenant à l'accord de siège entre la BCEAO et le CESAG et le Gouvernement du Sénégal relatif à l'extension au CESAG des immunités diplomatiques et juridiques dont jouit la Banque, signé le 6 mai 2009.

Le fonctionnement du Centre est assuré par trois organes :

- un **Conseil d'Administration** de 12 membres, présidé par le Gouverneur de la BCEAO, définit les grandes orientations du Centre ; il se réunit deux fois par an, en session ordinaire, en juin et en décembre, pour examiner respectivement le rapport de gestion et le budget du Centre ;
- un **Conseil Scientifique et Pédagogique** consultatif chargé de la supervision des programmes de formation et de recherche. Cet organe, composé de professeurs des Universités régionales, européennes et américaines, n'est pas encore fonctionnel ;
- une **Direction Générale** qui met en œuvre les décisions du Conseil d'Administration, organise et dirige les activités du Centre.

2.2.3.2. Organisation

Le CESAG est géré par un Directeur Général nommé par le Conseil d'Administration. Il est assisté dans ses fonctions par un Secrétaire Général et deux (02) Conseillers.

Pour mener à bien ses activités, le Centre s'est doté d'un organigramme entré en vigueur au mois de novembre 2014 dont la dernière mise jour date de 2017.

(Organigramme fonctionnel du CESAG : voir annexe)

2.2.4. Présentation du service informatique

Le Service Informatique du CESAG est l'organe au sein duquel nous avions effectué notre stage. Dans l'intérêt de notre étude, la connaissance de celui-ci s'avère plus que nécessaire.

2.2.4.1. Composition

Le service informatique est composé à ce jour de deux (02) agents permanents en CDI, un (1) agent en CDD et de deux (02) collaborateurs extérieures, chargés de mettre à la disposition des utilisateurs, des ressources et services informatiques. Il offre une assistance aux utilisateurs et garantit la sécurité du système d'information de l'établissement.

2.2.4.2. Missions

La mission du service informatique est organisée autour des activités suivantes :

- Préparer les cahiers de charges pour les appels d'offres ou consultations ;
- Etudier les offres issues d'appel d'offres ou de consultation ;
- administrer et exploiter les serveurs administratifs et communs ;
- maintenir le parc informatique, planifier les interventions d'installation, de configuration et de dépannage de matériels mis à la disposition de l'administration et des enseignants (hors laboratoires), et gérer les priorités ;
- établir l'inventaire du parc informatique et des logiciels en service dans tout l'établissement,
- gérer le réseau informatique filaire et WIFI et faire évoluer l'infrastructure matérielle dans tous les bâtiments,
- établir les schémas du réseau informatique ;
- gérer les serveurs d'annuaires et fournir des services numériques aux usagers (messagerie électronique, réseau sans fil, ...) ;

- gérer le site internet institutionnel et mettre à jour les informations qui s'y trouvent,
- mettre en place les mécanismes concernant la sécurité informatique, et assurer la veille sur l'évolution des risques ;
- mettre en place une politique de sauvegarde et d'archivage des données ;
- conseiller et informer les utilisateurs dans tout ce qui touche à l'informatique au sens large ;
- Assistance aux étudiants et aux séminaristes ;
- Faire évoluer le système dans son intégralité

Conclusion du deuxième chapitre

La connaissance de l'environnement d'une entité ou d'une organisation faisant objet d'une étude ou d'une mission est toujours capitale pour l'atteinte des objectifs.

Ce chapitre sur la présentation du CESAG nous a permis de le découvrir à travers son historique, mission, et vocation, son portefeuille d'activités, sa gouvernance et son organisation. De plus, il nous a aidé à mieux cerner le positionnement du support informatique (Service Informatique) dans l'organisation du CESAG.

Conclusion de la première partie

Cette première partie nous a permis d'appréhender la notion des systèmes d'information (SI), de sécurité des SI et de politique de sécurité du SI (PSSI). Elle nous a permis également d'étaler notre démarche quant à la conception d'une PSSI dans un premier temps. Secondairement, nous avions présenté l'entité qui fait l'objet de notre étude.

A travers cette étude théorique, nous avons mis en exergue les différents aspects de notre méthodologie. De même, nous avons passé en revue les outils et techniques qui vont nous permettre de recueillir, d'analyser et d'évaluer les informations nécessaires à la conception de notre PSSI. La suite de notre travail se poursuivra dans la deuxième partie dans laquelle nous procéderons à la réalisation pratique de notre étude.

DEUXIEME PARTIE :

CADRE PRATIQUE DE L'ELABORATION DE LA POLITIQUE DE SECURITE

Introduction de la deuxième partie

Cette deuxième partie a pour objectif de comprendre d'abord l'écosystème du réseau informatique de notre structure d'accueil en l'occurrence le CESAG et ce qui est effectué pour garantir la sécurité. C'est alors ensuite que nous aurions de meilleures orientations pour formuler notre politique de sécurité.

C'est pourquoi notre seconde partie est structurée en deux chapitres tout comme la première partie. Nous avons le chapitre 3 dans lequel nous procéderons à la description de l'existant et dans le chapitre 4 il s'agira de l'élaboration de la politique de sécurité.

CHAPITRE 3 : DESCRIPTION DE L'EXISTANT

L'étude de l'existant permet de décrire la (les) solution(s) existante(s), décrire l'organisation de l'entreprise et le fonctionnement de l'organe qui fait l'objet de notre étude, décrire l'environnement technique de l'étude.

C'est pourquoi dans ce chapitre nous allons, décrire le réseau informatique en présentant l'architecture du réseau l'ensemble des éléments qui le compose. Ensuite nous décrirons comment le système réseau est administré et comment sa sécurité et sa disponibilité sont maintenues.

3.1. Description du réseau informatique

Le réseau informatique du CESAG est un ensemble d'équipements et de logiciels reliés entre eux pour échanger des informations. Il est constitué de matériels informatiques tels que les ordinateurs portables, les ordinateurs bureautiques, les imprimantes, les onduleurs, les scanners, les serveurs et les switchs. Le parc logiciel est constitué des produits Microsoft Office, de Windows Serveur 2008, de logiciels comptable, d'analyse de données, de gestion budgétaire, logiciel de gestion de la sécurité du réseau et bien d'autres logiciels.

Il couvre l'ensemble du site de l'école et dessert toutes les structures organisationnelles de l'établissement à savoir :

- l'administration ;
- l'agora ;
- l'auditorium ;
- le bâtiment Yali ;
- la direction générale ;
- la résidence ;
- les salles informatiques ;
- les salles de cours ;

