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 : La Banque D'agriculture Et De Développement Rural (BADR)

Elaboré par :

Moussa Lyna

Encadré par :

Pr. LADOUZI Soumiya

Membres du jury :

Président : Dr. BELAIDI Ali

Examinateur : Pr. BENHIDJEB Taous Asmah

Année universitaire 2021/2022

RÉSUMÉ

L'objectif de cette étude est d'étudier l'impact de la sécurité des données sur la fidélisation de la clientèle à travers une étude quantitative. Nous avons mené un questionnaire afin de voir si le critère de sécurité fait partie des facteurs qui fidélisent la clientèle. Nous avons choisi de mener nos recherches au sein d'une des agences de la Banque BADR qui est considérée comme l'une des leaders du secteur bancaire algérien. Les résultats indiquent que le critère de sécurité est un facteur déterminant et une priorité absolue qui influencent la fidélisation de la clientèle. Cependant ; ce n'est pas un point d'arrêt pour renforcer continuellement les systèmes de sécurité, en particulier avec la large diffusion de la banque électronique qui présente un nouvel ensemble de défis avec chacun. En plus de préserver l'image de marque et la réputation des banques. Cela n'empêche pas l'entreprise de renforcer la sécurité de ses systèmes d'information, car l'image de marque et la réputation dépendent fortement de ce critère pour maintenir une clientèle.

. **Mots clés : impact - sécurisation des données - fidélisation client.**

Abstract

The aim of this study is to study the impact of data security on customer loyalty through a quantitative study. We conducted 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 one of their agencies of the BADR Bank which is considered as one of leading of the Algerian banking Sector. The results indicated that the security criterion is a defining factor and an absolute priority that influence the customer loyalty. However, it is not a stopping point from continuously strengthening the security systems especially with the wide spread of electronical banking which presents a new set of challenges with each. In addition to preserving the banks brand image and reputation. 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 تأثير أمن البيانات على ولاء العملاء من خلال دراسة كمية. أجرينا استبيانا لمعرفة ما إذا كان معيار الأمان من بين العوامل التي تخلق ولاء العملاء. لقد اخترنا إجراء أبحاثنا داخل إحدى وكالات التابعة لبنك بدر الذي يعتبر أحد رواد القطاع المصرفي الجزائري. وأشارت النتائج إلى أن معيار الأمان هو عامل محدد وأولوية مطلقة تؤثر على ولاء العميل. ومع ذلك؛ إنها ليست نقطة توقف عن التعزيز المستمر للأنظمة الأمنية خاصة مع الانتشار الواسع للخدمات المصرفية الإلكترونية التي تمثل مجموعة جديدة من التحديات مع كل منها. بالإضافة إلى الحفاظ على صورة العلامة التجارية للبنوك وسمعتها. ومع ذلك، فإن هذا لا يمنع الشركة من تعزيز أمن أنظمة المعلومات الخاصة بها، حيث تعتمد صورة العلامة التجارية وسمعتها 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 Mesdames Dr. Ladouzi Soumiya, qui a pris le soin de diriger ce travail.

Je remercie également tous les cadres de l’Agence Bancaire BADR notamment ceux de la division système d’information : Mr. Bouslimani Directeur de l’agence des systèmes d’information, madame Kebbal Djamila pour son suivi et ses précieux conseils tout au long de la durée de stage,

Mes remerciements aussi s’adressent à tous ma famille, qui ont contribué de près ou de loin à l’élaboration de ce travail.

Table des matières

Liste des Tableaux

Liste Des Figures

Liste Des Abréviations

BD : Base de données.

BADR : La banque de l'agriculture et de développement rural.

CIA : Confidentiality, Integrity, Availability.

DAI : Direction de l'audit interne.

DC : Département de la communication.

DG : La Direction Générale.

ISO : International Organisation for Standardization

PSSI : La Politique de Sécurité des systèmes d'information

RSSI : Le responsable de la Sécurité des systèmes d'information.

SDBD : Sous-direction Base de données

SGBD : Système de gestion de base de données

SI : Système d'information

SMSI : Un système de management de la sécurité de l'information

SPSS: Statistical Package for the Social Sciences.

TIC : L'évolution des Technologies de l'information et de la communication

INTRODUCTION

Grâce aux nouvelles technologies, les entreprises produisent plus en plus de données, et les échanges des données avec les partenaires et clients sont devenus plus en plus nombreux, cela implique des défis majeurs pour l'entreprise notamment en termes de sécurisation des données. Les organismes ont adopté plusieurs politiques de sécurité afin de garantir la sécurité de leur système d'information contre tous attaques ou menaces.

L'efficacité de ces systèmes d'informations nécessite un ensemble des dispositifs de sécurité et de confidentialité des données, d'où des efforts humains et financiers doivent mise en œuvre pour que l'organisation assure la protection de leur système d'information.

Les organisations risquent de perdre leur image dans le cas d'une mauvaise gestion des données, ce qui conduit de perdre de leur clientèle, car une bonne relation avec le client se base sur la confiance entre l'organisme et ce dernier. Une conscience de l'importance des données doit se construire pour les organisations ainsi que les usagers afin de créer une sphère de confiance entre ces deux.

Dans notre étude, nous avons choisi d'étudier le cas de la Banque d'agriculture et de développement rurale, du fait que la sécurité des systèmes d'information est un élément primordial dans ce secteur, parce que les banques sont considérées comme des réseaux de confiance. Elles ont pour mission de protéger l'argent et les autres objets de valeur pour leurs clients.

Afin de construire une vision claire en termes de sécurité des données et de fidélisation des clients de la banque BADR, nous avons formulé la question de recherche principale : Quel est l'impact de la sécurisation des données sur la fidélisation des clients de la BADR ?

Nous avons décomposé cette question principale en trois sous-questions :

1. Quelle est l'importance de la sécurisation des données pour la BADR ?
2. Comment les clients de la BADR jugent-ils la sécurisation de leurs données bancaires ?
3. Comment la sécurisation des données favorise-t-elle la fidélisation du client ?

Dans le but de répondre à notre problématique, nous mettons en évidence deux hypothèses de recherche :

Hypothèse 1 : les dispositifs actuels de sécurité des données de la banque permettent de Sécuriser les données.

Hypothèse 2 : La sécurisation des données clients est un facteur clé pour le rendre fidèle.

Pour mieux répondre aux différentes questions de notre recherche et de tester nos hypothèses, nous avons choisi de mettre en place un questionnaire auprès des clients de la BADR afin qu'ils donnent leurs avis sur la sécurité des données au sein de la banque.

Dans le cadre de notre étude, nous allons suivre le plan de travail suivant :

Chapitre 1 : Problématique

Dans ce premier chapitre, on va détailler tous les éléments essentiels de la problématique.

Chapitre 2 : Cadre théorique

Dans ce chapitre, nous allons présenter notre revue de littérature et toutes les notions relatives à la sécurisation des données et à la fidélisation client

Chapitre 3 : Cadre méthodologique

Nous allons définir la méthodologie de notre étude.

Chapitre 4 : Résultats et discussions

Nous allons d'abord exposer les différents dispositifs de sécurité mise en place par la BADR et par la suite discuter des résultats du cas pratique.

CHAPITRE 1 : PROBLEMATIQUE

Dans ce chapitre on va souligner notre problématique de la recherche, donc on va présenter le contexte de la recherche, sa contribution sur le plan théorique et managérial, ainsi que les objectifs de la recherche.

Dans une seconde partie, nous présenterons le contexte organisationnel choisi pour mener à bien cette étude.

1. Contexte de la recherche :

L'objectif de toute entreprise est de développer de relations avec ses clients, tout en faisant un profit. Cette pratique se concentre sur la relation à long terme avec les clients et la poursuite de leur satisfaction et de leur fidélité. La Banque a été l'une des premières à adopter cette stratégie en raison de la difficulté d'évaluer le service bancaire et le risques perçus par le client est élevé, ainsi que de la confiance est fondamentale dans ce secteur, et pour cela, la Banque vise à mieux répondre aux exigences et aux attentes de ses clients. En effet, la sécurité est parmi les attentes indispensables des clients bancaires, car ils souhaitent d'effectuer leurs transactions financières en toute sécurité. On parle donc de la sécurité comme élément important pour la banque et ses clients.

Dans ce contexte, nous avons centré notre recherche sur l'étude de la sécurité des données dans la banque d'agriculture et de développement rural (BADR) et d'étudier l'avis des usagers sur la sécurité afin de voir l'impact de la sécurisation de données sur la fidélisation clients.

2. Question de la recherche

Sur la base de contexte présenté ci-dessus, nous avons formulé la principale question de recherche : Quel est l'impact de la sécurisation des données sur la fidélisation client ?

À partir de cette problématique, les questions suivantes sont posées :

4. Quelle est l'importance de la sécurisation des données pour la BADR ?
5. Comment les clients de la BADR jugent-ils la sécurisation de leurs données bancaires ?
6. Comment la sécurisation des données favorise-t-elle la fidélisation du client ?

Cependant nos hypothèses de recherches sont formulées comme suit :

Hypothèse 1 : les dispositifs actuels de sécurité des données de la banque permettent de Sécuriser les données.

Hypothèse 2 : La sécurisation des données clients est un facteur clé pour le rendre fidèle.

3. Pertinence de la recherche

Dans cette section, nous expliquerons l'importance de cette étude d'un point de vue théorique et managérial.

3.1. Pertinence théorique

Après nos recherches sur le thème de la sécurité des données personnelles et son impact sur la fidélité des clients, nous avons constaté un manque d'études sur ce sujet, notamment en Algérie. Il est donc important de se concentrer sur ces concepts afin de sensibiliser les gens à l'importance de la sécurité lorsqu'ils entreprennent leurs diverses activités avec la compagne.

3.2. Pertinence managériale

La protection des données dans un environnement informatisé exige la sécurité de l'information dans les systèmes d'information, ceci est déterminant pour les décideurs de l'entreprise afin de minimiser les risques et d'assurer la continuité des activités en réduisant de façon proactive l'impact d'une violation de la sécurité. En outre, assurer la sécurité permet de renforcer la confiance entre les usagers et leur entreprise, ce qui conduit à leur fidélité.

4. Objectifs de la recherche

L'objectif principal de cette recherche est de savoir dans quelle mesure la sécurité des données affecte la fidélité des clients de la BADR. Pour atteindre cet objectif, nous avons fixé les objectifs secondaires suivants : Mesurer et évaluer la fidélité des clients de la BADR, mesurer la sécurité en étudiant les avis des usagers, et présenter les dispositifs actuels de la sécurité des systèmes d'information au sein de la BADR.

5. Contexte organisationnel

Dans cette dernière section nous allons présenter la BADR et l'agence BADR.

5.1. Présentation de la BADR

La banque de l'agriculture et de développement rural (**BADR**) est une organisation publique issue de la restructuration de la BABR, elle est créée le 13 mars 1982 par un décret 88- 106, sous forme d'une société nationale par actions au capital social de 2.200.000.000 Da. La **BADR** a pour activité principale de développer les secteurs agricoles, de la pêche et des ressources halieutiques, ainsi que la promotion du monde rural. Guide des banques.

La **BADR** soutient activement le développement de son territoire et les projets de ses clients dont le financement de l'agriculture, des industries agroalimentaires, de la pêche et de l'aquaculture. Tout autant de domaines la mettent au diapason des banques constituant ainsi un support pour le développement et l'amélioration de l'économie nationale (Khadidja & Bachir, 2018).

