الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MEMOIRE DE FIN D'ETUDES

Master en Management E-Gouvernement

L'impact de la sécurisation des données sur la fidélisation clients
Étude de cas : Société Nationale d'Assurances (SAA)

Elaboré par :

Mr. Chakib Racim LATROUS

Encadré par :

Dr. Sid Ali MELLOUD

Membres du jury :

Président : Dr. Hachemi MAHMOUDI

Examinateur : Dr. Mehdi BOUCHETARA

Année universitaire 2020/2021

RÉSUMÉ

Cette étude a pour objectif d'étudier l'impact de la sécurisation des données sur la fidélisation client à travers une étude quantitative, nous avons administré un questionnaire dans le but de voir si le critère de la sécurité figure parmi les facteurs qui fidélisent le client.

Nous avons choisi de mener notre recherche au sein de la société nationale d'assurance SAA qui est considérée comme le leader du marché économique algérien dans le domaine des assurances, les résultats nous ont permis de constater que le critère de sécurité n'est pas une priorité absolue du client pour le critère de fidélisation.

Mais cela n'empêche que la société doit renforcer la sécurité de ses systèmes d'information, car l'image de marque et la notoriété dépendent fortement de ce critère pour maintenir une base client.

Mots clés : impact – sécurisation des données – fidélisation client.

Abstract

The objective of this study is to study the impact of data security on customer loyalty through a quantitative study. We administered a questionnaire in order to see if the security criterion is among the factors that create customer loyalty.

We chose to conduct our research within the national insurance company SAA which is considered as the leader of the Algerian economic market in the field of insurance, the results allowed us to note that the security criterion is not an absolute priority of the customer for the loyalty criterion.

However, this does not prevent the company from strengthening the security of its information systems, as the brand image and reputation depend heavily on this criterion to maintain a customer base.

Keywords: Impact – Data security – Client loyalty.

ملخص

تهدف هذه الدراسة إلى دراسة أثر أمن البيانات على ولاء الزبائن من خلال دراسة كمية، قد قدمنا استبيانا لمعرفة ما إذا كان معيار الحماية من بين العوامل التي تبني ولاء الزبائن، واخترنا إجراء أبحاثنا في الشركة الوطنية التأمين التي تعتبر من قادة السوق الاقتصادية الجزائرية، وأتاحت لنا النتائج أن نلاحظ أن معيار الأمن ليس أولوية مطلقة للزبون بالنسبة لمعيار الولاء.

ولكن هذا لا يمنع الشركة من تعزيز أمن نظم المعلومات لأن الصورة التجارية والسمعة تعتمد بشكل كبير على هذا المعيار للحفاظ على قاعدة العملاء.

الكلمات المفتاحية: أثر – أمن المعلومات – ولاء الزبائن

REMERCIEMENTS

Tout d’abord, je tiens à remercier Dieu de m’avoir donné la volonté, le courage et la patience pour terminer ce travail.

Je tiens à remercier monsieur MELLOUD Sid Ali, qui a pris le soin de diriger ce travail.

Je remercie également tous les cadres de la société nationale d’assurances notamment ceux de la division système d’information : monsieur BENBOUZID Abdelhakim chef division des systèmes d’information, madame AMARA Radia pour son suivi et ses précieux conseils tout au long de la durée de stage, Monsieur AIT KACI Rabah pour son humble aide et ses conseils, monsieur DRICI Nacer pour son aide également, sans oublier aussi monsieur BOUDAOUD Ahcène.

Mes remerciements aussi s’adressent à tous mes amis sans exception et que la liste est longue à tous les citer, qui ont contribué de près ou de loin à l’élaboration de ce travail.

Je remercie mes très chers parents, qui ont toujours été là pour moi et qui m’ont apporté leur soutien moral tout le temps sans douter de moi.

TABLE DES MATIÈRES

RÉSUMÉ ..... **I**
REMERCIEMENTS ..... **III**
TABLE DES MATIÈRES ..... **IV**
LISTE DES TABLEAUX ..... **VII**
LISTE DES FIGURES ..... **VIII**
LISTE DES ABRÉVIATIONS ..... **IX**
INTRODUCTION GÉNÉRALE **1**
CHAPITRE 1 : PROBLÉMATIQUE **4**
1- Contexte de l'étude : **5**
1.1 Intérêt personnel : **5**
1.2 Le choix du lieu de stage : **5**
2- Question de recherche : **5**
2.1 Pertinence théorique : **6**
2.2 Pertinence managériale : **6**
3- Contexte organisationnel : **7**
3.1 Présentation de la société nationale d'assurances SAA **7**
3.2 Historique de la société nationale d'assurances **7**
3.3 Valeurs de la SAA **10**
3.4 Organigramme de la SAA : **11**
3.5 Présentation de la structure d'accueil (la division des Systèmes d'Information) **11**
3.6 Organigramme de la structure d'accueil **12**
CHAPITRE 2 : CADRE THÉORIQUE **14**
1- La revue de la littérature **15**
1.1 La sécurité comme facteur d'évolution : **15**
2- Cadre conceptuel : **21**
2.1 De la donnée à la connaissance : **22**
2.1.1 Les données : **22**
2.1.2 L'Information : **22**
2.1.3 La connaissance **22**
2.2 La gestion des risques dans les systèmes d'informations : **23**
2.3 Les fondamentaux de la gestion des risques : **24**

2.4 Définition des processus de gestion des risques : 26
2.5 La sécurité des données : 28
2.6 Les normes et standards de bonne pratiques : 29
2.7 L'évaluation de risque de sécurité de l'information : 30
2.8 La gestion stratégique de la sécurité : 30
2.9 Les types de support de stockage de données : 31
2.10 Amélioration des supports de stockage : 32
2.11 Les objectifs de la sécurité des données : 33
2.12 La Fidélisation : 35
2.12.1 La fidélisation comme facteur de la réduction des risques pour l'entreprise : 37
CHAPITRE 3 : CADRE MÉTHODOLOGIQUE 38
1- Posture épistémologique : 39
2- Approche méthodologique : 39
3- Méthode de collecte de données : 39
4- Instrument de mesure : 39
4.1 Questionnaire : 39
4.2 La structure du questionnaire : 40
5- Les échelles de mesure : 42
6- Échantillonnage : 42
6.2 Taille de l'échantillon : 42
6.3 Méthode d'échantillonnage : 42
7.1 Outil de collecte de l'information : 42
7.2 Mode d'administration : 42
7.3 Période de l'enquête : 43
7.4 Le test du questionnaire : 43
8- Traitement et analyse de données : 43
9- Les limites de la recherche : 43
CHAPITRE 4 : ÉTAT DES LIEUX ET BILAN DE LA RECHERCHE 44
1- État de l'existant du SI de la SAA : 45
1.1 Architecture physique : 45
1.2 Architecture logique 48
1.3 Base de données : 49
1.3.1 La première consolidation 49

1.3.2 La deuxième consolidation : 50

1.3.3 La récolte des données : 50

1.3.4 Intégrité des données : 50

2- Résultats et discussion : 50

2.1 Les résultats de la recherche 51

2.1.1 Répartition de l'échantillon selon le nombre de clients 52

2.1.2 Répartition de l'échantillon relatif aux raisons du choix de la compagnie : 53

2.1.3 Répartition de l'échantillon selon le type de clients : 54

2.1.4 Répartition de l'échantillon selon la durée d'assurance : 55

2.1.5 Répartition de l'échantillon selon les moyens de fidélité : 56

2.1.6 Répartition de l'échantillon selon le critère de la fidélisation : 58

2.1.7 Répartition de l'échantillon selon le sentiment de la préservation de la sécurité des données 59

2.1.8 Répartition de l'échantillon sur la volonté de changement de compagnie 60

2.1.9 Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie : 61

2.1.10 Répartition de l'échantillon selon la signification de la sécurité pour le client : 62

2.1.11 Répartition de l'échantillon sur l'efficacité des dispositifs actuels de sécurité des données : 63

2.1.12 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1 : 64

2.1.13 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2 : 65

2.1.14 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 : 66

2.1.15 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 4 : 67

2.1.16 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5 : 68

2.1.17 Répartition de l'échantillon selon le genre : 69

2.1.18 Répartition de l'échantillon selon la tranche d'âge : 70

2.1.19 Répartition de l'échantillon selon la catégorie socioprofessionnelle : 71

2.2 La discussion des résultats 73

CONCLUSION GÉNÉRALE 82

RÉFÉRENCES BIBLIOGRAPHIQUES 85

ANNEXE A : ORGANIGRAMME DE LA SAA 88

ANNEXE B : STRUCTURE DU QUESTIONNAIRE 90

LISTE DES TABLEAUX

Tableau 1 : l'historique de la SAA 7
Tableau 2: Répartition de l'échantillon selon le nombre de clients. 53
Tableau 3: Répartition de l'échantillon relatif aux raisons du choix de la compagnie 54
Tableau 4: Répartition de l'échantillon selon le type de clients 55
Tableau 5: Répartition de l'échantillon selon la durée d'assurance 56
Tableau 6: Répartition de l'échantillon selon les moyens de fidélité 57
Tableau 7: Répartition de l'échantillon sur la fidélisation 58
Tableau 8: Répartition de l'échantillon selon le sentiment de la préservation 60
Tableau 9: Répartition de l'échantillon sur la volonté de changement de compagnie 61
Tableau 10: Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie. 62
Tableau 11: Répartition de l'échantillon sur la signification de la sécurité pour le client 63
Tableau 12: Répartition de l'échantillon sur la l'efficacité des dispositifs actuels 64
Tableau 13: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1 65
Tableau 14: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2 66
Tableau 15: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 67
Tableau 16 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation 4 68
Tableau 17: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5 69
Tableau 18: Répartition de l'échantillon selon le genre 70
Tableau 19: Répartition de l'échantillon selon la tranche d'âge 71
Tableau 20: Répartition de l'échantillon selon la catégorie socioprofessionnelle 72
Tableau 21: Relation entre les variables partie 1 74
Tableau 22: Relation entre les variables partie 2 75
Tableau 23: Relation entre les variables partie 3 77
Tableau 24: Relation entre les variables partie 4 78
Tableau 25: Relation entre les variables partie 5 79
Tableau 26: Relation entre les variables partie 6 79

LISTE DES FIGURES

Figure 1 : Organigramme de la DSI 12
Figure 2 : Quadrant des risques liés à la gestion des données personnelles 16
Figure 3: les concepts de la gestion des risques 24
Figure 4 : Processus de gestion des risques 26
Figure 5: Les différentes zones de risque 27
Figure 6 : Roue de Deming 31
Figure 7 : Statistique de cause de perte de données 32
Figure 8 : Architecture réseau de la SAA 46
Figure 9 : Architecture logique de routage de la SAA 48
Figure 10 : Répartition de l'échantillon selon le nombre de clients 52
Figure 11 : Répartition de l'échantillon relatif aux raisons du choix de la compagnie 53
Figure 12: Répartition de l'échantillon selon le type de clients 54
Figure 13: Répartition de l'échantillon selon la durée d'assurance 55
Figure 14: Répartition de l'échantillon selon les moyens de fidélité 56
Figure 15: Répartition de l'échantillon selon le critère de la fidélisation 58
Figure 16 : Répartition de l'échantillon selon le sentiment de la préservation 59
Figure 17 : Répartition de l'échantillon sur le changement de compagnie. 60
Figure 18 : Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie. 61
Figure 19 : Répartition de l'échantillon selon la signification de la sécurité pour le client 62
Figure 20: Répartition de l'échantillon sur l'efficacité des dispositifs actuels 63
Figure 21 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1 64
Figure 22: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2 65
Figure 23: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 66
Figure 24 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation 67
Figure 25: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5 68
Figure 26: Répartition de l'échantillon selon le genre 69
Figure 27: Répartition de l'échantillon selon la tranche d'âge 70
Figure 28: Répartition de l'échantillon selon la catégorie socioprofessionnelle 71

LISTE DES ABRÉVIATIONS

-A-

ACL : Access List.

-B-

BD : Base de données

-C-

COBIT: Control Objectives for Information and Related Technology

-D-

DBDD : Direction de Base de données et de Développement

DC : Direction Central

DR : Direction Régional

DSI : Direction des systèmes d'informations

DT : Les données techniques

DTRM : Direction de Telecom Réseau et de Maintenance

-E-

ERP: Enterprise Resource Planning

-G-

GAFAM: Google, Amazon, Facebook, Apple et Microsoft.

-I-

ISO: International Organization for Standardization

-N-

NAS: Network Area Storage

-O-

ORASS: Object-Relationship-Attribute model for Semi-Structured data

-P-

PDCA: Plan, Do, Check, Act

-R-

RAID: Redundant Array of Inexpensive Disks

RGPD : Règlement Général sur la protection des données à caractère personnelle

RMS: Risk Management System

-S-

SAA : Société Nationale d'Assurances.

SAN : Storage Area Network

SD. D : Sous-direction du développement.

SD.M : Sous-direction de maintenance

SD. RT : Sous-direction Réseau et Telecom

SDBD : Sous-direction Base de données

SGBD : Système de gestion de base de données

SI : Système d'information

-T-

TIC : Technologie de l'Information et de la Communication

-V-

VPN: Virtual Private Network

VRF: Virtual Routing and Forwarding

-W-

WAN: Wide Area Network

INTRODUCTION GÉNÉRALE

L’avènement des Technologies de l’information et de la communication (TIC) a ouvert une panoplie de choix aux usagers et a facilité de manière considérable les transactions avec les organismes publics et privées, cependant ces transactions génèrent des données qui sont collectées par les différents canaux de communications et par la suite traitées pour offrir un meilleur produit à valeur ajoutée, ciblée et pertinente au client.

Le travail de collecte et traitement de données nécessitent énormément d’efforts financiers, technologiques et humains pour mettre en place un système d’information efficace afin de générer de la valeur.

L’ampleur que prend la donnée numérique dans notre vie et son facteur à caractère déterminant d’une personne notamment, ramène les utilisateurs à se soucier de la finalité quant à l’exploitation de ces données et de leurs destinations.

C’est le défi que doivent relever les organismes publics en mettant en place ou en améliorant leur système d’information pour répondre à cette exigence, car la garantie d’une bonne réputation et d’une forte base clientèle passe par une obligation d’assurer la confidentialité des données usagers.

L’importance de la sécurisation des données réside dans le fait que l’avenir est orienté vers le digital et de la nécessité de mettre en place des mécanismes de sécurité pour venir à bout des menaces dans le traitement de données des clients.

Une conscience des deux acteurs qui sont les organismes publics et les usagers sur la sécurité des données doit impérativement se construire afin de créer un environnement économique fiable et sécurisé.

Dans notre étude, nous avons choisi de travailler sur le cas de la Société Nationale d’assurances (SAA), du fait que la compagnie possède une large base client et aussi de sa renommée à l’échelle nationale.

Afin d’avoir une vision claire de l’efficacité de sécurité de leur système d’information et voir s’il répond aux exigences métiers qui sont les assurances, nous avons choisi de mettre en place

un questionnaire pour les clients de la SAA pour qu'ils donnent leur avis sur la prestation de services de la compagnie en termes de sécurité des données.

Pour ce faire, nous allons étudier tout au long de ce qui suit : quel est l'impact de la sécurisation des données sur la fidélisation des clients de la SAA ?

Durant l'élaboration de notre étude, nous allons suivre le plan de travail suivant :

Chapitre 1 : Problématique

Nous allons dans ce premier chapitre justifier le choix de la thématique et sa valeur ajoutée pour la société nationale d'assurances (SAA) tout en détaillant la problématique.

Chapitre 2 : Cadre théorique

Dans ce chapitre, nous allons définir les études qui ont été faites sur la sécurité et la fidélisation.

Chapitre 3 : Cadre méthodologique

Définir la méthodologie de travail.

Dans notre cas nous avons travaillé avec la méthode quantitative en élaborant un questionnaire.

Chapitre 4 : Résultats et discussions :

Nous allons d'abord décrire l'état de l'existant de la SAA et par la suite discuter des résultats du cas pratique obtenu à partir de la méthodologie choisie.

CHAPITRE 1 : PROBLÉMATIQUE

Nous allons durant ce chapitre discuter du choix et de la pertinence du thème ainsi que la problématique qui en découle.

1- Contexte de l'étude :

Cette étude a pour objectif principal de décrire l'état actuel de la sécurité des systèmes d'information au sein de la société nationale d'assurances (SAA), et d'étudier l'avis des usagers sur la sécurité.

Cette étude a pour but également de sensibiliser les usagers sur l'importance de la sécurité dans leur différente transaction financière avec la compagnie.

Le but du thème est d'accroitre nos connaissances dans la thématique de la sécurité des systèmes d'information tant important du fait de la polémique qui a eu lieu aux États-Unis lors des élections présidentielles de 2016 (Cambridge Analytica[1]), que nul n'est abordé jusqu'à maintenant dans les organismes publics algériens.

1.1 Intérêt personnel :

L'obtention du diplôme de master en management e-gouvernement passe par un stage en entreprise.

Pour ce faire, nous avons choisi de nous intéresser à la thématique de sécurité des systèmes d'information, plus précisément la protection des données collectées par les organismes publics. Nous estimons que la sécurité des systèmes d'information est importante dans le processus de digitalisation des administrations publiques.

1.2 Le choix du lieu de stage :

Pour l'élaboration de notre étude, nous avons choisi de faire notre stage au sein de la société nationale d'assurances (SAA) qui figure parmi les leaders économique et financier en Algérie compte tenu de sa grande clientèle et sa renommée dans tout le territoire national.

2- Question de recherche :

Dans le cadre d'amélioration de leur prestation de service, la société nationale d'assurances est en train de centraliser les données de ses agences et de ses directions régionales en les

[1] https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html (consulté le 10/08/2021 à 22 : 47)

consolidant vers la Direction centrale, nous estimons que la question liée à la protection et la sécurisation des systèmes d'information est maintenant devenue une problématique qui nécessite une attention particulière.

Garantir une transaction entre la compagnie et ses usagers fiable et sécurisé passe par l'amélioration ou la mise en place d'un système d'information qui répond aux normes de bonnes pratiques et qui est efficace contre toute sorte de menaces.

2.1 Pertinence théorique :

Il est important de mettre le point sur les notions de la sécurisation des données, qui est un sujet un peu mis à l'écart en Algérie.

Mettre en valeur la sécurité permettra de créer une sphère de confiance entre la compagnie et ses usagers.

2.2 Pertinence managériale :

La sécurité des systèmes d'information permettra aux décideurs de réduire le risque lié au business, du fait de son importance liée aux transactions et à la pérennité et l'image de marque de l'entreprise avec ses usagers et pour garantir leur fidélité.

Pour ce faire, il est important de voir si le système actuel répond à ces critères ou en nécessité d'amélioration.

De ce fait, nous avons élaboré une problématique qui tentera de nous éclairer si le système mis en place actuellement répond à cette exigence par la question principale qui est :

Quel est l'impact de la sécurisation des données sur la fidélisation client ?

De cette problématique s'éclate des questions liées au contexte de la sécurité des systèmes d'information et de la fidélisation client

- Quelle est l'importance de la sécurisation des données pour la SAA ?
- Comment cette sécurité va contribuer à la fidélisation du client ?

Pour répondre à ces questions, nous avons émis deux hypothèses que nous allons tester afin de finaliser notre recherche :

Hypothèse 1 : l'état actuel de la sécurité mis en place par la compagnie permet de sécuriser les données.

Hypothèse 2 : les dispositifs de sécurité actuels permettent de fidéliser le client.

Nous allons ensuite décrire l'environnement de la compagnie et son contexte organisationnel

3- Contexte organisationnel :

Nous avons effectué notre stage au sein de la société nationale d'assurances et nous allons avec ce qui suit présenter la compagnie et la structure d'accueil qui sont la direction des systèmes d'information, là où notre stage s'est déroulé.

3.1 Présentation de la société nationale d'assurances SAA

Entreprise Publique économique, agréée pour pratiquer l'ensemble des branches d'assurance, la Société Nationale d'Assurance SAA, est la première société d'assurance et de réassurance en Algérie.

Ce sont plus de 4140 collaborateurs qui perpétuent depuis 1963 des valeurs qui font l'identité de la SAA. Le savoir-faire, la responsabilité, le leadership et le respect des engagements sont incarnés chaque jour par des actions managériales et par un réseau bien établi, le plus dense du pays avec plus de 520 points de vente, répartis à travers tout le territoire national.

3.2 Historique de la société nationale d'assurances

Nous allons citer à travers un tableau récapitulatif les différents évènements qu'a subis la SAA depuis sa création en 1963 jusqu'à 2018.

