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

Mémoire de fin d'études

En vue de l'obtention d'un master académique en

« Entrepreneuriat et Management de projet »

La maitrise des risques liés à la sécurité des plateformes digitales.

Cas : DEVLOG

Élaboré par :

Mme. OUALI Racha

Mme. AKHROUF Aicha

Encadré par :

Dr. BELALI Mounir

Dr. DJENNADI Lydia

Dr. BEDAIDA Imad Eddine

Année Universitaire : 2023/2024

Résumé

La sécurité informatique est essentielle pour toutes les entreprises afin de protéger les données de leurs clients, respecter les réglementations et renforcer la confiance des parties prenantes.

L'entreprise **DEVLOG**, une start-up dynamique en Algérie spécialisée dans le développement d'applications informatiques innovantes, propose des solutions standards et sur-mesure pour répondre aux besoins spécifiques de ses clients. Notre étude se concentre sur la maîtrise des risques liés à la sécurité des plateformes digitales en élaborant une matrice AMDEC pour **DERMACARE**, clients de **DEVLOG**.

Pour ce faire, nous avons mené une étude qualitative basée sur des entretiens semi-directifs auprès du personnel travaillant dans l'entreprise, complétée par un travail d'observation ainsi que la technique d'immersion.

Les résultats de notre étude révèlent une diminution des risques indésirables suite à la mise en place des mesures immédiates visant à les ramener à un niveau modéré. Parallèlement, nous avons observé une augmentation des risques modérés, ce qui montre une progression dans notre aptitude à identifier et contrôler ces risques par le biais de mesures préventives et correctives.

Mots clés : AMDEC, maitrise des risques, plateforme digitale, risques, sécurité informatique.

Abstract

Information security is essential for all businesses to protect customer data, comply with regulations, and build stakeholder trust. DEVLOG, a dynamic start-up in Algeria specializing in the development of innovative IT applications, offers both standard and customized solutions to meet the specific needs of its clients. Our study focuses on managing risks related to the security of digital platforms by developing an FMEA matrix for DERMACARE, a client of DEVLOG.

To achieve this, we conducted a qualitative study based on semi-structured interviews with the company's staff, complemented by observation and immersion techniques. The results of our study reveal a reduction in undesirable risks following the implementation of immediate measures aimed at bringing them to a moderate level. At the same time, we observed an increase in moderate risks, indicating progress in our ability to identify and control these risks through preventive and corrective measures.

Keywords: FMEA, risk management, digital platform, risks, information security.

ملخص

يعتبر أمان المعلومات ضروري لجميع الشركات لحماية بيانات العملاء والامتثال للأنظمة وتعزيز ثقة الأطراف المعنية. تقدمDEVLOG ، وهي شركة ناشئة ديناميكية في الجزائر متخصصة في تطوير تطبيقات تكنولوجيا المعلومات المبتكرة، حلولاً قياسية ومخصصة لتلبية الاحتياجات الخاصة لعملائها. تركز دراستنا على إدارة المخاطر المتعلقة بأمان المنصات الرقمية من خلال تطوير مصفوفة AMDEC لعميلهم DERMACARE.

لتحقيق ذلك، أجرينا دراسة نوعية بناءً على مقابلات شبه موجهة مع موظفي الشركة، مُكملةً بالمراقبة وتقنيات الغمر. تكشف نتائج دراستنا عن تقليل المخاطر غير المرغوبة بعد تنفيذ تدابير فورية تهدف إلى خفضها إلى مستوى معتدل. وفي الوقت نفسه، لاحظنا زيادة في المخاطر المعتدلة، مما يشير إلى تقدم في قدرتنا على تحديد هذه المخاطر والسيطرة عليها من خلال التدابير الوقائية والتصحيحية.

الكلمات المفتا حية: AMDEC ، إدارة المخاطر، منصة رقمية، مخاطر، أمان المعلومات.

REMERCIEMENT

Au nom de mon créateur, celui qui facilite mes affaires et protège mes actions, à Toi la louange et la gratitude du début à la fin. "EL HAMDOULI'LLAH".

Tout d'abord, je souhaite remercier chaleureusement, ***Dr. BEDAIDA Imad Eddine,*** *pour son soutien indéfectible, ses conseils avisés et sa disponibilité tout au long de cette période. Sa bienveillance, son écoute attentive et sa capacité à guider avec discernement ont été une source de motivation constante pour moi. Je lui suis très reconnaissante, merci monsieur !*

Ainsi que ***DR. DJENNADI Lydia****,* ***Dr. BELALI Mounir****,* ***DR. GAHLEM Nadia****, Votre passion pour l'enseignement, votre dévouement et votre pédagogie envers vos étudiants sont exemplaires. Grâce à vous, j'ai non seulement acquis des connaissances précieuses, mais aussi développé une véritable passion pour la recherche.*

Je tiens à exprimer ma gratitude envers l'ensemble du corps professoral de l'École Nationale Supérieure de Management pour leur enseignement exceptionnel, ainsi qu'à l'équipe de DEVLOG pour l'expérience professionnelle enrichissante qu'ils m'ont offerte durant mon stage.

Je remercie du plus profond de mon cœur mes parents, a qui, quels que soient les mots que je pourrais prononcer, je ne pourrai jamais rendre justice. ***MON PERE*** *formidable qui m'a honoré de son nom qui pour moi est le plus beau titre et m'a donné son amour et son soutien sans compter. Et* ***MA MERE****, sous les pieds de laquelle dieu a placé le paradis, qui a toujours rêvé de voir ce jour et dont les yeux brillent de fierté en me voyant accomplir mes rêves.*

*Je tiens à exprimer ma gratitude envers mon frère****, OUALI Diaa E-ddine****, mon roc et la prunelle de mes yeux qui m'a soutenue avec amour dans mes moments de faiblesse, en renforçant ma confiance et ma détermination intérieures.*

Je remercie particulièrement Madame SAADI Dalila, qui a été mon soutien a l'école, ainsi que mes amis avec qui j'ai passé des moments mémorables durant mon parcours a l'ENSM (Amina, Amine, Imad, Hala, Iyad, Abdallah, Lydia, Aicha, Raouene), j'ai eu des souvenirs inoubliables grâce à vous, je vous souhaite le meilleur pour l'avenir.