Afin d'apporter la plus grande satisfaction à la clientèle, la BADR banque a mis plus de 7000 employés avec une équipes de 1200 chargés de clientèle à leur écoute à travers ses 321 agences, 39 groupements régionaux d'exploitation déployés sur le territoire nationale, ainsi qu'un nouveau système d'information pour plus de sécurité, facilité, efficacité et rapidité. C'est le réseau le plus dense en Algérie.

5.1.1. L'évolution historique de la BADR

La banque BADR a traversé trois étapes importantes de son histoire :

- *Première étape (1982, 1990) :*

Au cours de ces huit années, la BADR a acquis une notoriété et une expérience certaine dans le financement de l'agro-alimentaire et de l'industrie mécanique agricole. Cette spécialisation s'inscrivait, alors dans un contexte d'économie planifiée ou chaque banque publique avait son champ d'intervention.

- *Deuxième étape (1991-1999) :*

- La BADR a élargi son champ d'intervention vers les autres secteurs d'activités, et notamment, vers les PME/PMI, tout en restant un partenaire privilégié du secteur agricole.

- L'introduction des technologies informatique tel que le système « SWIFT[1] » pour l'exécution des opérations de commerce international.
- La mise en service de la carte de paiement et de retrait BADR.

En 1999, le capital social de la BADR a augmenté pour atteindre le seuil de 33.000.000.000 de dinars.

[1] SWIFT : est le numéro d'identification internationale d'une banque. Disponible sur : https://droitfinances.commentcamarche.com/faq/23422-code-swift-definition. consulté le 15-06-2022. a 7h.

- *Troisième étape (2000, 2020) :*
  - Etablissement d'un diagnostic exhaustif des forces et faiblesses de la BADR et élaboration d'un plan de mise à niveau de l'institution par rapport aux normes internationales.
  - Généralisation du système réseau local avec réorganisation du progiciel SYBU[2] en client-serveur
  - Concrétisation du concept de « Banque assise » avec « Services Personnalisables » (Agence Amirouche, Chéraga…).
  - L'accès à l'internationale par le lancement dans le système d'information international.

5.1.2. Structure de la BADR

La BADR est structurée en 21 directions centrales, le réseau qui se compose de 42 GRE (Group Régionale d'exploitation), 334 agences réparties sur l'ensemble du territoire national.

5.2. Présentation de la banque accueillante (Agence BADR de Blida) :

L'agence n° 426 Lien Agriculture et Développement Rural est la structure de base de l'exploitation qui a une relation directe avec le client, chargée de mettre en œuvre la politique élaborée par la Direction Générale de la Banque, qui a permis de soutenir les réseaux bancaires et de développer le portefeuille client Elle est affiliée à la Banque de l'Agriculture et du Développement Rural de la Place du Premier Novembre à Blida qui a été créée le 08/09/98.Ses effectifs à l'époque étaient de 15 employés, mais aujourd'hui le nombre est passé à plus de 40 employés.

[2] Sybu est un logiciel, disponible sur : https://sybu.co.za/wp/about/. Consulté le 15-06-2022, a 20h

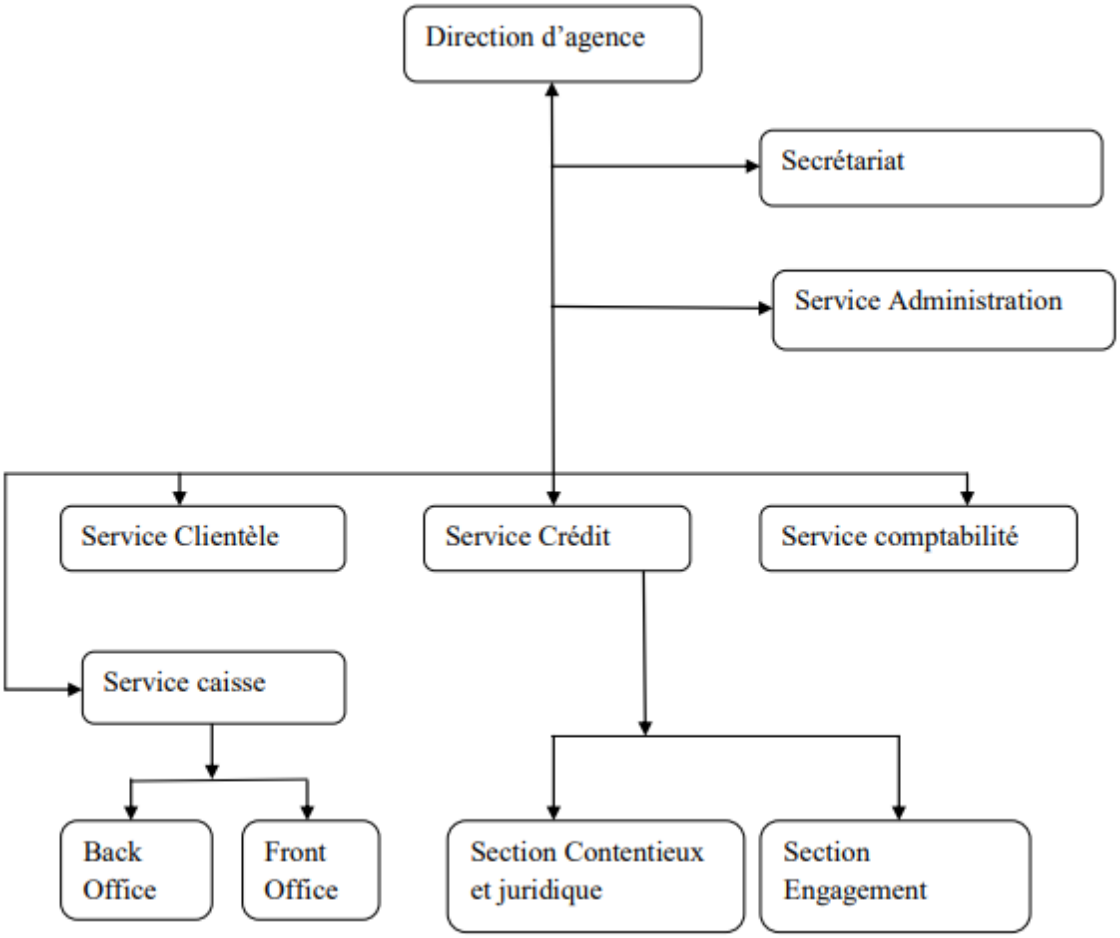


Figure 1:L'organigramme de l'agence BADR de Blida.

Conclusion

A titre de conclusion, il semble intéressant de mettre en évidence les questions actuelles qui se posent sur l'avenir de la banque BADR.

Dans le chapitre suivant ,nous avons détaillé le : CADRE THÉORIQUE.

CHAPITRE 2 : CADRE THÉORIQUE

L'évolution des Technologies de l'information et de la communication (TIC) durant ces dernières décennies implique l'apparition de divers risques pour les organismes publics et les usagers : les menaces sont toujours plus nombreuses et leurs impacts de plus en plus fort sur l'entreprise et ces clients. C'est pourquoi, la sécurisation des données dans les organisations est un enjeu important,

Ce chapitre sera consacré dans la première partie à 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, et dans une deuxième partie à la présentation des termes liés à la sécurité des données et à la fidélisation client.

1. Revue de la littérature

La qualité du service a été définie sur le marketing des services comme une évaluation globale du service par le client(McKecnie et al., 2011). (Khatab et al., 2019)a lié la qualité du service à la satisfaction de la clientèle(Khalaf Ahmad & Ali Al-Zu'bi, 2011) et à la fidélisation de la clientèle(Khalaf Ahmad & Ali Al-Zu'bi, 2011), concluant qu'un client satisfait sera fidèle à l'organisation. La fidélité peut être définie comme un engagement profond afin de racheter des produits ou des services dans les préférences de l'utilisateur (re0.0000). De plus, la littérature sur la qualité du service souligne qu'il existe un vaste corpus de recherches sur la qualité du service (Khatab et al., 2019; McKecnie et al., 2011) et l'impact de ses dimensions (c'est-à-dire la tangibilité, la fiabilité, l'assurance, la réactivité et l'empathie) sur la satisfaction et la fidélité des clients(BOUSSALEM1*, 2022) en particulier dans le secteur bancaire.

En outre, l'objectif principal de la sécurité des données est de protéger les ressources précieuses, telles que le matériel, les logiciels et les informations. Au cours des dernières années, la sécurité des données est devenue un facteur décisif et un obstacle crucial pour une variété d'organisations qui offrent des services qui ont besoin que leurs informations soient protégées et correctement gérées(McCarthy, 2006). (Singh et al., 2020) a révélé que la sécurité et la confidentialité sont une dimension critique de la banque en ligne, l'étude a expliqué que les clients ont tendance à utiliser la banque en ligne si elle est signe de confiance. De même,(Khalaf Ahmad & Ali Al-Zu'bi, 2011) confirme que la sécurité a un impact significatif sur la satisfaction et la fidélité des clients. Par exemple, (Khadidja et al., 2018) a analysé les raisons de la fidélisation de la clientèle algérienne dans les banques publiques, les résultats ont montré que malgré le fait que le marché algérien s'est ouvert aux banques étrangères et malgré l'intégration des nouvelles technologies par ces dernières, la fidélisation de la clientèle algérienne réside auprès de la banque publique pour des raisons de sécurité donc la relation entre le client algérien et la banque publique est une relation de confiance et de sécurité même si le les banques étrangères sont plus développées.

Le tableau (Table 1) représente une sélection d'études qui ont quelque peu analysé la sécurité comme facteur de fidélisation et de satisfaction de la clientèle. Alors que (Intyaswati, 2017) a observé que la fidélité des clients est influencée par les perceptions des clients sur la sécurité des transactions. En outre,(Hammoud et al., 2018) visait à examiner l'impact de la qualité du service E-Banking sur la satisfaction de la clientèle lorsque l'un des facteurs analysés était la sécurité, l'auteur a conclu que, bien que la dimension de la sécurité ait eu un impact positif et significatif sur la satisfaction de la clientèle. Cependant, son impact semblait être inférieur à

celui des autres facteurs de qualité de service. De même, (Yoon, 2010) a étudié la satisfaction de la clientèle dans le secteur bancaire et les résultats ont montré que, parallèlement à d'autres facteurs, la sécurité exerçait une influence significative sur la satisfaction du client.