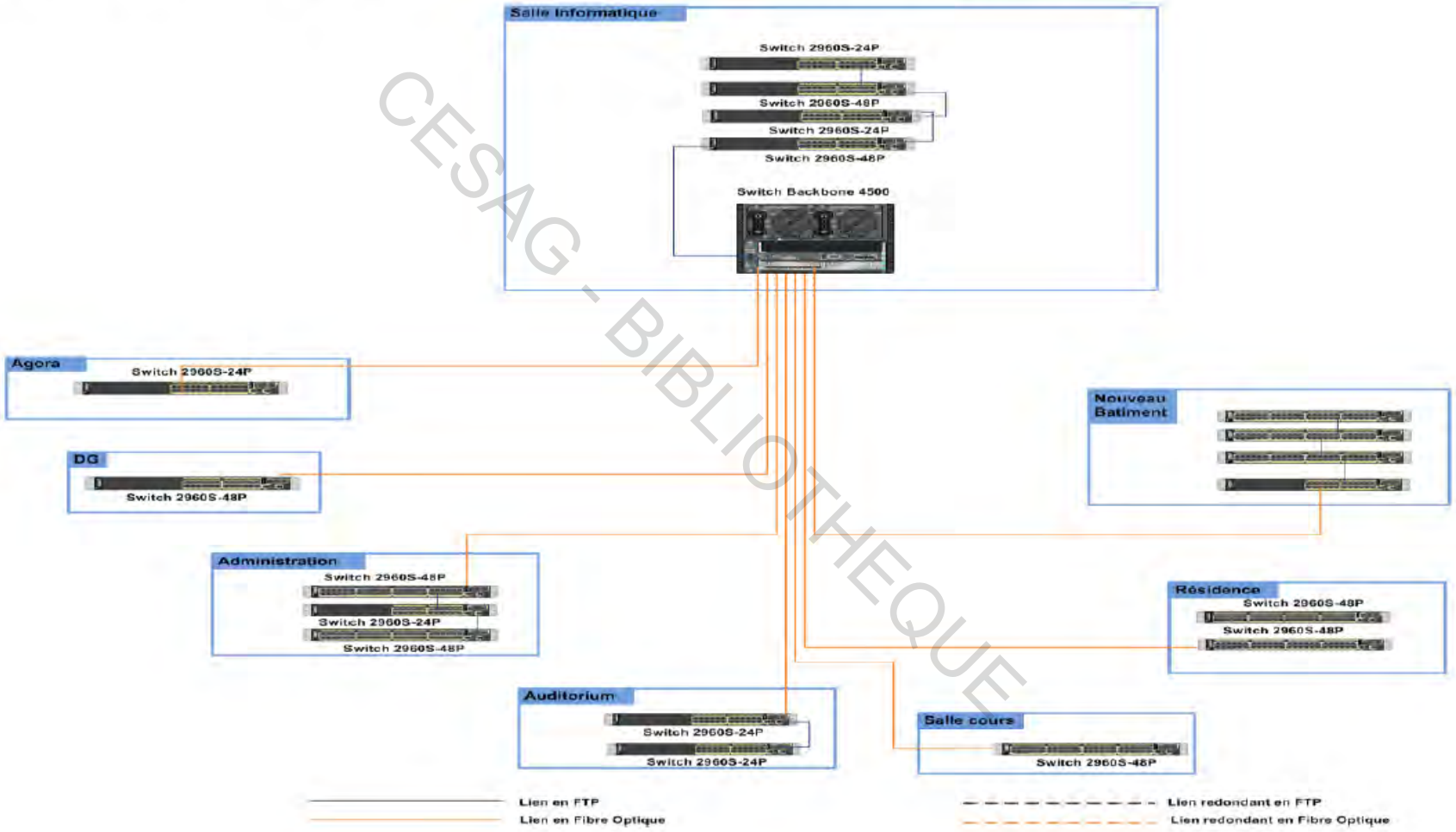
Le réseau se présente sous l'architecture de type LAN (Local Area Network), constitué de liens FTP et de fibres optiques. Des liens de doublures ont été mise en place afin de palier à l'indisponibilité des principaux liens. Des switchs ont été installés dans chacun des bâtiments du site afin de servir de hub pour l'ensemble des utilisateurs.

Le réseau est piloté par le firewall **FortiGate 300 C**. C'est un boîtier conçu pour les grandes entreprises. Il supporte la haute disponibilité, qui comprend une réplication automatique sans coupure de réseau. Ces caractéristiques font de lui, le meilleur choix pour les applications les plus critiques. Il fonctionne 24 h / 24, 7 j / 7 et permet de :

- faire des mises à niveau des micro-logiciels et des logiciels en général ;
- mettre au point un VPN ;
- assurer la gestion du trafic et l'ensemble des services réseau de l'entreprise (programme de contrôle des applications, IPS, AV, AV / Botnet, logiciel malveillant mobile) Service, filtrage Web, antispam, Cloud, y compris épidémie de virus et service de désarmement et de reconstitution du contenu, service d'évaluation de la sécurité, service de sécurité industrielle et service CASB).

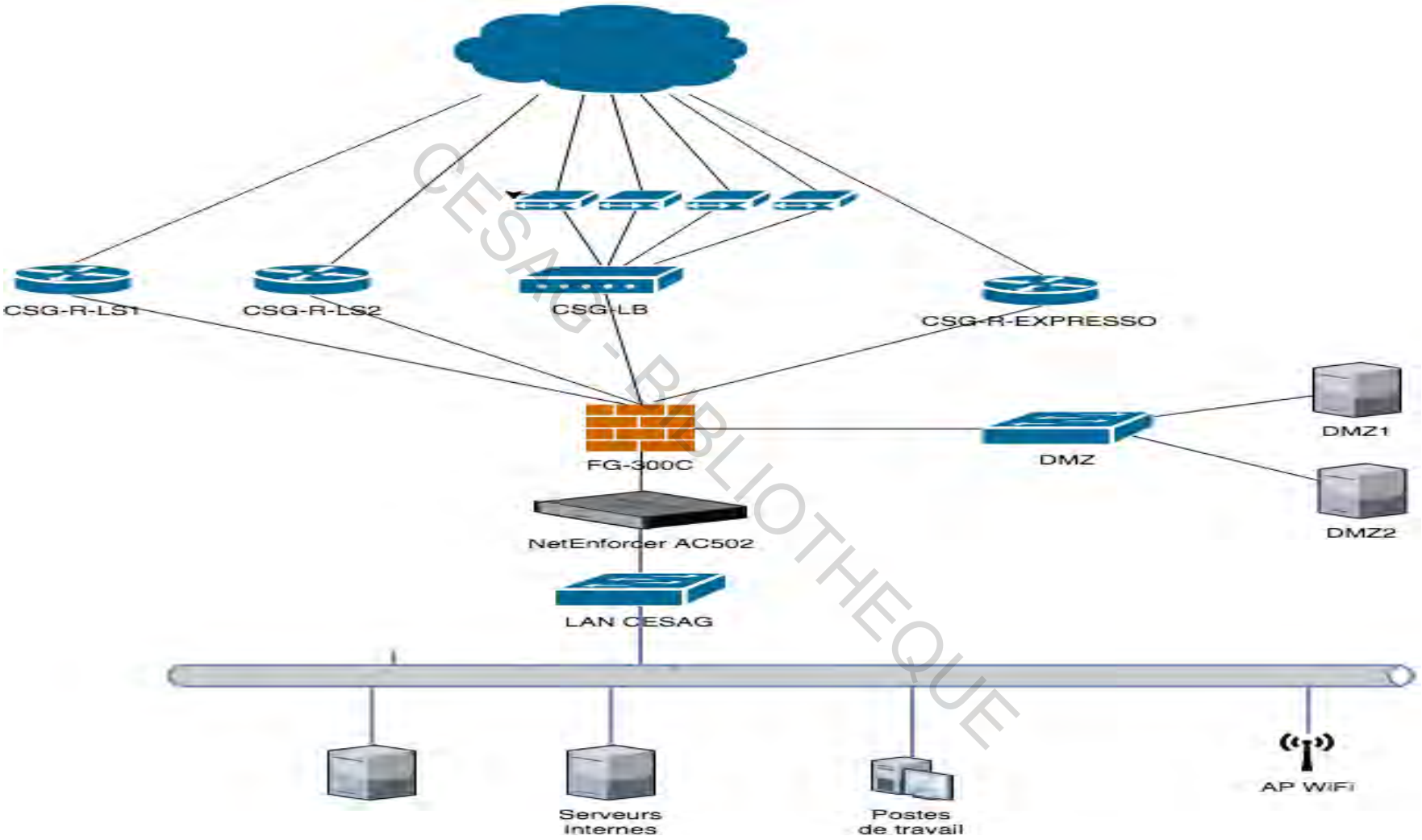
Afin d'effectuer une description holistique du réseau informatique du CESAG, deux (02) architectures seront présentées dans les pages suivantes.