MERCI A VOUS TOUS !

Remerciement

Tout d'abord, je remercie chaleureusement mes parents. Leur amour inconditionnel, leur soutien indéfectible et leurs encouragements constants ont été essentiels pour moi. Vous avez toujours cru en moi, même dans les moments les plus difficiles, et c'est grâce à votre soutien que j'ai pu mener à bien ce projet. Vos sacrifices et votre dévouement sont inestimables, et je vous en suis infiniment reconnaissant.

Je souhaite aussi exprimer ma profonde reconnaissance envers mes encadrants, Dr BEDAIDA Imad eddine et Dr DJENNADI Lydia et Dr BELALI Mounir, vos expertises, vos conseils avisés et votre disponibilité ont été des éléments clés dans la réalisation de ce mémoire. Vous avez su me guider avec patience et rigueur, et m'aider à surmonter les défis rencontrés tout au long de ce travail. Votre soutien académique et professionnel a été inestimable, et je vous en suis très reconnaissant.

Je tiens également à remercier DR GAHLAM Nadia pour son soutien pendant les formations à l'incubateur. Son aide et son encouragement ont été très précieux dans cette période intense.

Je tiens également à remercier mes frères AKHROUF Tahar, Rami, Houssayen, Wassim

Mes remerciements s'adressent également à mes tuteurs de stage, CHENOUF Imad et LEKOUARA Sara, pour leur conseils pratiques tout au long de cette expérience professionnelle ont été d'une grande valeur

Liste des abréviations

AACDHB : Association Algérienne de Chirurgie Digestive et HépatoBiliaire.

ADS : Advertisement.

AIC : Algeria Invest Conference.

AJS : Algerian Journal of Surgery.

AMDEC : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité.

AOT : Ahead Of Time.

APT : Advanced Persistent Threats.

ARS : Agence Régionale De Santé.

C : criticité.

CAT : Cyversecurity Awarness and Training.

C.I.D.P: Confidentialité, Integrité, Disponibilité, preuve et non repudiation.

CRM : Customer Relationship Management.

D : Détection.

DDos : Distributed Denial of Service.

DGS : Direction générale de la santé.

DOM : Document Objet Model.

EDR : Endpoint Detection and Response.

ERP : entreprise ressources operationnels.

F : Fréquence.

FMEA : Failure Mode and Effects Analysis.

FTA : Analyse par Arbre de Défaillance.

FTOPSIS : Fuzzy Technique for Order of Preference by Similarity to Ideal Solution.

G : Gravité.

HEC : Hautes Études Commerciales.

IA : Artificial Intelligence.

IEC : International Electrotechnical Commission.

IOT : Internet of Things.

ISO : International Organization for Standardization.

JIT : Just In Time.

MDR : Managed Detection and Response

ML : Machine Learning.

MVC : Modelé Vu Contrôleur.

NGAV : Next-Generation Antivirus

NPD : New Product Development.

NPM : Node.js Package Manager.

R-A : Recherche-Action

ROAM : Resolved, Owned, Accepted, Mitigated.

RPN : Risk Priority number.

SMQ : Système management Qualité.

SPSS : Statistical Package for the Social Sciences.

Liste des tableaux

Liste des figures

Table des matières

INTRODUCTION GENERALE

La transformation digitale change profondément notre interaction avec la technologie. La plupart des gens sont maintenant connectés en permanence et utilisent de nombreux services en ligne. Cependant, cette connectivité constante nous expose à des risques de sécurité. Les cybercriminels peuvent accéder à nos informations privées, les modifier ou les détruire, et il y a aussi le risque que nos données soient accidentellement divulguées. Dans ce monde interconnecté, les individus, les entreprises et les infrastructures nationales sont vulnérables. Les conséquences des cyberattaques réussies peuvent être graves, tant économiquement que socialement. Ainsi, la sécurité informatique est devenue un enjeu crucial pour tout le monde, des citoyens aux professionnels et décideurs politiques.

L'évolution digitale transforme radicalement notre interaction avec la technologie. La majorité des gens sont désormais en ligne en permanence, profitant d'une multitude de services digitaux. Cependant, cette connectivité omniprésente nous expose à des risques de sécurité informatique, avec des cybercriminels qui peuvent compromettre, altérer ou anéantir nos informations privées. Il existe aussi un danger réel de divulgation accidentelle de nos données personnelles. Dans ce contexte interconnecté, non seulement les individus, mais aussi les entreprises et les infrastructures nationales essentielles sont à risque. Les impacts d'attaques cybernétiques réussies peuvent être dévastateurs sur le plan économique et social. De ce fait, la sécurité des systèmes informatiques est devenue une question cruciale pour chacun, des simples citoyens aux professionnels et décideurs politiques. (Kremer, Ludovic, Didier , & Vincent, mai 2019)

Contexte de l'étude

Selon le rapport annuel "State of Stalkerware" de Kaspersky, environ 29 312 personnes ont été affectées par les stalkerwares en 2022, un chiffre proche des 32 694 utilisateurs touchés en 2021. Cette même étude classe l'Algérie au 12ème rang mondial des pays les plus touchés par ces logiciels malveillants. Selon les données recueillies, 59 % des ordinateurs des entreprises algériennes ont été touchés par des logiciels malveillants en 2022, plaçant ainsi l'Algérie au deuxième rang en Afrique pour les attaques cybernétiques.[1]