Tableau 1 : l'historique de la SAA

Date	Evénement
1963	Création de la SAA une compagnie à capitaux mixtes Algéro-égyptiennes ; la société voit le jour en tant que compagnie d'assurance généraliste sous l'appellation SAA.

	En décembre 1963, le premier point de vente ouvre ses portes à Alger-Centre, sous l'enseigne SAA Assurance.
1966	Institution du monopole de l'Etat sur les opérations d'assurance par Ordonnance N°66.127, ayant conduit à la nationalisation de la SAA par ordonnance N° 66.129.
1976	SAA se spécialise dans la branche des risques simples. Développe des offres adaptées aux particuliers, aux professionnels, aux collectivités locales et institutions relevant du secteur de la santé.
1989	Dans le cadre de l'autonomie des entreprises, la SAA transforme son mode de gouvernance et devient une EPE au capital de 80 000 000 DA.
1990	SAA élargit son champ d'activités aux risques industriels, de l'engineering, de transport, risques agricoles et assurances de personnes.
1995	Ouverture du marché aux investisseurs nationaux et étrangers. Réintroduction des intermédiaires privés (agents généraux, courtiers et bancassurance), mise en place d'outils de contrôle du marché et création de la commission de supervision des assurances.

1997	Refonte de l'organisation du réseau. Une organisation tournée vers la performance. Rémunération des agences directes sur la base de leurs performances opérationnelles.
2003	Nouveau découpage régional. Introduction de l'ERP ORASS et développement d'un système d'information adapté aux besoins de la SAA.
2004	Réorganisation structurelle. Création de division par segment de marché afin de booster la productivité. Fin du mandat de la SAA en tant que gestionnaire du FSI (Fonds Spécial d'Indemnisation) et création du Fond de Garantie automobile.
2010	Séparation des assurances de personnes de celle relative aux assurances de dommages.
2011	Le capital social de la SAA est porté à 20 Milliards DA.
2015	Lancement du programme de Relooking du Réseau. SAA se lance pleinement dans la diversification de son portefeuille par le développement des branches hors automobile.
2016	Changement de siège social, une tour intelligente qui renforce la compagnie dans sa dynamique commerciale.

2017	SAA fait passer son Capital social à 30 Milliards de DA, soit 275 Millions de Dollars. SAA présente les indicateurs les plus élevés du marché.
2018	Signature de la convention cadre de partenariat et lancement des bureaux de souscription au niveau des showrooms Renault. Signature de la convention avec MERILCO (base de données de lutte contre la fraude pour la branche automobile). Mise en place d'un site pilote pour une plateforme de gestion des sinistres automobile. Relookage de 68 agences et aménagement de 17 agences.

3.3 Valeurs de la SAA

Les valeurs qui sont celles de la SAA trouvent leurs racines dans les fondements de la société Algérienne forgée à travers son histoire millénaire. Ainsi le respect de la parole donnée et des engagements pris à l'égard des clients et partenaires, constitue le moteur de toute action ou décision quotidienne de nos collaborateurs. La confiance mutuelle constitue la base de nos relations avec l'ensemble de nos partenaires.

De même que la simplicité et la sincérité de notre langage, se traduisent au quotidien dans nos relations avec nos assurés.

- SAVOIR-FAIRE

  Capitalisé tout au long de l'existence de l'entreprise, est la richesse que partagent tous les collaborateurs.

- RESPONSABILITE

  C'est le maître-mot de notre stratégie managériale. Faire face aux risques avec clairvoyance.

- LEADERSHIP

  Être leader au quotidien au sens entier du mot.

- RESPECT DES ENGAGEMENTS

  Être pleinement conscient de nos responsabilités et de notre rôle économique et social.

3.4 Organigramme de la SAA :

(Voir ANNEXE-A)

3.5 Présentation de la structure d'accueil (la division des Systèmes d'Information)

La direction des systèmes d'information est appelée au sein de la SAA la division système d'information avec plus de rôles et de prérogatives.

La division système d'information composée d'un chef division.

La hiérarchie est composée de deux directions :

1- **La direction réseau télécom et maintenance** (DTRM) est éclaté en 2 sous-directions :
- Sous-direction réseau télécom qui est composée de 7 membres ingénieurs IT
- Sous-direction maintenance qui est composée de 3 membres maintenancier

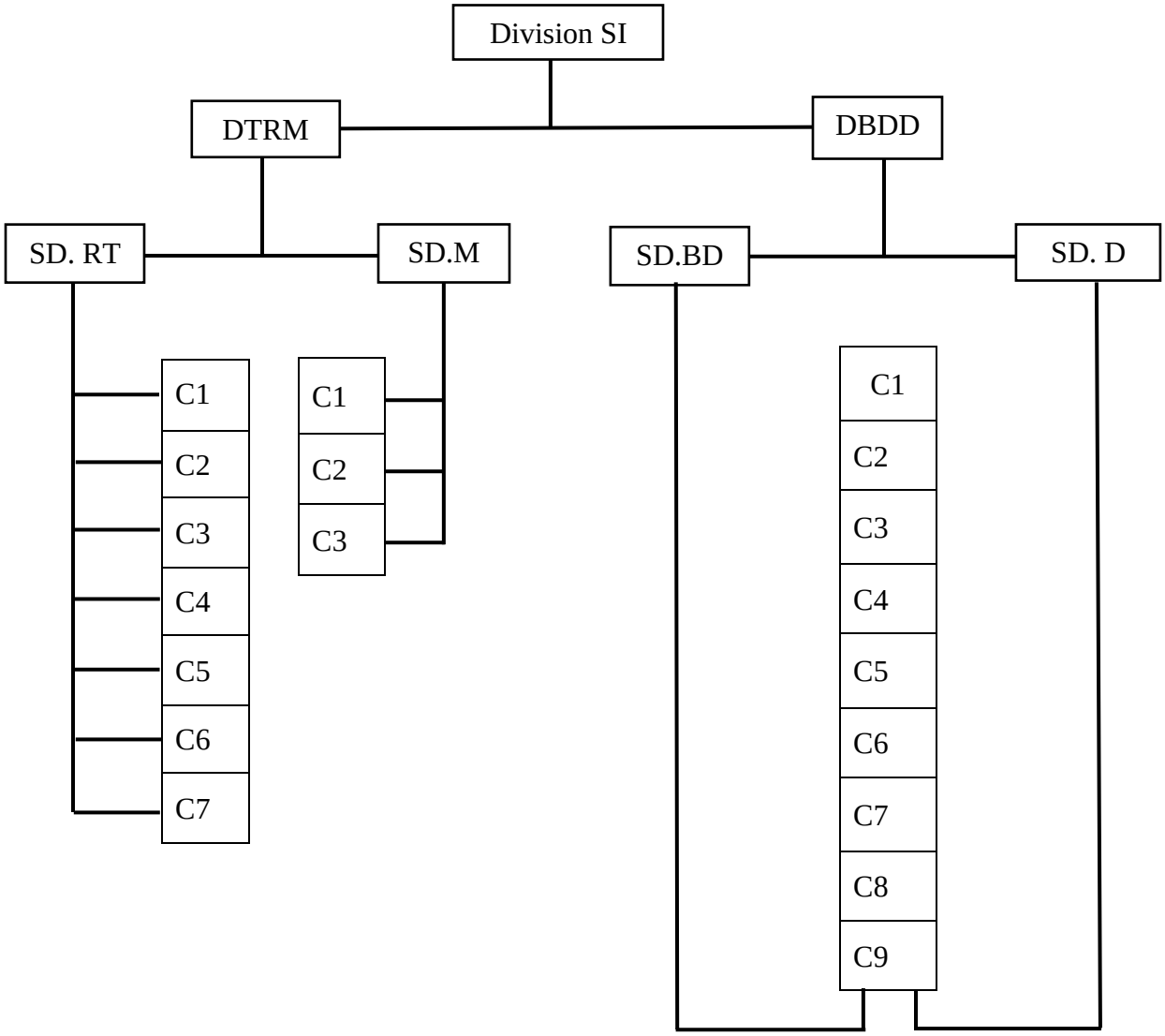
2- **La direction base de données et développement** : éclaté en 2 sous-directions contenant au total 9 membres :
- Sous-direction base de données
- Sous-direction développement

Notre stage s'est déroulé au sein des deux directions sous la surveillance du chef de division.

Voici ci-dessous un organigramme représentatif de la division système d'information de la SAA

3.6 Organigramme de la structure d'accueil

Figure 1 : Organigramme de la DSI



Source : élaboré par nos soins.

*C1 jusqu'à C9 représentent les collaborateurs.

Pour conclure ce chapitre présentatif, on pourra dire que l'évolution des TIC et leur importance dans notre quotidien et leur relation avec les organismes publics, nous a motivé à nous intéresser à cette thématique tant importante dans le monde et qui nécessite beaucoup plus d'attention en Algérie.

Nous allons voir avec ce qui suit, les différents travaux de recherche sur la sécurité et la fidélisation et les bonnes pratiques liés, aussi nous allons voir les concepts clés pour comprendre encore plus l'enjeu lié à cette problématique de recherche

CHAPITRE 2 : CADRE THÉORIQUE

Ce chapitre est divisé en deux parties, la première partie est la revue de la littérature ou nous allons aborder les différents travaux qui ont démontrés la valeur que possède les données au sein des entreprises et de comment les sécuriser.

En second lieu nous allons définir les termes liés à la sécurité des données et à la fidélisation client.

1- La revue de la littérature

À travers la revue nous allons mettre en évidence certains travaux qui ont traité de la sécurité des données et de la fidélisation client

1.1 La sécurité comme facteur d'évolution :

L'évolution numérique a impacté les pratiques et les habitudes des entreprises de manière considérable et l'enjeu de nos jours pour la pérennité d'une entreprise repose sur la maitrise des aspects technologiques pour garantir la sécurité de leur activité et de leur collaborateur et d'empêcher une mauvaise manipulation sur les données.

(Dupont, 2010), décrit deux tendances lors de son étude, la première est que l'administration publique est moins bien protégée que les entreprises privées, la deuxième est que la disparition d'information n'est pas seulement à cause de facteurs externe, mais aussi dû à la négligence des collaborateurs.

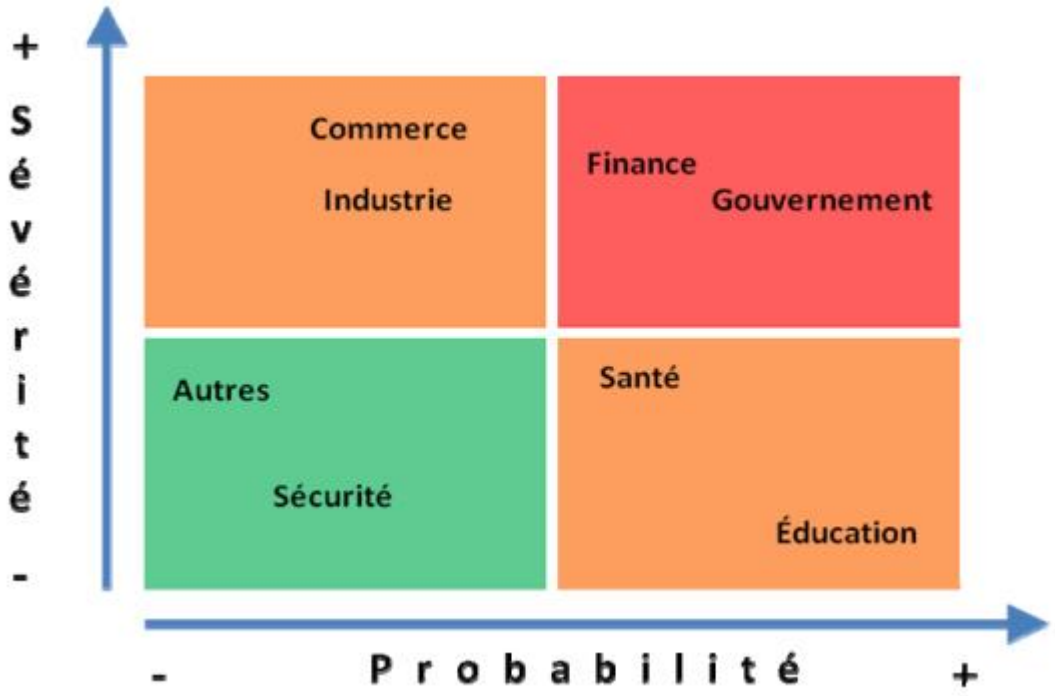
L'analyse sectorielle du phénomène par l'auteur a permis de constater que la disparition des données touche de manière très différente chaque secteur d'activité.

L'auteur évoque deux incidents qui se sont produits, le premier a eu lieu aux États-Unis entre 2006 et 2008 touchant plusieurs grandes entreprises de distribution et des opérateurs de paiements qui ont subi un vol de plus de 200 millions de numéros de carte de crédit par un pirate informatique nommée Albert Gonzalez, et l'autre aussi au Royaume-Uni par le ministère anglais du Budget qui avait égaré des données bancaires de 25 millions de bénéficiaires d'allocations familiales.

Selon Dupont, (2010) : *« Ces deux incidents, abondamment médiatisés, ont permis aux opinions publiques occidentales de prendre conscience, d'une part de l'ampleur des quantités de données accumulées par les organisations publiques et privées sur leurs usagers ou leurs clients, et d'autre part des pratiques frisant l'insouciance qui régissent le traitement de celles-ci. »*[2]

L'auteur montre que le secteur financier est le plus susceptible de subir des risques liés à la sécurité des données en établissant un graphe Sévérité/ probabilité du risque.

Figure 2 : Quadrant des risques liés à la gestion des données personnelles



Source : (Dupont, 2010)

L'auteur conclut que le premier incident est résultat d'une utilisation d'une technologie de chiffrement obsolète ou pas chiffrés et qui ne répondent pas aux normes de protection adéquates, Tandis que le second incident est la conséquence d'un mauvais calcul des coûts induits.

Dupont appelle les organisations a procédé à une analyse précise de leur situation et de mettre en place des techniques modernes de préventions pour sécuriser leurs données.

[2] Ibid.

Avec l'émergence des réseaux sociaux, de nouvelles pratiques ont vu le jour au sein des entreprises pour la collecte de données pour s'aligner avec les nouvelles tendances et offrir un service innovant au client.

« *En effet, la priorité stratégique des entreprises s'oriente aujourd'hui de plus en plus vers la maîtrise du maximum de données sur les individus (prospects, clients, consommateurs, salariés, futurs collaborateurs, etc.* » ((Terre, 2000) cité dans Dumoulin, R., & Lancelot Miltgen, C. (2012))

Les géants du numérique comme Facebook et Google ont été critiqués à mainte reprise sur la façon dont ils gèrent les données personnelles des internautes et de leur vie privée en général de façon laxiste ce qui induit à une méfiance et une faible volonté d'échanger les données.(Dumoulin & Lancelot Miltgen, 2012).

Wang et Wang, (1998) cité dans Dumoulin & Lancelot Miltgen (2012) décrit six pratiques font de cette méfiance justifiée, la collecte excessive, le stockage non autorisé, les erreurs ou altération des données, l'accès impropre par des personnes non autorisé, l'utilisation interne par la réception des offres non souhaités et l'utilisation externe par des tierces non autorisé.

Selon l'auteur ces pratiques engendrent une insatisfaction pouvant aller jusqu'au boycott du service et d'une bouche à oreille négatif. (Culnan et Armstrong (1999) cité dans Dumoulin & Lancelot Miltgen (2012))

L'auteur décrit quatre critères qui vont solliciter des réactions négatives de la part du consommateur (Lancelot Miltgen (2006) cité dans Dumoulin & Lancelot Miltgen (2012))

Le premier critère est l'absence ou le manque de garantie de confidentialité des données, le second étant la sollicitation de données trop personnelles, le troisième en relation avec le second qui est la sollicitation de données non pertinentes à la transaction et le dernier critère est le fait que l'individu perçoit plus de risque à céder ces données que des bénéfices qu'il en retire.

Ces critères peuvent pousser le consommateur à s'abstenir ou même de boycotter la marque.

L'auteur propose plusieurs solutions pour palier à ce problème notamment la mise en place d'une politique de respect de la vie privé claire, précise et éthique qui se réfère à la

réglementation en vigueur ainsi qu'une adoption d'une méthode de collecte de données limités seulement aux données nécessaires à la transaction et qui ne soient pas sensibles.

Une autre solution consiste à rassurer le consommateur en lui offrant d'avantages de privilèges comme les cadeaux les bons de réductions lors de la fourniture de données, tout cela pour une vision gagnant-gagnant de l'échange de données personnelles.

D'autres auteurs ont démontré la valeur importante de la donnée au sein de l'entreprise, on peut citer (Deville de Periere, 2013), qui stipule que l'information doit être considéré comme un élément de performance dans l'entreprise qui est génère par le partage et l'échange mais cette information doit être mis à l'abri du fait de son caractère confidentielle et authentique voire un facteur stratégique qui touche à l'ensemble de l'économie.

L'auteur décrit les données comme le patrimoine économique qui doit être protégé et sécurisé au sein des entreprises car leur survie dépend des moyens employés pour leur protection

(Deville de Periere, 2013) comme (Dupont, 2010) se sont mis d'accord sur le fait que les nouvelles technologies ont influencés les pratiques et ont rendu difficile la distinction entre ce qui doit rester secret comme données de ce qui peut être rendu publiques.

(Deville de Periere, 2013) estime que les évolutions technologiques ont procurés au système d'information un rôle majeur dans la société moderne puisqu'il devient le moteur économique des pays et dépendent étroitement de sa disponibilité et sa capacité à garder les informations authentique et confidentiel.

Même si selon l'auteur la donnée en elle-même ne présente pas un caractère sensible, cependant fusionner un ensemble de données pour créer un ensemble cohérant et à valeur ajouté pourra procurer une valeur stratégique et économique très significative.

L'auteur donne un exemple d'attaque subit par un ministère en évoquant la gravité de l'incident qui a touché le ministère des finances français par une intrusion d'un cheval de Troie injecté dans un fichier PDF et qui a infecté 150 postes et qui a engendré des conséquences graves.

Selon l'auteur l'explosion des réseaux sociaux présente un véritable danger pour l'entreprise car le simple fait qu'un collaborateur accède à un réseau social, il peut exposer l'ensemble de données de l'entreprise et attirer des personnes malveillantes qui peuvent nuire à l'entreprise.

De ce fait L'auteur déclare que : *« La divulgation d'informations, comme la présence de programmes malveillants, peut mettre en danger la sécurité de l'entreprise voire entrainé des pertes de données. Ces craintes sont totalement justifiées, puisque le nombre d'entreprises victimes d'une mauvaise utilisation des réseaux sociaux, ont augmenté de 70% en 2009 »*[3]

L'auteur décrit aussi un autre phénomène de malveillance qui touche les internautes comme le social engineering qui présente une perte estimée à 1,5 Millard de dollars par an pour les entreprises et qui touche des informations stratégiques et confidentielles : projets, contrats, licenciements voire même les déplacements des personnels et qui pourra profiter la concurrence et nuire considérablement à l'image de l'entreprise et lui porter des conséquences notables sur le marché.

Selon l'auteur les salariés internautes ne mesurent pas le degré de danger qu'ils subissent lors de la réception d'un courrier électronique ou lors du téléchargement d'une pièce jointe.

L'auteur déclare que : *« seuls 6,21% des messages qu'il reçoit, en moyenne, sont de vrais mails, et que tous les autres pourraient être classés comme courriers indésirables, »* et que : *« Plus de 90% de l'ensemble des messages reçus sur les serveurs des messageries des entreprises dans le monde sont donc suspects ».*

L'auteur sensibilise ces lecteurs sur le fait que le social engineering n'est pas la seule menace, et que beaucoup d'autres menaces tel que les malware, spyware, botnets, chevaux de Troie et virus sont des menaces imminentes et qui peuvent nuire considérablement au patrimoine de l'entreprise à chaque instant pour s'emparer des données personnelles et sensibles des salariées si les mesures nécessaires ne sont pas prises.

[3] Ibid.

(Le Cœur, 2016) sur la même lancée que (Dupont, 2010) et (Deville de Periere, 2013) estime que : *« Les deux risques majeurs sont la perte irréversible de données mais également l'impact négatif sur l'image de l'entreprise. Une telle négligence pourrait ternir durablement l'image d'une entreprise aux yeux de ses clients et de ses prospects. »*

Le caractère précieux que possède la donnée lui procure une place importante au sein des entreprises pour toutes les stratégies quelles souhaitent adoptés.