Figure 11 : Architecture LAN cible du réseau



Source : Documentation CESAG

Figure 11 : Architecture LAN du réseau



Source : Manuel d'administration du réseau, Service Informatique CESAG

3.2. Administration du réseau informatique

Le premier responsable de la sécurité du réseau informatique du CESAG est le Responsable de Service Informatique (RSI). Dans l'exercice de ses fonctions et en ce qui concerne l'administration du réseau, il réalise les activités suivantes :

- l'élaboration des procédures et règles relatives à la gestion du système d'information (GSI) relatif au réseau;
- la gestion la formation des utilisateurs ;
- la supervision de la gestion des serveurs ;
- le contrôle la disponibilité de la ligne Internet ;
- l'administration du firewall (ajout de nouvelles règles en cas de besoin, contrôle des journaux pour prévenir les attaques de pirates) ;
- la gestion des entrées et sorties du matériel informatique;

Il est assisté dans cette tâche par un Administrateur Réseaux et Systèmes (ARS) et un Technicien Réseau (TR) comme signifié dans le manuel de procédure. L'ARS a pour activité :

- contrôler le câblage réseau ;
- définir clairement les mesures de sécurité du câblage réseau ;
- contrôler l'accès aux panneaux de raccordement et aux salles des câbles ;
- identifier nominativement chaque personne ayant accès au système ;
- définir les règles de choix et de dimensionnement des mots de passe ;
- mettre en place des moyens techniques permettant de faire respecter les règles relatives aux mots de passe ;
- ne pas conserver les mots de passe sur les systèmes informatiques ;
- supprimer ou modifier systématiquement les éléments d'authentification par défaut sur les équipements ;

Et le TR a pour tâche :

- protéger le câblage réseau ;
- utiliser un marquage clairement identifiable sur les câbles ;

- utiliser une liste documentée des raccordements à effectuer ;
- utiliser câble fibre optique ;
- utiliser un blindage ;

3.3. Menaces liées à la sécurité

Nous présenterons les menaces de sécurité l'ensemble du SI avant de les restreindre au système réseau.

3.3.2. Cartographie des risques du SI

Ci-dessous, se trouve les menaces liées à la sécurité du SI :

Tableau 2 : Risques généraux liés au SI

		Niveau de risque brut			Niveau de risque résiduel
N°	**Libellé du Risque**	**Probabilité (P) du risque (1 à 6)**	**Gravité (G) du risque (1 à 6)**	**Criticité du risque (P x G = C/36)**	**Criticité du risque (P x G = C/36)**
1	Risque lié à la gouvernance et à la gestion du processus décisionnel en matière informatique (décisions d'investissements, projets, choix technologique, etc.).	5	5	25	25
2	Risque lié à la dégradation du patrimoine informationnel du CESAG en raison d'une non-formalisation de la cartographie du système d'information et une connaissance insuffisante des différents flux informationnels et modalités de stockage.	4	5	20	20
3	Déficit de soutien opérationnel des utilisateurs au lancement des nouvelles applications en raison d'un sous dimensionnement de l'équipe projet et de l'équipe de support (problème de conduite du changement).	5	4	20	20

Source : rapport d'élaboration de la Cartographie des risques des processus du CESAG

Ci-dessous, se trouve les menaces liées à la sécurité du réseau :

Tableau 3 : Risques liés au réseau

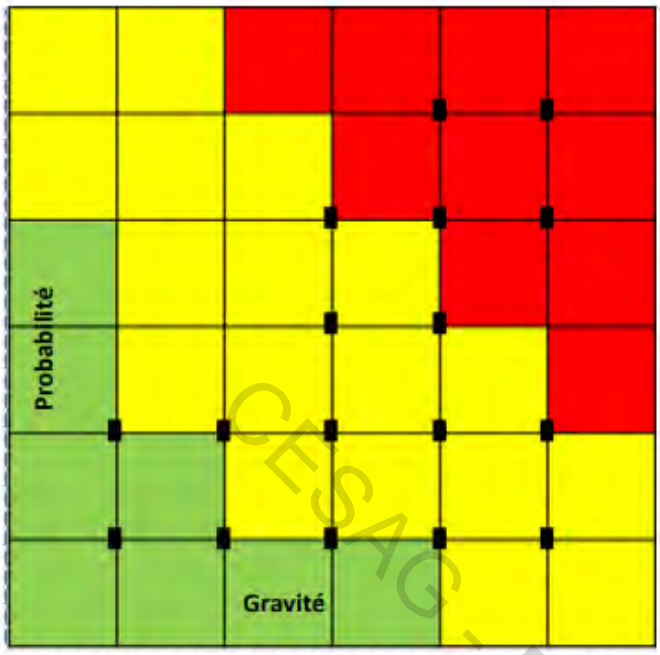
		Niveau de risque brut			Niveau de risque résiduel
N°	**Libellé du Risque**	**Probabilité (P) du risque (1 à 6)**	**Gravité (G) du risque (1 à 6)**	**Criticité du risque (P x G = C/36)**	**Criticité du risque (P x G = C/36)**
1	Risques d'intrusion dans le réseau, de disponibilité des ressources.	4	6	24	24
2	Risques liés au changement et à la prise en des évolutions futures (Politiques statiques)	3	5	15	15
3	Cumul de fonctions entrainant des risques d'erreur, des lourdeurs dans de l'exécution des tâches.	3	3	9	9
4	non visibilité des activités liées à la sécurité réseau par la Direction entrainant des risques de négligences et de démotivations	3	3	9	9
5	Risques d'interférence dans la mise en œuvre des projets avec la politique globale de sécurité.	2	3	6	6
6	Risques liés aux accès non autorisés aux ressources du réseau	3	6	18	18
7	Risques liés à l'intégrité des données	5	6	30	30
8	Risques liés à la répudiation, la traçabilité des actions sur les ressources du réseau	2	6	10	12

Source : nous-même avec approbation du RSI

3.3.2. Matrice des risques résiduels du SI

Les risques identifiés ont été qualifiés comme l'indique la figure ci-dessous :

Figure 13 : Matrice des risques



PROCESSUS « SYSTÈME D'INFORMATION »

- Nombre de sous processus : N/A
- Nombre de risques : 61

- Risques critiques (18-36) : 10
- Risques sensibles (5-16) : 21
- Risques faibles (1-4) : 30

- Indice de criticité : 22%

- Probabilité moyenne : 2,18
- Gravité moyenne : 3,25
- Criticité moyenne : 7,08

Commentaires :

Le processus « Système d'information » comporte au total 61 risques dont 16,40% représente des risques critiques. Il s'agit du processus qui présente le plus grand nombre de risques critiques au sein du macro processus; ce qui s'explique par la faiblesse des contrôles mis en place au niveau de ce processus qui reste en réalité l'un des processus majeur de l'organisation.
Aussi, la gravité moyenne de 3,25 est une alerte sur l'impact considérable lors de la survenance des risques de ce processus.

Source : rapport d'élaboration de la Cartographie des risques des processus du CESAG

3.4. Gestion de la sécurité du réseau informatique

La gestion de la sécurité du réseau informatique est organisée autour des activités suivantes :

- la maintenance informatique préventive permettant d'assurer un contrôle des équipements informatiques afin de prévenir toute dégradation ou panne inattendue et le bon fonctionnement du matériel informatique présent sur le réseau ;
- les câbles électriques ou de télécommunications transportant des données sont protégés contre toute interception ou dommage ;

- tout matériel équipé des supports de stockage est contrôlé en cas de mise au rebut afin que toutes les données à caractère personnel soient supprimées de manière sécurisée. Si ce matériel contient des données à caractère personnel sensibles, des mesures spécifiques sont prises pour détruire physiquement ce matériel ou supprimer les informations au moyen de techniques qui rendent impossible toute récupération.
- le firewall FORTIGATE 300 C a été installé afin de se protéger contre tout incident ou plusieurs évènements qui concourent à menacer la sécurité du réseau ;
- former l'utilisateur sur les étapes à suivre afin d'atténuer la propagation d'une infection (virus informatique) dans le réseau ;
- la sauvegarde est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique ;
- des copies de sauvegarde des informations et logiciels sont réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue ;
- empêcher les accès non autorisés aux services disponibles sur le réseau. Une politique relative à l'utilisation du réseau devrait être conçue à cet effet ;
- Il est attribué à chaque utilisateur un identifiant unique et exclusif. Il est exigé que le mot de passe soit tenu secret pour éviter qu'un tiers non autorisé puisse accéder à la ressource ou au service réseau ;
- contrôler et de protéger physiquement les supports afin d'empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) des biens et l'interruption des activités de l'organisme ;

Dans le tableau qui suit, se résume le résultat de l'étude de la gestion de la sécurité du réseau.