Table 2:une sélection d'études qui ont quelque peu analysé la sécurité

Reference	Méthodologie	Hypothèse	Résultat
(Intyaswati, 2017)	Approche quantitative+ récupération de données à l'aide d'une méthode d'enquête	H1 : La sécurité des consommateurs influence la fidélité à la marque H2 : La protection de la vie privée des consommateurs influence la fidélité à la marque H3 : La sécurité des consommateurs et la confidentialité, ensemble, influencent la fidélité à la marque H4 : La confiance dans la marque en tant que variable intermédiaire entre la sécurité des consommateurs et la relation de fidélité à la marque H5 : La confiance dans la marque en tant que variable intermédiaire entre la confidentialité des consommateurs et la relation de fidélité à la marque	H1 accepté H2 accepté H3 ne sont pas acceptés H4 accepté H5 accepté
(Hammoud et al., 2018)	Quantitatif+ Récupération de données à l'aide d'une méthode d'enquête + descriptive	H1 : L'efficacité des services E-Banking a un impact positif sur la satisfaction client. H2 : La fiabilité des services E-Banking a un impact positif sur la satisfaction client. H3 : La sécurité et la confidentialité des services E-Banking ont un impact positif sur la satisfaction des clients. H4 : La réactivité et la communication dans le service E-Banking ont un impact positif sur la satisfaction client.	H1 : Pris en charge H2 : Pris en charge H3 : Pris en charge H4 : Pris en charge
(Yoon, 2010)	Une méthode qualitative	H1 : Facilité d'utilisation H2 : Conception H4 : Vitesse de transaction H3 : Sécurité H5 : Contenu de l'information H6 : Support client	H2 : Pris en charge H4 : Pris en charge H5 : Pris en charge H6 : Pris en charge H1 : rejeté H3 : rejeté

2. Cadre Conceptuel

La partie suivante traite les deux termes : la sécurisation des données et la fidélisation client, afin que vous ayez une compréhension plus large sur ces deux concepts.

2.1. Qu'est-ce que la sécurité de l'information ?

- **Data VS Information**

Selon la définition donnée par Davis et Olson :

"Information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or prospective actions or decisions."

Les données peuvent être définies comme un groupe de lettres, de chiffres et de caractères spéciaux sous forme de texte, d'images, d'enregistrements vocaux, etc. Par exemple, le numéro 124578 peut être un numéro de compte bancaire, un numéro d'identification, etc. Le nombre dans cet exemple représente un fait brut et s'appelle donc des données (Bressan et al., 2005).

L'information apporte de la clarté aux données, et de façon très simple on peut dire que l'information est une donnée qui peut être traitée pour produire du sens (figure2.). Ce sont des données connexes qui permettent aux utilisateurs de prendre des décisions. Par exemple, les informations personnelles comprennent les données bancaires telles que les détails de la carte de guichet automatique, les détails de transaction, les mots de passe bancaires et d'autres détails personnels. En outre, l'information se caractérise par les éléments suivants :

- Disponibilité : L'information est accessible au besoin. Par exemple, si un utilisateur a enregistré des données sur le cloud, elles doivent être disponibles lors de l'accès
- Exactitude : L'information est exacte ; les décisions des utilisateurs sont basées sur son exactitude. Par exemple, un employé estime les délais du projet et le budget de l'utilisateur est alloué en fonction de ces informations. Si les informations ne sont pas exactes, cela peut entraîner des retards dans le projet ou même la résiliation.
- Authenticité : l'authenticité fait référence à l'originalité de l'information, l'information ne doit pas être modifiée ou altérée par quiconque. Par exemple, si vous présentez un projet à votre client, il doit être original et authentique.

- Confidentialité : Seules les personnes autorisées qui ont des droits d'accès peuvent voir les informations. Par exemple, le solde bancaire de l'utilisateur est confidentiel, de sorte que seul le personnel autorisé peut y accéder.
- Intégrité : fait référence à la totalité de l'information, l'état de l'information doit être intact et non corrompu. Par exemple, l'utilisateur a enregistré une information importante dans la base de données **(BD)**, une fois récupérée, elle doit être de la même manière qu'elle a été enregistrée.

Figure 2:Le traitement de l'information brute.

- **Définition de la sécurité de l'information**

Dans un aspect général, la sécurité signifie la protection d'actifs précieux contre toute forme d'attaque, qu'il s'agisse d'une invasion de réseaux, de vandalisme, d'une catastrophe naturelle ou d'une mauvaise utilisation. En fin de compte, chaque individu tente de se sécuriser au mieux de ses capacités, compte tenu de son environnement(Bressan et al., 2005)

La sécurité de l'information c'est la pratique consistant à protéger les informations contre toute utilisation non autorisée en plus de la prévention de l'accès, de l'utilisation, de la modification et de la destruction non autorisés des informations. En d'autres termes, il s'agit de la protection des données et des systèmes contre toute utilisation abusive intentionnelle et non intentionnelle (Par exemple, divulgation, modification et suppression)(Bressan et al., 2005).

- **La sécurité des données :**

En sécurité des systèmes d'information, la sécurité des données est la branche qui s'intéresse principalement aux données, en complément des aspects de traitement de l'information(Bressan et al., 2005)

2.2. Qu'est-ce qu'un SI, SMSI et RSSI

Un system d'information est un ensemble de ressources matériels, logiciels, humain, qui permettant la collection, traitement, stockage et diffusion de l'information au sein d'une organisation. Chaque secteur, chaque entreprise et chaque service interprète ce dernier différemment. De plus, l'information est un composant essentiel pour son bon fonctionnement et nécessite, par conséquent, d'être bien sécurisé. L'entreprise doit mettre en place un système de management de la sécurité d'information (Abhishek Chopra Mukund Chaudhary, 2020.)

Un système de management de la sécurité de l'information (SMSI) : est un ensemble de politiques et de procédures permettant de gérer systématiquement les données sensibles d'une organisation. L'objectif d'un SMSI est de minimiser les risques et d'assurer la continuité des activités en limitant de manière proactive l'impact d'une violation de la sécurité. Un SMSI traite généralement du comportement et des processus des employés, ainsi que des données et de la technologie. Il peut être ciblé sur un type particulier de données, telles que les données client, ou il peut être mis en œuvre de manière globale qui fait partie de la culture de l'entreprise. De plus, Il permet de garantir **la confidentialité** des biens sensible (donnée personnelles, administratives, métier etc.) d'un organisme. De plus, il permet de mettre en place des mesures pour préserver **l'intégrité** de l'information (modification intentionnel ou non intentionnel de l'information) **ainsi la disponibilité** de celles-ci seulement aux personnes autorisées. Lorsque on discute les problèmes de sécurité, il est souvent utile d'avoir un modèle comme base ou comme base de référence. Ce dernier offre un ensemble cohérent de terminologie et de concepts. Donc il faut savoir que Le **SMSI** repose sur le modèle CIA Triade composé de trois pilier majeur(Singh et al., 2020) (voir figure) :

- Confidentialité (. e. i. en anglais Confidentiality)
- L'intégrité (e. i. en anglais Integrity)
- Disponibilité (e. i. en anglais Availability)

Figure 3: Le CIA Triade

L'intégration d'un SMSI nécessite (Bressan et al., 2005):

- Sensibiliser les parties prenantes de l'organisme,
- Attribuer des responsabilités liées à la sécurité d'information,
- Prendre en compte l'engagement de la direction et des intérêts de chaque département dans l'organisme,
- Attribuer un rôle clé pour le RSSI, qui a de but de veiller à l'identification et à l'appréciation des risques.

Le responsable de la Sécurité des systèmes d'information (RSSI), il est responsable de mettre en place les mesures de contrôle, assurer la maintenance et améliorer de manière continue de la politique de sécurité pour prévenir de ramener le niveau de risque informatique en dessus adéquates afin de réaliser les objectifs de sécurité de l'information fixés. Pour atteindre tout cela, la RSSI doit définir les mesures adéquates pour la réalisation ces objectifs de sécurité d'information (Bressan et al., 2005).

2.3. Les standards de la sécurité d'information

La sécurisation des informations est un grand défi. Cela inclut non seulement la protection de vos informations personnelles, mais aussi des organisations qui stockent vos informations personnelles sur leurs systèmes. Nous donnons aux organisations notre consentement pour conserver nos renseignements et ils ont la responsabilité de les protéger contre les mauvaises

mains. C'est ainsi qu'un ensemble de normes et de standards ont été créés afin de mettre en œuvre **SMSI** robuste(Bressan et al., 2005).

La famille de normes **ISO 27000** est un ensemble de normes internationales de sécurité de l'information, destinées protéger l'information. Elles offrent un ensemble de spécifications, de code de conduites et de lignes directrices sur les meilleures pratiques pour les organisations afin d'assurer une gestion solide de la sécurité de l'information. Néanmoins la conformité à une norme ne garantit pas formellement un niveau de sécurité. Les normes ne prennent pas en compte l'état de l'art récent et les exigences réglementaires(Abhishek Chopra Mukund Chaudhary, 2020.). Voici quelques-unes des principales normes inclues dans la série 27000 :

Table 3:La famille de normes ISO 27000

27001	Systèmes de management de la sécurité de l'information
27002	Code de bonnes pratiques
27004	Mesures du management de la sécurité
27005	Gestion des risques
270035	Gestion des incidents de sécurité
Tél. 27037	Traitement des preuves numériques (forensiques)
.....	

Dans le cadre de la mise en place de la sécurité au sein d'une organisation (Bressan et al., 2005):

- La norme ISO 27001 est considérée comme la norme la plus célèbre de la famille des ISO/CEI207000 et l'une des plus délivrées. Il permet à une organisation de mettre en place, mettre en œuvre, mettre à jour et d'améliorer le système de management de la sécurité. Les exigences fixées dans l'ISO 27001 couvre tous les types d'organisations, quels que soient son type, sa taille et sa nature. Également, elle définit une gestion globale et le cadre de contrôle pour le traitement des risques de sécurité de l'information.

- La norme ISO 27002 définit un ensemble des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information. Ce document permet aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un SMSI selon l'ISO/CEI 27001.
- La norme ISO 27005 définit des lignes directrices relatives à la gestion des risques de sécurité dans une organisation. Une organisation peut s'appuyer sur ce processus de gestion de risques pour intégrer la sécurité.

2.4. 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 » (Lalanne et al., 2013)ont identifié trois finalités se dégagent de la gestion des risques SI :

- L'amélioration de la sécurité des systèmes d'informations,
- La justification du budget alloué à la sécurité du SI.
- L'approbation de la crédibilité du SI à l'aide des analyses effectuées

La gestion des risques, vue par son pilotage, consiste à identifier les risques et proposer des mesures de traitement. L'élaboration d'une stratégie est composée d'une multitude de prises de décisions. Décrit ce qu'il appelle « la nature décisionnelle profonde du management des risques » en mettant en parallèle le modèle de la décision par Simon (Figure 3) et le schéma classique de la gestion des risques(Figure 4) (Céline Tea., 2010).

Le modèle canonique de prise de décision de H. Simon distingue quatre phases (Figure 3) :

- La phase d'intelligence : compréhension de la situation en la problématisant c'est à dire en en proposant une représentation ;
- La phase de conception : formule des voies de solutions possibles ;
- La phase de choix : sélection ;
- La phase de bilan : on fait un bilan de la solution retenue, cette phase peut déboucher sur une réactivation du processus de décision.