Car selon (Chen, 2017) et dans le même courant de pensé que les auteurs précédemment cités, estime que : *« Les données sont devenues une denrée précieuse pour toute stratégie commerciale. Toute information permettant d'établir un profil numérique permet de cibler les services et produits qui vous correspondent. Mais si ces données sont accessibles aux entreprises, elles le sont aussi aux hackers »*

L'auteur met en garde les entreprises que les stratégies adoptées pour établir un profil numérique de ciblage de service adapté aux consommateurs le sont aussi pour les personnes nuisibles et malveillantes.

C'est pour cela qu'il faut selon (Chen, 2017) maitrisés les traitements sur les données car elles sont si mal traitées nuisibles à l'image de l'entreprise et estime que : *« Pour une entreprise soucieuse de son image de marque et de la protection de ses données, il est important de maîtriser les différents droits accordés aux personnes utilisant ces logiciels, notamment si ces celles-ci ne font plus partie de l'équipe qui les utilise. De nombreux cas de piratage entraînant la diffusion de messages sensibles ou nuisant à l'image de marque sur des comptes officiels sont dus à une mauvaise administration des droits d'accès et d'écriture ».*

L'explosion des réseaux sociaux a changé complétement la façon de collecter, de traiter et de protéger les données et qui est rendu difficile pour les entreprises classiques économiques et financières à cause des entreprises tel que Facebook et Google.

Car de nos jours, la protection des données est devenue une inquiétude qui préoccupe de nombreux expert de la sécurité, selon une étude faites en 2017 par le magazine américain « The Economist » proclamait que la ressource la plus convoité dans le monde n'est plus le pétrole mais la donnée, ce qui fait maintenant le business model de compagnie tel que Facebook et

Google, ces compagnies ont désormais collecté une quantité immense de données, ce qui leur procure une force concurrentiel énorme.(Elvy, 2017, p. 1371).

A partir de 2018 avec la mise en place du règlement générale sur la protection des données à caractère personnelle RGPD, les GAFAM se sont vu modérés de leur collecte de données en Europe.

Selon Kaspersky[4] un des géants de la sécurité des systèmes d'informations : *« Le RGPD est une nécessité peu importe le domaine d'activité que vous exercez, que ce soit le domaine des ressources humaines, le marketing, le droit, l'informatique et la sécurité, il aurait un impact sur la façon de travailler, si vous manipuliez des données personnelles à l'intérieur de l'union européen, que ce soit un détail sur un employée un client ou une information de prospect, le RGPD apportera un changement dans les pratiques de travail et c'est à vous de les appliquer »*[5].

Après avoir fait le point sur les différents travaux de recherche sur notre thématique nous allons par la suite définir les concepts clés de notre recherche dans la partie suivante.

2- Cadre conceptuel :

Dans cette partie nous allons définir les concepts suivants relatives à notre thème de recherche

1- Les données, Informations et connaissances
2- Les risques sur les systèmes d'informations
3- La sécurité des systèmes d'informations
4- La fidélisation

Tout d'abord nous allons définir c'est quoi une donnée, une information et une connaissance.

[4] https://www.kaspersky.com/about (consulté le 15/08/2021 à 15 :30)
[5] https://www.kaspersky.com/gdpr (consulté le 15/08/2021 à 15 : 30)

2.1 De la donnée à la connaissance :

2.1.1 Les données :

La donnée est issue du latin ‘datum’ qui signifie quelque chose de donné et du grec ‘dido’ de donner.

(Kyriazoglou, 2019) définit les données comme étant le plus bas niveau d’abstraction des données non traité, comme des caractères, des images, des numéros et des représentations de quantités physiques et faits, résultats des mesures etc., ces données combinées vont créer une information et encore plus une connaissance.

Ces données sont traitées avec des systèmes informatisés et stockés dans les différents périphériques de stockage numérique et transmis à tous les utilisateurs ayant les droits d’accès pour les différents traitements possibles.

2.1.2 L’Information :

L’information est originaire du Latin (‘in’ + ‘formare’) qui signifie un concept, ou une idée.

Le terme ‘formare’ est issue du terme ‘morphe’ en Grec ancien = form (du Grec ancien dieu Morpheus, le dieu de la figure/forme).

Elle est la résultante de données traités pour leur procurer une forme à travers l’emploie d’une série de règles à la donnée pour ainsi la diffuser aux personnes concernées.

2.1.3 La connaissance

La connaissance est la résultante de la somme des faits, des données traitées et des informations obtenues à partir des différentes expériences représentent le monde qui se trouve en constante évolution dans lequel les organisations opèrent et survivent.
Selon Nonaka, Toyama et Konno (2000) cité dans (Paquet, (2006), p.9), *« la connaissance est un processus dynamique créé à travers une interaction sociale entre individus et organisations. La connaissance est spécifique à un contexte »*.

Blumentritt et Johnston (1999), puis Balmisse (2002) cité dans (Paquet, (2006), p.10) mettent le point sur la différence entre les concepts de donnée, information et connaissance. Selon les auteurs : *« une donnée est un élément brut livré en dehors de tout contexte. Par exemple, 10 millions d'Euros est une donnée. Il est impossible de l'interpréter en dehors d'un contexte. Il pourrait s'agir tout aussi bien d'un chiffre d'affaires, d'un résultat d'exploitation, d'un total de bilan ou encore du prix d'un immeuble. Elle n'a aucune valeur en soi. Par contre, cette donnée devient une information lorsqu'elle est contextualisée. Si cette valeur de 10 millions d'Euros est avancée alors que la discussion porte sur le résultat d'exploitation d'une entreprise pour l'année 2004, elle prend de la valeur et acquiert le statut d'information. »*

Pour Balmisse (2002) cité dans (Paquet, (2006), p.11) : « *l'information naît de la compréhension des relations qui peuvent exister entre plusieurs données mais elle est statique. La connaissance naît de la compréhension et de l'assimilation des règles qui régissent les modèles ou les schémas mentaux sous-jacents à ces relations, permettant ainsi de comprendre comment la situation évoluera si les données se modifient. La connaissance permet d'aboutir à une action. Mais cette connaissance ne peut être considérée comme une vérité universelle et indiscutable. Elle est fortement dépendante de l'individu qui la porte, empreinte de ses croyances et de son système de valeur Elle peut aussi être vue comme un processus dynamique en ce sens qu'elle est créée à travers une interaction sociale entre individus et organisation qui capitalisent l'information »* et rajoute que « La mise en commun des informations en provenance de plusieurs sources et la réflexion sur l'articulation de celles-ci à l'intérieur d'un modèle génère de la connaissance »

Maintenant que nous avons défini les trois concepts de notre travail de recherche, nous allons ensuite définir les risques que peuvent subir lors des différents traitements tout au long de leur cycle de vie du système d'information dans l'entreprise.

2.2 La gestion des risques dans les systèmes d'informations :

La gestion des risques est définie par l'ISO comme : *« l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque »* Mayer et Humbert, (2006) p.1.

Selon Mayer et Humbert, (2006), trois finalités se dégagent de la gestion des risques SI :

La première étant l'amélioration de la sécurité des systèmes d'informations, la seconde est la justification du budget allouer à la sécurité du SI.

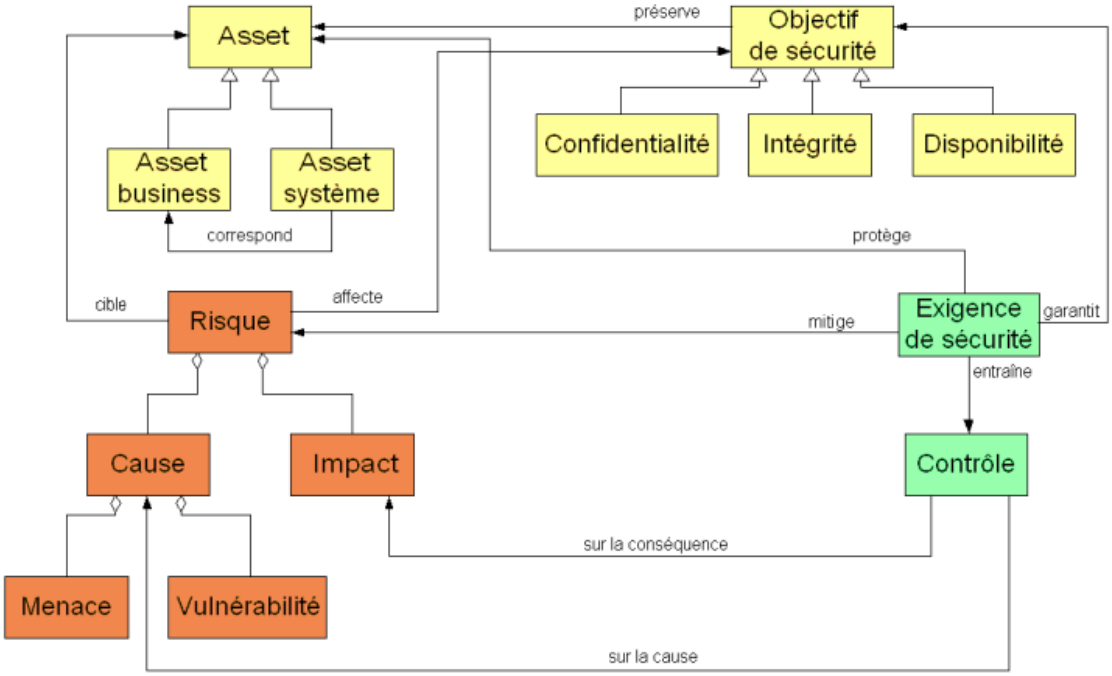
Et la dernière est l'approbation de la crédibilité du SI à l'aide des analyses effectuées.

2.3 Les fondamentaux de la gestion des risques :

Pour mieux comprendre la gestion des risques, ses objectifs et ses limites, il faut tout d'abord comprendre les concepts clés et les processus qui en sont employé :

La gestion des risques se compose de trois blocs interdépendants, la première étant l'organisation de la cible qui est définie par les assets, ses besoins en sécurité, en second lieu, les risques pesant sur les assets et enfin les mesures prises qui ont pour but d'assurer un certain niveau de sécurité.

Figure 3: les concepts de la gestion des risques



Source : Mayer et Humbert, (2006), p.2

Mayer et Humbert, (2006) définissent les assets *: « comme étant l'ensemble des biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement. »*

Les deux auteurs expliquent les assets comme étant composés, d'assets niveau Business qui sont liée à l'activité de l'entreprise, comme par exemple : des numéros carte bancaire et la gestion des transactions, les assets business sont gérés par les assets SI et sont particulièrement dépendant du SI nommé ' Assets système'.

Dans les assets système on retrouve toute l'architecture technique, matériel, logiciel pour mieux gérer et sécuriser les assets business, dans un ensemble formant le SI, dans une perspective d'objectifs de sécurité : confidentialité, intégrité et disponibilité. '. (Mayer et Humbert, (2006), p.2).

Ces assets sont vulnérables aux risques de sécurité, Mayer et Humbert, (2006) définissent le risque à travers le guide 73 de l'ISO : *« par la combinaison de la probabilité d'un événement et de ses conséquences. »* et mettent en place une équation du risque qui est couramment utilisé et reconnue dans le domaine de la gestion des risques :

Tel que : RISQUE = MENACE * VULNERABILITE * IMPACT

Depuis cette équation, on pourra définir les quatre concepts liés à la gestion des risques SI :

La menace est considérée comme la source du risque, une attaque potentiellement dangereuse pour les assets.

La vulnérabilité est une caractéristique de l'asset qui constitue une faiblesse ou une faille qui peut être exploité

L'impact représente la conséquence du risque sur les activités de l'organisation, il peut être qualifié en tant que sévérité du risque sur un SI, tandis que la menace et la vulnérabilité présente un risque potentiel.

Afin de réduire les risques sur les assets et de les protéger, une politique de traitements des risques est mise en place constitué d'exigences de sécurité, ces exigences vont se traduire par des contre-mesures pour satisfaire au mieux les exigences

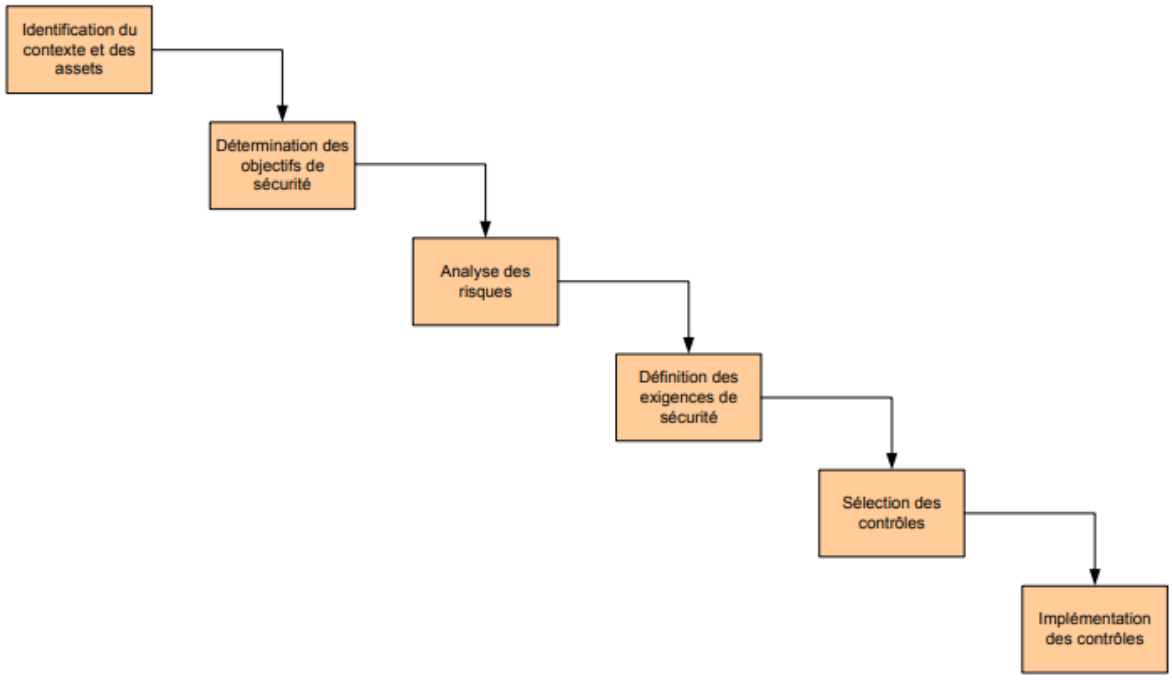
On pourra appliquer les contrôles sur la menace et la vulnérabilité afin de réduire la cause du risque et sur l'impact afin de réduire la conséquence du risque.

2.4 Définition des processus de gestion des risques :

Après avoir mis le point sur les concepts lié à la gestion des risques SI, nous allons maintenant voir les processus intervenants dans celui-ci :

La figure suivante représente un schéma illustratif des processus de la gestion des risques.

Figure 4 : Processus de gestion des risques



Source : Mayer et Humbert, (2006), p.4

Mayer et Humbert, (2006) définissent les six étapes de la gestion des risques que nous allons expliquer brièvement tout au long de ce qui suit :

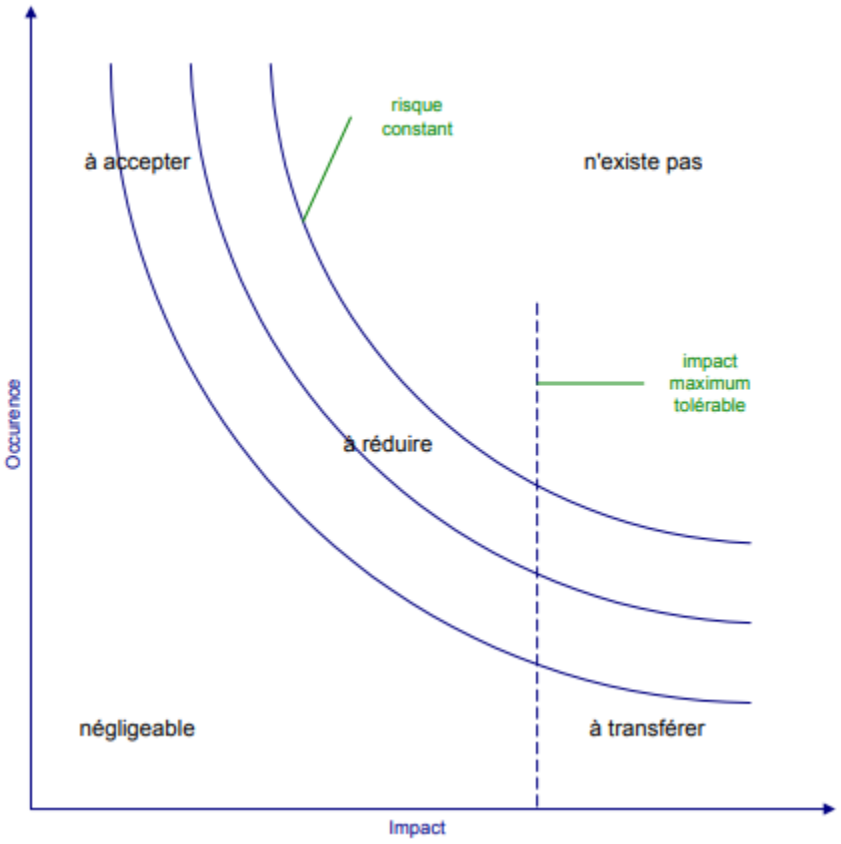
La première étape consiste en l'identification du contexte ou domaine des assets, cette étape consiste en la prise de connaissance de l'état des assets au niveau organisationnel, environnemental et de son SI, pour déterminant les limites du système sur lequel porte l'étude de la gestion des risques.

La seconde étape consiste en la spécification des objectifs de sécurité : la confidentialité, l'intégrité et la disponibilité des assets.

La troisième étape est l'analyse des risques qui constitue le cœur de la gestion des risques dans le but d'identifier et estimer chaque composante du risque qui sont : menace, vulnérabilité et impact, et de prendre les mesures nécessaires, cette étape est également appelée « appréciation du risque ».

Afin d'estimer le risque Mayer et Humbert, (2006) propose un graphe pour le traitement des risques en les classant par 5 zones de risque présenté dans la figure suivante :

Figure 5: Les différentes zones de risque



Source : Mayer et Humbert, (2006), p.5

La première catégorie présente les risques négligeables se sont les risques avec une occurrence et un impact faible.

La seconde catégorie présente les risques à forte occurrence et à impact important, ce risque ne doit pas subvenir car s'il se produit, il remettra en cause toute l'activité de l'entreprise.

La troisième catégorie concerne les risques à forte occurrence et à impact faible, ce risque est acceptable puisqu'il relève de quelques mesures opérationnelles pour palier au risque.

La quatrième catégorie ce sont les risques à occurrence faible mais à impact lourd et considérable, ces risques-là sont à transférer, couvert par une assurance ou une tierce partie.

La cinquième catégorie concerne les risques à réduire qui sont la base de la gestion des risques, traités au cas par cas en diminuant le risque pour qu'il tende le plus possible à l'origine de l'axe.

La quatrième étape de la gestion de risque est la définition des exigences de sécurité qui va permettre de réduire les risques identifiés, soit par l'assistance des référentiels, soit par des experts système et sécurité.

La définition des exigences de sécurité se fait de façon incrémentale, du fait de son importance et de sa complexité en commençant par des exigences générales qui définiront la stratégie adoptée pour contrer les risques, ensuite par les exigences génériques qui vont toucher le niveau opérationnel SI et aussi sur le niveau système informatique à travers la gestion des comptes utilisateurs par exemples.

La cinquième étape est constituée de la sélection de contrôles ou aussi appelé contre-mesures, car une fois les exigences définis, on procède à l'application de ces derniers en définissant les choix techniques des solutions de sécurité

Enfin la dernière étape consiste à l'implémentation dans le SI des contrôles et de les tester et évaluer pour palier à d'éventuels risque résiduel qui peuvent encore exister.

Nous avons défini les risques et les différents processus de la gestion des risques, nous allons par la suite voir les différents mécanismes employés pour la sécurité des données.

2.5 La sécurité des données :

Selon Razafy, Randriamaroson et Rakotomiraho, (2016), p.134, La sécurité des données est devenue une activité primordiale pour les entreprises. Pas seulement pour conserver et sauvegarder des données mais aussi à rendre les données disponibles pour une utilisation ultérieure aux personnes habiletés.

L'auteur a défini les trois objectifs de sécurité tel que :

- La confidentialité : l'information est disponible uniquement aux personnes autorisées,
- L'intégrité : l'assurance de la non modification ou la non l'altération d'une information
- La disponibilité : l'assurance que l'information est à la demande et au temps minimum aux personnes responsable du traitement.

S'ajoute aux trois objectifs, la non répudiation qui est le fait que l'auteur de la modification ne nie pas son action, et la preuve qui est la garantie que l'émetteur est un utilisateur identifié avec les droits et privilèges d'accès et que le récepteur est bien autorisé à accéder à l'information.