Tableau 4 : Résultat du diagnostique

	Opérationnel	Fonctionnel	Organisationnel
Satisfaisant	Inventaire des biens Maintenance informatique préventive Contrôle d'accès réseau Authentification et identification	Personnel compétent	Sortie des actifs du SI Mise au rebut des actifs SI Gestion de projet SI
A améliorer	Sécurité du câblage Atténuation des menaces Atténuation des incidents Réalisation de sauvegarde Manipulation des supports	Gestion du système d'information Politique de sauvegarde Soutien opérationnel aux utilisateurs Elaboration des stratégies informatiques Conception et réalisation des études évolutives de l'informatique	Investissement SI Choix technologique Place du SI au sein de l'organisation Prise en compte des recommandations des missions d'audit
Critique	Réaction en cas d'infection	Effectif adéquat Cumul de poste	Formalisation de la cartographie du SI Fréquence des missions d'audit SI

Source : nous-même avec approbation du RSI

Conclusion du troisième chapitre

La description du réseau informatique du CESAG, a permis de comprendre le fonctionnement de ce dernier et les différents dispositifs mis en place pour assurer sa sécurité. Au regard de cette description, il ressort que, bien que le Service Informatique dans son organisation arrive à gérer la sécurité du réseau, il n'en demeure pas moins de souligner que cette pratique n'est pas formellement soutenue par une documentation écrite dédiée à la gestion de la sécurité réseau. Il convient de remarquer également que la Direction Générale devrait s'impliquer davantage dans de système de management de la sécurité du SI et de production de documents pouvant l'orienter dans sa stratégie de sécurité.

Toutes ces raisons nous amènent à doter la Direction Générale d'une PSSI qui traduirait sa vision stratégique en matière de sécurité.

CHAPITRE 4 : ELABORATION DE LA PS

Le chapitre précédent nous a permis de prendre connaissance de la description du réseau informatique, de la façon dont celui-ci est administré et le dispositif mis en œuvre pour assurer sa sécurité. Dans ce dernier chapitre, il est question de dérouler notre démarche d'élaboration de la PSSI. Il s'agira ici de définir l'objectif et le périmètre de la PS, à la suite desquels nous définiront également puis de de recenser l'ensemble des éléments qui compose le réseau, d'identification et qualification des risques associés au réseau et de choisir les mesures de sécurité adéquates au management de la sécurité du réseau.

4.1. Objectif

Cette politique couvre tout le système réseau, équipements de communications, applications et logiciels et dispositifs de sécurité. Tous les événements liés à la sécurité du réseau doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.

Tous les rapports de failles de sécurité ou évènements relatifs aux biens informationnels du CESAG sont concernés par la présente politique. En plus, les faiblesses et les anomalies détectées au niveau du système réseau doivent être traitées conformément à la présente politique.

Tous les utilisateurs doivent adopter l'utilisation de cette politique et sont responsables d'assurer la sécurité et la sûreté de l'infrastructure réseau qu'ils utilisent ou manipulent.

4.2. Périmètre

Cette politique s'applique à tous les employés de la société CESAG ainsi qu'à toute l'infrastructure.

4.3. Rôles et responsabilité

Le tableau ci-dessous présente les différents acteurs concernés par cette politique.

Tableau 5 : Identification des acteurs avec leurs rôles et responsabilité

Pratique de gestion clé	*Direction Générale*	*Direction de la formation*	*Directeur des Ressources Pédagogiques*	*Responsable du Service Informatique*	*Administrateur Réseaux et Systèmes*	*Technicien Réseau*	*Utilisateur*
Définir, diffuser la stratégie, les politiques au sein de l'organisation et aligner la structure du SI avec les objectifs de l'organisation.	A	C	C	R	I	I	I
Établir des normes, des politiques et un cadre de management de la sécurité	A	C	C	R	I	I	I
Évaluer les risques, les atténuer efficacement, et les rendre transparents pour les parties prenantes.	C	C	C	R	I	I	I
Veiller à la gestion et à la vérification au quotidien des processus d'administration réseau.	I	I	I	A	R	C	I
Veiller à la gestion et à la maintenance au quotidien des moyens du réseau.	I	I	I	A	C	R	I

R : personne Responsable

A : personne qui Approuve

C : personne Consultée

I : personne Informée

4.4. Règles générales de sécurité

Les règles suivantes s 'appliquent à l'ensemble du réseau du CESAG et à ses composants

- Schéma réseau

Le CESAG doit maintenir son schéma de réseau actuel, illustrant les flux des données, celui-ci doit indiquer toutes les connexions aux données.

Ce schéma doit être tenu à jour : il doit être modifié suite à tout changement du réseau et être contrôlé une fois par trimestre.

- Configuration des équipements

Les configurations des équipements réseau doivent être sécurisées telle que décrite dans les documents correspondants :

- Standard de configuration des switchs et routeurs
- Standard de configuration des firewalls

L'application de ces règles de durcissement de configuration doit faire l'objet d'un compte-rendu conformément à la procédure de gestion du changement

- Architecture des Firewalls

Il est obligatoire d'installer un pare-feu au niveau de chaque connexion internet et entre toute zone démilitarisée (DMZ) et la zone de réseau interne.

- Règles de filtrage

Les règles de filtrage sont les suivantes :

- Restreindre le trafic entrant et sortant au trafic strictement nécessaire ;
- Certains protocoles sont réputés non- fiables pour des échanges sur internet. A l'inverse, certains protocoles sont jugés acceptables pour une communication vers l'externe ;
- Déployer une zone démilitarisée pour limiter le trafic entrant et sortant aux seuls protocoles nécessaires ;
- Limiter le trafic internet entrant aux adresses IP dans la zone démilitarisée ;
- N'autoriser aucun acheminement direct entrant ou sortant du trafic entre internet et le LAN ;
- Appliquer des masques IP pour empêcher la conversion des adresses internes et leur divulgation sur internet.

- Modification réseau

Toute modification sur le réseau doit être réalisée conformément aux règles de gestion du changement dans la procédure correspondante.

- Réseau sans fil

Tout réseau sans fil (Wi-Fi, radio, GSM…) fait l'objet d'un contrôle d'accès dans les infrastructures du CESAG. Des tests semestriels doivent être effectues pour contrôler qu'aucune borne d' accès Wi-Fi n'a été installée

- Revue périodique des règles de filtrage

Il est obligatoire d'examiner les règles des pares-feux et des routeurs au moins tous les six mois

4.5. Règles de sécurité

La déclinaison des exigences de sécurité se présentent comme suit :

Tableau 6: Règles de sécurité

Mesures / Règles de sécurité 1/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
1 Gouvernance du SI à mettre en évidence	1,1	Orientations de la direction en matière de sécurité du SI ***Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.***
	1.1.1	Veiller à la mise en œuvre de la présente politique de sécurité du réseau informatique *Un ensemble de politiques de sécurité du SI et spécifiquement celui du réseau doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.*
	1.1.2	Revue des politiques de sécurité *La politique de sécurité doit être revue à intervalles programmés ou en cas de changements majeurs pour garantir sa pertinence, son adéquation et son effectivité dans le temps.*
2 Organisation de la sécurité réseau	2,1	Organisation interne ***Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité du réseau au sein de l'établissement.***
	2.1.1	Fonctions et responsabilités liées à la sécurité de l'information *Toutes les responsabilités en matière de sécurité du réseau doivent être définies et attribuées.*
	2.1.2	Séparation des tâches *Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'établissement.*
	2.1.3	Relations avec les autorités *Des relations appropriées avec les autorités compétentes doivent être entretenues.*
	2.1.5	La sécurité du réseau dans la gestion de projet *La sécurité du réseau doit être considérée dans la gestion de projet (intégration ou amélioration du SI), quel que soit le type de projet concerné.*

Mesures / Règles de sécurité 2/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
3 Contrôle d'accès	3,1	Exigences métier en matière de contrôle d'accès ***Limiter l'accès au réseau, à l'information et aux moyens de traitement de l'information.***
	3.1.1	Politique de contrôle d'accès au réseau *Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité.* *Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation.*
	3,2	Gestion de l'accès utilisateur *Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés au réseau*
	3.2.1	Enregistrement et désinscription des utilisateurs *Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.*
	3.2.2	Distribution des accès utilisateurs *Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble du réseau.*
	3.2.3	Gestion des droits d'accès à privilèges *L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.*
	3.2.4	Gestion des informations secrètes d'authentification des utilisateurs *L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.*
	3.2.5	Revue des droits d'accès utilisateurs *Les propriétaires d'actifs (ordinateur, serveurs, réseau) doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.*
	3.2.6	Suppression ou adaptation des droits d'accès *Les droits d'accès aux informations et au réseau de l'ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.*
	3,3	Responsabilités des utilisateurs ***Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.***
	3.3.1	Utilisation d'informations secrètes d'authentification *Les utilisateurs doivent suivre les pratiques établies pour l'utilisation des informations secrètes d'authentification.*