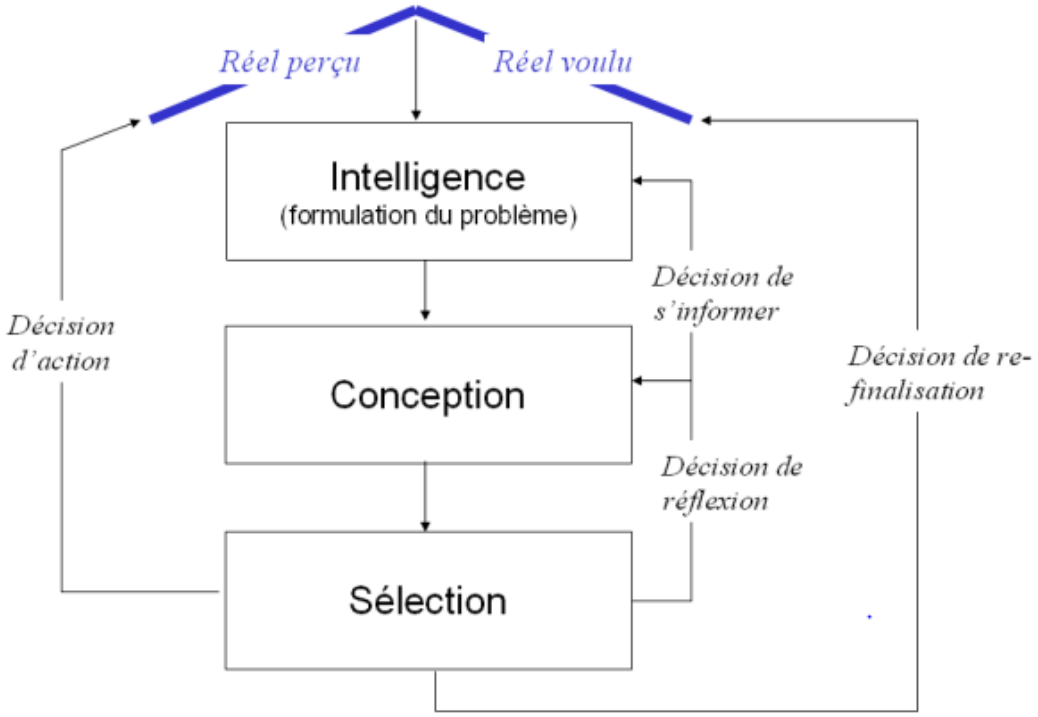


Figure 4 : représentation d'un processus de décision par H. Simon (Céline Tea., 2010)

Figure 4 représente le schéma de la gestion des risques au triptyque classique de la gestion des risques : identification – traitement – financement va s'ajouter une étape, l'anticipation que le système d'information pour la gestion des risques doit donner les moyens de réaliser(Céline Tea., 2010).

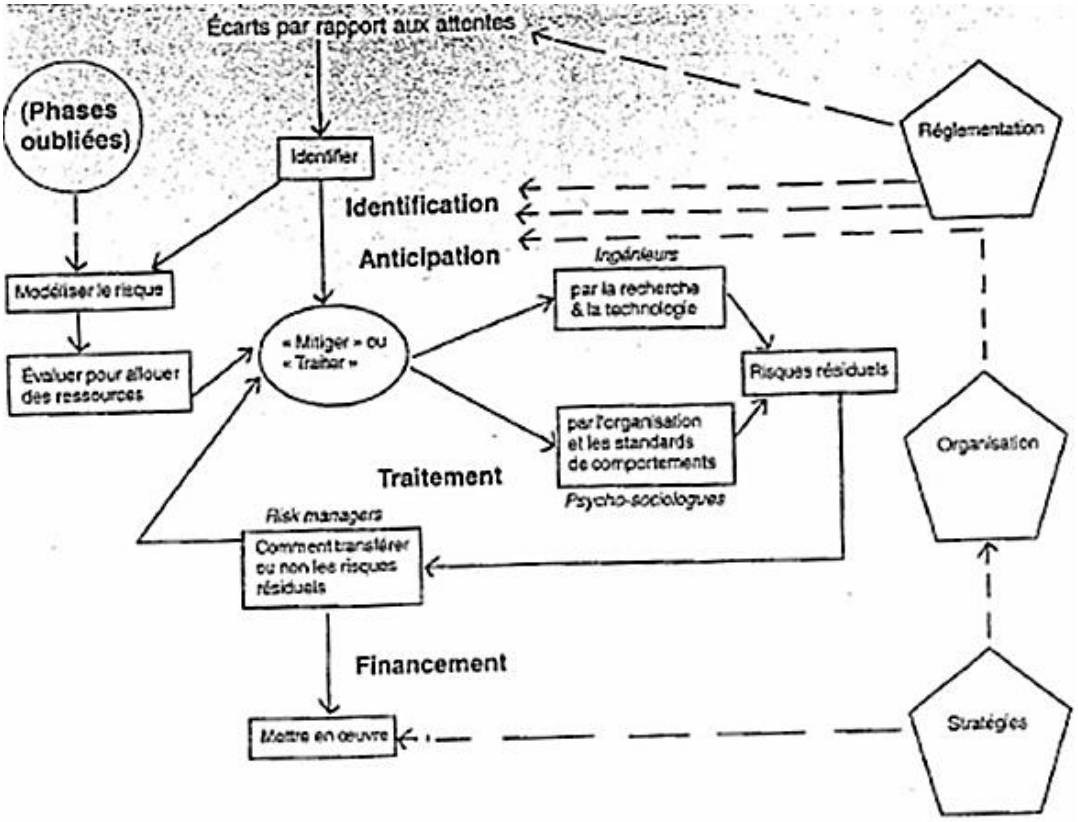


Figure 5 : Schéma complet de la gestion des risques par Munier (2002)(Céline Tea., 2010)

Le système d'information pour la gestion des risques constitue « l'apport d'informations qui autorise une appréciation plus sûre du champ des possibles et une anticipation plus correcte des résultats susceptibles de découler des actions projetées » d'après (Lalanne et al., 2013) .Le système d'information n'impose pas au gestionnaire son action. Les décisions de ce dernier ne sont pas automatisées, mais doivent être éclairées.

La gestion des risques identifie les risques de SI dans les organisations, en effet, ces organisations ont de nombreux échanges de données avec d'autres sociétés (nationales ou internationales) ou avec de nombreux partenaires et clients, et pour cela, ils ont appliqué plusieurs normes pour aider à sécuriser l'information et les processus d'échanges. L'ISO/IEC 27005 est la norme la plus récente en matière de gestion de la sécurité de l'information, c'est une norme de gestion des risques ; elle répond, lorsqu'elle est appliquée, à toutes les exigences de l'ISO 27001(Lalanne et al., 2013).

2.4.1. Les risques liés à la sécurité du système d'information

Avec l'arrivée de l'outil informatique et du Web 2.0 au cœur des organisations, les systèmes d'informations de celles-ci se sont vus complétement bouleversés. La collecte, la mémorisation, le traitement et la diffusion de l'information se fait aujourd'hui énormément avec des systèmes informatisés(Lalanne et al., 2013). Il est désormais possible de conserver beaucoup plus de données dans un espace réduit (support numérique) et de les dupliquer de manière très simple. Les organisations se voient désormais sujet à trois grands types de risques au niveau de leur SI :

- L'intégrité de l'information : modification ou la suppression de l'information,
- La confidentialité de l'information : révélation des informations à un tiers non autorisé,
- La disponibilité de l'information : provoqué par des pannes, erreurs voire malveillances.
- Une amélioration continue de la sécurité : donc un niveau croissant de sécurité

2.4.2. Les objectifs de la gestion des risques de sécurité

- Identifier les menaces et les vulnérabilités associées susceptibles d'avoir un impact négatif sur les activités de l'organisation. Les ressources peuvent alors être allouées efficacement pour mettre en œuvre des contrôles qui réduisent la probabilité et/ou l'impact potentiel des menaces en cours de réalisation.
- Fournir des conseils aux structures de l'organisation pour identifier, analyser et documenter les risques susceptibles d'affecter leur environnement.
- Maitriser et surveiller les risques pouvant affecter l'atteinte des objectifs stratégiques et opérationnels de l'organisation.
- Améliorer la performance de l'organisation dans l'utilisation de ses ressources et dans le choix des contrôles implémentés et renforcés en fonction des risques et ce, dans un souci d'économie, d'efficacité et d'efficience.

2.4.3. Enjeux d'un SMSI

Tout organisme possédant des données dites « sensible » nécessite la sécurisation de son système d'information à travers la mise en place d'un SMSI. Il permet d'offrir une meilleure gestion des risques majeurs. De plus, l'utilisation de ce type de systèmes permet donc de répondre aux objectifs de la sécurité de l'information tout en se conformant aux

réglementations, Grâce à l'intégration d'un SMSI, l'organisation répond aux exigences liées à la sécurité des clients et à leurs données sensibles.

Un SMSI peut apporter plusieurs avantages dans une organisation, tels que :

- Garantir la sécurité de l'information et des données sensibles.
- Identifier les risques et mettre des contrôles en place pour les gérer ou les éliminer.
- Permettre la confidentialité, l'intégrité et la disponibilité des informations d'un organisme.
- Valoriser et impliquer le personnel car celui-ci fait partie du SI.
- Rassurer les clients et les parties prenantes.
- Promouvoir les bonnes pratiques de sécurité.
- Éviter les ruptures d'activité en anticipant les risques.
- Réduire la probabilité d'erreur de Technologie de l'information et de la communication.
- Délimiter les champs de la sécurité.
- Protéger l'organisation.

2.5. Data sécurité dans les organisations publiques

Avec les technologies émergentes, la sécurité des données est devenue un sujet de discussion majeur. La protection des données dans les environnements informatisés se situe à l'intersection de plusieurs aspects : le cadre règlementaire de la protection des données, la gestion des données et la sécurité de l'information dans les systèmes d'information, la sécurité des réseaux publics de télécommunication. De ce fait, il convient de les envisager de manière conjointe(Céline Tea., 2010).

Prenons l'exemple du secteur bancaire, qui est le plus sensible à ce sujet. Les transactions bancaires font désormais partie intégrante de notre vie quotidienne et, par conséquent, la sécurisation des données est un défi permanent. En outre, le fondement du système bancaire réside dans le maintien de la confiance et de la crédibilité, à l'ère numérique, si les banques ne parviennent pas à sécuriser des informations importantes telles que les détails des comptes, les soldes des comptes et les historiques des transactions, leurs clients perdront confiance en eux et ne se sentiront peut-être pas en sécurité en déposant de l'argent là-bas. De nos jours, les gens effectuent beaucoup de transactions financières via les services bancaires en ligne et les guichets automatiques. Les deux doivent être gardés en sécurité. Les banques font donc beaucoup

d’efforts pour protéger les transactions et les données en ligne contre les menaces potentielles à la cybersécurité (Céline Tea., 2010).

Les organisations publiques doivent prendre la sécurité des données au sérieux car une fuite de données ou un piratage fait courir un risque à l’image de l’entreprise, sans parler des conséquences financières et logistiques si une fuite de données se produit réellement.

2.6. Fidélisation Clientèle

Sur la base d’études antérieures, de nombreux facteurs qui influencent la fidélité des clients. Cependant, dans l’étude, nous nous sommes concentrés sur une dimension assez importante de la qualité de service qui est la sécurité, en particulier la sécurité des données et son impact sur la fidélité et la satisfaction des clients. Des études telles que (Intyaswati, 2017; Khalaf Ahmad & Ali Al-Zu’bi, 2011) ont suggéré que la haute sécurité offre moins de satisfaction de la clientèle en raison d’une documentation élevée et d’autres procédures bancaires dans l’application ou l’obtention de produits et services bancaires. Cependant, (Khalaf Ahmad & Ali Al-Zu’bi, 2011; Khatab et al., 2019) Plusieurs études ont analysé l’impact des dimensions de la qualité de service sur la satisfaction et la fidélisation de la clientèle. Cependant, il y a un manque de littérature en ce qui concerne le secteur bancaire en Algérie. Notre étude examine l’impact de la sécurité des données sur la fidélisation de la clientèle alors que le cas de l’étude est le secteur bancaire.