Assurer la sécurité de données est la garantie de l'assurance des trois objectifs de la sécurité qui sont la disponibilité, l'intégrité et la confidentialité, s'ajoute à ces trois objectifs un autre qui est la non répudiation.

Parmi les problèmes que peuvent subir les données est la destruction qui représente un impact important pour un particulier qui voit ses données endommagées, ou pour une entreprise soucieuse de sa réputation et engendré par la suite de graves dégâts qui peuvent s'étendre à l'atteinte de la vie privée des clients.

La garantie de la disponibilité des données pour les utilisateurs ayant accès et dans un délai minimal, constitue un enjeu majeur et une préoccupation pour les entreprises

2.6 Les normes et standards de bonne pratiques :

Pour arriver à garantir cette exigence les entreprises se réfèrent aux normes et les méthodes standards qui ont pour objectif d'établir un système de gestion de la sécurité de l'information et aussi afin de définir le périmètre à gérer.

Selon Razafy et al, (2016), Parmi les normes utilisées dans la sécurité des données est celle de COBIT (Control objectives for Information and related Technology) et de l'ISO 17799.

2.7 L'évaluation de risque de sécurité de l'information :

Selon Razafy et al, (2016) L'évaluation des risques permet de définir et mettre en place les outils nécessaires et les investissements adéquats dans l'entreprise.

La norme (ISO 27002 :2005) cité dans Razafy et al, (2016), p.136 « La sécurité de l'information » permet de protéger l'information contre une large gamme de menaces de manière à garantir la fluidité et la continuité des transactions et à optimiser le retour sur investissements.

D'après la norme (ISO/CEI 27005 :2008) cité dans Razafy et al, (2016), p.137 « *un risque est la probabilité qu'une menace donnée tire parti des vulnérabilités d'un actif ou d'un groupe d'actifs et cause dès lors du tort à l'organisation* ».

2.8 La gestion stratégique de la sécurité :

Selon la norme ISO 27005 la mise en place de sécurité passe par un cycle continue de PDCA (Plan, Do, Check, Act) la roue de Deming.

Nous allons expliquer brièvement les quatre concepts de la roue de Deming :

PLAN : consiste en l'identification, l'évaluation et la définition des actions de réductions des risques.

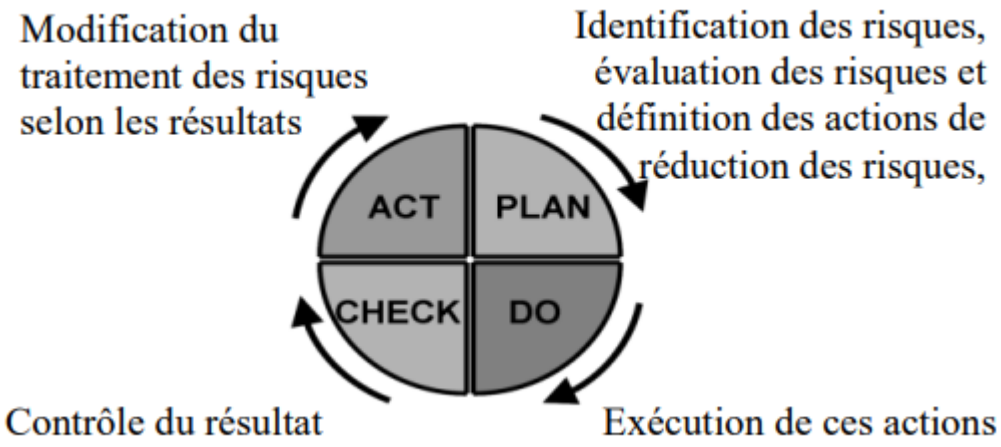
DO : mettre en pratique le plan préétabli.

CHECK : à travers cette étape les résultats sont contrôlés.

ACT : la réaction au traitement selon le résultat apparu.

La figure suivante illustre la roue de Deming :

Figure 6 : Roue de Deming



Source : Razafy et al, (2016), p.137

Cette méthode est très importante lors de l'auto-évaluation, pour savoir si les mesures appliquées répondent aux exigences ou nécessitent d'être corrigés.

Après la définition des normes et des pratiques ainsi que la stratégie pour la sécurisation des données, il est important de garantir le support technique soit fiable pour le stockage et la conservation mais aussi pour rendre les données disponibles aux utilisateurs ayant les droits et les privilèges d'accès.

2.9 Les types de support de stockage de données :

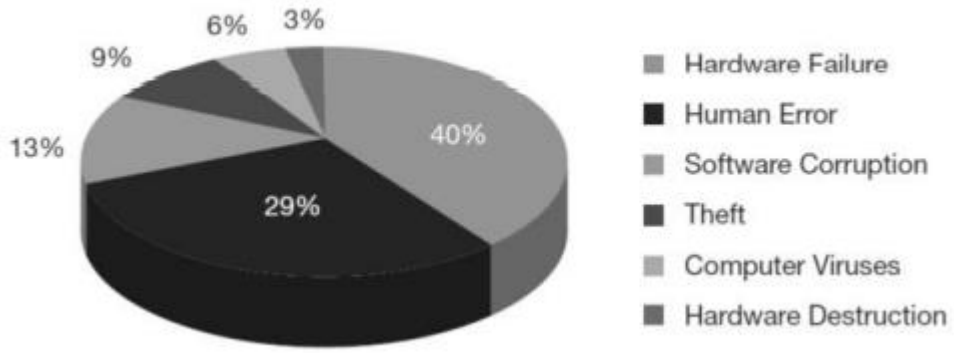
Selon Razafy et al, (2016), p.137, plusieurs types de support de sauvegarde ont vu le jour et la capacité est de plus en plus évolutif selon les besoins de stockage, et le choix du support dépend énormément de l'exploitation ou du traitement qui sera fait.

De nouveaux supports de stockage ont émergés pour pallier le manque d'espace et la dégradation du matériel.

2.10 Amélioration des supports de stockage :

Razafy et al, (2016), p.138 estime que : *« 40% des pertes de données sont dus à la défaillance matérielle. Des améliorations ont été faites pour augmenter la fiabilité d'enregistrement des informations. Des solutions logicielles et des solutions matérielles sont disponibles et leurs utilisations dépendent de l'utilisateur. »*

Figure 7 : Statistique de cause de perte de données



Source : Razafy et al, (2016), p.138

Parmi les supports innovateurs de stockage nous pouvons citer :

Le RAID : qui est acronyme de Redundant Arrays of Inexpensive Disks, son principe est établi à partir de la duplication des données sur plusieurs disques pour aider à la construction des données en cas de panne d'un des disques.

Son utilisation pénalise les performances mais la lecture est augmentée lors de l'enregistrements d'informations dupliqués sur plusieurs disques.

La baie de stockage en réseau NAS : (Network Attached Storage) est un serveur de stockage des fichiers en réseau, sa principale fonction est le stockage des données en volume pour tous les clients appartenant au même réseau comportant plusieurs technologies et choisie selon le rapport qualité/prix

La technologie RAID est utilisé pour sécuriser les données stockées contre toutes défaillances matérielles.

Le réseau de stockage SAN : cette technologie par rapport au NAS, procure un accès bas niveau aux disques directement par accès bloc au disque, et chaque serveur voit son espace disque comme son propre espace.

Le stockage sur un cloud : est considéré comme une offre de service par un tiers, l'accès au stockage se fait à partir d'un réseau local ou à partir d'internet

Le service cloud permet à tous les utilisateurs d'en bénéficier même ceux n'ayant pas de compétences techniques, géré par le fournisseur de service qui lui offre un cloud privé pour les entreprises contrairement au cloud public, dans les deux cas le fournisseur garantie la confidentialité des données.

Base de données : est une entité pour le stockage de données de façon structurés et ordonnées utilisés par des programmes ou des utilisateurs afin de mettre en commun ou en relation un ensemble de données

La base de données est gérée avec un système de gestion communément appelé SGBD : système de gestion de base de données, afin de faciliter l'accès aux données et assurer leur sécurité.

Nous allons maintenant expliquer les trois objectifs de la sécurité en donnant les types de technologie pour chaque critère :

2.11 Les objectifs de la sécurité des données :

Razafy et al, (2016) définit les trois objectifs de la sécurité que nous allons énumérer ci-dessous :

2.11.1 La disponibilité : est définie comme l'assurance pour les personnes ayant droits et privilèges d'accès à une donnée ou à un ensemble de données dans le temps nécessaire au traitement.

Nous pouvons citer plusieurs formes de disponibilité tel que :

Sauvegarde et archivage :

La sauvegarde permet de stocker une copie des données sur un autre support pour la restauration ultérieure lors de la suppression ou l'altération de la copie originale.

L'archivage est le stockage d'informations tout au long de la durée ou la politique d'archivage des entreprises, à la fin de cette durée les données sont automatiquement effacés.

Synchronisation : est une réplication de données dans l'environnement de production ou de secours pour assurer la disponibilité et la reprise en cas de panne.

Selon deux modes de fonctionnement : le mode synchrone les sauvegardes sont faites simultanément

Pour le mode asynchrone les sauvegardes sont faites à un intervalle de temps différé.

L'intégrité : c'est la garantie ou la certitude de la non modification ou la non altération d'une information, pour remédier à ces problèmes le responsable du traitement enregistre les actions pour vérifier par la suite la non altération des données.

On peut citer plusieurs formes d'intégrité tel que :

Traçabilité et audit : ces deux concepts sont essentiels pour assurer le suivi de l'intégrité pour garantir que seulement les personnes autorisées ont effectués des traitements

La traçabilité est le fait de garder un historique sur toute l'activité de traitement sur une donnée de son origine jusqu'au changement effectué.

L'audit est concerné dans la lecture, modification et suppression et intervient lors des traitements effectués sur les informations en cas de doute pour vérifier l'intégrité de la donnée.

Protection des données : consiste en la mise en place de règles de sécurité qui stipule que seulement les personnes autorisées auront accès pour consultation, modification en utilisant des technologies de stockage tel que le système d'exploitation et les bases de données.

2.11.2 La confidentialité : Razafy et al, (2016), p.142 définit ce concept par : *« l'assurance que l'information ne soit accessible qu'aux personnes autorisées, qu'elle ne sera pas divulguée en dehors d'un environnement spécifié ».*

Nous pouvons citer plusieurs formes de confidentialité tel que :

Gestion des accès : par la mise en place de mécanismes d'authentification, et que chaque utilisateur devra avoir son propre compte propre à lui, en lui attribuant ou en lui enlevant des autorisations spécifiques de traitements, comme le dicte la norme ISO 17799 et la norme ISO 15408

Pour une entreprise, on parle d'attribution ou création de rôle utilisateur, ou bien l'ajout de l'utilisateur à un groupe d'utilisateurs avec leurs propres privilèges d'accès.

Verrouillage de fichier : c'est l'attribution de mots de passe à un fichier, pratique lorsque la gestion des accès n'est pas applicable.

Cryptage : protégés les documents contre les accès non autorisés ou les intrus de l'externe

Il existe cependant une multitude de choix de cryptage selon le degré de confidentialité.

Pour conclure, on pourra dire que la connaissance et la maitrise de ces aspects important de la sécurité vont considérablement aider les entreprises à mieux protéger et à sécuriser leur système d'informations.

Nous allons maintenant définir le concept de fidélisation ainsi que ces différentes théories.

2.12 La Fidélisation :

La fidélité est une relation durable avec les clients constitue un enjeu essentiel pour les entreprises (Webster, (1992) cité dans Sahut, J. M., Moez, K., & Mutte, J.-L. (2011). De ce fait, la recherche en marketing, de nombreux travaux à l'étude de la création et du développement des relations de long terme notamment en Business-to-Business ont été consacré (Dwyer & al., 1987 ; Sheth & Parvatyar, (1995) cité dans (Sahut et al., 2011))

La littérature marketing s'est intéressée à la définition du concept de fidélité à la marque, nous pourrons citer la définition de Jacoby et Keyner (1973) (cité dans (Sahut et al., 2011))) qui stipule que *« la fidélité est une réponse comportementale biaisé exprimé dans le temps par une entité de décision, considérant une ou plusieurs marques prises dans un ensemble, en fonction d'un processus de décision »*, cette définition montre le caractère d'achat répété dans le temps et orienté dans un paradigme transactionnel.

Cette approche a suscité nombreuses critiques selon l'auteur, et de nouvelles approches ont vu le jour notamment celle de Roux, (1985) et Raj, (1985) (cité dans (Sahut et al., 2011)) qui décrivent la nouvelle approche en plus du comportement d'achat répété, comme étant : *« un ensemble de facteur psychologique d'évaluation et de prises de décision d'ordre cognitif, affectif et conatif, la relation entre le vendeur et l'acheteur devient alors au centre des préoccupations et abouti à la conception du paradigme relationnel ».*

Cette théorie est faisable à travers une relation basée sur la création d'une bonne confiance pour optimiser les transactions avec les partenaires futurs.

Depuis, quatre courants de pensée de la fidélité ont vu le jour en créant deux orientations, le premier est transactionnel, et ou relationnelle, tandis que le second est behavioriste ou cognitive, au croisement de ces quatre théories apparaissent plusieurs nouvelles théories. (Frissou, (2006) cité dans Sahut et al, (2011)).

On peut citer la théorie de l'achat répété, cette théorie se décline à travers la probabilité que l'acte d'achat se répète à un intervalle de temps ultérieur, on dit qu'elle est événementielle, on la voit surtout dans le secteur bancaire avec le programme de fidélité qui offre des points aux clients à chaque fois qu'il fait une transaction pour ensuite stimuler l'acte d'achat dans un temps ultérieur afin de renforcer sa fidélité.

La seconde théorie est celle de l'achat préféré ou raisonné, elle se traduit par un comportement psychologique biaisé à travers l'attachement du consommateur à une marque

Cette théorie est utilisée par les sociétés d'assurance afin de raisonner le client par un système de croyance en éveillant la curiosité du consommateur sur la marque comme étant la référence qualité/prix

Pour faire fonctionner au mieux cette théorie l'entreprise doit créer et innover dans ces produits car les préférences et les croyances des consommateurs changent constamment.

La troisième est celle de la théorie de la relation imposée qui se traduit par le fait d'enfermer le client dans une relation d'échange qui n'a pas plus au moins désiré mais dans lequel il est contraint pour des raisons économiques ou psychologiques.

Cette théorie de fidélisation imposé est utilisée chez les opérateurs téléphoniques et les compagnies d'assurances avec un contrat d'une durée minimale de 12 à 24 mois, le client est là contraint de respecter la durée totale de son contrat auprès de l'entreprise.

La quatrième et dernière théorie est la théorie de la relation désirée qui contrairement aux théories précédentes, se traduit par une relation choisie et désirée par le client avec un engagement volontaire de sa part et détermine son niveau d'engagement envers la marque fondée sur la confiance.

Cette théorie fait la politique de communication de plusieurs entreprises du secteur financier, notamment les banques en offrant des services adaptés et désirée par le client qui lui s'engage volontairement au service offert.

Cette théorie fait la politique de communication de plusieurs entreprises du secteur financier, notamment les banques en offrant des services adaptés et désirée par le client qui lui s'engage volontairement au service offert.

2.12.1 La fidélisation comme facteur de la réduction des risques pour l'entreprise :

Trinquecoste, (1996), p.18, décrit la fidélisation des consommateurs aux produits de l'entreprise comme une barrière défensive contre les attaques des concurrents et renforce la place de l'entreprise dans le marché pour une position de monopole

La fidélité est un signe d'encrage dans le marché pour gagner en notoriété et en pérennité, ce qui contribue à la réduction de risques pour l'entreprise.

Pour conclure, maintenant que nous avons défini tous les concepts liée à la sécurité des données et à la fidélisation à travers ce chapitre théorique, on pourra dire que tous les auteurs se sont mis d'accord sur le fait que la sécurisation des données présente un enjeu majeur dans la société numérique moderne, et la mise en place des dispositifs de sécurité afin de pallier aux problèmes de l'atteinte aux données confidentiels et à la vie privée des usagers qui risquent de nuire à l'image de marque de l'entreprise et de lui faire perdre sa notoriété et son chiffre d'affaires.

Nous voulons savoir à travers les chapitres suivants, si la sécurisation des données a un impact sur la fidélisation des clients.

CHAPITRE 3 : CADRE MÉTHODOLOGIQUE

Dans ce chapitre, nous allons définir la posture épistémologique et la méthodologie utilisées dans notre travail de recherche sur l'impact de la sécurisation des données sur la fidélisation client au sein de la société nationale d'assurances (SAA).

1- Posture épistémologique :

Ce travail de recherche s'inscrit dans une posture épistémologique de type positiviste, menant à une réflexion hypothético-déductive de recherche sur une problématique, à l'aide d'hypothèses qui se portent sur une théorie à confirmer ou à infirmer.

À travers la revue de la littérature et le cadre conceptuel, nous nous sommes aperçus de l'importance de la question de recherche dans le monde de l'entreprise et qui nous a menés à adopter un paradigme positiviste.

2- Approche méthodologique :

Notre étude se base sur une méthodologie quantitative dans le but de collecter les données, cette méthode est plus adaptée et plus rapide à administrer dans notre cas d'étude.

3- Méthode de collecte de données :

Nous avons utilisé plusieurs sources pour la collecte d'informations sur la thématique : articles, site web, rapports, afin de recueillir le maximum de données sur notre thématique étudiée et pour arriver à un résultat fiable et satisfaisant.

Nous avons choisi la méthode quantitative car c'est la méthode la plus abouti pour collecter des informations sur les clients de la SAA et cela de façon anonyme, ce qui permet aux répondants de répondre honnêtement aux questions et qui se traduit par un questionnaire de recherche sur l'impact de la sécurité des données sur la fidélisation client.

4- Instrument de mesure :

Nous avons utilisé comme instrument de mesure, le questionnaire de recherche qui parait le mieux adapté à notre étude, afin d'atteindre l'objectif de recherche.

4.1 Questionnaire :

Le questionnaire est un outil de collecte d'informations pour une étude ou une recherche.

Ces données permettent de tester les hypothèses préétablies dans le but de les confirmer ou de les affirmer.

Le questionnaire est composé de questions à choix uniques ou /et à choix multiple permettant de répondre suivant les différentes préoccupations.

La revue de la littérature nous a permis de choisir la forme des questions à poser sur les répondants, pour des réponses pertinentes à notre recherche.

Nous nous sommes inspirés par des questionnaires sur la fidélisation client des étudiants d'années précédentes ainsi que d'autres universités et nous avons essayé d'inclure nos propres questions après la concertation avec les cadres de la société nationale d'assurances (SAA) et avec l'accord de notre encadreur, nous avons pu établir le questionnaire adapté à notre étude.

4.2 La structure du questionnaire :

Notre questionnaire a été construit sur la base du plan suivant :

La première question « Q1 » est une question de sélection, si le répondant satisfait ou non notre critère de recherche qui est la clientèle de la SAA.

Cette catégorie que nous appelons « **catégorie client de la SAA** » contient les questions posées ; si le répondant choisit de répondre par « OUI » ce qui veut dire qu'il est client de la compagnie.

Cette catégorie contiendra :

- La question Q2 concerne le critère de choix du client pour la SAA.
- La question Q3 sur le type de client particulier et ou professionnel.
- La question Q4 sur l'ancienneté de clientèle.

Après la réponse à la question Q4, une sous-catégorie de questions liée à la fidélisation du client tels que :

- La question Q5 : est une question à choix multiple sur les moyens de rendre un client fidèle.
- La question Q6 : sur le sentiment de fidélisation du client.
- La question Q7 : sur le sentiment de la sécurité des données des clients.
- La question Q8 : sur la volonté de changement de compagnie d'assurance.

- La question Q9 : la sécurité comme motif de changement de compagnie.

A l'issue, une nouvelle catégorie de questions liée à la sécurité des données telles que :

- La question Q10 : sur la signification de la sécurité pour le client.
- La question Q11 : sur l'efficacité des dispositifs de sécurité pour le client.

Les questions de Q12 à Q16 sont des questions d'échelle de mesure basées sur l'échelle de Likert, le répondant se voit choisir un chiffre allant de 1 à 5 :

- De **1** qui signifie « **pas du tout d'accord** » jusqu'à **5** qui signifie « **tout à fait d'accord** ».

La question Q12 contient l'affirmation suivante :

« La sécurisation des données clients permet de le fidéliser, car si le client est rassuré que ces données sont bien protégées, il restera client fidèle à la compagnie ».

La question Q13 contient l'affirmation suivante :

« Protéger les données des clients d'une compagnie d'assurance est un facteur clé pour le fidéliser ».