Face à l`augmentation alarmante des cyberattaques, le gouvernement algérien, sous la direction du président de la république, a pris la décision de créer une École nationale supérieure de cybersécurité.[2] Cette initiative, annoncée lors du Conseil des ministres le 12

[1] https://www.kaspersky.fr/about/press-releases/2023_la-derniere-etude-de-kaspersky-revele-que-malgre-une-legere-baisse-en-2022-le-probleme-des-stalkerwares-reste-un-phenomene-mondial
[2] https://cybersecuritymag.africa/creation-ecole-nationale-cybersecurite-algerie

septembre 2023, vise à renforcer la sécurité nationale en centralisant et en optimisant les efforts de cybersécurité. Pour contrer cette tendance, le projet, mené par le ministère de l'Enseignement supérieur en collaboration avec le ministère de la Défense nationale, se focalisera sur la formation spécialisée afin d'armer le pays des compétences requises pour protéger ses infrastructures numériques essentielles.

Dans ce contexte, **DEVLOG**, une entreprise de développement web, joue un rôle crucial. En tant qu'acteur clé dans la création et la maintenance de plateformes digitales, **DEVLOG** est directement confronté aux défis de sécurité numérique. La maitrise des risques pour la sécurité des plateformes digitales repose sur une méthode systématique. Elle commence par une analyse approfondie des risques potentiels. Cela comprend l'évaluation des vulnérabilités, la mise en place de mesures de prévention et de protection, ainsi que la création de plans d'action et de récupération en cas d'incident. Cette approche s'appuie sur des études de perception des risques, des analyses de l'impact économique et une compréhension scientifique des réactions sociales aux différentes sources du risque. (Aven & Ortwin , 2010). Il est important de noter que notre étude a été appliqué sur la plateforme de **DERMACARE**, qui est un client de l'entreprise **DEVLOG**.

Objectif et problématique de l'étude

L'objectif principal de cette étude est de **maitriser les risques** liés à la sécurité des plateformes numériques, en se concentrant particulièrement sur la plateforme du client **DERMACARE,** comme évoqué précédemment.

Dans ce cadre, nous essayons de trouver l'outil le plus adéquat qui nous permettra d'assurer la protection et la résilience de la plateforme contre les menaces potentielles, tout en fournissant des conseils utiles aux responsables de la sécurité.

Pour répondre à nos objectifs d'étude, notre question de recherche se formule ainsi :

Comment concevoir et mettre en œuvre un processus d'évaluation des risques pour garantir la sécurité des plateformes digitales chez DEVLOG ?

A partir de cette question de recherche nous avons identifié des sous questions comme suit :

- Quels sont les principaux risques liés à la sécurité des plateformes digitales chez **DEVLOG** ?
- Quels critères doivent être pris en compte pour évaluer l'impact et la criticité de ces risques ?

- Quel outil spécifique serait le plus adapté pour répondre aux besoins de **DEVLOG** en matière de sécurité des plateformes digitales ?

Méthode

Dans le cadre de notre étude, nous avons entrepris une étude qualitative basée sur une recherche-action visant à comprendre les enjeux de sécurité dans le contexte des plateformes digitales. À cet effet, nous avons mené des entretiens semi-structurés avec quatre employés de **DEVLOG**. Les données recueillies ont été traitées de manière sémantique à l'aide du logiciel NVIVO 11.

La sélection de ces participants a été effectuée en considérant qu'ils représentaient l'ensemble des travailleurs de **DEVLOG**.

Ces entretiens, menés de manière à garantir la cohérence et la comparabilité des réponses, ont permis aux participants de partager leurs opinions, expériences et suggestions concernant les aspects liés à la sécurité des plateformes digitales, y compris les risques et les mesures de prévention.

Pertinence de l'étude :

- **Intérêt académique**

Cette étude comble un vide dans la littérature en sécurité digitale en proposant une méthodologie pratique pour évaluer et gérer les risques des plateformes digitales. Elle enrichit la recherche académique en offrant une approche qualitative rigoureuse.

- **Intérêt professionnel**

La pertinence de ce sujet réside dans sa capacité à fournir des outils et des connaissances nécessaires pour améliorer la sécurité des plateformes digitales, protéger les données sensibles et renforcer la confiance des utilisateurs dans un environnement numérique de plus en plus menaçant.

Plan du document :

Ce mémoire s'inscrit dans une démarche de maîtrise des risques liés à la sécurité des plateformes digitales, en se concentrant particulièrement sur la plateforme DERMACARE, un client de DEVLOG. Ce document contient :

Une introduction générale présente la thématique de recherche et les objectifs de notre étude, ainsi que la pertinence du sujet. Dans un premier temps, le premier chapitre est consacré à la revue de la littérature, suivie d'un cadre conceptuel où sont définies les notions

de base. Le deuxième chapitre se divise en deux sections : la première section aborde l'approche épistémologique, la présentation de la méthodologie de recherche où nous avons opté pour une étude qualitative basée sur la recherche-action, les méthodes et outils de collecte des données, ainsi que le traitement des données ; la deuxième section présente l'organisme d'accueil.

Le troisième chapitre est également structuré en deux sections. La première section présente les résultats de l'étude qualitative menée, tandis que la deuxième section propose une discussion approfondie de ces résultats, en les comparant avec les conclusions de notre revue de littérature. Enfin, la conclusion générale, rappellera l'objectif de l'étude, la structure méthodologique, la méthodologie de recherche, ainsi que les contributions, les implications, les obstacles et les perspectives de notre étude.