(Khatab et al., 2019)définit la fidélité comme « un engagement profond à racheter ou à patroniser un produit/service préféré de manière cohérente à l’avenir, provoquant ainsi des achats répétitifs de même marque ou de même marque, malgré les influences situationnelles et les efforts de marketing susceptibles de provoquer un changement de comportement ». En particulier, la fidélité peut être définie comme l’intention ou la prédisposition d’un client d’acheter à nouveau auprès de la même organisation. Par conséquent, la loyauté a été un facteur clé pour atteindre le succès et la durabilité de l’entreprise au fil du temps. D’une manière générale, Fidélisation est la variable d’adaptation de la satisfaction du client et de la performance économique. La question qui semble la plus intéressante est le bouche-à-oreille des clients satisfaits qui attire de nouveaux clients. Les clients satisfaits, avec leurs publicités de bouche à oreille, peuvent affecter l’intention d’achat de ceux qui n’ont pas eu de relation avec une certaine entreprise. En outre, de nombreux chercheurs ont utilisé la recommandation de service à d’autres clients comme un proxy pour la fidélisation de la clientèle(Intyaswati, 2017). Outre la

recommandation, d'autres éléments qui ont été largement utilisés pour mesurer la fidélité de la clientèle sont considérés comme le fournisseur de services de premier choix.

2.6.1. Satisfaction de la clientèle

Bien que la satisfaction du client soit l'objectif de tous les services, ce n'est pas le seul et d'autres objectifs tels que l'avantage concurrentiel et la réalisation de profits sont inclus, et les avantages de la satisfaction du client conduiront finalement à une plus grande fidélité des clients. Maintenir les clients à long terme plutôt que l'attraction continue de nouveaux clients pour remplacer ceux qui ont coupé les liens avec l'entreprise est plus bénéfique. (Whence, 2016)a défini la réunion complète de ses attentes et peut être décrit comme le sentiment ou l'attitude d'un client envers un produit ou un service après son utilisation. Au sens traditionnel du terme, la satisfaction était une transaction - une construction spécifique qui résultait d'un jugement immédiat après l'achat ou d'une réaction affective(Hammoud et al., 2018).

Conclusion

Assurer la sécurité des données collectées par les organismes publics est devenu primordial aujourd'hui afin de créer une sphère de confiance entre la compagnie et ses usagers.

On rappelle que cette sécurité implique une veille efficace sur les aspects de l'intégrité, la disponibilité, la confidentialité de l'information et aussi sur les nouveaux critères telles que la traçabilité ou la confiance. De plus, avec la quantité importante de données circulantes, les organisations publiques sont de plus en plus vulnérables à des risques forts, donc elles doivent connaitre avec exactitude la nature du risque auquel elles doivent faire face. La gestion des risques couvre tous les points susceptibles de problème dans les organisations, et analyse les risques afin de garantir la sécurité des systèmes d'informations et par conséquence la confiance des clients.

CHAPITRE 3 : CADRE MÉTHODOLOGIQUE

Dans ce chapitre, nous allons définir l'approche épistémologique et la méthodologie choisies dans notre étude sur l'impact de la sécurisation des données sur la fidélisation client, donc on va présenter les méthodes de recherche et les instruments de collecte que nous avons utilisés dans notre étude.

1.Approche épistémologique

Notre objectif est de découvrir à quel point le concept de la sécurité des données est commun chez les clients de la BADR et de connaitre l'état actuel de la sécurité dans cette banque, et afin d'explorer la réalité, nous avons choisi le courant positiviste, et pour cela nous avons suivi une démarche de type hypothético-déductif qui démarre avec une problématique et des questions et se transforment en hypothèses qui vont être testé par la suite.

2.Approche méthodologique

Ce travail de recherche est basé sur une approche quantitative, qui nous aide à relier la partie théorique à la partie pratique en recueillant des données pour ce sujet. Cette méthode nous permet d'arriver à une conclusion qui soutient notre objectif de l'étude.

3.Méthode de collecte de données

Afin de collecter les informations nécessaires sur les clients de la BADR, nous avons effectué une enquête par questionnaire, ce qui permet de connaitre l'avis des usages sur la sécurité des données.

4.Instrument de mesure

Nous avons utilisé le questionnaire comme instrument de mesure, et cela pour récolter le plus possible d'informations.

4.1. Le questionnaire

Pour mieux appréhender l'avis des clients en matière de la sécurité de données et de fidélisation dans la banque BADR nous avons mené un questionnaire.

Le questionnaire est un outil de collecte d'informations, composée d'une suite de questions présentées dans un ordre prédéfini.

4.2. La structure du questionnaire

Le questionnaire est divisé en trois catégories :

Catégorie 1 :

La première catégorie contient trois questions sures : le type de client particulier ou professionnel, le critère de choix du client pour la BADR, et l'ancienneté de clientèle.

Sous-catégorie :

Dans le but de mesurer la fidélité du client de la BADR, nous avons développé une sous-catégorie qui comprend trois dimensions :

- Le comportement : si les clients achètent plus chez la BADR.
- Recommandation : si les clients préconisent les produits / services de la BADR à leur entourage.
- Rétention/Préférence : si les clients restent chez la BADR et se tournent moins vers les concurrents.

De plus, nous avons inclus dans cette partie deux questions sur la sécurité pour voir le lien entre la fidélisation et cette dernière.

Catégorie 2 :

Dans une deuxième catégorie nous essaierons de connaître le jugement du client concernant la sécurisation des données bancaires personnelles. Ensuite nous avons soumis quatre questions basées sur l'outil de Likert qui propose 5 degrés d'accord (Pas du tout d'accord, pas d'accord, neutre, d'accord, tout à fait d'accord).

Catégorie 3 :

La troisième catégorie est une fiche signalétique a trois questions qui nous permet d'identifier les profils des répondants. Les questions signalétiques dans ce questionnaire ; le genre, l'âge, la classe socioprofessionnelle.

5.Les échelles de mesure

Les échelles de mesure que nous avons utilisées pour évaluer les variables de l'étude :

- Une échelle standard de 0 (pas du tout probable) à 10 (très probable) : nous permet d'évaluer la probabilité qu'un produit ou qu'un service soit recommandé par ses clients.

- Une échelle de Likert de 1 (Pas du tout d'accord) à 5 (tout à fait d'accord) : afin d'évaluer la sécurité.

6.Echantillonage

Cette partie se compose de trois éléments principaux : la population de l'étude, la méthode d'échantillonnage et la taille de l'échantillon.

6.1. Population de l'étude

L'échantillon pour notre étude est les clients de la BADR, qui se compose de 41,66 % de femmes et 58,33 % d'hommes.

6.2. Méthode d'échantillonnage

Nous avons suivi une méthode d''échantillonnage non probabiliste par convenance, pour obtenir l'avis des clients sur la sécurité de leurs données et si cela a un impact sur leur fidélité à la banque BADR.

6.3. Taille de l'échantillonnage

Notre échantillon est constitué de 48 personnes tous domiciliés au sein de la BADR agence n°426 de Blida.

8. Méthode de traitement et analyse de données

Afin d'effectuer le traitement et l'analyse nos données quantitatives, nous avons utilisé l'outil SPSS (Logiciel d'analyse statistique des données) win version 22.

7. Mode d'administration du questionnaire

Le mode d'administration pour notre recherche était face à face (nous avons distribué le questionnaire à la clientèle), et par voie électroniques pour les clients qui ont accepté de nous communiquer leurs emails.

CHAPITRE 4: ÉTAT DES LIEUX ET BILAN DE LA RECHERCHE

Introduction

Le présent chapitre est composé en deux parties :

- Les dispositifs actuels de sécurité mise en place par la BADR.
- La seconde partie contient les résultats de notre recherche ainsi que la discussion de ces derniers à travers le questionnaire administré.

1. Les Dispositifs actuels de sécurité mise en place par La BADR

La sécurité de l'information de la Banque consiste à protéger les informations traitées d'une multitude de risques : qu'il s'agisse de menaces (actions extérieures ou intérieures malveillantes) ou de vulnérabilités (risques propres aux systèmes et applications). Permettant ainsi de garantir la **confidentialité**, **l'intégrité**, la **disponibilité** des données ainsi que leur traçabilité.

Cette sécurité doit être assurée par la mise en œuvre de mesures adéquates regroupant les structures organisationnelles de la Banque, les règles, les processus, les procédures mais également le système d'information. L'ensemble de ces mesures doit être déterminé, documenté, implémenté, audité et amélioré aussi souvent que nécessaire pour atteindre les objectifs spécifiques en matière de sécurité de l'information qui sont spécifiés dans la Politique de Sécurité du Système d'Information-**PSSI**- de la Banque.

L'analyse des risques doit considérer à la fois la sécurité physique, la sécurité au niveau système, la sécurité au niveau applicatif, la sécurité au niveau réseaux et communications etc.

La Direction Générale (**DG**) fournit les orientations stratégiques en matière de sécurité du système d'information et apporte son appui indispensable à la mise en place des différentes solutions de sécurité de l'information.

1.2. Objectifs Généraux

La Banque a toujours accordé une importance particulière à la protection de son patrimoine informationnel, s'engageant à respecter scrupuleusement les dispositions législatives et réglementaires qui régissent l'utilisation des données et des informations, ainsi que les principes de sécurité de l'information :

-La Disponibilité : L'aptitude d'un système à assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite.

-**L’intégrité** : La protection de l'exactitude et de l'entièreté de l'information et des méthodes de traitement de celle-ci.

- La Confidentialité : le caractère réservé d'une information dont l'accès et la diffusion sont limités aux seules personnes autorisées à la connaître.

- **La Preuve (ou Traçabilité)** : La conservation des traces de l'état et des mouvements de l'information.

Les dispositifs spécifiques de sécurité du système d'information de la Banque, objet de la présente décision réglementaire, ont pour objectif d'assurer un niveau de sécurité optimal du système d'information de la Banque ; ce niveau de sécurité permet donc d'assurer la protection des informations tant en assurant leur disponibilité, leur intégrité que leur confidentialité et traçabilité. De plus, la mise en œuvre des dispositifs spécifiques de sécurité du système d'information permet à la Banque de s'aligner sur les normes universelles ainsi que sur les réglementations bancaires algériennes.

1.3. Domaine d'application

Les dispositifs spécifiques de sécurité s'appliquent au système d'information et à tous ses composants supportant les métiers de la Banque, qu'ils soient existants ou à développer Ces politiques concernent l'ensemble du cycle de vie de ce système d'information. Elles sont élaborées pour l'ensemble des métiers de la Banque Plus précisément, sont concernés par ces politiques :

- Le système d'Information actuel et ses évolutions ;
- Toute personne ayant accès au Système d'Information de la BADR aussi bien les salariés, le personnel externe, les sous-traitants, les prestataires que les stagiaires ou encore les apprentis appelés à en user.
- L'organisation, l'environnement physique, le développement, l'exploitation et la maintenance du Système d’Information.
- La totalité du cycle de vie du Système d'Information ainsi que des données pouvant être traitées, transportées et stockées sur celui-ci.