La question Q14 contient l'affirmation suivante :

« La sécurisation des données permettra d'instaurer une confiance entre la compagnie et le client et de faire valoir l'image de marque de la compagnie ».

La question Q15 contient l'affirmation suivante :

« Une conscience de sécurité doit se construire entre le client et l'entreprise pour contribuer à la prévention des risques ».

La question Q16 contient l'affirmation suivante :

« Les compagnies d'assurances doivent améliorer continuellement leur dispositif de sécurité en mettant en place les mesures nécessaires afin de venir à bout des différentes menaces ».

A la fin, le répondant est redirigé vers une dernière catégorie qui contient des questions de signalétique pour clôturer et envoyer le questionnaire.

La question Q17 contient le genre du répondant, soit Homme ou Femme.

La question Q18 contient la tranche d'âge du répondant.

La question Q19 concerne la catégorie socioprofessionnelle du répondant.

Pour terminer cette série de questions, nous avons laissé le soin aux répondants de donner leurs avis et commentaires sur le questionnaire avec une dernière question ouverte.

5- Les échelles de mesure :

Une variable a été mesurée à partir de l'échelle de Likert allant de 1 à 5.

- « Pas du tout d'accord » à « tout à fait d'accord ».

6- Échantillonnage :

6.1 Population d'étude :

Nous avons ciblé les clients de la SAA pour notre étude.

6.2 Taille de l'échantillon :

Afin de construire un échantillon représentatif pour notre étude, nous nous sommes fixés pour objectif d'atteindre une centaine de clients ou clients potentiels.

Nous avons reçu 111 réponses, et pour faciliter notre étude nous avons choisi de travailler sur 100 réponses

Parmi ces 100 réponses, nous avons 34 clients de la SAA et 66 qui ne le sont pas.

Nous allons nous focaliser sur les 34 clients afin d'élaborer notre étude.

6.3 Méthode d'échantillonnage :

Notre étude nous a mené à choisir un échantillonnage non probabiliste par convenance, pour interroger les clients de la SAA sur l'impact de la sécurisation des données sur la fidélisation client.

7- Modalités pratiques de l'enquête :

7.1 Outil de collecte de l'information : le Questionnaire.

7.2 Mode d'administration : le questionnaire a été administré en ligne à l'aide de l'outil Google Forms.

7.3 Période de l'enquête :

La période de collecte de données s'est déroulée du samedi 11 septembre 2021 au mardi 21 septembre 2021.

7.4 Le test du questionnaire : le test du questionnaire a été partagé sur les deux réseaux sociaux Facebook et LinkedIn à travers des groupes d'étudiants et aussi dans des groupes destinés aux cadres professionnels.

8- Traitement et analyse de données :

Pour traiter et analyser le questionnaire, nous avons travaillé avec la suite bureautique Microsoft Office Excel 2019 qui est une solution que nous estimons pratique pour notre étude de cas et afin de voir la relation entre les différentes variables à travers un tableau croisé dynamique comme celui que nous avons administré.

9- Les limites de la recherche :

La limite principale que nous avons constaté durant notre étude est le manque d'engagement des gens à répondre à notre questionnaire et cela, malgré la période que nous supposons assez longue pour une collecte importante de réponses.

Certains d'entre eux avaient complètement éloignée l'idée que la sécurité des données figure parmi les critères de la fidélisation, d'autres estiment qu'ils ne comprennent pas le thème de recherche, en refusant ainsi de répondre à notre questionnaire.

CHAPITRE 4 : ÉTAT DES LIEUX ET BILAN DE LA RECHERCHE

Le présent chapitre est scindé en deux parties, à savoir :

- La première partie contient l'état de l'existant du SI de la Compagnie Nationale d'Assurances « SAA »
- La seconde partie contient les résultats de notre recherche ainsi que la discussion de ces derniers à travers le questionnaire administré.

1- État de l'existant du SI de la SAA :

Dans cette partie, nous allons décrire l'état actuel l'ensemble des éléments constituant les solutions techniques nécessaires à l'installation et mise en service d'une infrastructure réseau informatique WAN d'entreprise et sécurité au niveau des 465 sites (Data center, Siège, directions régionales, agences) de la SAA et une solution d'administration centralisée pour la gestion de la plateforme globale en répondant à l'ensemble des besoins exprimés.

Dans ce cadre, nous avons divisé ce dernier en 3 parties :

- Sites centraux (Principal et Backup)
- Directions Régionales (DR)
- Sites distants (Agences)

La sécurité du réseau est basée sur l'organisation suivante :

1.1 Architecture physique :

C'est une architecture décentralisée basée sur un modèle hiérarchique à **trois niveaux** :

- **Niveau primaire** (data center de production à Alger/ data center de relève à Batna),
- **Niveau secondaire** (les directions régionales),
- **Niveau Tertiaire** (les agences au niveau de tout le territoire national).

Elle permet le raccordement des agences aux directions régionales et des directions centrales aux deux data center par le biais des routeurs Cisco.

L'interconnexion des sites est mise en place grâce à l'infrastructure IP/MPLS (RMS) qui est assurée par Algérie Télécom.

Chaque agence de la SAA possède une base de données interne à l'agence où sont stockées les informations des clients.

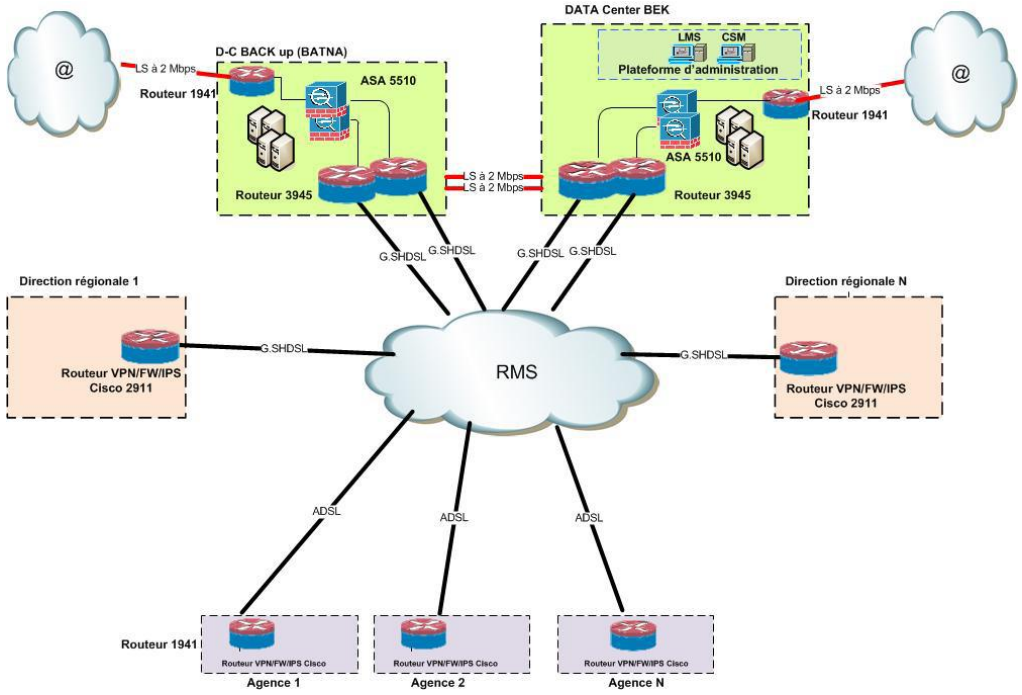
On distingue chaque agence avec son propre adressage IP (adresse privée commençant par 172.16.X.X).

La connectivité inter agence, agence-Direction Régionale et/ou Agence-Direction Centrale passe par deux moyens de communication :

- **La connectivité LAN (Local Area Network)** permet une meilleure sécurité des données car les informations sont seulement transférables uniquement dans le réseau de la SAA.
- **La connectivité WAN (Wide Area Network)** permet une meilleure sécurité des données, car les informations sont uniquement transférables sur le réseau interne de la SAA (un seul réseau intranet) et doit obligatoirement passer par le service IP/MPLS d'Algérie Telecom conformément à la réglementation en vigueur.

Pour ce qui est de la consolidation des données, l'opération se fait au niveau des Directions Régionales ainsi qu'au niveau central.

Figure 8 : Architecture réseau de la SAA



Source : document interne.

Description de l'interconnexion des sites :

L'interconnexion des sites se fait par régions, les Agences correspondantes à une région se connecteront à leurs propres Direction Régionale, et toutes les Directions Régionales se connecteront au Site principal et éventuellement au site Backup en cas de sinistre.

Centralisation Internet et Messagerie :

Les Agences ont une connexion Internet centralisée au niveau des Data Centers, un utilisateur peut se connecter à Internet en contactant un serveur proxy au niveau du Data Center.

Pour cela, un serveur proxy sur chaque Data Center est installé et exploite les deux liens Internet au niveau des Data Centers Bab Ezzouar et Batna et ce, en configurant sur les postes utilisateurs les paramètres Proxy correspondants (Une partie d'utilisateurs passent par Bab Ezzouar et l'autre partie passent par Batna).

Concernant le serveur de messagerie, il est hébergé au niveau du Data Center Principal de Bab Ezzouar, son Backup est hébergé au niveau de Batna, les utilisateurs ont ainsi une messagerie centralisée au niveau des deux Data Centers.

Description des liens WAN de la SAA :

Les deux sites Data center sont reliés à Internet chacun avec un lien LS à 2 Mbps pour la centralisation de la connexion Internet de tous les sites et la sécurité du réseau WAN en éliminant ainsi des accès non contrôlés des agences.

L'interconnexion entre les deux sites Data center est reliée à travers deux liaisons spécialisés (LS) à 2 Mbps chacune pour la réplication des informations et des données du site Data center principal vers le Data center backup. Ces deux liaisons sont également exploitées pour la redondance des autres liens SHDSL au niveau des Data Centers.

L'interconnexion des sites régionaux au site Data center principal, ou en cas de sinistre au site Data center backup, se fait via le réseau RMS, les liens au niveau de tous les sites ainsi que la DG sont de type G. SHDSL à 2,3 Mbps.

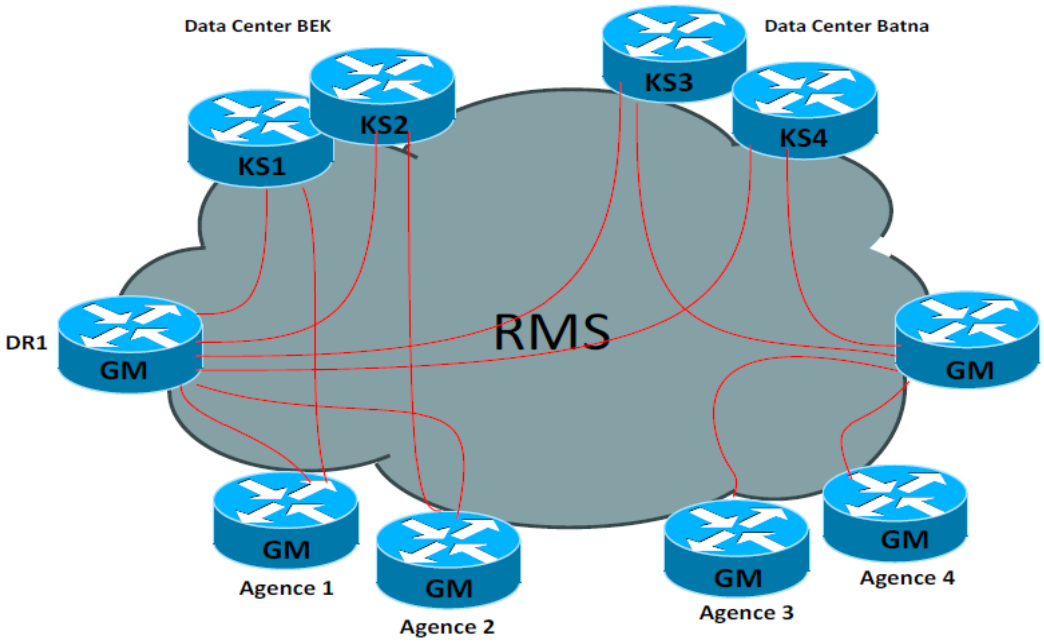
L'interconnexion des Agences aux sites Régionaux (Directions Régionales) ou la DG se fait via le réseau RMS, le lien au niveau des Directions est comme décrit plus haut (en G. SHDSL à 2,3 Mbps, et au niveau des Agences les liens sont de types ADSL à 1 Mbps).

1.2 Architecture logique

L'architecture logique est dépendante d'Algérie Télécom, qui offre un accès au réseau RMS de type **niveau 3** (Layer 3), c'est-à-dire que la gestion du routage du réseau WAN de la SAA est assurée par Algérie Télécom et ont à pointer le trafic vers les Gateways (PE) que l'ISP nous fournira en utilisant une **VRF (Virtual Routing and Forwarding)** dédiée à la SAA, cette VRF isolera le trafic de la SAA au sein du réseau RMS d'Algérie Télécom.

Le schéma ci-dessous nous montre l'architecture logique de la solution.

Figure 9 : Architecture logique de routage de la SAA



Source : document interne.

La communication interagence, inter DR n'est en effet pas possible puisqu'un mécanisme d'ACL (Access List) est mis en place pour prévenir cela, par contre les agences peuvent communiquer directement avec la direction centrale pour obtenir une information absente au niveau de l'agence.

La sauvegarde est assurée au niveau de chaque agence vers le site central à un intervalle de J-1

Le site de Backup au niveau de Batna est mis en place afin de prévenir toute altération pour assurer la haute disponibilité.

Si le site central tombe en panne la réplication est assurée grâce au site backup situé au niveau de Batna

Et tout le réseau (agence et DR) est automatiquement basculé vers le site backup pour assurer la reprise d'activité

La sécurité est assurée de deux manières :

- Les ACL (Access List) prévenir la transversalité des communications (agence-agence et DR-DR)
- La solution VPN pour crypter ces informations et garantir leur confidentialité.

1.3 Base de données :

1.3.1 La première consolidation

La première consolidation des données se fait via l'agence vers la direction régionale à qui elle est attachée au niveau des 15 directions régionales.

Cette première consolidation se fait tous les jours automatiquement en insérant les nouveaux ajouts ou modifications via des manipulations du SGBD (insert).

Chaque fin du mois, la direction régionale se voit dotée d'une base de données consolidée totale faite de manière manuelle.

1.3.2 La deuxième consolidation :

Chaque chef département envoie la base de données de la direction régionale consolidée au site central via le réseau WAN.

Au niveau du site central se fait une réplication hebdomadaire de la base de données consolidée vers le site de BATNA Backup.

1.3.3 La récolte des données :

Le chef département au niveau de la direction régionale récupère 2 documents importants chaque fin de semaine qui sont :

- Les données techniques DT ;
- Les données comptables DC ;

Via le réseau WAN pour des raisons marketing.

1.3.4 Intégrité des données :

L'intégrité des données est respectée au niveau de l'agence et aucune violation n'est autorisée à se produire

Le personnel habilité à manipuler les données est soumis à des autorisations offertes par la direction générale

L'intégrité des données est protégée par des contraintes mises en place qu'on appelle : les polices de contrôle : chargé de vérifier s'il n'y a pas violation à l'intégrité de la donnée.

Passons maintenant à la seconde partie de notre chapitre qui concerne les résultats et la discussion sur le questionnaire de recherche :

2- Résultats et discussion :

Nous allons présenter dans la partie suivante les résultats obtenus du questionnaire et les discuter par la suite.

2.1 Les résultats de la recherche

Dans cette première partie, on passe en revue les différents résultats de notre recherche.

L'échantillon de l'étude se compose de 100 répondants, constitué de 34 clients de la SAA et de 66 répondants qui ne sont pas clients.

2.1.1 Répartition de l'échantillon selon le nombre de clients

Figure 10 : Répartition de l'échantillon selon le nombre de clients

Source : Elaboré par nos soins via Google Forms

Nous avons relevé que 66 personnes ont répondu par « non » et que 34 personnes ont répondus par « oui » (clients SAA).

Nous allons nous intéresser particulièrement à la catégorie des clients qui représentent 34% des répondants.

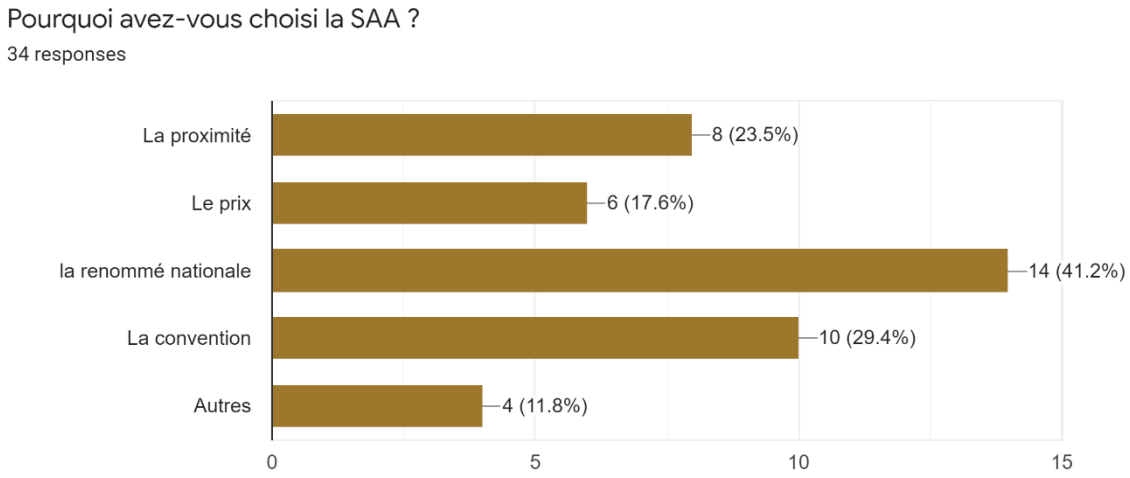
Tableau 2: Répartition de l'échantillon selon le nombre de clients.

Nombre client	Fréquence	Pourcentage
Clients	34	34%
Autres	66	66%
Total	**100**	**100%**

Source : Elaboré par nos soins à partir des résultats de recherche

2.1.2 Répartition de l'échantillon relatif aux raisons du choix de la compagnie :

Figure 11 : Répartition de l'échantillon relatif aux raisons du choix de la compagnie



Source : Elaboré par nos soins via Google Forms

Nous constatons que le critère de « renommée nationale » représente 41,2%, c'est le critère principal de choix des clients de la compagnie.

En seconde position, le critère de « la convention » équivaut à 29,4%.

Le tableau suivant permet de montrer que le critère de renommée nationale est le critère de choix pour les clients avec 8 clients soit 23,53% de la totalité.

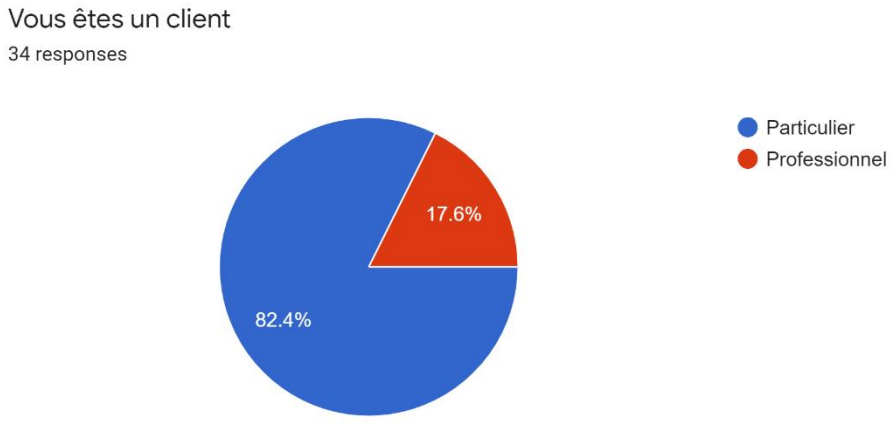
Tableau 3: Répartition de l'échantillon relatif aux raisons du choix de la compagnie

La cause du choix	Fréquence	Pourcentage
La renommée nationale	8	23,53%
Le convention	7	20,59%
La proximité	5	14,71%
Autres	4	11,76%
Le prix	2	5,88%
La renommée nationale, la convention	2	5,88%
Le prix, la renommée nationale	2	5,88%
La proximité, la renommée nationale	2	5,88%
La proximité, le prix	1	2,94%
Le prix, la convention	1	2,94%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.3 Répartition de l'échantillon selon le type de clients :

Figure 12: Répartition de l'échantillon selon le type de clients



Source : Elaboré par nos soins via Google Forms

Nous constatons que les clients particuliers représentent la majorité avec un taux de 82,4% soit 28 clients, tandis que les clients professionnels représentent seulement 17,6% soit 6 clients.