CHAPITRE 1 : ÉTAT DE L'ART

La sécurité des plateformes numériques est devenue un enjeu majeur pour les organisations, tant du secteur privé que public, confrontées à un environnement numérique en constante évolution. La gestion des risques de sécurité sur les plateformes numériques est un défi complexe, nécessitant une approche stratégique et globale pour prévenir les cyberattaques et assurer la protection des données sensibles.

Ce chapitre se concentre sur la gestion des risques numériques et la cybersécurité. Nous allons examiner les recherches passées sur ces sujets. Nous verrons aussi comment intégrer la gestion des risques dans la transformation digitale des organisations. De plus, nous aborderons les bases de la gestion des risques, l'analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC), et leur application dans le contexte numérique. Ces éléments sont importants pour comprendre comment protéger les plateformes digitales contre les cyberattaques et assurer leur bon fonctionnement.

Section 1 : Le risque dans le numérique ; Exploration des travaux existants.

1. Étude antérieures et analyse critique :

La revue de la littérature est une étape importante de la recherche académique scientifique, elle consiste à examiner et à résumer les recherches récentes sur un sujet donné. Cela implique la lecture et l'analyse des articles, des livres, des synthèses et d'autres sources afin d'acquérir un aperçu des connaissances actuelles sur le sujet. Cette étape permet d'évaluer l'état de la recherche actuelle, de déterminer les lacunes et de démontrer la nécessité d'une nouvelle recherche.

1.1 Le management des risques

L'article de MATRADI Sara et al (2023), intitulé Évaluation de l'intégration de l'approche axée sur les risques en respectant la norme ISO 9001 version 2015 visait à examiner l'implémentation des pratiques de gestion des risques par une entreprise certifiée ISO 9001 :2015 dans un cadre au Maroc et à comprendre comment l'approche fondé sur les risques a été intégré. Les auteurs ont opté pour une approche qualitative basée sur une étude de cas spécifique pour analyser la rédaction des risques. Les résultats de l'étude ont montré que L'entreprise avait adapté son Système de Management de la Qualité (SMQ) en mettant l'accent particulière à la gestion des risques pour être conforme à la norme ISO 9001-2015. En conclusion cet article met l'accent sur l'importance d'intégrer une approche axée sur les risques dans le système de gestion de la qualité (SMQ) d'une entreprise pour garantir la

conformité aux normes, pour améliorer l'efficacité des processus et montrer un engagement envers la gestion des risques. Cependant, les lacunes et les limites de l'étude comprennent qu'elle s'étend à une seule entreprise industrielle, qu'elle se concentre sur la norme ISO 9001-2015 sans traiter spécifiquement les critères de sécurité des plates-formes, qu'il n'y a pas d'analyse des risques et qu'il faut une approche qui couvre plusieurs champs d'expertise pour une maîtrise plus globale des risques de ce domaine.

Maryem ALAOUI et al (2022), ont présenté un cadre théorique complet pour comprendre le management des risques dans les organisations dans leur article « Gestion des risques : Cadre théorique ». Ils ont souligné l'importance de comprendre et d'appliquer des méthodes efficaces de gestion des risques pour faire face aux incertitudes et aux événements indésirables susceptibles d'avoir un impact négatif sur les processus organisationnels.

Dans cette étude, les auteurs ont examiné divers aspects de la gestion des risques, notamment les concepts clés, les méthodes d'identification et d'évaluation des risques et le rôle important des systèmes d'information dans ce processus. Ils ont souligné que les facteurs de risque peuvent avoir un impact positif ou négatif, tout en soulignant que la gestion des risques peut créer à la fois des pertes potentielles et des opportunités d'amélioration.

Les méthodes de recherche sélectionnées ont privilégié une approche qualitative et a mis l'accent sur une analyse approfondie des principes et méthodes de gestion des risques.

Les auteurs ont visé à fournir des recommandations concrètes pour introduire les concepts théoriques de gestion des risques dans les organisations dans le but d'augmenter leur résilience et leur capacité à faire face aux défis actuels et futurs. En somme, cet article a fourni des informations théoriques précieuses sur la gestion des risques et a souligné l'importance cruciale de cette discipline pour garantir la durabilité et la performance organisationnelle dans un environnement économique en constante évolution.

L'étude menée par Lamiae Benhayoun-Sadafiyine et al (2022), a examiné les risques liés à l'utilisation des technologies numériques dans la transformation numérique des entreprises, trois principales catégories de risques ont été identifié par cinq experts en transformation numérique. Bien que la gestion efficace des technologies numériques ait été cruciale pour réduire les risques associés, il ne faut pas négliger les menaces externes. Assurer la sécurité des données et le respect des réglementations a été tout aussi important pour limiter les vulnérabilités.

Cet article a souligné à quel point il est vital de considérer ces enjeux afin de mener à bien la transformation numérique. Pourtant, l'analyse aurait pu aller plus loin en se penchant précisément sur les risques cybernétiques comme les attaques et fuites en ligne.

La poursuite des recherches aurait renforcé les recommandations visant à faire face aux risques associés à la transformation numérique pour les entreprises. Pour relever les défis de la révolution numérique, il était essentiel de faire face aux risques externes tout en améliorant la sécurité et la conformité internes.

A la lumière des articles précédents, on peut conclure que la gestion des risques est un élément essentiel du succès et de la durabilité des entreprises, surtout lorsqu'il s'agit de mettre en place un système de management de la qualité et de mener une transformation numérique. Cela implique non seulement d'anticiper et de gérer les incertitudes, mais aussi de s'adapter aux défis liés à l'utilisation croissante du numérique, comme la sécurité des données et la conformité réglementaire. En récapitulant, la prise en compte et la gestion efficace des risques sont cruciales pour assurer la pérennité et la performance globale des entreprises.