Mesures / Règles de sécurité 3/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
3 Contrôle d'accès	3.4.2	Sécuriser les procédures de connexion *Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.*
	3.4.3	Système de gestion des mots de passe *Le système qui gère les mots de passe doit être interactif et doit garantir la qualité des mots de passe.*
	3.4.4	Utilisation de programmes utilitaires à privilèges *L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.*
4 Sécurité physique et environnementale	4,1	Zones sécurisées ***Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'ensemble de l'installation réseau.***
	4.1.1	Périmètre de sécurité physique *Des périmètres de sécurité doivent être définis et respectés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.*
	4.1.2	Contrôle d'accès physique *Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.*
	4.1.3	Sécurisation des bureaux, des salles et des équipements *Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.*
	4.1.4	Protection contre les menaces extérieures et environnementales *Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.*
	4,2	Matériels ***Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'établissement.***
	4.2.1	Emplacement et protection du matériel *Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.*
	4.2.2	Services généraux *Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux.*

Mesures / Règles de sécurité 4/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
4 Sécurité physique et environnementale	4.2.3	Sécurité du câblage *Les câbles électriques et du réseau filaire doivent être protégés contre toute interception ou tout dommage.*
	4.2.4	Maintenance du matériel *Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité.*
5 Sécurité logique et des données	5,1	Protection contre les logiciels malveillants ***S'assurer que le réseau et les données sont protégés contre les logiciels malveillants.***
	5.1.1	Mesures contre les logiciels malveillants *Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.*
	5,2	Sauvegarde ***Se protéger de la perte de données.***
	5.2.1	Sauvegarde des informations *Des copies de sauvegarde de l'information, des logiciels et d'autres données doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.*
	5,3	Journalisation et surveillance ***Enregistrer les événements et générer des preuves.***
	5.3.1	Journalisation des événements *Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.*
	5.3.2	Protection de l'information journalisée *Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé.*
	5.3.3	Journaux administrateur et opérateur *Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.*
	5.3.4	Synchronisation des horloges *Les horloges de l'ensemble des systèmes de traitement de l'information concernés de l'établissement ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.*

Mesures / Règles de sécurité 5/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
5 Sécurité logique et des données	5,4	Maîtrise des logiciels en exploitation ***Garantir l'intégrité des systèmes en exploitation.***
	5.4.1	Installation de logiciels sur le réseau *Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur le réseau.*
	5,5	Gestion des vulnérabilités techniques ***Empêcher toute exploitation des vulnérabilités techniques.***
	5.5.1	Gestion des vulnérabilités techniques *Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.*
	5.5.2	Restrictions liées à l'installation de logiciels *Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.*
	5,6	Considérations sur l'audit des systèmes d'information spécifiquement l'audit du réseau informatique ***Réduire au minimum l'impact des activités d'audit sur le réseau***
	5.6.1	Mesures relatives à l'audit du réseau *Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.*
6 Sécurité des communications	6,1	Gestion de la sécurité du réseau ***Garantir la protection de l'information sur le réseau et des moyens de traitement de l'information sur lesquels elle s'appuie.***
	6.1.1	Contrôle du réseau *Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.*
	6.1.2	Sécurité des services de réseau *Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.*
	6.1.3	Cloisonnement des réseaux *Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux.*

Mesures / Règles de sécurité 6/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
6 Sécurité des communications	6,2	Transfert de l'information ***Maintenir la sécurité de l'information transférée au sein de l'organisme et vers une entité extérieure.***
	6.2.1	Politiques et procédures de transfert de l'information *Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.*
	6.2.2	Accords en matière de transfert d'information *Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.*
	6.2.3	Messagerie électronique *L'information transitant par la messagerie électronique doit être protégée de manière appropriée.*
	6.2.4	Engagements de confidentialité ou de non-divulgation *Les exigences en matière d'engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.*
7 Gestion des incidents liés à la sécurité de l'information	7,1	Gestion des incidents liés à la sécurité de l'information et améliorations ***Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité du réseau.***
	7.1.1	Responsabilités et procédures *Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.*
	7.1.2	Signalement des événements liés à la sécurité du réseau *Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.*
	7.1.3	Signalement des failles liées à la sécurité du réseau *Les utilisateurs doivent noter et signaler toute faille de sécurité observée ou soupçonnée sur le réseau.*
	7.1.4	Appréciation des événements liés à la sécurité du réseau et prise de décision *Les événements liés à la sécurité du réseau doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité du réseau.*

Mesures / Règles de sécurité 7/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
7 Gestion des incidents liés à la sécurité de l'information	7.1.5	Réponse aux incidents liés à la sécurité du réseau *Les incidents liés à la sécurité du réseau doivent être traités conformément aux procédures documentées.*
	7.1.6	Tirer des enseignements des incidents liés à la sécurité du réseau *Les connaissances recueillies à la suite de l'analyse et de la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.*
	7.1.7	Collecte de preuves *Il doit-être défini et appliqué des procédures d'identification, d'analyse et de de gestion des risques visant protéger le réseau en cas de contrôle.*
8 Aspects de la sécurité du réseau dans la gestion de la continuité de l'activité	8,1	Continuité de la sécurité de l'information ***La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité.***
	8.1.1	Organisation de la continuité de la sécurité du réseau *Le CESAG doit déterminer ses exigences en matière de sécurité du réseau et de continuité d'exploitation du réseau dans des situations défavorables, comme lors d'une crise ou d'un sinistre.*
	8.1.2	Mise en œuvre de la continuité de la sécurité du réseau *Le Service doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité du réseau au cours d'une situation défavorable.*
	8.1.3	Vérifier, revoir et évaluer la continuité de la sécurité du réseau *Le Service doit vérifier les mesures de continuité de la sécurité du réseau mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables.*

Mesures / Règles de sécurité 8/8		
Thématiques	**Id**	**Objectif / Mesures & Règles de sécurité**
9 Conformité	9,1	Conformité aux obligations légales et réglementaires ***Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité du réseau, éviter toute violation des exigences de sécurité.***
	9.1.1	Identification de la législation et des exigences contractuelles applicables *Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par le CESAG pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour.*
	9.1.2	Droits de propriété intellectuelle (DPI) *Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.*
	9.1.3	Protection des enregistrements *Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.*
	9.1.4	Protection de la vie privée et protection des données à caractère personnel *La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.*
	9,2	Revue de la sécurité réseau ***Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.***
	9.2.1	Revue indépendante de la sécurité du réseau *Des revues régulières et indépendantes de l'approche retenue pour gérer et mettre en œuvre la sécurité du réseau (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité du réseau) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.*
	9.2.2	Conformité avec les politiques et les normes de sécurité *Les responsables doivent régulièrement vérifier la conformité aux procédures de management de la sécurité dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.*
	9.2.3	Vérification de la conformité technique *Le système d'information (réseau) doit être examiné régulièrement quant à sa conformité avec les politiques et les normes de sécurité définies.*

4.6. Revue de la politique

La présente politique de sécurité doit être maintenue à jour, il peut être révisé autant de fois que nécessaire mais au moins une fois par an.

Conclusion du quatrième chapitre

Ce dernier chapitre a été consacré à la formulation de la PS du réseau informatique du CESAG suivant la méthodologie de travail décrite au chapitre 2.

À travers le diagnostic de l'existant, nous avions pu identifier les menaces auxquels est exposé le réseau. La PS vient donc en réponse comme dispositif de sécurité.

Conclusion de la deuxième partie

La description du réseau informatique du CESAG présentée dans le chapitre 3 a permis de comprendre son fonctionnement et de prendre conscience des menaces encourues. Cette description a été le socle des exigences de sécurité mises en place dans le chapitre 4.

Cette partie de notre étude nous a permis de conforter notre compréhension de la gestion de la sécurité du réseau et d'approfondir nos connaissances des mesures de sécurité des SI en générale et des réseaux informatiques en particulier.

Ainsi, à travers notre approche par les risques, nous avions formulé une politique de sécurité répondant aux attentes de sécurités du réseau et adaptée au contexte du CESAG.