Le tableau ci-après démontre les résultats obtenus :

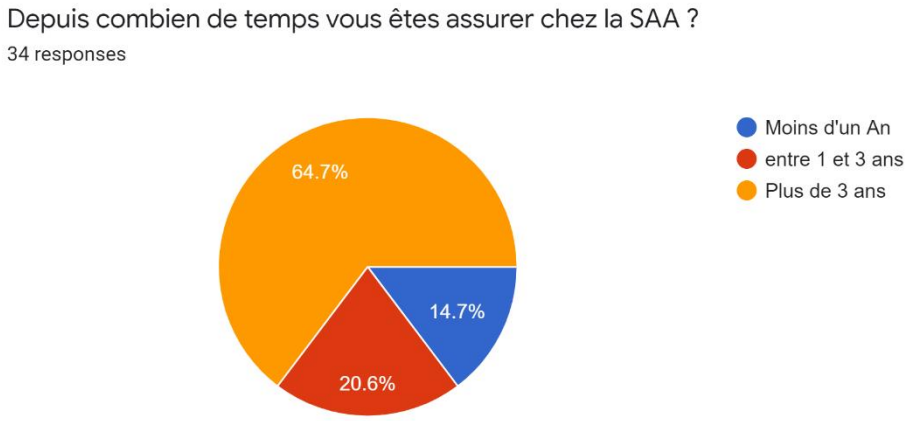
Tableau 4: Répartition de l'échantillon selon le type de clients

Type	Fréquence	Pourcentage
Particulier	28	82,4%
Professionnel	6	17,6%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.4 Répartition de l'échantillon selon la durée d'assurance :

Figure 13: Répartition de l'échantillon selon la durée d'assurance



Source : Elaboré par nos soins via Google Forms

Nous constatons que :

- 64,7% des clients sont assurés depuis plus de 3 ans, soit 22 clients.
- 20,6%, soit 7 clients déclarent qu'ils sont assurés depuis plus d'un An.
- 14,7%, soit 5 clients à moins d'un An.

Le tableau suivant illustre les résultats obtenus :

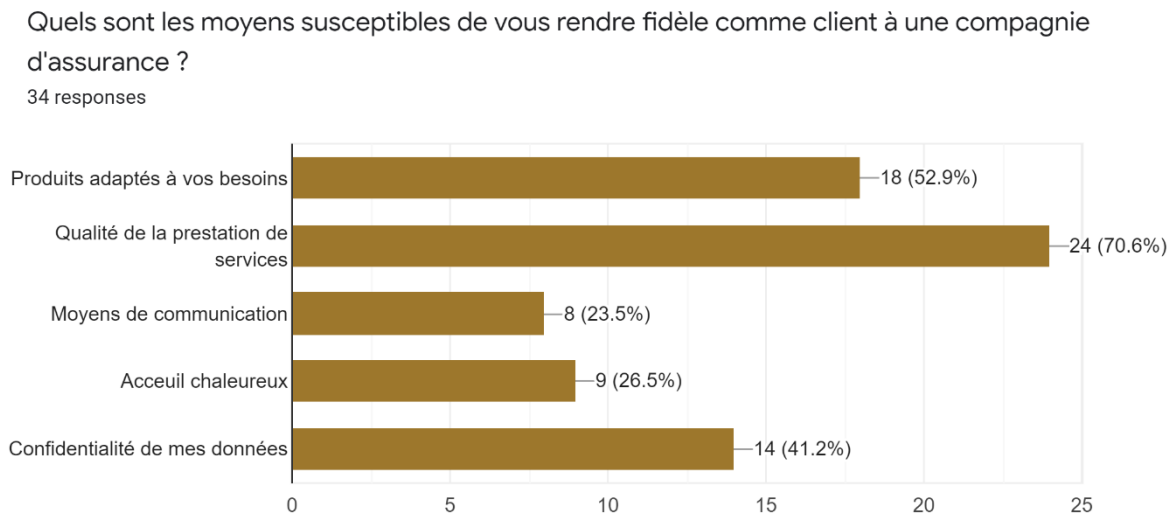
Tableau 5: Répartition de l'échantillon selon la durée d'assurance

Durée d'assurance	Fréquence	Pourcentage
Moins d'un An	5	14,7%
Entre 1 et 3 ans	7	20,6%
Plus de 3 ans	22	64,7%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.5 Répartition de l'échantillon selon les moyens de fidélité :

Figure 14: Répartition de l'échantillon selon les moyens de fidélité



Source : Elaboré par nos soins via Google Forms

Ce graphe permet de montrer que parmi les moyens de rendre un client fidèle, sont :

- La qualité de prestation de service,
- Les produits adaptés aux besoins
- La confidentialité des données.

La qualité de service avec 70,6% représente le critère le plus choisi par les clients.

Ensuite, les produits adaptés aux besoins, la confidentialité des données avec respectivement 52,9% et 41,2%.

Tableau 6: Répartition de l'échantillon selon les moyens de fidélité

Les moyens de fidélité	Fréquence	Pourcentage
Produits adaptés à vos besoins, Qualité de la prestation de services, Confidentialité de mes données	8	23,52%
Produits adaptés à vos besoins, Qualité de la prestation de services, Moyens de communication	6	17,64%
Qualité de la prestation de services, Confidentialité de mes données	3	8,82%
Qualité de la prestation de services, Accueil chaleureux	3	8,82%
Qualité de la prestation de services, Moyens de communication, Accueil chaleureux, Confidentialité de mes données	2	5,88%
Qualité de la prestation de services	2	5,88%
Qualité de la prestation de services, Moyens de communication, Confidentialité de mes données	2	5,88%
Confidentialité de mes données	1	2,94%
Produits adaptés à vos besoins, Qualité de la prestation de services, Accueil chaleureux, Confidentialité de mes données	1	2,94%
Produits adaptés à vos besoins	1	2,94%
Produits adaptés à vos besoins, Accueil chaleureux	1	2,94%
Accueil chaleureux	1	2,94%
Produits adaptés à vos besoins, Qualité de la prestation de services, Moyens de	1	2,94%

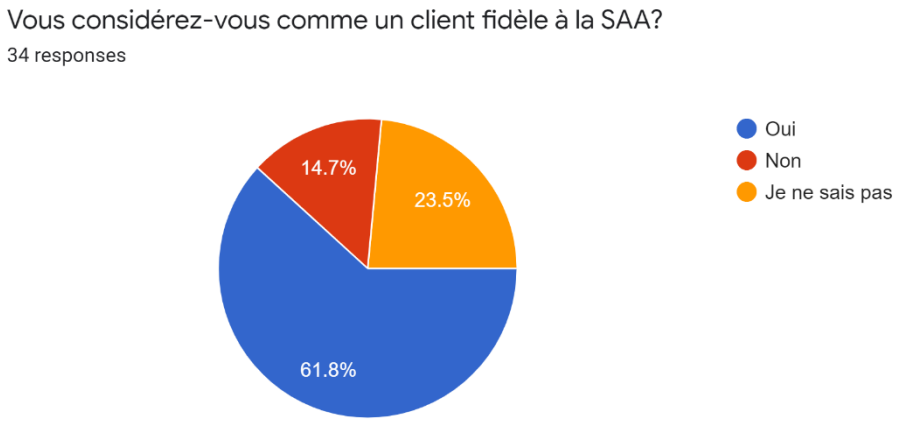
communication, Accueil chaleureux, Confidentialité de mes données		
Produits adaptés à vos besoins, Confidentialité de mes données	1	2,94%
Produits adaptés à vos besoins, Qualité de la prestation de services	1	2,94%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

Ce tableau permet de confirmer que les trois critères de la qualité de prestation de service, les produits adaptés aux besoins et la confidentialité des données sont les plus représentés avec 8 clients et un taux de 23%.

2.1.6 Répartition de l'échantillon selon le critère de la fidélisation :

Figure 15: Répartition de l'échantillon selon le critère de la fidélisation



Source : Elaboré par nos soins via Google Forms

Il est démontré que la majorité des clients (61,8%) représentant 21 clients, se déclarent fidèle à la SAA.

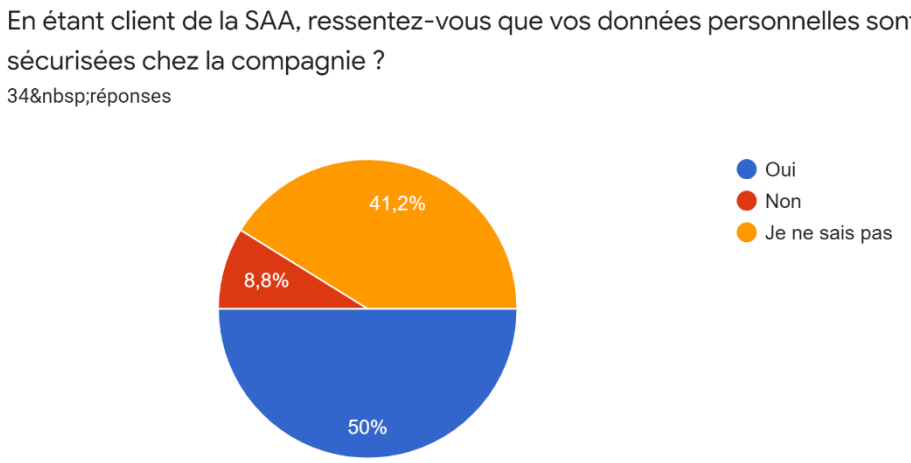
Tableau 7: Répartition de l'échantillon sur la fidélisation

Client fidèle	Fréquence	Pourcentage
Oui	21	61,8%
Non	5	14,7%
Je ne sais pas	8	23,5%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.7 Répartition de l'échantillon selon le sentiment de la préservation de la sécurité des données

Figure 16 : Répartition de l'échantillon selon le sentiment de la préservation de la sécurité des données



Source : Elaboré par nos soins via Google Forms

Ce graphe permet de constater que la moitié (50%) des clients ressentent que leurs données sont protégées et sécurisées.

On peut observer aussi que 41,2% des clients ne savent pas si leurs données sont protégées ou pas.

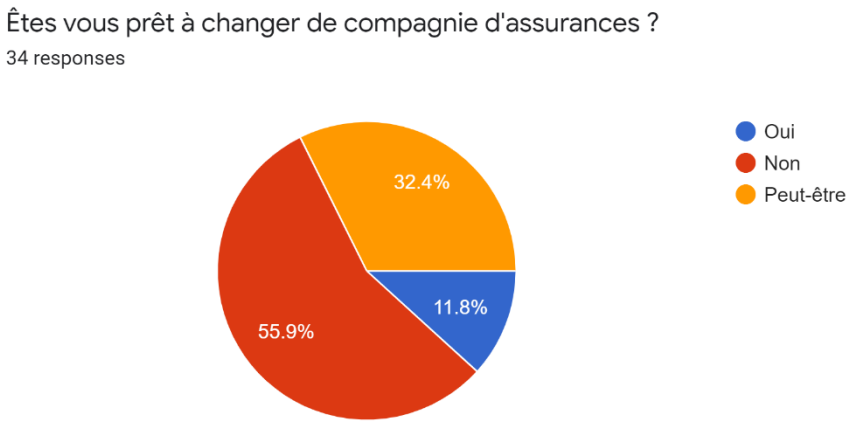
Tableau 8: Répartition de l'échantillon selon le sentiment de la préservation de sécurité des données.

Données sécurisées	Fréquence	Pourcentage
Oui	17	50%
Non	3	8,8%
Je ne sais pas	14	41,2%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.8 Répartition de l'échantillon sur la volonté de changement de compagnie

Figure 17 : Répartition de l'échantillon sur le changement de compagnie.



Source : Elaboré par nos soins via Google Forms

Nous constatons que la majorité des répondants (55,9%) soit 19 clients déclarent qu'ils ne veulent pas changer de compagnie.

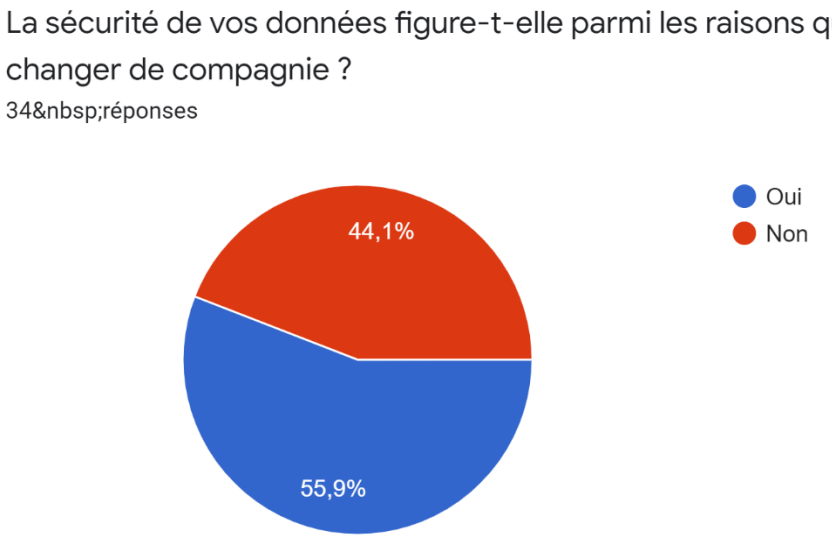
Tableau 9: Répartition de l'échantillon sur la volonté de changement de compagnie

La volonté de changement	Fréquence	Pourcentage
Oui	4	11,8%
Non	19	55,9%
Peut être	11	32,4%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.9 Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie :

Figure 18 : Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie.



Source : Elaboré par nos soins via Google Forms

Nous remarquons que 55,9% soit 19 clients estiment que la sécurité est parmi les raisons qui pousse à changer de compagnie, alors que 44,1% soit 15 clients estiment le contraire.

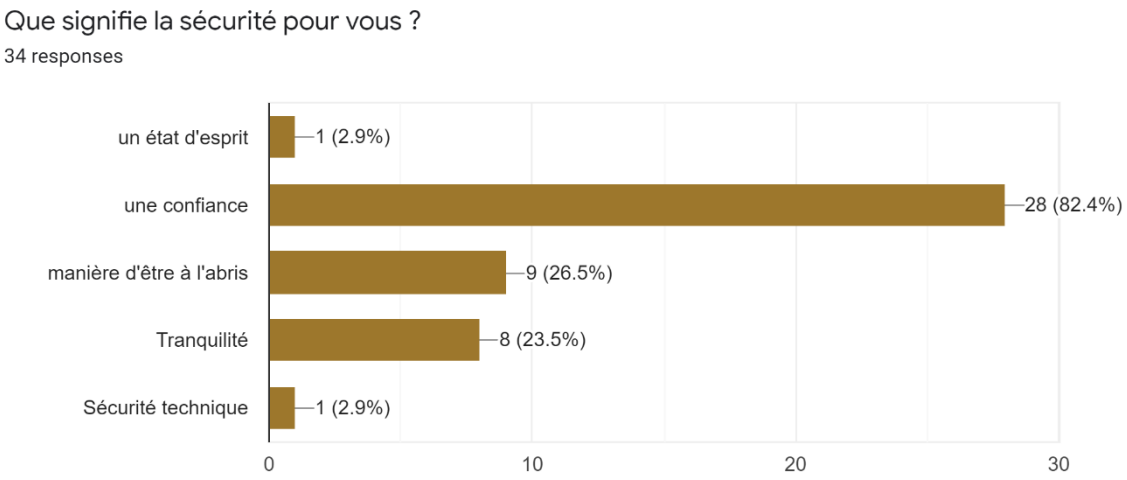
Tableau 10: Répartition de l'échantillon selon le critère de sécurité comme raison de changement de compagnie.

La raison de sécurité	Fréquence	Pourcentage
Oui	19	55,9%
Non	15	44,1%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche.

2.1.10 Répartition de l'échantillon selon la signification de la sécurité pour le client :

Figure 19 : Répartition de l'échantillon selon la signification de la sécurité pour le client



Source : Elaboré par nos soins via Google Forms

Ce graphique permet de constater que la grande majorité des clients considère la sécurité comme un élément de confiance envers la compagnie avec un taux de 82,4%.

Dans le tableau qui suit, il est démontré que le critère de confiance définit seul la sécurité pour la grande majorité des répondants soit 19 clients avec un taux de 55,88%.

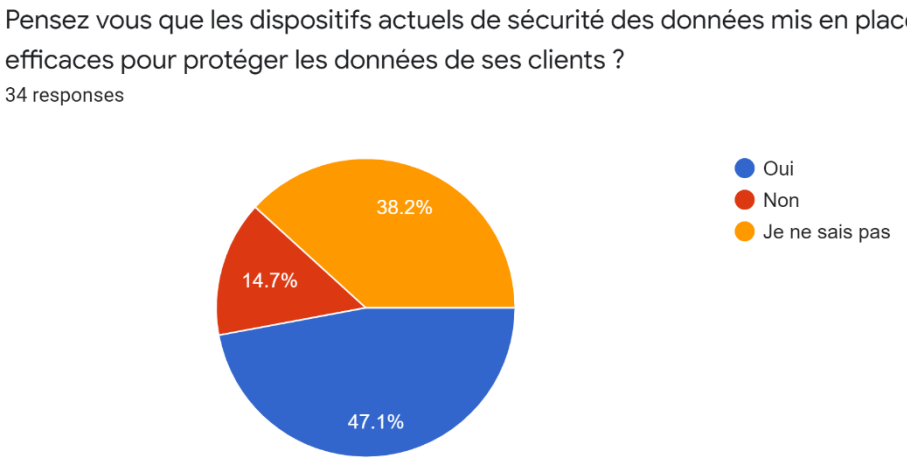
Tableau 11: Répartition de l'échantillon sur la signification de la sécurité pour le client

Signification de sécurité	Fréquence	Pourcentage
Une confiance	19	55,88%
Une confiance, une tranquillité	4	11,76%
Manière d'être à l'abri	4	11,76%
Une confiance, manière d'être à l'abri, tranquillité	2	5,88%
Une confiance, manière d'être à l'abri	2	5,88%
Tranquillité	1	2,94%
Sécurité technique	1	2,94%
Un état d'esprit, une confiance, manière d'être à l'abri, une tranquillité	1	2,94%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.11 Répartition de l'échantillon sur l'efficacité des dispositifs actuels de sécurité des données :

Figure 20: Répartition de l'échantillon sur l'efficacité des dispositifs actuels de sécurité des données



Source : Elaboré par nos soins via Google Forms

Ce graphe nous permet de constater que 47,1% soit 16 clients pensent que le dispositif actuel de sécurité des données est efficace.

Tableau 12: Répartition de l'échantillon sur la l'efficacité des dispositifs actuels de sécurité des données

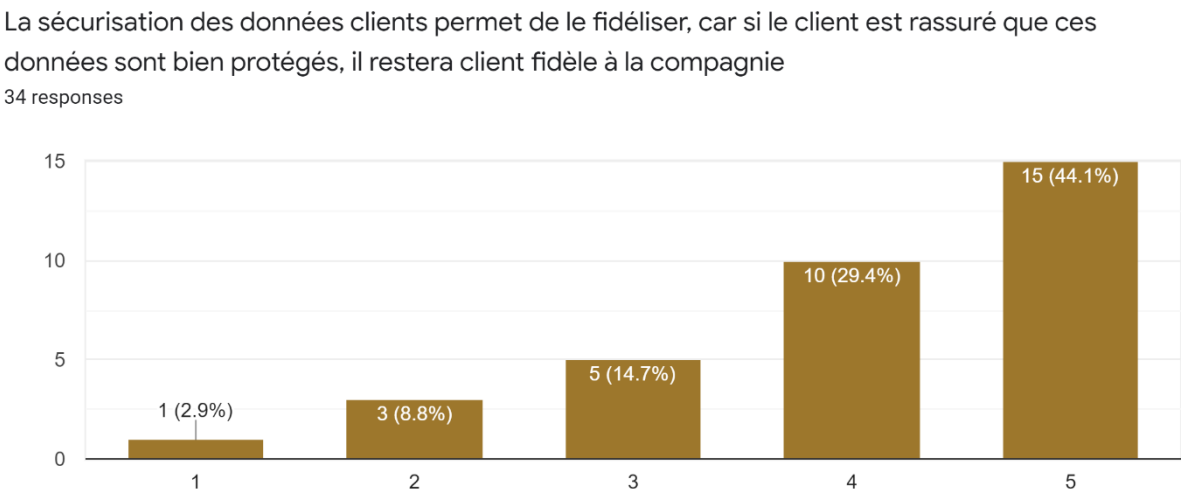
Efficacité des dispositifs actuels de sécurité des données	Fréquence	Pourcentage
Oui	16	47,1%
Non	5	14,7%
Je ne sais pas	13	38,2%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.12 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1 :

L'affirmation 1 : La sécurisation des données clients permet de le fidéliser, car si le client est rassuré que ces données sont bien protégées, il restera client fidèle à la compagnie.