1.2. Le management des risques numériques et cybersécurité

ACHIR. C et al (2024), ont souligné l'importance d'intégrer l'intelligence artificielle dans la gestion des risques d'une organisation. Cette intégration a permis d'améliorer l'efficacité, la réactivité et la pertinence des stratégies de gestion des risques. De plus, l'utilisation de l'intelligence artificielle a ouvert des opportunités telles qu'une meilleure compréhension des risques, l'automatisation de certaines tâches, une meilleure détection des fraudes et des fraudes et des améliorations des processus.

Ils ont souligné l'impact de l'intégration de l'intelligence artificielle dans la gestion des risques d'une organisation et ont souligné que cette convergence des technologies offre une opportunité d'améliorer la gestion des risques. Il a notamment évoqué une meilleure prévision des risques, l'automatisation de certaines tâches, l'amélioration de la fraude et de sa détection, ainsi que la prise de décisions plus éclairées.

Cependant, les auteurs ont également souligné que la mise en œuvre de ces technologies n'est pas sans défis, notamment en matière de confidentialité, de sécurité et d'éthique.

En mettant en évidence ces aspects, les auteurs ont souligné l'importance de comprendre et de tirer parti des avancées technologiques pour améliorer la gestion des risques dans un environnement en constante évolution. Cependant, l'article ne présente pas, de recommandations spécifiques ou de bonnes pratiques pour faire face aux risques associés aux plateformes numériques qui utilisent l'intelligence artificielle et le big data.

HAMMACHE Souria et al (2022), dans leurs articles ont examinés en détail les éléments qui ont eu Influence sur l'intention d'achat des consommateurs en Algérie sur les plates-formes numériques.

Les auteures ont utilisé dans son étude une approche quantitative. Les données ont été collectées entre août 2021 et octobre 2021 à l'aide d'un questionnaire structuré distribué via la plate-forme "Google Forms" et des copies papier, puis traiter par le logiciel SPSS. La population cible comprenait 360 consommateurs algériens.

L'article souligne que l'un des facteurs les plus important de l'intention d'achat c'est le risque perçu par le consommateur. Les consommateurs algériens ont mis l'accent sur la qualité du produit, la sécurité liés aux méthodes de payement et le délai de livraison.

Deuxièmement, l'intention des consommateurs d'acheter en ligne a été fortement impactée par les stratégies de marketing digitale, telles que la publicité et les offres spéciales. Enfin, la motivation d'achat est cruciale pour expliquer le désire d'achat en ligne des consommateurs algériens. Même si la contribution est substantielle, l'article présentes des limites. Ce dernier n'a pas discuté des risques liés à la sécurité des achats en ligne ou à la protection des données des consommateurs contre l'usage abusif. Il n'a pas non plus inclus les cyberattaques et les menaces les plus graves.

Selon les recherches de Mohammad Hijji et al (2022), Les résultats ont révélé que le cadre CAT a était efficace pour sensibiliser et former les employés aux menaces de cybersécurité, particulièrement aux offenses basées sur l'ingénierie sociale. Le but de la recherche était de créer un cadre de sensibilisation et de formation à la cybersécurité (CAT) pour soutenir les entreprises à protéger leurs actifs et leurs données contre les cybermenaces, notamment les attaques basées sur l'ingénierie sociale pendant épidémie de COVID-19. Les auteurs ont utilisé une approche mixte en combinant une revue de la littérature, des études empiriques, des entretiens avec des experts en cybersécurité et des études de cas pour déterminer l'efficience du cadre CAT.

L'article a souligné la pertinence de sensibiliser et de former les personnels à la cybersécurité, en particulier sur le web, et a mis en avant le cadre CAT comme un outil envisageable pour accroître la position de sécurité des organisations face aux risque cybernétiques.

L'article d'Ankit Kumar Jain et al (2021), a étudié les risques liés à la sécurité et à la confidentialité des plateformes de médias sociaux en ligne. Et les solutions existantes pour assurer la protection des usagers. En analysant des études scientifiques, des rapports et des

études de cas existants, leur étude qualitative a visé à identifier les tendances et les problèmes de sécurité et de confidentialité dans ces réseaux.

Les constatations ont montré que les réseaux sociaux en ligne aient été de plus en plus populaires, cela augmente le risque lié à la sécurité et la confidentialité des utilisateurs. Les avancées de la recherche académique pour protéger ces réseaux ont parfois été difficiles à mettre en œuvre et pratiques. Par conséquent, Il est crucial que les utilisateurs soient conscients des risques potentiels des risques potentiels et des bonnes pratiques de sécurité lorsqu'ils ont utilisé les réseaux sociaux en ligne. En conclusion, l'article examine les risques liés à la sécurité et la confidentialité des réseaux sociaux en ligne et met en avant l'importance de continuer les recherches dans ce domaine. Cependant, il présente certaines lacunes, telles que L'absence de considération d'autres catégories de plates-formes digitales, une approche pratique déficiente dans les directives, la nécessite d'une analyse approfondie des solutions proposées et l'absence de perspectives des acteurs.

Selon Abeeku Sam Edu et al (2021), dans leur article ont examiné les risques associés à l'utilisation des technologies de IoT « Internet des objets », de l'analyse de données massives et du cloud computing dans les établissements financiers. Pour évaluer ces risques, ils ont utilisé des méthodes quantitatives et qualitatives telles que la FMEA et la FTOPSIS. L'enquête a mobilisé 234 spécialistes de la sécurité financière et a souligné des désagréments importants tels que la sous-utilisation de groupes électrogènes, les vulnérabilités de pare-feu et l'omission d'audits de sécurité. De plus, des problèmes liés à la configuration digitale et à la fiabilité des plates-formes ont été notifié.