CONCLUSION GENERALE

La PS donne des orientations sur la stratégie de gestion de la sécurité. C'est un référentiel par lequel les dirigeants s'assurent que la stratégie de la sécurité de leur SI s'aligne avec la stratégie générale de l'organisation.

Au démarrage de cette étude, l'objectif principal était de doter du CESAG un manuel de gouvernance et de gestion de la sécurité de son réseau informatique. La conception de ce manuel s'est appuyée sur le processus de gestion de la sécurité mis en œuvre par le Service Informatique. Et ce, afin de fournir un outil en adéquation avec les besoins et les enjeux de la sécurité du SI.

En réponse à cet objectif, nous avions mené une étude préalable portant sur la revue de la littérature relative à notre thématique. Ce qui nous a permis de mieux cerner les notions et la méthodologie à adopter afin de concevoir notre PS. Dans la deuxième partie de notre étude, nous avions mis en application les éléments évoqués dans la première partie à travers la description de l'existant du réseau informatique du CESAG et le déroulement de notre démarche. Cette dernière partie a favorisé la compréhension du processus de gestion de la sécurité réseau et surtout d'évaluer les risques qui pèsent sur le réseau informatique et plus largement sur le SI. Grâce à des outils de méthodologie, une analyse des risques portant sur l'ensemble du SI de façon générale et sur le réseau informatique en particulier, nous avions pu formuler une politique de sécurité qui permettra aux dirigeants d'avoir une meilleure vue quant à la gouvernance de leur SI et au Service Informatique une boussole pour la gestion de la sécurité.

Les professionnels de la sécurité affirment qu'on ne peut piloter efficacement la sécurité d'un SI sans une PS. A ce jour, nous pouvons dire que notre établissement dispose désormais d'un instrument formel du pilotage de la sécurité de son SI, en l'occurrence de son réseau informatique.

Cependant, cette étude représente une infirme partie de la PS de l'ensemble du SI. Des PS des autres composantes du SI de notre établissement devraient être conçues afin d'avoir une PS générale. Aussi, c'est un travail qui demande à être corrigé, amélioré, enrichi et développé par d'autres études dans l'optique d'une amélioration continue.

ANNEXES

Annexe 1 : Inventaire du matériel informatique

Catégorie	Désignation	Emplacement	Nombre
ORDINATEUR	ORDINATEURS DE BUREAU POUR LE PERSONNEL	Bureaux	71
	ORDINATEURS POUR LES BESOINS DE LA FORMATION	Laboratoires informatiques	98
	ORDINATEURS POUR LES COURS	Salles de cours	22
ONDULEUR	ONDULEUR	Bâtiment C	1
	ONDULEUR MERLIN GUERIN	Salle des serveurs 305	1
	ONDULEUR MGE GALAXY 300	MBF pour la salle des marchés	1
	ONDULEUR	Salle E1 incubateur	1
	ONDULEUR APC	Salle des serveurs	1
	SYSTEME D'AUTONOMIE DE BATTERIE ETANCHE	Salle de Serveurs	1
SCANNER	HP SCANJET 5700	Bureau 304	1
	HP SCANJET	Bureau Scolarité (Lamine)	1
	SCAN JET PROFESSIONNEL	Bureau Scolarité (Joël DIEHIOU)	1
	SCAN JET PROFESSIONNEL	Chantal OUEDRAOGO	1
	SCAN JET PROFESSIONNEL	Salle Numérisation	1
	SCAN JET PROFESSIONNEL	Salle Numérisation	1
	SCAN JET PRODUCTION	Salle Numérisation	1
	SCANNER EPSON GT55N/DS-560	CESAG exécutive (Mously SEYE)	1
	SCANNER EPSON GT55N/DS-560	CESAG grande école (Agnès SARR)	1
	SCANNER EPSON GT55N/DS-560	CESAG langues (Emma SOKOBA)	1
	SCANNER EPSON GT55N/DS-560	DRC (Aby SANE)	1
	SCANNER EPSON GT55N/DS-560	CESAG -PRO	1
	SCANNER EPSON GT55N/DS-560	Lionnel DASILVEIRA	1
SERVEUR	SERVEUR PHYSIQUE	Salle des serveurs	8
	SERVEUR VIRTUEL		16
	BAIE DE STOCKAGE		2

Annexe 2 : Inventaire des logiciels

Catégorie	Désignation	Nombre de licence
Logiciels Microsoft Windows	Licences Windows 7	225
	Licences Windows 2008 Serveur	5
	Licences Microsoft office 365 2016	100
	Licences Microsoft Office 365 pour les étudiants	2000
Logiciels Sage Sari i7 sous SQL	COMPTABILITÉ	10
	IMMOBILISATION	10
	GESCOM	10
	PAIE	2
Logiciels d'analyse de Données	SPSS	15
	SPHINX	24
	EPI INFO	illimité
	R	illimité
Logiciels de Gestion budgétaire	PHEB	10
	Gestion budgétaire sous Access	illimité
Pare feu	FortiGate 300 C.	1

Annexe 3: Identification des acteurs basé sur COBIT 5

Tableau RACI (Responsable Approbateur Consulté et Informé)							
Pratique de gestion clé	*Acteur 1*	*Acteur 2*	*Acteur 3*	*Acteur 4*	*Acteur 5*	*Acteur 6*	*Acteur 7*
Activité 1	A	C	C	R	I	I	I
Activité 2	A	C	C	R	I	I	I
Activité 3	C	C	C	R	I	I	I
Activité 4	I	I	I	A	R	C	I
Activité 5	I	I	I	A	C	R	I