Figure 21 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1



Source : Elaboré par nos soins via Google Forms

Nous constatons que 44,1% soit 15 clients sont tout à fait d'accord avec l'affirmation 1.

Tableau 13: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 1

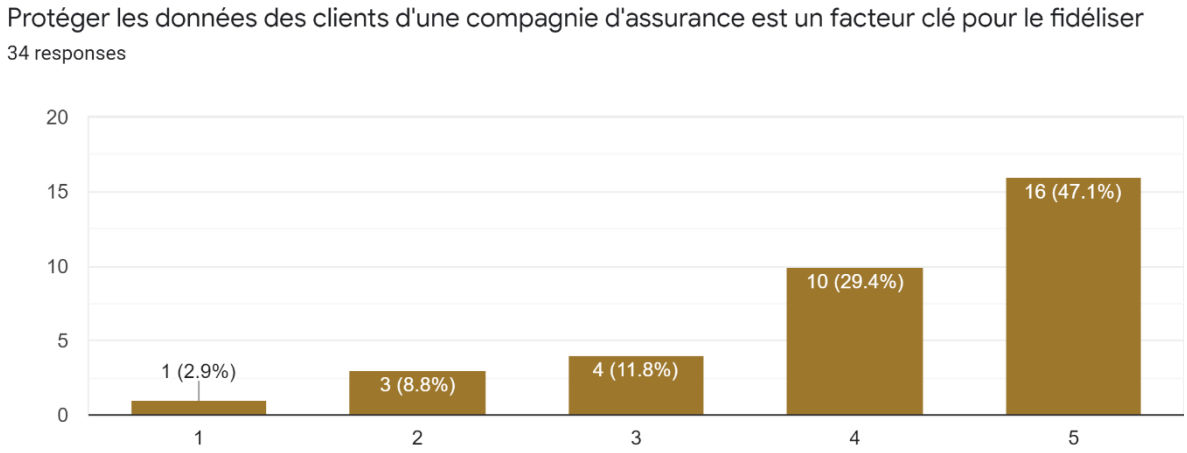
Degré	Fréquence	Pourcentage
1	1	2,9%
2	3	8,8%
3	5	14,7%
4	10	29,4%
5	15	44,1%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.13 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2 :

Affirmation 2 : Protéger les données des clients d'une compagnie d'assurance est un facteur clé pour le fidéliser.

Figure 22: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2



Source : Elaboré par nos soins via Google Forms

Ce graphe permet d'observer que 47,1% soit 16 clients sont tout à fait d'accord avec l'affirmation 2.

Tableau 14: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 2

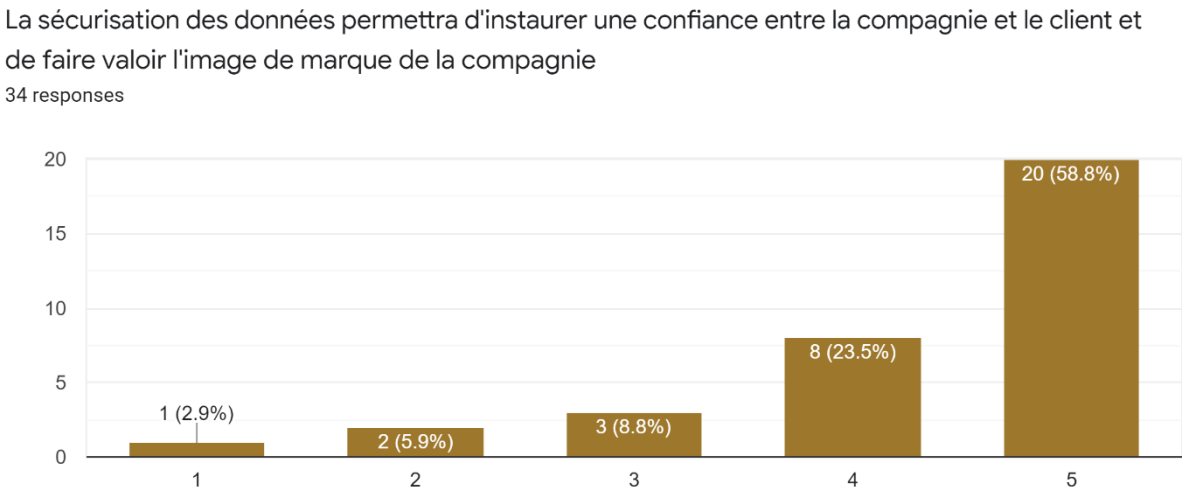
Degré	Fréquence	Pourcentage
1	1	2,9%
2	3	8,8%
3	4	11,8%
4	10	29,4%
5	16	47,1%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.14 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 :

Affirmation 3 : La sécurisation des données permettra d'instaurer une confiance entre la compagnie et le client et de faire valoir l'image de marque de la compagnie

Figure 23: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3



Source : Elaboré par nos soins via Google Forms

Nous constatons que 58,8% soit 20 clients sont tout à fait d'accord avec l'affirmation 3.

Tableau 15: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3

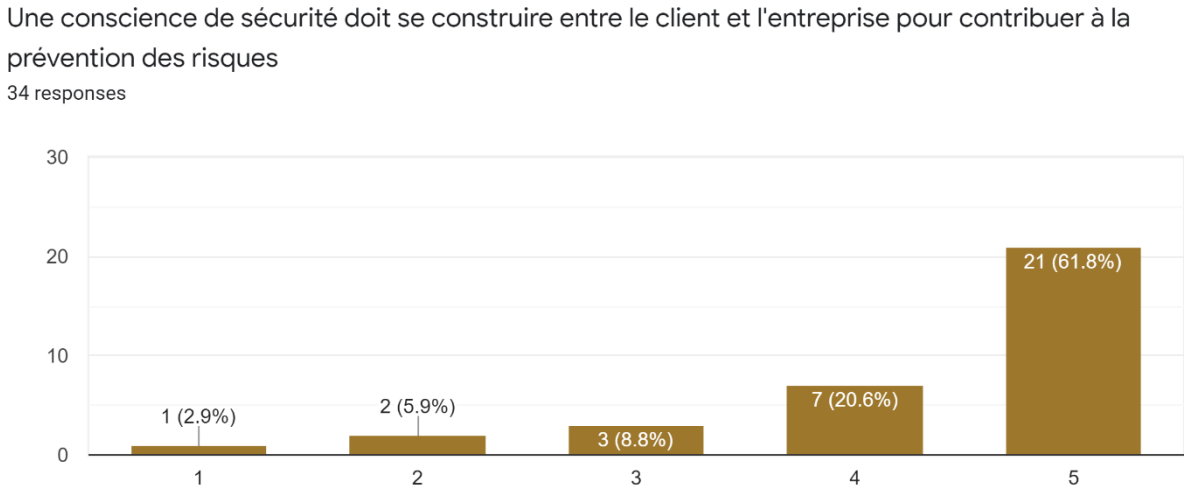
Degré	Fréquence	Pourcentage
1	1	2,9%
2	2	5,9%
3	3	8,8%
4	8	23,5%
5	20	58,8%
Total	**34**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.15 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 4 :

Affirmation 4 : Une conscience de sécurité doit se construire entre le client et l'entreprise pour contribuer à la prévention des risques.

Figure 24 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation



Source : Elaboré par nos soins via Google Forms

Ce graphe nous permet de voir que la majorité des clients 61,8% soit 21 clients sont tout à fait d'accord avec l'affirmation 4.

Tableau 16 : Répartition de l'échantillon selon le degré d'accord avec l'affirmation 4

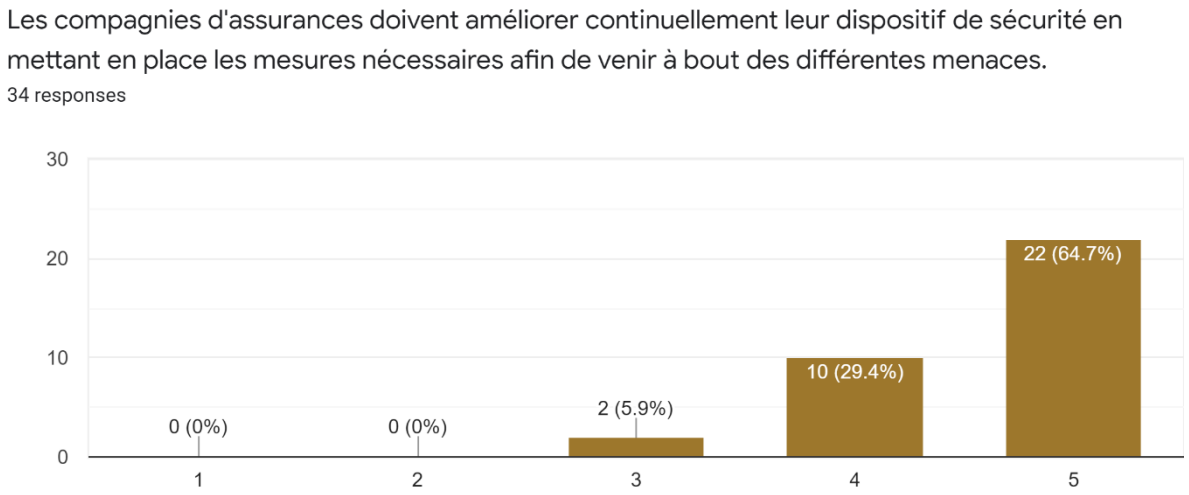
Degré	Fréquence	Pourcentage
1	1	2,9%
2	2	5,9%
3	3	8,8%
4	7	20,6%
5	21	61,8%
Total	**34**	**100%**

Source : Elaboré par nos soins à partir des résultats de recherche

2.1.16 Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5 :

Affirmation 5 : Les compagnies d'assurances doivent améliorer continuellement leur dispositif de sécurité en mettant en place les mesures nécessaires afin de venir à bout des différentes menaces.

Figure 25: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5



Source : Elaboré par nos soins via Google Forms

Ce graphique permet d'observer que 66,7% soit 22 clients déclarent être tout à fait d'accord avec l'affirmation 5.

Tableau 17: Répartition de l'échantillon selon le degré d'accord avec l'affirmation 5

Degré	Fréquence	Pourcentage
1	0	0%
2	0	0%
3	2	5,9%
4	10	29,4%
5	22	64,7%
Total	**34**	**100%**

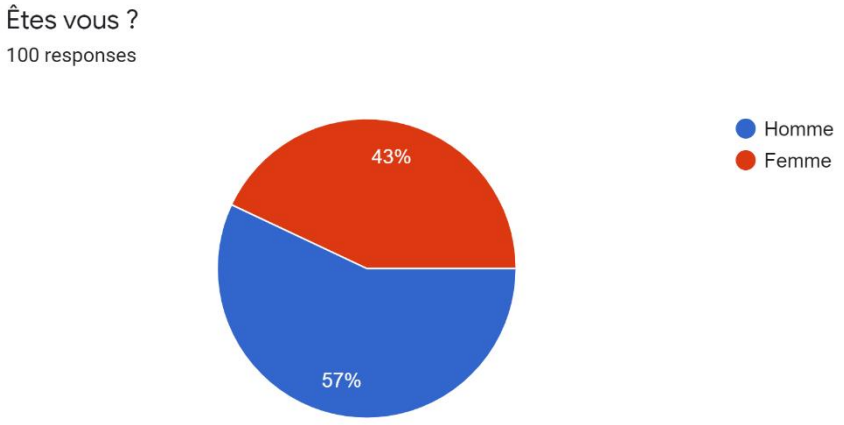
Source : élaboré par nos soins à partir des résultats de recherche

Les trois dernières catégories de ce questionnaire permettront de renseigner sur le genre du répondant (hommes/femmes), la catégorie d'âges et la catégorie socio professionnelle.

Après le remplissage de tous les champs, les clients de la SAA et les autres sont redirigés vers les trois dernières catégories pour clôturer le questionnaire.

2.1.17 Répartition de l'échantillon selon le genre :

Figure 26: Répartition de l'échantillon selon le genre



Source : Elaboré par nos soins via Google Forms

On constate que 57% des répondants sont des hommes et 43% sont des femmes.

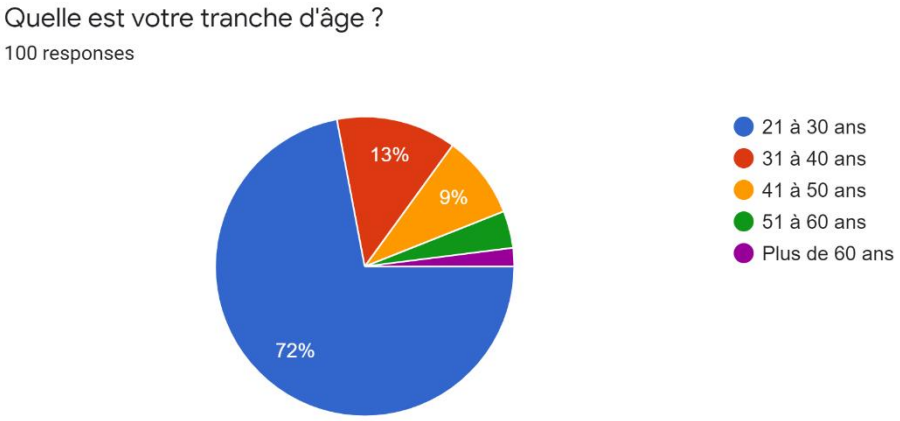
Tableau 18: Répartition de l'échantillon selon le genre

Genre	Fréquence	Pourcentage
Hommes	57	57%
Femmes	43	43%
Total	**100**	**100%**

Source : élaboré par nos soins à partir des résultats de recherche

2.1.18 Répartition de l'échantillon selon la tranche d'âge :

Figure 27: Répartition de l'échantillon selon la tranche d'âge



Source : Elaboré par nos soins via Google Forms

Ce graphe permet d'observer que :

- La majorité des répondants sont âgés de 21 à 30 ans (72%) soit 72 répondants.
- La seconde catégorie est celle de 31 à 40 ans avec 13 répondants,
- Ensuite celle de 41 à 50 ans (9%) soit 9 répondants.

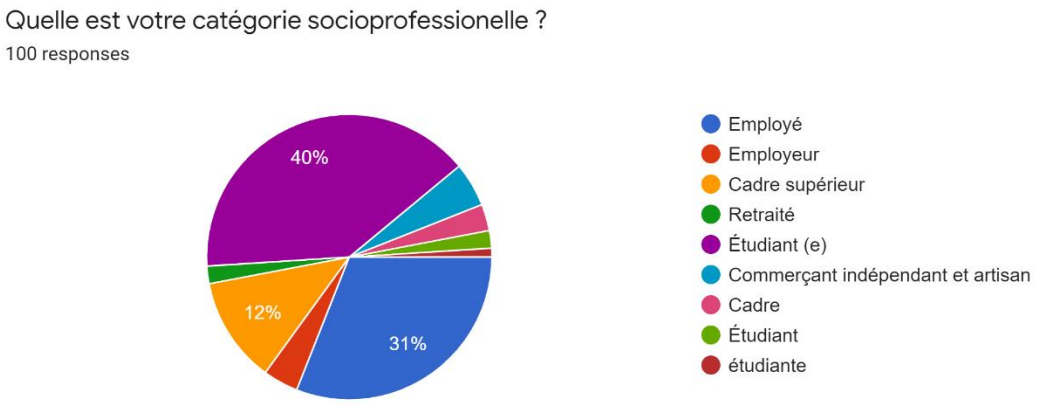
Tableau 19: Répartition de l'échantillon selon la tranche d'âge

La tranche d'âge	Fréquence	Pourcentage
21 à 30 ans	72	72%
31 à 40 ans	13	13%
41 à 50 ans	9	9%
51 à 60 ans	4	4%
Plus de 60 ans	2	2%
Total	100	100%

Source : élaboré par nos soins à partir des résultats de recherche

2.1.19 Répartition de l'échantillon selon la catégorie socioprofessionnelle :

Figure 28: Répartition de l'échantillon selon la catégorie socioprofessionnelle



Source : Elaboré par nos soins via Google Forms

Ce graphique confirme le précédent pour les jeunes répondants puisque la majorité des répondants sont des étudiants avec 43% soit 43 répondants, s'ensuit 31% soit 31 répondants issue de la catégorie des employés.

Tableau 20: Répartition de l'échantillon selon la catégorie socioprofessionnelle

La catégorie socioprofessionnelle	Fréquence	Pourcentage
Employés	31	31%
Employeurs	4	4%
Cadre supérieurs	15	15%
Etudiants	43	43%
Commerçants et artisans	5	5%
Retraités	2	2%
Total	100	100%

Source : élaboré par nos soins à partir des résultats de recherche

Une dernière partie a été dédiée aux commentaires, pour les personnes souhaitant s'exprimer et donner leur avis.

Après avoir fait le point sur les différentes réponses du questionnaire, nous avons sélectionné deux commentaires sur le questionnaire de la part d'un des répondants qui affirme que :

« Après avoir répondu à ce questionnaire spontanément, j'aimerai vous faire part en tant employé à la SAA que cet aspect de la sécurité des données n'est pas vraiment tenu en compte par les clients. Cordialement »

Un autre répondant estime que : *« La sécurité des données clients est importante mais n'est pas un critère décisif dans l'optique de fidéliser les clients. »*.

2.2 La discussion des résultats

Nous passons maintenant à la partie concernant la discussion des résultats que nous avons énumérés précédemment.

Notre recherche s'est terminée avec les résultats suivant :

Pour éclaircir la lecture du tableau, nous allons découper le tableau en des parties liés entre elles

Tableau 21: Relation entre les variables partie 1

Pourquoi avez-vous choisi la SAA ?	Nbr 1	Vous êtes un client ?	Nbr 2	Depuis combien de temps vous êtes assuré chez la SAA ?	Nbr 3
La renommée nationale	8	Particulier	28	Plus de 3 ans	22
La convention	7	Professionnel	6	Entre 1 et 3 ans	7
La proximité	5			Moins d'un An	5
Autres	4				
Le prix	2				
La renommée nationale, La convention	2				
Le prix, la renommée nationale	2				
La proximité, la renommée nationale	2				
La proximité, Le prix	1				
Le prix, La convention	1				
Total	**34**		**34**		**34**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

Tableau 22: Relation entre les variables partie 2

Quels sont les moyens susceptibles de vous rendre fidèle comme client à une compagnie d'assurance ?	Nbr 4	Vous considérez-vous comme un client fidèle à la SAA ?	Nbr 5	En étant client de la SAA, ressentez-vous que vos données personnelles sont protégées et sécurisé chez la compagnie ?	Nbr 6
Produits adaptés à vos besoins, Qualité de la prestation de services, Confidentialité de mes données	8	Oui	21	Oui	17
Produits adaptés à vos besoins, Qualité de la prestation de services, Moyens de communication	6	Je ne sais pas	8	Je ne sais pas	14
Qualité de la prestation de services, Confidentialité de mes données	3	Non	5	Non	3
Qualité de la prestation de services, Accueil chaleureux	3				
Qualité de la prestation de services, Moyens de communication, Accueil chaleureux, Confidentialité de mes données	2				

Qualité de la prestation de services	2				
Qualité de la prestation de services, Moyens de communication, Confidentialité de mes données	2				
Confidentialité de mes données	1				
Produits adaptés à vos besoins, Qualité de la prestation de services, Accueil chaleureux, Confidentialité de mes données	1				
Produits adaptés à vos besoins	1				
Produits adaptés à vos besoins, Accueil chaleureux	1				
Accueil chaleureux	1				
Produits adaptés à vos besoins, Qualité de la prestation de services, Moyens de communication, Accueil chaleureux, Confidentialité de mes données	1				

Produits adaptés à vos besoins, Confidentialité de mes données	1				
Produits adaptés à vos besoins, Qualité de la prestation de services	1				
Total	**34**		**34**		**34**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

Tableau 23: Relation entre les variables partie 3

Êtes-vous prêt à changer de compagnie d'assurances ?	Nbr 7	La sécurité de vos données figure-elle parmi les raisons qui vous pousse à changer de compagnie ?	Nbr 8	Que signifie la sécurité pour vous ?	Nbr 9
Non	19	Oui	19	Une confiance	19
Peut être	11	Non	15	Une confiance, Tranquillité	4
Oui	4			Manière d'être à l'abris	4
				Une confiance, manière d'être à l'abris, Tranquillité	2
				Une confiance, manière d'être à l'abris	2
				Tranquillité	1

				Sécurité technique	1
				Un état d'esprit, une confiance, manière d'être à l'abris, Tranquillité	1
Total	**34**		**34**		**34**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

Tableau 24: Relation entre les variables partie 4

Pensez-vous que les dispositifs actuels de sécurité des données mis en place par la SAA sont efficaces pour protéger les données de ses clients ?	Nbr 10	Affirmation 1	Nbr 11	Affirmation 2	Nbr 12
Oui	16	5	15	5	16
Je ne sais pas	13	4	10	4	10
Non	5	3	5	3	4
		2	3	2	3
		1	1	1	1
Total	**34**		**34**		**34**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

Tableau 25: Relation entre les variables partie 5

Affirmation 3	Nbr 13	Affirmation 4	Nbr 14	Affirmation 5	Nbr 15
5	20	5	21	5	22
4	8	4	7	4	10
3	3	3	3	3	2
2	2	2	2	2	
1	1	1	1	1	
Total	**34**		**34**		**34**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

Tableau 26: Relation entre les variables partie 6

Êtes-vous ?	Nbr 16	Quelle est votre tranche d'âge ?	Nbr 17	Quelle est votre catégorie socioprofessionnelle ?	Nbr 18
Homme	57	21 à 30 ans	72	Etudiant (e)	43
Femme	43	31 à 40 ans	13	Employé	31
		41 à 50 ans	9	Cadre supérieur	12
		51 à 60 ans	4	Commerçant indépendant et artisan	5
		Plus de 60 ans	2	Employeur	4
				Cadre	3
				Retraité	2
Total	**100**		**100**		**100**

Source : Elaboré par nos soins via Microsoft Office Excel 2019

A partir des données résultantes du tableau croisé dynamique établi via Excel, Il est à signaler que les clients particuliers de la SAA qui ont contracté des assurances depuis plus de 3 ans ont opté pour le critère de la « renommée nationale » lors de leur choix de la société, cela dénote l'état de la confiance, de la notoriété de cette compagnie.