Cette étude a souligné l'importance pour les institutions financières d'adopter des méthodes efficaces de gestion des risques pour protéger leurs plateformes en ligne contre les cybermenaces. Il a été particulièrement important de protéger les données et les systèmes pour garantir la confidentialité, l'intégrité et l'accessibilité des informations personnelles. Pour garantir la discrétion, l'intégrité et l'accessibilité des informations privées, la protection des données et des systèmes a nécessité une attention particulière. L'article a également souligné des domaines nécessitant une attention attentive, notamment le fait que les résultats ne peuvent pas être généralisés à d'autres secteurs industriels en raison du profil des experts interrogés, de la nouveauté de l'intégration de ces technologies et de la fiabilité des points de vue des experts en sécurité par rapport des données. Ces lacunes mettent en lumière l'importance de réaliser des recherches continues pour identifier et réduire les dangers récents de la sécurité numérique.

L'article de Marc BOURREAU et al (2020), intitulé "Plates-formes numériques : réguler avant qu'il ne soit trop tard", Avait pour objectif d'analyser les problèmes liés à la régulation des plates-formes numériques. Leur approche qualitative reposait sur une analyse conceptuelle et théorique des enjeux, mettant en lumière la nécessité d'une action régulatrice préventive pour éviter des effets néfastes sur la concurrence et la société. Les résultats ont souligné l'importance de réguler proactivement ces plates-formes pour éviter tout impact négatif sur la concurrence et l'écosystème économique.

De plus, ils ont souligné l'importance de surveiller les pratiques des grandes plates-formes, en particulier en ce qui Il s'agit de l'accès aux données et les évolutions technologiques, afin de maintenir une concurrence équitable. Cependant, l'étude présente certaines limites, notamment le fait qu'elle se concentre principalement sur la concurrence plutôt que sur une analyse approfondie des risques liés à la sécurité des données et des utilisateurs, qu'il n'y a pas de recommandations spécifiques pour renforcer la sécurité des plates-formes et des données.

Les vulnérabilités et les problèmes de sécurité du cadre Hadoop dans le contexte de la technologie Big Data ont été abordés dans l'article de Gurjit Singh Bhathal et al (2019), Ils ont utilisé une analyse conceptuelle et théorique des défis liés aux plates-formes numériques pour mettre en avant l'importance de sécuriser les données face aux nouvelles technologies et aux risques potentiels. Les résultats de cet article ont mis en évidence l'importance d'adopter une approche préventive pour contrôler ces plates-formes afin d'éviter tout effet négatif sur la concurrence et le système économique. De plus, Ils ont souligné l'importance de surveiller les pratiques des grandes plateformes, en particulier en ce qui concerne l'accès aux données et les progrès technologiques, afin de garantir un environnement concurrentiel équitable.

Les insuffisances de l'étude comprennent la restriction à un seul cadre sans comparaison avec d'autres cadres Big Data, la priorité accorder aux vulnérabilités spécifiques à Hadoop, l'absence d'études approfondies sur les pratiques de gestion des risques liées à la sécurité et l'accent mis principalement sur les vulnés. La pertinence de l'article aurait été renforcée par une approche plus globale qui inclurait une analyse approfondie des meilleures pratiques de gestion des risques, des études de cas et une comparaison avec d'autres cadres.

Le Dr Jitendra SHARMA et al (2017), dans leur article ont examiné l'impact des caractéristiques démographiques sur le comportement des consommateurs en ligne en termes de risque perçu tel que l’Age, le genre, le revenu, l'éducation et la profession. Pour analyser

les interprétations des utilisateurs d'e-commerce, les chercheurs ont utilisé une approche mixte qui combinait des méthodes qualitatives et quantitatives en organisant des discussions de groupe et en utilisant un questionnaire structuré. Les résultats ont mis en évidence que des caractéristiques démographiques tels que le genre et le salaire étaient liés aux perceptions du risque par les utilisateurs en Inde, et que les risques liés à la performance et au fond étaient importants. A rebours de certaines études antérieures, l'étude n'a pas corroboré une relation inverse entre l'éducation et la tolérance au risque. Les résultats ont montré qu'en vue d'améliorer leurs expériences d'achat en ligne, les E-commerçants ont dû comprendre et contrôler ces risques. Bien que les résultats aient été positifs, l'étude a manqué de clarté, notamment en ne se concentrant pas sur les risques liés à la sécurité des plates-formes, En ne prenant pas le temps d'examiner les protocoles de sécurité mises en place par les entreprises d'e-commerce. En ne fournissant pas de données spécifiques sur les désagréments de sécurité et en extrapolant les résultats sans prendre en compte les différences culturelles et régionales.

Richter Bays et al (2015), ont utilisé une approche qualitative en triant les publications selon des classifications et des sous-catégories après une analyse approfondie de la littérature spécialisée, pour but de passer en revue la sécurité des réseaux virtuels, Les auteurs ont sondé pour repérer les risques principaux qui persistent sur ces environnements, présenter les moyens existants de les sécuriser et discuter de diverses angles de la sécurité des réseaux virtuels dans le but de éduquer et de propager des informations sur la sécurité des infrastructures de réseaux virtuels.

Les recherches basées sur l'émulation des réseaux ont également pris en compte les frais supplémentaires des équipements de sécurité pour s'assurer qu'elles étaient convenables dans le monde réel. Les notions de virtualisation des réseaux doivent également être protégées contre des périls telles que la divulgation des données confidentielles et les attaques par refus de service.

Cependant, en raison de la récurrence des attaques visant à causer des perturbations, les publications dans le domaine se focalisent principalement sur les menaces de perturbation et les contre-mesures associées. En résumé, l'article a souligné l'importance de protéger les données et les services dans les environnements de virtualisation des réseaux. Il a mis en lumière des risques telles que l'accès non autorisé, les attaques de type "Dos" et la divulgation de données sensibles, et de prendre des mesures efficaces pour réduire ces risques.