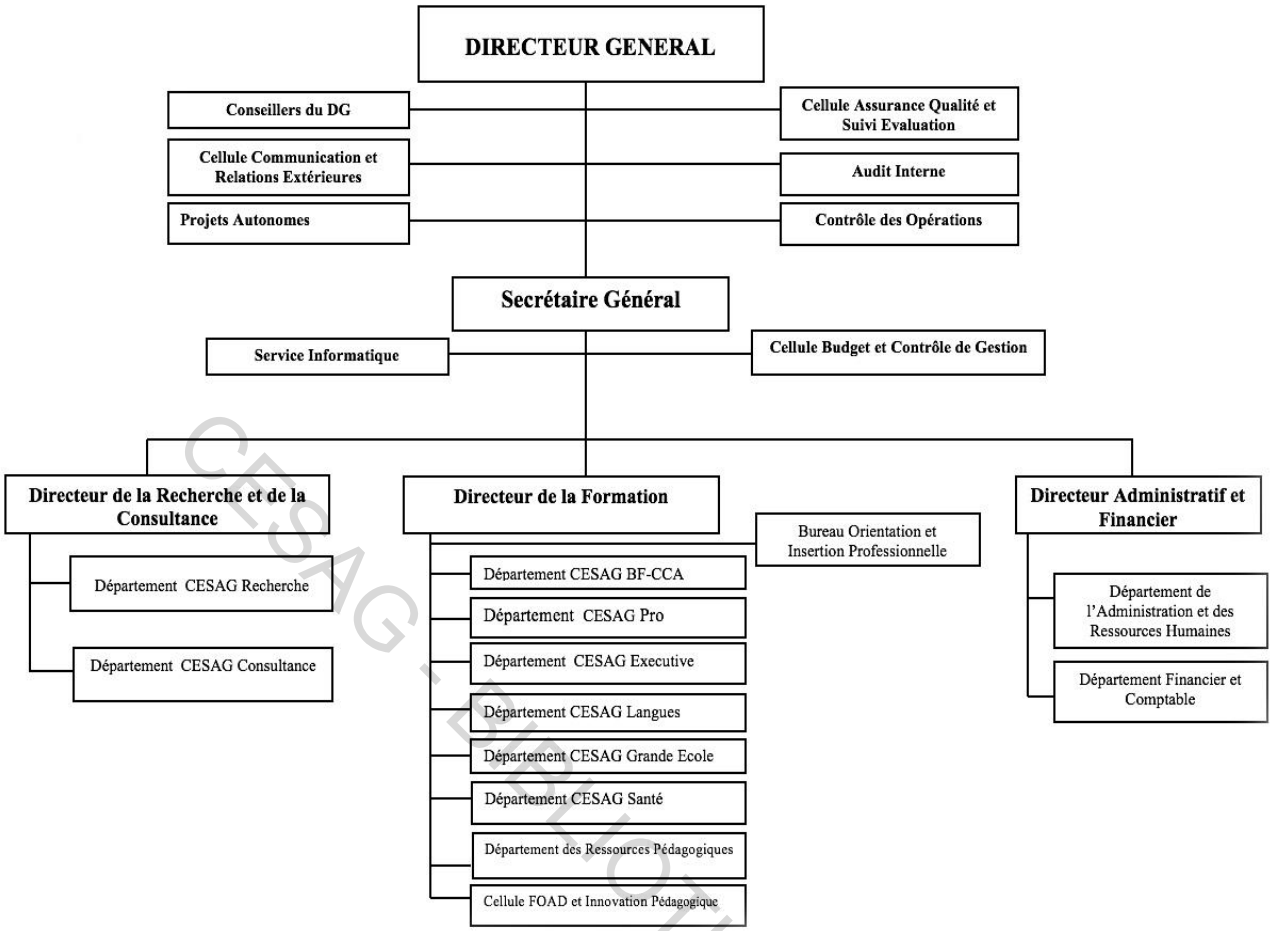
R : personne Responsable

A : personne qui Approuve

C : personne Consultée

I : personne Informée

Annexe 4: Organigramme fonctionnel du CESAG



Annexe 5 : Guide d'entretien

Les enjeux de la sécurité

1. Quelles peuvent-être les conséquences liées à la sécurité du réseau ?
2. Quel sont les points faibles du réseau ? quelle analyse faites-vous de ces risques ?
3. Contre quels risques allez-vous vous protéger exactement ? Où se situent la plupart des risques ?
4. Quel est le rôle de la direction par rapport à la sécurité du SI ?
5. Comment la direction s'assure-t-elle qu'elle possède les compétences, les connaissances et le savoir-faire appropriés pour la sécurité du SI ?
6. Quelle est la place de la sécurité du SI dans la stratégie d'entreprise actuelle ?
7. Comment la Direction envisage-t-elle la structure d'un de sécurité ?
8. Comment la valeur et la contribution du SI de l'organisation sont-elles définies et évaluées ?
9. Comment surveille-t-on et évalue-t-on les risques et tendances, ainsi que leur influence potentielle sur l'organisation ?
10. En quoi une politique de sécurité est-elle un facteur indispensable ?

Fixer les objectifs de la PS

1. Qui sera responsable de la sécurité du réseau ?
2. De quoi doit-on tenir compte pour que la politique de sécurité soit parfaitement harmonisée aux processus de l'entreprise ?
3. A quelle fréquence évaluez-vous les risques liés à la sécurité ?
4. A quel niveau de vulnérabilité se situez-vous le réseau sur une échelle de 1 à 4 ?
5. Quel niveau de sécurité souhaitez avoir ?
6. Qu'attendez-vous de la politique de sécurité ?

Fixer les exigences de sécurité applicable

1. Quelles méthodes d'authentification des utilisateurs employez-vous ?

Comment les mots de passe sont-ils attribués ? Existe-t-il un risque pour que les mots de passe soient transmis oralement, soient empruntés, voire volés ?

La gestion des mots de passe est-elle rigoureuse (Chaque utilisateur dispose-t-il d'un mot de passe ? Le mot de passe comporte-t-il au minimum 8 caractères dont un numérique, un alpha numérique, une majuscule et minuscule ? Est-il changé tous les 30 ou 60 jours?

2. Comment jugez-vous l'efficacité de la méthode d'authentification ?
3. Certaines ressources sont-elles interdites d'accès à certains employés ou enseignants et prestataires ? Si oui, lesquelles ?

4. Faut-il surveiller ou restreindre l'accès à certaines ressources ou périphériques sensibles, ou bien faut-il identifier les utilisateurs ayant accédé à certaines ressources pendant une période donnée ?
5. Le réseau est-il ouvert à des intervenants extérieurs ?
6. Certaines données pourraient-elles être utilisées contre la société si elles tombaient entre des mains hostiles ?
7. Possède-t-on une licence pour chacun des logiciels utilisés sur le réseau ?
8. En cas de connexions externes, les ports sont-ils protégés par un système de rappel automatique ?

Sécurité physique

9. L'ensemble des composants réseaux sont-ils correctement répertoriés dans un outil de gestion de parc ?
10. Les ordinateurs sont-ils actuellement protégés contre les virus ?
11. Comment contrôler en permanence les anomalies survenant sur votre réseau et comment réagir immédiatement et de façon adéquate ?
12. Un plan de secours a-t-il en cours d'élaboration ? Ce plan couvrira-t-il tous les systèmes du réseau ?
13.L'emplacement des serveurs sont-ils dotés d'un système de régulation thermique et d'une alimentation de secours ?
14. Comment comptiez-vous organiser une supervision régulière et efficace des mesures de sécurité prises ?
15. Le système d'exploitation réseau dispose-t-il d'outils de surveillance intégrés ?
16. Qui sera responsable de la surveillance du comportement du réseau ?

Sécurité logique

17. Quelles sont les contraintes du pare-feu ?
18. Un pare-feu est-il suffisant ou vous faut-il davantage ?
19. Où se situent les problèmes de sécurité dans l'usage de la messagerie électronique ?
20. Comment sécurisez-vous les transactions Web ?

Gestion des données

21. Les données sont-elles régulièrement sauvegardées ?
22. Les données du serveur sont-elles rigoureusement répliquées ?
23. Les fichiers obsolètes sont-ils régulièrement purgés ?
24. Le système de sauvegarde est-il régulièrement testé pour vérifier sa qualité ?

Annexe 6: Questionnaire d'entretien des rôles et responsabilités dans le MSSI

Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Réponse fournie
A. ORGANISATION ET PILOTAGE				
Un organigramme de la fonction informatique est-il formalisé et actualisé de manière régulière ?	Connaissance des parties prenantes afin d'apprécier la maîtrise de : • Rôles et responsabilités des actions et des contrôles • Séparation des tâches	Chef de service	OUI	OUI
Le management de la fonction informatique est attribué à une personne dédiée ?	• Centralisation des décisions en lien avec la stratégie de l'entreprise • Mise en place de points de contrôle et de reporting par la direction	Chef de service	OUI	OUI
Si oui, à qui est rattachée hiérarchiquement cette personne ?	Identification du niveau de contrôle	Chef de service	DG	DG
Un responsable de la sécurité informatique est nommé au sein de l'organisation ?	Maîtrise et coordination des actions de sensibilisation et de surveillance de la sécurité de l'information	DG	Comité d'audit ; audit interne ; DG	RSI
Le directeur financier a défini des points de contrôle permettant de superviser la production de l'information comptable et financière ?	Apprécier le niveau de maîtrise du système d'information par le directeur financier	DFC	OUI	NON
B. MANAGEMENT ET RESPONSABILITÉ				
Les fiches de poste des collaborateurs en charge de la fonction informatique sont-elles formalisées ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH	OUI	OUI
Les fiches de postes des managers précisent-elles leur responsabilité relative au système d'information ?	Maîtrise des RACI Principe de non-répudiation renforcée	DRH	OUI	OUI
Pour chaque application, un responsable d'application est-il nommé ?	Maîtrise du fonctionnement des applications et de leur évolution	DFC, RSI, DG, Direction métier	OUI	NON
Pour chaque donnée critique, un propriétaire de données est-il nommé ?	Maîtrise des inventaires, des flux et des traitements de données	DAF, RSI, DG, Direction métier	OUI	NON