Dans cette étude nous avons détaillé les dispositifs de sécurité suivantes :

- Dispositif de gestion des risques de sécurité.
- Dispositif de lutte contre les logiciels malveillants
- Dispositif de gestion des risques de sécurité spécifique de cryptographie

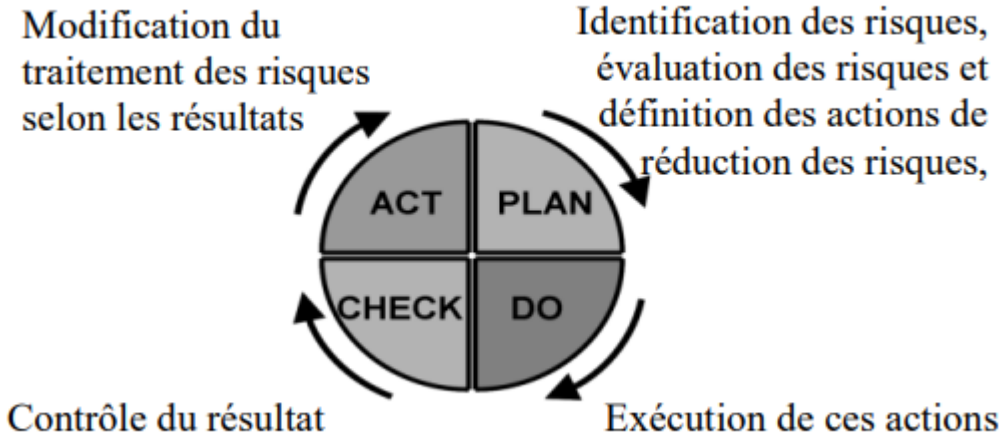
2. Dispositif de gestion des risques de sécurité

Le processus de gestion du risque en sécurité de l'information peut être itératif pour les activités d'appréciation et/ou de traitement du risque.

Des itérations sont possibles :

- Si l'appréciation des risques n'est pas satisfaisante, la cartographie des risques de sécurité comporte des lacunes, des erreurs ou n'est pas suffisamment exhaustive ;
- Si les décisions et/ou les actions de traitement de risques identifiées dans le plan d'actions ne sont pas compatibles, sont inadéquates ou quand les risques résiduels identifiés ne sont pas validés (acceptés);
- Lors de l'analyse périodique du risque, Dans le cadre de la révision et de l'amélioration continue.

Le modèle exposé ci-dessous doit être déroulé séquentiellement, et ce dans le cadre d'un cycle (Plan, Do, Check, Action) (Figure4).



3 .

Figure 6: cycle (Plan, Do, Check, Action)

Dispositif de lutte contre les logiciels malveillants

La lutte contre les logiciels malveillants comporte toutes les mesures préventives destinées à identifier, arrêter et supprimer tout logiciel malveillant pouvant présenter une menace pour la sécurité des systèmes informatiques de la Banque. Ces menaces peuvent être sous la forme de virus, vers, chevaux de Trole, rançongiciel etc.

L’utilisation seule d'outils de détection de logiciels malveillants est insuffisante et il est nécessaire de conforter la sécurité technique par des actions de prévention et de prémunition contre les logiciels malveillants, à l'instar de la sensibilisation des utilisateurs à la sécurité du système d'information.

Le présent dispositif a pour objet de définir les orientations de la banque en matière de lutte contre les logiciels malveillants. Ce dispositif s’applique à l’ensemble des actifs électronique de la banque.

4. Dispositif de gestion des risques de sécurité spécifique de cryptographie

Cryptographie est une technique permettant d'assurer la sécurité et la confidentialité des données dans les systèmes d'Information et de Communication.

Il est nécessaire d'utiliser des mesures cryptographiques pour répondre à différents objectifs de sécurité de l'information tels que :

- La confidentialité : le chiffrement des données permet de protéger l'information sensible ou critique, durant son stockage ou sa transmission :
- Authentification : l'utilisation de techniques cryptographiques permet d'authentifier les utilisateurs et les autres entités demandant un accès ou engageant une transaction avec des utilisateurs, des entités et des ressources du système.

Le présent dispositif de sécurité a pour objet de définir les orientations de la Banque en matière de cryptographie. Ce dispositif s’applique à l'ensemble des actifs informatiques de la Banque et doit être diffusé aux structures centrales.

2. Les résultats de la recherche

À travers cette section, on présente les différents résultats du questionnaire.

2.1. La fidélisation des clients de la BADR

1. Êtes-vous un client particulier ou professionnel ?

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

Question n° 1	Fréquence	Pourcentage
Particulier	32	66.7
Professionnel	16	33.3
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

À travers le tableau, nous notons que la plupart des réponses de clients de la Banque Badr à la première question étaient particulier, par 66,7%, puis professionnelles, par 33,3%, ce qui indique que la plupart des clients de la Banque de développement local de Badr sont des clients particuliers.

2 Pourquoi avez-vous choisi Badr ?

Table 5:raisons du choix d'avoir un compte à la BADR

Question° 2	Fréquence	Pourcentage
Réputation	27	56.3
Proximité	10	20.8
Diversité de l'offre produit	5	10.4
Recommandations de votre entourage	6	12.5
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

En ce qui concerne le choix de la banque, 56.3 % ont choisis cette banque pour sa réputation. 20.8% l'ont fait pour sa proximité et 12.5% pour la recommandation. Ce qui prouve que la banque étudiée présente une bonne image auprès de ses clients.

3. Depuis quand vous êtes client de cette banque ?

Table 6:Répartition de l'échantillon selon l'ancienneté

Question n° 3	Fréquence	Pourcentage
1-3 ans	5	10.4
4-7 ans	16	33.3
8 ans et plus	27	56.3
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

A travers le tableau, nous constatons que 56.3% sont des clients depuis plus de 8ans, et 33.3% pour la tranche de client entre 4 et 7 ans, suivi de la tranche de client entre 1 et 3 ans avec seulement 10.4%. Ce qui indique que le dégrée d'ancienneté est élevé pour la plupart des clients.

4. Quelles sont les raisons susceptibles de vous rendre un client fidèle à la BADR ?

Table 7:Répartition de l'échantillon selon les raisons de fidélité

Question n° 4	Fréquence	Pourcentage
Des produits adaptés à vos besoins	6	12.5
Qualité des services/produits offerts	27	56.3
Sécurité des données (protéger les données contre les menaces malveillantes)	15	31.2
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

Ce tableau montrer que la qualité des services/produits est la première raison qui rendre le client fidèle, avec un taux de 56.3%, puis la sécurité des données avec 31.2 %. Cela montre que la qualité est un facteur de choix pour les clients de la banque.

5. Avez-vous l'intention de renouveler l'achat du service / produit auprès d'Al Badr ?

Table 8:Répartition de l'échantillon selon la dimension de renouvellement d'achat

Question n° 6	Fréquence	Pourcentage
Oui	27	56.2
Non	07	14.6
Je ne sais pas	14	29.2
Total	**48**	**100**

Source : Elaboré par nos soins via le programme SPSS.

Selon le tableau, 56.2% des clients ont l'intention de renouveler l'achat, 29.2 % ne savent pas, et seulement 14.6% ont dit non.

6. En tant que client Badr, avez-vous le sentiment que vos données personnelles sont protégées et sécurisées chez la banque ?

Table 9:Répartition de l'échantillon selon le sentiment de la préservation de la sécurité des données.

Question n° 6	Fréquence	Pourcentage
Oui	31	64.6
Non	6	12.5
Je ne sais pas	11	22.9
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

On peut constater que la majorité des clients (64.6%) ressentent que leurs données sont protégées et sécurisées, et 22.9% ne savent pas si leurs données sont protégées ou pas.

7. Avez-vous un compte dans d'autres banques ?

Table 10:Avez-vous un compte dans d'autres banques?

Question n° 7	Fréquence	Pourcentage
Oui	21	43.8
Non	27	56.2
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

Plus de la moitié des clients n'ont pas des comptes dans d'autre banque.

8. La sécurisation de vos données est-elle l'une des raisons qui vous poussent à changer de la banque ?

Table 11:Répartition de l'échantillon selon le critère de sécurité comme raison de changement de la banque.

Question n° 8	Fréquence	Pourcentage
Oui	43	89.6
Non	5	10.4
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

On peut constater que la majorité des répondants (89.6%) dites oui, et cela indique que la sécurité est l'un des raisons qui poussent les clients à changer la banque.

9.Sur une échelle standard de 0 à 10, quelle est la probabilité que vous recommandiez la BADR à vos amis / collègues ?

Question n° 9	Valeur
Nombre total de fréquence	310
Moyenne arithmétique	6.64
Écart type	2.07
Taille de l'échantillon	48

Source : Elaboré par nos soins via le programme SPSS.

Du tableau, nous voyons l'échelle moyenne obtenue de 1 à 10 estimée à 6,64 avec une fréquence totale de 310 et un écart-type de 02,7 qui est supérieur à la valeur moyenne de 5 et cela indique que la probabilité de recommandation est plutôt élevée.

10. Si demain l'un du concurrents de la BADR vous propose le même nouveau produit qu'elle, pensez-vous que vous l'achèteriez de préférence chez la BADR ?

Table 12:Répartition de l'échantillon selon la dimension de préférence d'achat chez la BADR

Question n° 10	Fréquence	Pourcentage
Oui	27	56.2
Je ne sais pas	21	43.8
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

Nous remarquons que 56.2% des clients de la Badr sont prêts à acheter des produits dans le cas où le produit est égal en qualité et en prix avec les banques concurrentes.

2.3. La sécurisation des données

11. Que signifie la sécurité pour vous ?

Table 13: Répartition de l'échantillon selon la signification de la sécurité pour le client

Question n° 11	Fréquence	Pourcentage
État d'esprit	11	22.9
Confiance	32	66.7
Tranquillité	5	10.4
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

On constate que la majorité des clients considèrent la sécurité comme un indicateur de confiance avec un taux de 66.7 %.

12. S'agissant de vos données bancaires personnelles (de compte, des indications présentes sur votre carte bancaire, du code secret associé à votre carte,etc), diriez-vous que vous êtes plus, moins ou autant vigilant que ?

Table 14: Répartition de l'échantillon selon le dégrée de vigilance

Source : Elaboré par nos soins via le programme SPSS

Question n° 12	**Plus vigilant**		**Autant vigilant**		**Moins vigilant**		**Total**	
	Fréquence	**Pourcentage**	**Fréquence**	**Pourcentage**	**Fréquence**	**Pourcentage**	**Fréquence**	**Pourcentage**
Les clés de votre maison	32	66.7	10	20.8	06	12.5	48	100
Votre téléphone portable	15	31.3	28	58.3	05	10.4	48	100
Vos papiers d'identité	28	58.3	05	10.4	15	31.3	48	100

D’après les résultats du tableau, nous notons que 66.9 % sont vigilant à leur données bancaires personnels plus qu’à leur clé de maison, et 58.3% donnent le même dégrée de vigilance en ce qui concerne leur données bancaire et leur téléphone portable, et enfin, 58.3% sont vigilant à leurs données bancaires plus qu’à leurs papiers d’identité. Cela montre que la vigilance est très élevée dans le cas de leurs données bancaires.