Après l’examen des articles ci-dessus, on constate que la gestion des risques dans le monde numérique est essentielle pour garantir la sécurité et la confidentialité des données, ainsi que pour maintenir la confiance des utilisateurs. L'intégration de l'intelligence artificielle offre des opportunités d'amélioration, mais nécessite une surveillance constante pour prévenir les abus. Dans le commerce en ligne, la qualité des produits et la sécurité financière sont des facteurs déterminants pour les consommateurs. La sensibilisation à la cybersécurité est cruciale pour les entreprises, tout comme la protection des données personnelles sur les réseaux sociaux. Enfin, dans le secteur financier, la gestion efficace des risques est essentielle pour maintenir la confidentialité des informations et la confiance des clients. En résumé, la maîtrise des risques numériques est un défi crucial mais nécessaire dans un monde en constante évolution.

1.3. Analyse des modes de défaillances, de leurs effets et de leurs criticités (AMDEC)

L'article de Joseph Kelada (1998), sur l'AMDEC (Failure Modes, Effects, and Severity Analysis) s’est concentré sur une description détaillée de cette technique et de ses applications en matière de qualité et de prévention des risques. L'objectif principal a été de fournir une compréhension approfondie de l'AMDEC, de ses étapes, de ses objectifs et de ses avantages potentiels aux entreprises ayant cherché à améliorer la fiabilité, la sécurité et la qualité de leurs produits et processus.

Les livrables de l'AMDEC ont inclus l'identification systématique des modes de défaillance potentiels, l'évaluation de la cause sous-jacente de la défaillance, l'analyse de l'impact de la défaillance sur l'ensemble de l'entreprise, la hiérarchisation des risques en fonction de leur gravité et des actions préventives ou correctives, contient des suggestions d'action.

Enfin, l'AMDEC a été présentée comme une méthode puissante pour identifier, évaluer et prioriser les risques de défaillance potentiels, permettant aux entreprises d'anticiper les problèmes, de prendre des mesures préventives et d'améliorer la qualité et la fiabilité des produits et des processus, contribue à améliorer la sécurité.

Mohamed Mouda et al (2013), ont souligné l'importance de l'AMDEC informationnelle pour l'amélioration des processus industriels, en se concentrant sur l'analyse des risques informationnels dans un environnement industriel en constante évolution.

Ils ont adapté l'AMDEC aux opérations industrielles et ont souligné l'importance de cette approche pour une compréhension plus approfondie et une amélioration des processus

industriels en se concentrant sur les aspects temporels et organisationnels de l'information industrielle.

En identifiant les types d'erreurs courants et en suggérant des méthodes d'analyse des risques, une AMDEC informative devient un outil précieux pour assurer le contrôle opérationnel des processus et renforcer la compétitivité des entreprises.

Cet article est cependant limité car il se concentre principalement sur les risques informationnels et procéduraux industriels et ne considère pas d'autres aspects de la sécurité des plateformes, tels que les risques physiques et les risques de cybersécurité.

On constate que les articles soulignent l'importance de comprendre et de mettre en œuvre la méthode AMDEC pour améliorer la fiabilité, la sécurité et la qualité des produits et des processus dans les organisations industrielles. La méthode AMDEC est appliquée à la conception d'installations fiables et maintenables et à la définition du plan préventif initial. On constate également l'importance de la méthode informationnelle AMDEC pour améliorer les processus industriels ou se concentrer sur l'analyse des risques informationnels. La méthode AMDEC est adaptée pour une meilleure amélioration des processus industriels, garantissant la fiabilité et la sécurité des systèmes industriels.

La maîtrise des risques constitue une approche préventive visant à détecter, estimer et atténuer les risques potentiels, en planifiant des réponses adaptées et en surveillant en performances les évolutions pour ajuster les stratégies en conséquence.

Bien que l'importance d'une telle approche systématique ait été observée, les études antérieures se sont rarement concentrées exclusivement sur la maîtrise des risques liés à la sécurité des plateformes numériques. C'est pourquoi il est essentiel de combler cette lacune en menant une étude approfondie et nuancée sur la gestion des risques dans ce domaine. En vue d'améliorer la sécurité et la résilience des plates-formes en ligne face aux cyberattaques de plus en plus sophistiquées, une meilleure compréhension des vulnérabilités et une évaluation pointue des menaces sont nécessaires.

Section 2 : Cadre conceptuel

Cette section explore la gestion des risques pour les plateformes numériques.

Couvre des sujets tels que la sécurité informatique, la gestion des risques, la cybersécurité, les plateformes numériques, les menaces informatiques, les vulnérabilités, l'évaluation des risques, les normes et la conformité réglementaire, les meilleures pratiques, avec diverses définitions et éléments clés de la gestion des risques.

1. LES NOTIONS DE BASE DU MANAGEMENT DES RISQUES

1.1. La notion risque

Toutes les organisations sont soumises à des influences internes et externes qui influencent la stratégie et maintiennent l'organisation dans un état constant d'incertitude.

Cette incertitude peut compromettre la réalisation des objectifs et constitue un risque. Le terme « RISQUE » fait référence à une combinaison de deux facteurs, Un aléa est un événement, un phénomène, un danger ou la possibilité d'un événement pouvant affecter notre environnement. D'un autre côté « ENJEU » qui peut s'agir de personnes, d'équipements ou de travaux ou un environnement susceptible d'être affecté par cet événement.