Annexe 7: Questionnaire d'entretien du contrôle interne des SI

Question	Enjeu / Risque associé	Interlocuteur cible	Réponse attendue	Réponse fournie
Existe-t-il une matrice de définition des rôles utilisateurs dans l'entreprise ?	Séparation des fonctions	RSI	OUI	OUI
Les autorisations d'accès font-elles l'objet de revues qualitative et quantitative ?	Analyse des comportements des utilisateurs dans le cadre de la prévention des fraudes	RSI	OUI	NON
Les demandes d'évolution sur le SI financier sont-elles tracées ? Si oui, comment ?	Vérification des autorisations accordées en lien avec chaque modification pour prévenir l'introduction de biais dans les applications	RSI	OUI	NON
Qui met en oeuvre les évolutions ? Suivant quelle procédure ?	Revue des rôles et responsabilités en lien avec la surveillance du respect de la séparation des fonctions	RSI	RSI	RSI
Les procédures de sauvegarde sont-elles formalisées ? Si cloud, les clauses contractuelles sont-elles conformes aux besoins de l'entreprise (RPO, RTO) ?	Garantie de reprise et de continuité d'activité	RSI et DFC	OUI	OUI
Des tests de restauration sont-ils menés ? Sur quel périmètre, avec quelles parties prenantes et avec quelle fréquence ?	Garantie de reprise et de continuité d'activité	RSI et DFC	OUI	NON
Une cartographie du système d'information est formalisée et maintenue à jour de manière régulière ?	• Connaissance des applications sources et des traitements • Maitrise des risques liés aux évolutions du SI	RSI et/ou DFC	OUI	OUI

BIBLIOGRAPHIE

Ouvrages

1. REIX R. (1998), *Systèmes d'information et management des organisations*,
2. GHERNAOUTI Solange (2016), *Cybersécurité, Sécurité informatique et réseaux*, Dunod, 384 pages
3. DELMOND Marie-Hélène & al. (2008), Dunod,
4. LAFITTE Michel (2003), *Sécurité des systèmes d'information et maîtrise des risques*, RB édition, 128 pages
5. FORAY Bernard (2011), *La fonction RSSI, Guide des pratiques et retours d'expérience,* Dunod, 350 pages
6. SORNET Jacques, HENGOAT Oona, LE GALLO Nathalie (2016), *Systèmes d'information de gestion*, Dunod, 457 pages
7. FERNANDEZ-TORO Alexandre (2016), *Sécurité opérationnelle,* Eyrolles, 442
8. GHERNAOUTI Solange (2016), *Cybersécurité, Sécurité informatique et réseaux,* Dunod, 384 pages
9. SOUILLE Arnaud, KOKOS Ary, BILLOIS Gérôme (2016), *Sécurité informatique Pour les DSI, RSSI et administrateurs*, Eyrolles, 645 pages
10. LLORENS Cédric, LEVIER Laurent, VALOIS Denis (2010), *Tableaux de bord de la sécurité réseau*, Eyrolles, 581 pages
11. PILLOU, Jean-François, BAY, Jean-Philippe (2013), *Tout sur la sécurité informatique,* Dunod, 272 pages
12. DELMOND Marie-Hélène, PETIT Yves, GAUTIER Jean-Michel (2010), *Management des systèmes d'information,* Dunod, 269 pages
13. NF ISO/CEI 27001 version 2013
14. PUJOLLE Guy (2018), Les réseaux : *L'ère des réseaux cloud et de la 5G - Edition 2018-2020*, Eyrolles, 805 pages
15. Claude SERVIN (2013), *Réseaux et Télécoms Ed. 4*, Dunod, 736 pages
16. Guide de l'ANSSI version 2004
17. ISACA (2012), *Cobit 5 : Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise,* 98 pages
18. ORANGE BUSINESS SERVICES (2007), *mémo :politique et gestion de la sécurité du système d'information,* 19 pages
19. DESWARTE Y. & MÉ L. (2002), *Sécurité des réseaux et systèmes répartis,* Hermès Lavoisier, 380 pages
20. Rodolphe ORTALO (1998), *Thèse : Évaluation quantitative de la sécurité des systèmes d'information*, 193 pages
21. Jacques THEVENOT (2011), *Master Systèmes d'Informations*, Eska, 536 pages

22. Michel Volle (2000), *e-commerce,* Economica, 366 pages

Webographie

1. https://fr.wikipedia.org/wiki/Politique_de_s%C3%A9curit%C3%A9_du_syst%C3%A8me_d%27information
2. https://www.ivision.fr/mettre-en-place-une-politique-de-securite-informatique-les-bonnes-pratiques/
3. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/securite_information/elaboration_politique_securite_information.pdf

TABLE DES MATIERES

DEDICACE……ii
REMERCIEMENTS iii
LISTE DES SIGLES ET ABREVIATIONS iv
LISTE DES FIGURES ET TABLEAUX vi
LISTE DES ANNEXES vi
SOMMAIRE vii
INTRODUCTION GENERALE 1
PREMIERE PARTIE : 6
REVUE DE LITTERATURE ET METHODLOGIE DE L'ETUDE 6
CHAPITRE 1 : POLITIQUE DE SECURITE D'UN SYSTEME D'INFORMATION 8
1.1. Enjeux de la sécurité du système d'information au sein d'une entreprise 9
1.1.1. Définition du système d'information 9
1.1.2. Rôle du système d'information 11
1.1.3. Sécurité des systèmes des systèmes d'information : qu'est-ce que c'est ? 12
1.1.4. Pourquoi la sécurité des SI ? 14
1.1.4.1. Enjeux stratégiques 14
1.1.4.2. Enjeux organisationnels 15
1.1.5. Le management de la sécurité d'un SI 15
1.2. Politique de sécurité 18
1.2.1. Définitions 18
1.2.2. Objectifs 18
1.3. Normes, méthodes et bonnes pratiques 19
1.3.1. ISO/IEC 27001 20
1.3.2. ISO/IEC 27002 20
1.3.3. COBIT 21
1.3.4. MEHARI 22
1.3.5. EBIOS 23
1.3.6. OCTAVE 24
CHAPITRE 2 : METHODOLOGIE ET CADRE DE L'ETUDE 26
2.1. Méthodologie de l'élaboration d'une PS 27
2.1.1. Les outils de collecte et d'analyse de données 27
2.1.1.1. L'observation physique 27
2.1.1.2. L'entretien 28
2.1.1.3. L'analyse documentaire 28

2.1.1.4. La cartographie des risques 28
2.1.2. Démarche de l'élaboration d'une PSSI 30
..... 30
2.1.2.1. Le Contexte 31
2.1.2.1.1. Préciser les enjeux de sécurité 31
2.1.2.1.2. Identifier les textes applicables 31
2.1.2.1.3. Fixer les objectifs de la PSSI 31
2.1.2.2. Définir les moyens du réseau et le champ d'application 32
2.1.2.2.1. Recenser les moyens du réseau 33
2.1.2.2.2. Champ d'application de la PSSI 33
2.1.2.3. Identifier les acteurs et qualifier les principaux risques du SI 34
2.1.2.3.1. Identification des acteurs 34
2.1.2.3.2. Identifier les principaux risques liés au SI 34
2.1.2.3.3. Préciser la stratégie de traitement des risques 34
2.1.2.4. Choisir les mesures de sécurité 35
2.1.2.4.1. Organisation des exigences et des règles 36
2.1.2.4.2. Fixer les exigences de sécurité applicables 36
2.1.2.4.3. Décliner les exigences de sécurité en règles 37
2.1.2.5. Revue de la politique de sécurité 37
2.1.3. Modèle d'analyse 37
2.2. Présentation du CESAG 39
2.2.1. Historique, Mission et Vocation 39
2.2.1.1. Historique 39
2.2.1.2. Mission 39
2.2.1.3. Vocation 40
2.2.2. Portefeuille d'activités 40
2.2.3. Gouvernance et Organisation 41
2.2.3.1. Gouvernance 41
2.2.3.2. Organisation 42
2.2.4. Présentation du service informatique 42
2.2.4.1. Composition 42
2.2.4.2. Missions 42
DEUXIEME PARTIE : 45
CADRE PRATIQUE DE L'ELABORATION DE LA POLITIQUE DE SECURITE 45
CHAPITRE 3 : DESCRIPTION DE L'EXISTANT 47
3.1. Description du réseau informatique 48
3.2. Administration du réseau informatique 52

3.3. Menaces liées à la sécurité 53
3.3.2. Cartographie des risques du SI 53
3.3.2. Matrice des risques résiduels du SI 55
3.4. Gestion de la sécurité du réseau informatique 55
CHAPITRE 4 : ELABORATION DE LA PS 59
4.1. Objectif 60
4.2. Périmètre 60
4.3. Rôles et responsabilité 61
4.4. Règles générales de sécurité 62
4.5. Règles de sécurité 64
4.6. Revue de la politique 72
CONCLUSION GENERALE 74
ANNEXE 76
BIBLIOGRAPHIE 84
TABLE DES MATIERES 86