13. Pour vous, la banque idéale aujourd’hui c’est celle qui… ?

Table 15:Pour vous, la banque idéale aujourd’hui c’est celle qui

Question° 13	Fréquence	Pourcentage
Assure la sécurité de vos données bancaires (contre les attaques virales)	15	31.3
Est joignable dès que vous avez besoin	11	22.9
Vous alerte en cas de mouvements suspects sur vos comptes	11	22.9
Vous conseille et vous accompagne dans vos placements financiers (immobilier, épargne, etc.)	6	12.5
Vous offre des services innovants	5	10.4
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

Les trois réponses les plus citées sont : assure la sécurité de vos données bancaires contre les attaques virale avec un taux 31.3%, est joignable dès que vous avez besoin (22.9%) ainsi que vous alerte en cas de mouvements suspects sur vos comptes avec un taux aussi de (22.9 %).

- Sur une échelle de 1 (pas du tout d’accord) à 5 (tout à fait d’accord), veuillez expliquer à quel point vous êtes d’accord avec les affirmations suivantes :

13.La protection des données clients contre les menaces malveillantes permet de le fidéliser.

Table 16:Répartition de l’échantillon selon le degré d’accord avec l’affirmation de question n 13

Question n° 13	Fréquence	Pourcentage
Je ne suis pas d’accord.	6	12.5
Neutre	11	22.9
Je suis d’accord	5	10.4

Je suis tout à fait d'accord	26	54.2
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

Ce tableau permet d'observer que 54.2% sont tout à fait d'accord avec l'affirmation 1.

14.La sécurité des données est un facteur déterminant de la fidélisation client.

Table 17:Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 de question n 14.

Question n° 14	Fréquence	Pourcentage
Je ne suis pas d'accord.	5	10.4
Neutre	6	12.5
Je suis d'accord	10	20.8
Je suis tout à fait d'accord	27	56.3
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

56.3% des clients interrogés disent qu'ils sont tout à fait d'accord avec l'affirmation 2.

15. Garantir la sécurité des données renforcera la confiance entre la banque et le client.

Table 18:Répartition de l'échantillon selon le degré d'accord avec l'affirmation 3 de la question n° 15

Question n° 15	Fréquence	Pourcentage
Je suis d'accord	16	33.3
Je suis tout à fait d'accord	32	66.7
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

A travers le tableau, nous constatons que la plupart des clients (66.7%) sont tout à fait d'accord avec l'affirmation 3.

16- Les agences bancaires (BADR) doivent améliorer continuellement leur dispositif de sécurité.

Table 19:Répartition de l'échantillon selon le degré d'accord avec l'affirmation 4 de la question n° 16

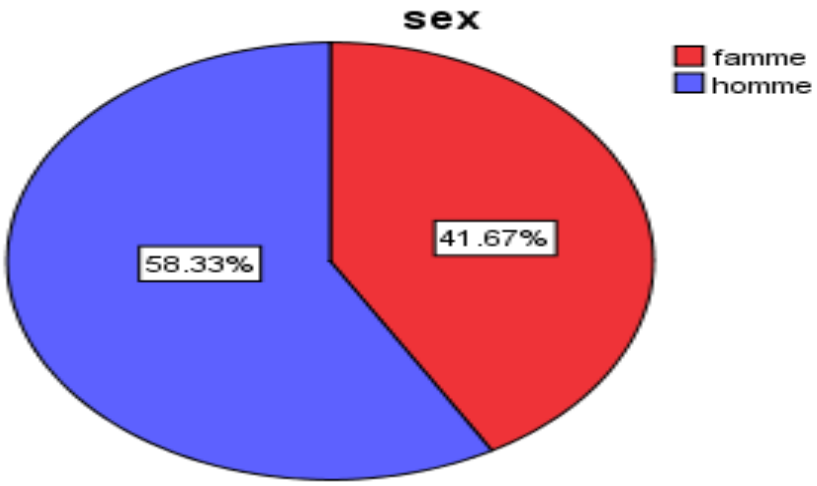
Question n° 16	Fréquence	Pourcentage
Je suis d'accord	26	54.2
Je suis tout à fait d'accord	22	45.8
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

D'après ce tableau, nous remarquons que 54.2 % sont d'accord avec l'affirmation 4 et 45.8% sont tout à fait d'accord.

- **Répartition de l'échantillon selon les variables sociodémographiques :**
  - **Répartition de l'échantillon de client par sexe**

Figure 4:Répartition de l'échantillon de client par sexe



Source : Sortie SPSS.

Table 20:Répartition de l'échantillon par sexe

Sexe	Fréquence	Pourcentage
Hommes	28	58.33

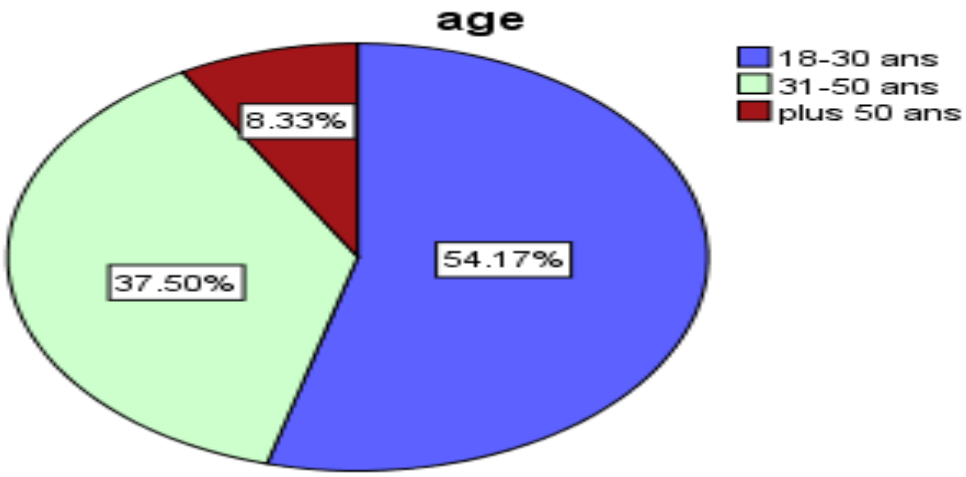
Femmes	20	41.67
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS.

Dans notre échantillon 58.33% sont des hommes et 41.67% des femmes

- **Répartition de l'échantillon par âge**

Figure 5: Répartition de l'échantillon par âge



Source : Sortie SPSS.

Figure 6:Répartition de l'échantillon de par âge

Groupe	Fréquence	Pourcentage
18-30 ans	26	54.2
31-50 ans	18	37.5
Plus de 50 ans	4	8.3
Total	48	100.0

Source : Elaboré par nos soins via le programme SPSS

On peut observer que :

- 54.2% des clients sondés ont un âge compris entre 18 ans et 30 ans.
- 37.5% sont dans la tranche d'âge qui s'étend entre 31 ans et 50 ans.
- La tranche de 50 ans est constitué seulement de 8.3%.

- **Répartition de l'échantillon selon la profession**

Table 21:Répartition de l'échantillon selon la profession

Classe socio-professionnelle	Fréquence	Pourcentage
Commerçant	14	29.2
Fonctionnaire	10	20.8
Ouvrier	2	4.2
Chef d'entreprise	3	6.3
Étudiant(e)	3	6.3
Sans-emploi	3	6.3
Retraité(e)	13	27.1
Total	**48**	**100**

Source : Elaboré par nos soins via le programme SPSS

D'après le tableau, nous avons constaté que 29.2 % des clients enquêtés sont des commerçant, 20.8 % représente les fonctionnaires, et 27.1% des clients sont des retraités, la catégorie ouvrière présente 4.2%. En ce qui concerne les catégories (chef d'entreprise, étudiant, sans-emploi) sont toutes présentées par un pourcentage de 6.3%.

3. La discussion des résultats :

Selon les résultats présentés ci-dessus, nous avons remarqué que la majorité des clients ont choisis la BADR pour le critère de la réputation, cela indique que leur image joue un rôle important pour le succès et la continuité de cette banque. En effet, ce résultat explique pourquoi le dégrée d'ancienneté est élevés.

En ce qui concerne la fidélité, on a vu que les critères de qualité des services et de sécurité des données sont les deux critères essentiels pour rendre un client fidèle.

On outre, les questions posées pour le but de mesurer la fidélité nous ont permet de conclue que la plupart des clients sont fidèle à la BADR, et donc la banque réponde aux exigences de ses clients.

De plus, les clients sondés s'estiment que leurs données sont protégées, cela montre qu'ils font confiance à leur banque dans la sécurisation de leurs données.

D'âpres les réponses des clients aux questions relatives à la sécurité, nous sommes arrivés à deux conclusions :

- La première est que les clients donnent une attention accrue pour les données bancaires.
- La deuxième est par rapports à leurs attentes, d'où nous avons constaté que la sécurisation des données est un facteur dominant pour une banque idéale.

Enfin, la majorité des répondants ont acceptées toutes les affirmations qu'on a cité dans le questionnaire, cela veut dire que la sécurité des données joue un rôle primordial dans la vie des usagers.

Après discussion de nos résultats, nous pouvons conclure que les deux hypothèses citées au début sont valides :

H01 : les dispositifs actuels de sécurité des données de la banque permettent de

Sécuriser les données. (Validée)

H02 : La sécurisation des données clients est un facteur clé pour le rendre fidèle. (Validée)

Conclusion

Garantir la sécurité de l'information est devenu primordial aujourd'hui afin de permettre aux entreprises de persister dans un marché de plus en plus concurrentiel. On rappelle que cette sécurité implique d'appliqué des dispositifs de sécurité efficace pour assurer la disponibilité, la confidentialité et l'intégrité de l'information. Dans le cas où ces systèmes d'information ne sont pas exploités de façons appropriées, la confiance peut être affaiblie entre la compagne et ses clients, et par conséquent la relation entre eux.

Le secteur bancaire est plus susceptible de subir des risques liés à la sécurité des données, car l'argent est un produit qui nécessite une relation de confiance, donc l'efficacité des systèmes d'information doit être un point d'ancrage pour la banque. Une politique de sécurité doit être adaptée à l'organisme et à ses évolutions.

À travers le stage que nous avons effectué au sein de la banque d'agriculture et de développement rurale (BADR), et grâce au questionnaire et les réponses que nous y avons eu, nous avons réalisé un résultat principal qui est : les clients de la BADR sont fidèles à la banque car elle répond à leurs exigences, où la sécurité des données personnelles figurait parmi leurs principales exigences, cela nous permet d'évaluer nos hypothèses comme suit :

La première hypothèse (H01) indiquant que les dispositifs actuels de sécurité des données de la banque permettent de sécuriser les données est validée.

La deuxième hypothèse (H02) indiquant que la sécurisation des données clients est un facteur clé pour le rendre fidèle est validée.

De plus, nous avons constaté une conscience des clients envers la valeur de la sécurité des données, et son importance, mais avec l'évolution continue des technologies de l'information et de communication (TIC), cette prise de conscience reste relative. Les banques doivent sensibiliser continuellement les clients et de fournir des conseils sur les bases d'une bonne sécurité, en publiant des articles sur leurs sites, en envoyant des courriels à leurs clients, ces engagements peuvent améliorer l'image de la banque et renforcer la fidélité de ses clients.