Parmi les moyens susceptibles de fidéliser ces clients, on peut citer les critères suivants :

- Les produits adaptés aux besoins ;
- La qualité des prestations de service ;
- La confidentialité des données ;

En effet les clients questionnés sur le critère de la sécurité de leurs données s'estiment protégées et sécurisés. Ce critère est indispensable pour la fidélisation des clients, qui signifie pour la grande majorité un critère de confiance.

Les cinq affirmations énumérées dans notre sondage ont suscité un intérêt certain pour la plupart des clients et ont tous adhérer à ces affirmations.

Ces clients appartiennent à la catégorie des jeunes âgés entre 21 et 30 ans d'âge.

Ce qui renforce le sentiment de la sécurité des données, qui reste primordial, mais par contre il ne constitue pas un critère de choix lors de la fidélisation du client.

Enfin, le client cherche des produits adaptés à ses besoins et une meilleure prestation de service

D'où la confirmation de l'hypothèse 1 qui stipule que : « l'état actuel de la sécurité mis en place par la compagnie permet de sécuriser les données ».

Par contre l'hypothèse 2 qui stipule que « les dispositifs de sécurité actuelle permettent de fidéliser le client. » est rejetée par l'autre partie qui estime que le critère de sécurité n'est pas un élément de fidélisation.

Pour conclure ce chapitre, nous pouvons dire que la sécurité des données est très importante pour le maintien de la notoriété et l'image de l'entreprise, mais elle n'est pas essentielle à la fidélisation du client, qui cherche des prestations de service de qualité à la hauteur de ses espérances. Il reste fidèle à une entreprise non pas, par rapport à la sécurité de ses données mais par rapport aux conventions et aux services qui lui fournissent des avantages et du gain de temps.

CONCLUSION GÉNÉRALE

Notre recherche sur la thématique de l'impact de la sécurisation des données sur la fidélisation client avait pour objectif de voir si le critère de la sécurité des données peut contribuer à la fidélisation du client.

Nous avons effectué notre stage de trois mois au sein de la société nationale d'assurances (SAA) afin confirmer ou d'infirmer notre résultat de recherche qui se portait sur les deux volets de sécurité des données et la fidélisation client.

À travers le questionnaire de recherche et les réponses que nous avons eus, nous nous sommes rendu compte que le critère de sécurité n'est pas une priorité lors de la fidélisation client et que le client cherche d'autres moyens susceptibles de le rendre fidèle à une marque ou à un service.

Néanmoins, la sécurité des données est devenue une exigence dans le monde entier pour chaque entreprise souhaitant mettre en place une politique de collecte de données de ses clients, notamment avec l'émergence des réseaux sociaux qui ont changé radicalement les habitudes de travail.

La sécurité nécessite dorénavant une attention particulière, car le monde économique tend vers la digitalisation des services et que les technologies évoluent vite, les entreprises se voient avoir du mal à rattraper ou même ne pas avoir de volonté de suivre et peuvent avoir des conséquences graves qui peuvent toucher même l'image de l'entreprise et sa notoriété dans le marché.

Nous avons aussi remarqué une conscience des clients envers la sécurité des données et la connaissance de sa valeur dans le monde numérique, mais cette conscience reste virtuelle ou théorique, car dès qu'il s'agit de réalité du terrain, elle ne devient plus un critère pour le client lors de son choix sur les facteurs qui le rendent fidèle.

Notre travail a rencontré un manque d'engagement de la part des personnes auxquelles s'adressait le questionnaire en premier lieu, certains d'entre eux vont même écarter la notion de sécurité du domaine des assurances, car d'après eux, ce critère est loin d'être leur facteur déterminant pour leur choix ou l'écarte carrément et le second problème était la crise sanitaire du covid 19 qui ne nous a pas permis de nous déplacer à notre guise afin de peaufiner notre travail de recherche.

Il est nécessaire d'effectuer davantage de recherche sur la thématique afin de découvrir la vraie raison qui pousse les clients à ne pas se soucier de la sécurité des données et même contribuer à la construction de la conscience sur la sécurité en général.

Pour clôturer ce travail, nous avons pris le soin de faire quelques recommandations que nous jugeons pertinentes au développement de la conscience des clients sur la sécurité des données.

En premier, il serait judicieux de mettre en place des compagnes de sensibilisation pour les collaborateurs sur les dangers auxquelles est confronté le monde de l'entreprise en donnant des exemples sur ce qui se passe ailleurs dans le monde afin de les faire ressentir que les données qu'ils manipulent représentent un patrimoine précieux pour le bon fonctionnement et la pérennité de toute l'entreprise.

En second lieu, l'entreprise pourra créer un climat de confiance avec ses clients en leur offrant les services sur des supports numériques, de valoriser et mettre en avant la sécurité comme critère de référence pour l'entreprise en garantissant la confidentialité de leurs données.

Pour l'entreprise en interne, l'acquisition de nouvelles technologies innovantes pour s'aligner avec ce qui se fait de mieux dans le monde.

Ceci étant quelques recommandations que nous espérons va contribuer à l'amélioration de la relation des clients avec l'entreprise dans un monde où la concurrence est rude.

RÉFÉRENCES BIBLIOGRAPHIQUES

Bibliographie

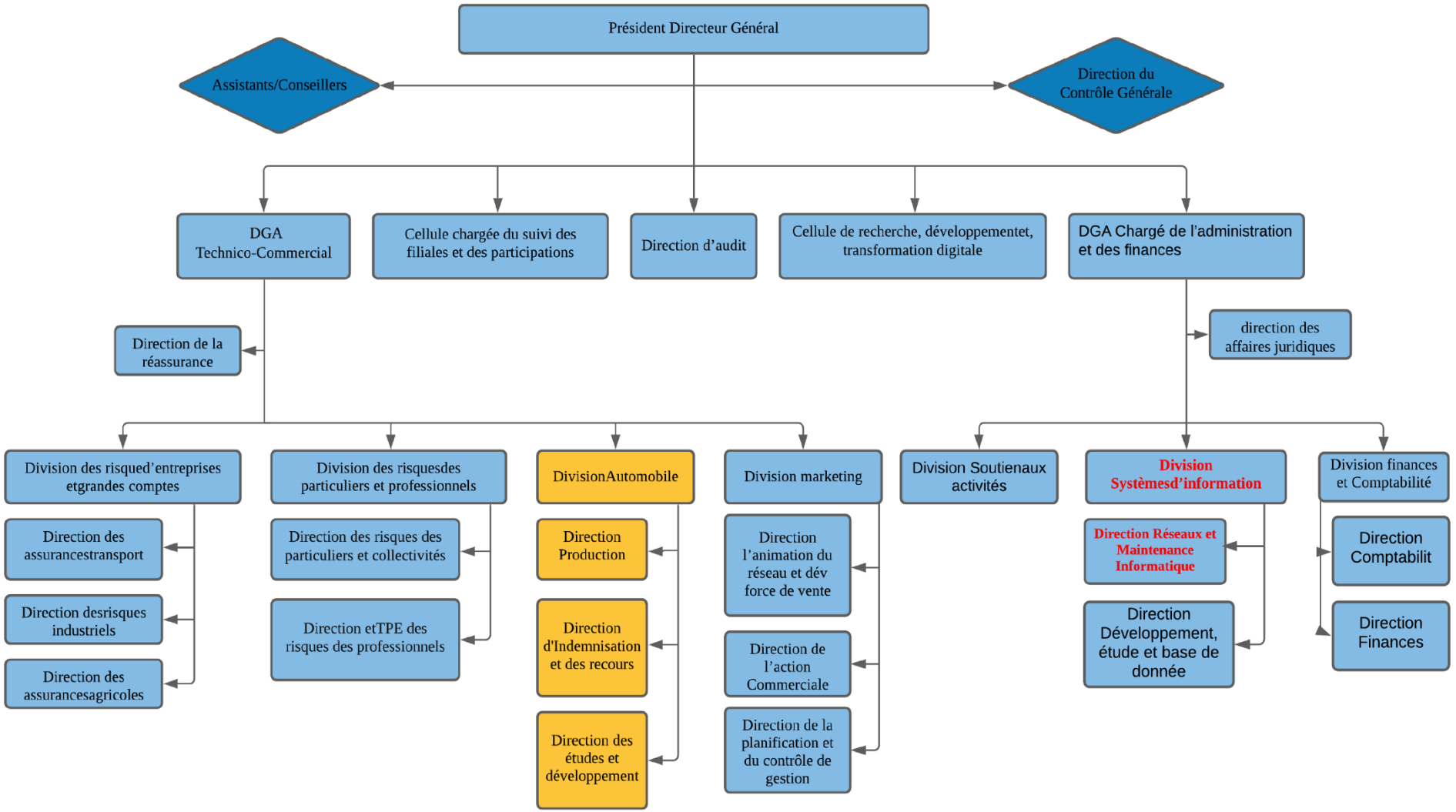
- Chen, A. (2017). Gérer les données personnelles fournies aux applications. *I2D - Information, données & documents*, *54*(3), 47. https://doi.org/10.3917/i2d.173.0047
- Deville de Periere, D. (2013). Les enjeux de la sécurité de l'information dans le monde économique. *Marché et organisations*, *18*(2), 19. https://doi.org/10.3917/maorg.018.0019
- Dumoulin, R., & Lancelot Miltgen, C. (2012). Entreprise et respect de la vie privée du consommateur. De l'usage autorisé à l'utilisation souhaitable des données personnelles. *Revue française de gestion*, *38*(224), 95-109. https://doi.org/10.3166/rfg.224.95-109
- Dupont, B. (2010). Les organisations : Sentinelles aveugles de la sécurité des données personnelles ? *Sécurité et stratégie*, *3*(1), 27. https://doi.org/10.3917/sestr.003.0027
- Elvy, S.-A. (2017). PAYING FOR PRIVACY AND THE PERSONAL DATA ECONOMY. *Columbia Law Review*, *117*(6), 1369-1459. JSTOR.
- Kyriazoglou, J. (2019). *Données et de confidentialité*. 5.
- Le Cœur, J. (2016). Sécuriser les données personnelles de son entreprise. *I2D - Information, données & documents*, *53*(1), 25. https://doi.org/10.3917/i2d.161.0025
- MAYER Nicolas, HUMBERT Jean-philippe(2006) «la gestion des risques pour les systèmes d'informations» Article paru dans le magasine MISC n°24
- Paquet, P. (2006). *De l'information à la connaissance*. 25.
- Razafy N. R., Randriamaroson R. M, Rakotomiraho S, (2016), "la sécurisation des données" "MADA-ETI",1(14), ISSN 2220-0675, pp. 134-143. www.madarevues.gov.mg
- Sahut, J. M., Moez, K., & Mutte, J.-L. (2011). Satisfaction et fidélisation aux services d'internet Banking, quelle influence sur la fidélité à la banque ? *Management & Avenir*, *47*(7), 260. https://doi.org/10.3917/mav.047.0260
- Trinquecoste, J.-F. (1996). FIDÉLISER LE CONSOMMATEUR : UN OBJECTIF MARKETING PRIORITAIRE. Décisions Marketing, 7, 17–23. http://www.jstor.org/stable/40592523

Sitographie

- https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html (consulté le 10/08/2021 à 22 :47)

- https://la.saa.dz/fr/about (consulté le 11/08/2021 à 19 : 42)
- https://www.kaspersky.com/about (consulté le 15/08/2021 à 15 :30)
- https://www.kaspersky.com/gdpr (consulté le 15/08/2021 à 15 : 30)

ANNEXE A : ORGANIGRAMME DE LA SAA


Président Directeur Général
Assistants/Conseillers
Direction du Contrôle Générale
DGA Technico-Commercial
Cellule chargée du suivi des filiales et des participations
Direction d'audit
Cellule de recherche, développementet, transformation digitale
DGA Chargé de l'administration et des finances
Direction de la réassurance
direction des affaires juridiques
Division des risqued'entreprises etgrandes comptes
Division des risquesdes particuliers et professionnels
DivisionAutomobile
Division marketing
Division Soutienaux activités
Division Systèmesd'information
Division finances et Comptabilité
Direction des assurancestransport
Direction desrisques industriels
Direction des assurancesagricoles
Direction des risques des particuliers et collectivités
Direction etTPE des risques des professionnels
Direction Production
Direction d'Indemnisation et des recours
Direction des études et développement
Direction l'animation du réseau et dév force de vente
Direction de l'action Commerciale
Direction de la planification et du contrôle de gestion
Direction Réseaux et Maintenance Informatique
Direction Développement, étude et base de donnée
Direction Comptabilit
Direction Finances

ANNEXE B : STRUCTURE DU QUESTIONNAIRE

Étude de l'impact de la sécurisation des données sur la fidélisation client

Dans le cadre de la préparation de notre mémoire de fin d'études de cycle master académique spécialité Management E-Gouvernement à l'École nationale supérieure de management (ENSM) situé au pôle universitaire de Koléa — wilaya de Tipaza.

L'intitulé de la thématique est : « l'impact de la sécurisation des données sur la fidélisation client » au sein de la Société Nationale d'assurances (SAA)

Notre étude se concentre sur l'étude de ces deux (2) volets qui sont :

- La sécurité des données.

- La fidélisation client.

Et voir s'il y' a une relation d'impact entre eux.

Durant l'élaboration de notre mémoire, nous sommes arrivés à nous poser la problématique de recherche suivante :

Quel est l'impact de la sécurisation des données sur la fidélisation client ?

Afin d'aboutir à un résultat concret de notre recherche, nous vous prions de nous consacrer de votre temps afin de répondre aux questions ci-dessous :

N. B. : (les réponses à ce questionnaire seront uniquement utilisées à des fins purement académiques.)

Question : **Êtes-vous client de la Société Nationale d'Assurances (SAA) ?**

☐ Oui

☐ Non

Merci de nous avoir consacré de votre temps pour répondre à ce questionnaire

Pour rappel : les réponses à ce questionnaire sont uniquement utilisées à des fins purement académiques, aucune réponse du questionnaire ne serait divulguée à une tierce personne.

Question 1 : **Pourquoi avez-vous choisi la SAA ?**

- ☐ La proximité
- ☐ Le prix
- ☐ La renommée nationale
- ☐ La convention
- ☐ Autres

Question 2 : **Êtes-vous un client ?**

- ☐ Particulier
- ☐ Professionnel

Question 3 : **Depuis combien de temps êtes-vous assuré chez la SAA ?**

- ☐ Moins d'un an
- ☐ Entre 1 et 3 ans
- ☐ Plus de 3 ans

Fidélisation Client

La fidélisation est un attachement à une marque du fait de sa bonne prestation de service où d'un privilège attribué à un client par rapport à un autre, dans un marché concurrentiel très fort.

Question 1 : **Quels sont les moyens susceptibles de vous rendre fidèle comme client à une compagnie d'assurance ?**

- ☐ Produits adaptés à vos besoins
- ☐ Qualité de la prestation de
- ☐ Moyens de communication
- ☐ Accueil chaleureux
- ☐ Confidentialité de mes données

Question 2 : **Vous considérez-vous comme un client fidèle à la SAA ?**

- ☐ Oui
- ☐ Non
- ☐ Je ne sais pas

Question 3 : **En étant client de la SAA, ressentez-vous que vos données personnelles sont protégées et sécurisées chez la compagnie ?**

- ☐ Oui
- ☐ Non
- ☐ Je ne sais pas

Question 4 : **Êtes-vous prêt à changer de compagnie d'assurances ?**

- ☐ Oui
- ☐ Non
- ☐ Peut-être

Question 5 : **La sécurité de vos données figure-t-elle parmi les raisons qui vous poussent à changer de compagnie ?**

- ☐ Oui
- ☐ Non

Sécurité des données

La sécurité est devenue un atout majeur pour la protection des données et à la pérennité d'une entreprise, dans un monde où les évolutions technologiques sont très rapides et par conséquent les moyens de nuire à une entreprise se développent en parallèle.

Question 1 : **Que signifie la sécurité pour vous ?**

- ☐ Un état d'esprit
- ☐ Une confiance
- ☐ Une manière d'être à l'abri
- ☐ Une tranquillité

Question 2 : **Pensez-vous que les dispositifs actuels de sécurité des données mis en place par la SAA sont efficaces pour protéger les données de ses clients ?**

- ☐ Oui
- ☐ Non
- ☐ Je ne sais pas

- **Sur une échelle de 1 => (pas du tout d'accord) à 5 => (tout à fait d'accord). Quel est votre degré d'accord avec les affirmations ci-dessous ?**

Veuillez choisir un des numéros de ce qui suit.

Affirmation 1 : **La sécurisation des données clients permet de le fidéliser, car si le client est rassuré que ces données soient bien protégées, il restera client fidèle à la compagnie.**

(1) Pas du tout d'accord

(2) Pas d'accord

(3) Ni d'accord ni pas d'accord

(4) D'accord

(5) Tout à fait d'accord

Affirmation 2 : **Protéger les données des clients d'une compagnie d'assurance est un facteur clé pour le fidéliser.**

(1) Pas du tout d'accord

(2) Pas d'accord

(3) Ni d'accord ni pas d'accord

(4) D'accord

(5) Tout à fait d'accord

Affirmation 3 : **La sécurisation des données permettra d'instaurer une confiance entre la compagnie et le client et de faire valoir l'image de marque de la compagnie.**

1. Pas du tout d'accord
2. Pas d'accord
3. Ni d'accord ni pas d'accord
4. D'accord
5. Tout à fait d'accord

Affirmation 4 : **Une conscience de sécurité doit se construire entre le client et l'entreprise pour contribuer à la prévention des risques.**

1. Pas du tout d'accord
2. Pas d'accord
3. Ni d'accord ni pas d'accord
4. D'accord
5. Tout à fait d'accord

Affirmation 5 : **Les compagnies d'assurances doivent améliorer continuellement leur dispositif de sécurité en mettant en place les mesures nécessaires afin de venir à bout des différentes menaces.**

(1) Pas du tout d'accord

(2) Pas d'accord

(3) Ni d'accord ni pas d'accord

(4) D'accord

(5) Tout à fait d'accord

Catégorie clients

Question 1 : **Êtes-vous ?**

☐ Homme

☐ Femme

Question 2 : **Quelle est votre tranche d'âge ?**

☐ 21 à 30 ans

☐ 31 à 40 ans

- [ ] 41 à 50 ans
- [ ] 51 à 60 ans
- [ ] Plus de 60 ans

Question 3 : **Quelle est votre catégorie socioprofessionnelle ?**

- [ ] Employé
- [ ] Employeur
- [ ] Cadre supérieur
- [ ] Retraité
- [ ] Étudiant(e)
- [ ] Commerçant indépendant et artisan

Merci de nous faire part de vos commentaires.

Réponse longue