Annexe

Age					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	18-30 ans	26	54.2	54.2	54.2
	31-50 ans	18	37.5	37.5	91.7
	Plus 50 ans	4	8.3	8.3	100.0
	Total	48	100.0	100.0	

Statistiques				
		Sex	Age	Classe socio Professionnelle
N	Valide	48	48	48
	Manquante	0	0	0

Tableaux de Fréquences

Sex					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	Femme	20	41.7	41.7	41.7
	Homme	28	58.3	58.3	100.0
	Total	48	100.0	100.0	

Class_Socioprofissionnelle					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	Commerçant	14	29.2	29.2	29.2
	Fonctionnaire	10	20.8	20.8	50.0
	Ouvrier	2	4.1	4.1	54.1
	Chef d'entreprise	3	6.3	6.3	60.5
	Etudiant (e)	3	6.3	6.3	66 .8
	Sans emploi	3	6.3	6.3	73.1
	Retraite	13	27	27	100.0
	Total	48	100.0	100.0	

Diagramme en secteurs

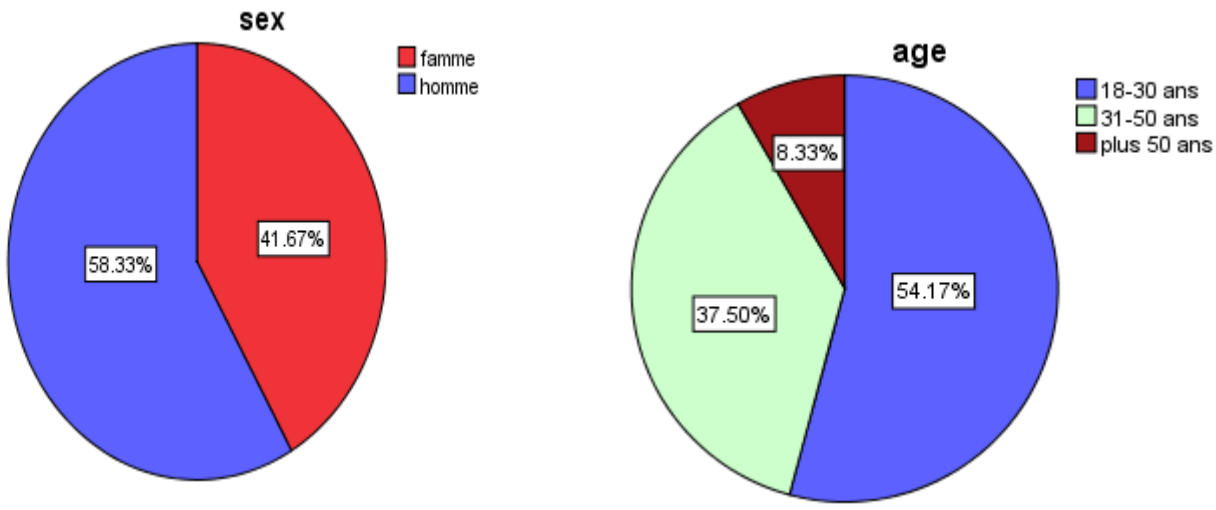


Tableau de fréquences

Question1					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	32	66.7	66.7	66.7
	2	16	33.3	33.3	100.0
	Total	48	100.0	100.0	

Question2					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	27	56.3	56.3	56.3
	2	10	20.8	20.8	77.10
	5	5	10.4	10.4	87.5
	6	6	12.5	12.5	100.0
	Total	48	100.0	100.0	

Question3					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	5	10.4	10.4	10.4
	2	16	33.3	33.3	43.7
	3	27	56.4	56.4	100.0
	Total	48	100.0	100.0	

Question4					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	6	12.5	12.5	12.5
	2	27	56.3	56.3	68.8
	4	15	31.2	31.2	100.0
	Total	48	100.0	100.0	

Question5					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	27	56.2	56.2	56.2
	2	7	14.6	14.6	70.8
	3	14	29.2	29.2	100.0
	Total	48	100.0	100.0	

Question6					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	31	64.6	64.6	64.6
	2	6	12.5	12.5	77.1
	3	11	22.9	22.9	100.0
	Total	48	100.0	100.0	

Question7					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	21	43.8	43.8	43.8
	2	27	56.2	56.2	100.0
	Total	48	100.0	100.0	

Question8					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	43	89.6	89.6	89.6
	2	5	10.4	10.4	100.0
	Total	48	100.0	100.0	

Question9					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	4	16	33.3	33.3	33.3
	5	5	10.4	10.4	43.7
	7	5	10.4	10.4	54.1
	8	12	25.0	25.0	79.1
	9	10	20.9	20.9	100.0
	Total	48	100.0	100.0	

Question10					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	27	56.3	56.3	56.3
	3	21	43.7	43.7	100.0
	Total	48	100.0	100.0	

Question11					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	11	22.9	22.9	22.9
	2	32	66.7	66.7	89.6
	3	5	10.4	10.4	100.0
	Total	48	100.0	100.0	

Question12-A1					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	32	66.7	66.7	66.7
	2	10	20.8	20.8	87.5
	3	6	12.5	12.5	100.0
	Total	48	100.0	100.0	

Question12-A2					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	15	31.3	31.3	31.3
	2	28	58.3	58.3	89.6
	3	5	10.4	10.4	100.0
	Total	48	100.0	100.0	

Question12-A3					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	28	58.3	58.3	58.3
	2	5	10.4	10.4	68.7
	3	15	31.3	31.3	100.0
	Total	48	100.0	100.0	

Question13					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	16	33.3	33.3	33.3
	2	27	56.3	56.3	89.6
	3	5	10.4	10.4	100.0
	Total	48	100.0	100.0	

Question14					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	15	31.3	31.3	31.3
	3	33	68.7	68.7	100.0
	Total	48	100.0	100.0	

Question15-A1					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	2	11	22.9	22.9	22.9
	3	5	10.4	10.4	33.3
	4	32	66.7	66.7	100.0
	Total	48	100.0	100.0	

Question15A2					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	11	22.9	22.9	22.9
	2	5	10.4	10.4	33.3
	3	10	20.8	20.8	54.1
	4	22	45.9	45.9	100.0
	Total	48	100.0	100.0	

Question15A3					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	10	20.8	20.8	20.8
	2	6	12.5	12.5	33.3
	3	20	41.7	41.7	75.0
	4	12	25.0	25.0	100.0
	Total	48	100.0	100.0	

Question15A4					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	5	10.4	10.4	10.4
	2	11	22.9	22.9	33.3
	3	15	31.3	31.3	64.6
	4	17	35.4	35.4	100.0
	Total	48	100.0	100.0	

Question15A5					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	3	21	43.8	43.8	43.8
	4	27	56.2	56.2	100.0
	Total	48	100.0	100.0	

Question15A6					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	2	15	31.3	31.3	31.3
	3	5	10.4	10.4	41.7
	4	28	58.3	58.3	100.0
	Total	48	100.0	100.0	

Question16					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	1	11	22.9	22.9	22.9
	2	15	31.3	31.3	54.2
	3	11	22.9	22.9	77.1
	4	6	12.5	12.5	89.6
	6	5	10.4	10.4	100.0
	Total	48	100.0	100.0	

Question17					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	2	6	12.5	12.5	12.5
	3	11	22.9	22.9	35.4
	4	5	10.4	10.4	45.8
	5	26	54.2	54.2	100.0
	Total	48	100.0	100.0	

Question18					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	2	5	10.4	10.4	10.4
	3	6	12.5	12.5	22.9
	4	10	20.8	20.8	43.7
	5	27	56.3	56.3	100.0
	Total	48	100.0	100.0	

Question19					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	4	16	33.3	33.3	33.3
	5	32	66.7	66.7	100.0
	Total	48	100.0	100.0	

Question20					
		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	4	26	54.2	54.2	54.2
	5	22	45.8	45.8	100.0
	Total	48	100.0	100.0	

Reference

Abhishek Chopra Mukund Chaudhary. (n.d.). *Implementing an Information Security Management System*.

BOUSSALEM1*, A. (2022). *Customer Relationship Management and The Quality of Banking Services Case Study on Algerian Banking Sector*. *01*, 0–2. https://doi.org/10.1002/1873-3468.14404

Bressan, S., Ceri, S., Bellahsene, Z., Hunt, E., Ives, Z., Unland, R., & Rys, M. (2005). Information Security. In *Lecture Notes in Computer Science* (Vol. 3671).

Céline Tea., H. A. L. (2010). *Retour d ' expérience et données subjectives : quel système d ' information pour la gestion des risques ? Céline Tea To cite this version : HAL Id : pastel-00005574 Docteur l ' École Nationale Supérieure d ' Arts et Métiers*.

Gb31103. (2012). Customers Satisfaction and its Implications for Bank Performance in Nigeria. *Social Sciences*, *5*(1), 13–29.

Hammoud, J., Bizri, R. M., & El Baba, I. (2018). The Impact of E-Banking Service Quality on Customer Satisfaction: Evidence From the Lebanese Banking Sector. *SAGE Open*, *8*(3). https://doi.org/10.1177/2158244018790633

Intyaswati, D. (2017). The Role Of Consumer Privacy And Security On Brand Loyalty. *Jurnal Ilmu Komunikasi*, *6*(2), 12–19.

Khadidja, Z., & Bachir, B. (2018). The Algerian bank between eco-regulations and development of customer loyalty. *Financial Markets, Institutions and Risks*, *2*(2), 93–99. https://doi.org/10.21272/fmir.2(2).93-99.2018

Khalaf Ahmad, A. M., & Ali Al-Zu'bi, H. (2011). E-banking Functionality and Outcomes of Customer Satisfaction: An Empirical Investigation. *International Journal of Marketing Studies*, *3*(1), 50–65. https://doi.org/10.5539/ijms.v3n1p50

Khatab, J. J., Esmaeel, E. S., & Othman, B. (2019). The influence of service quality on customer satisfaction: Evidence from public sector and private sector banks in kurdistan/iraq. *International Journal of Advanced Science and Technology*, *28*(20), 865–872.

Lalanne, V., Munier, M., & ... (2013). Gestion des Risques dans les Systèmes d'Information Orientés Services. *... Systèmes d'Information ...*. http://munier.perso.univ-pau.fr/research/papers/2013/2013-SARSSI-VL/SARSSI_2013_VL_MM_AG.pdf

McCarthy, E. (2006). Protecting Client Data. *Journal of Financial Planning, June*, 26.

McKecnie, S., Ganguli, S., & Roy, S. K. (2011). Generic technology-based service quality dimensions in banking: Impact on customer satisfaction and loyalty. *International Journal of Bank Marketing*, *29*(2), 168–189. https://doi.org/10.1108/02652321111107648

Singh, R., Pandiya, B., Upadhyay, C. K., & Singh, M. K. (2020). IT-governance framework considering service quality and information security in banks in India. *International Journal of Human Capital and Information Technology Professionals*, *11*(1), 64–91. https://doi.org/10.4018/IJHCITP.2020010105

Whence, R. L. O. (2016). Whence Consumer Loyalty? Both. *25th Russian Particle Accelerator Conference, RuPAC 2016*, *63*(1999), 493–495.

Yoon, C. (2010). Antecedents of customer satisfaction with online banking in China: The effects of experience. *Computers in Human Behavior*, *26*(6), 1296–1304. https://doi.org/10.1016/j.chb.2010.04.001