Il existe de 'ombreuses façons de définir le terme « risque », comme :

- La probabilité ou la probabilité factuelle d'un événement considéré comme dommageable.
- La définition du risque repose sur l'idée d'un danger potentiel ou d'un dysfonctionnement plus ou moins prévisible et pouvant causer un préjudice.
- Le risque est le résultat de ce qui peut être perdu et de la probabilité de le perdre réellement (Benhayoun-Sadafiyine & Boughzala, 2020), Cette définition met l'accent sur l'idée selon laquelle le risque est associé à l'incertitude quant à la survenance d'un événement indésirable et à ses conséquences possibles sur les activités et les objectifs d'une organisation.
- Ou encore comme "Éventualité d'un évènement futur, incertain ou d'un terme indéterminé, ne dépondant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage".[3]

[3] http://www.ineris.fr/

Tableau 1: *définition du risque*

Organisations	Définitions
ISO Guide 73 ISO 31000	L'impact de l'incertitude sur les objectifs varie et peut être positif ou négatif et, dans certains cas, conduire à des écarts par rapport aux attentes initiales. De même, le risque est souvent défini par un événement, un changement de circonstances ou un résultat.
Institute of Risk Management (IRM)	Le risque découle de la probabilité d'un événement et de son issue. Ces conséquences peuvent être positives ou négatives.
"Orange Book " de HM Treasury	L'incertitude des résultats dans une plage d'exposition donnée résulte d'une combinaison d'effets et de probabilités d'événements potentiels.
Institute of Internal Auditors	Incertitude quant à la survenance d'événements pouvant affecter la réalisation des objectifs. Les risques sont évalués en fonction des résultats et des probabilités.

:

Source : (HOPKIN, 2010)

Toutes les définitions ci-dessus notent que le risque est souvent décrit en termes d'événements, de changements de circonstances, de résultat ou de combinaison de ces facteurs et de la manière dont ils affectent la réalisation des objectifs.

1.1.1. Les caractéristiques du risque :

Un risque est défini par deux aspect principaux

- Probabilité d'occurrence (ou fréquence) : Il s'agit d'une mesure de la probabilité qu'un événement particulier se produise.

Plus la probabilité est élevée, plus le risque est susceptible de se réaliser.

- Impact ou gravité : Il s'agit du niveau d'impact qu'aura le risque s'il se produit.

L'impact peut être mesuré en termes de pertes financières, de dommages matériels, de blessures et d'atteinte à la réputation.

Plus l'impact est grave, plus le risque est élevé.

Ces deux mesures permettent aux organisations d'évaluer et de classer les risques en fonction de leur importance relative, permettant ainsi aux organisations de maitriser les ressources pour gérer les risques.

1.1.2. Les niveaux des risques :

Il est important de distinguer trois types de risques : le risque inhérent, le risque de contrôle et le risque résiduel. (Camélia, 2018)

a) Les risques inhérents ou bruts : sont des risques qui existent avant que des mesures correctives internes ne soient prises, tels que des déficiences dans les procédures, les activités de gestion ou les systèmes informatiques.

Deux critères sont généralement pris en compte pour évaluer le risque inhérent : la fréquence et l'impact. (Risque Brut = Fréquence x Gravité), Le risque inhérent est souvent calculé comme le produit de la fréquence et de l'impact

b) Le risque résiduel ou net : est le risque qui subsiste après la mise en œuvre de contrôles tels que les contrôles internes, la couverture financière ou le partage des risques.

Ceci est calculé en multipliant la fréquence par l'effet de l'élément de contrôle. (Risque Net = Fréquence x Effet x Elément de contrôle)

c) Le risque de contrôle : est le risque associé aux imperfections des outils utilisés par la direction pour réduire le risque inhérent.

Ces failles peuvent être liées à la conception ou à la mise en œuvre de ces outils.

1.2. La démarche du management des risques

La gestion des risques est la tâche de tous les acteurs sociaux. Il doit être complet et couvrir toutes les activités, processus et actifs de l'entreprise.

1.2.1. Définition du management des risques :

Le management des risques est un processus qui aide une organisation à identifier, évaluer et gérer les risques qui peuvent l'empêcher d'atteindre ses objectifs.

En d'autres termes, cette méthode de gestion des risques identifie les risques potentiels pour l'organisation et prend des mesures spécifiques pour réduire leur impact.

En tant que système dynamique, la gestion des risques s'adapte aux changements internes et externes qui peuvent affecter les risques auxquels une organisation est confrontée.

Cela comprend une approche proactive pour prévoir les risques émergents et mettre en œuvre des mesures préventives et correctives appropriées.

Tableau 2: *Définitions du management des risques*

Auteur / organisation	Définition
(Bahamid & Doh, 2017)	La gestion des risques implique l'analyse systématique, l'identification des risques, dans le but de maximiser l'opportunité et l'impact des événements positifs tout en réduisant la probabilité et l'impact des événements négatifs afin d'atteindre les objectifs, et la correspondance incluse.
(Thompson, Zimmerman, Mindar, & Taber, 2016)	La gestion des risques est un processus systématique et coordonné d'identification, de surveillance, d'évaluation, de classification et de contrôle des risques auxquels une organisation est exposée.
ISO 31000	La norme ISO 31000 Version 2018 – Gestion des risques – Lignes directrices définit la gestion des risques comme les activités coordonnées visant à gérer et contrôler une organisation en matière de risques.
ISO/IEC 27001	Le management des risques est l'activité coordonnée de gestion et de contrôle des risques d'une organisation, y compris l'évaluation des risques, la prise de décision en matière de risques, l'acceptation et le traitement des risques. En prenant en compte les intérêts des parties prenantes.
Institute of Risk Management (IRM)	Un processus conçu pour aider les organisations à comprendre, évaluer et répondre à tous les risques afin d'augmenter les chances de succès et de réduire la probabilité d'échec.

Source : élaborer par nous-mêmes

Le management des risques est un élément essentiel de l'exécution de la stratégie de toute organisation.

Il s'agit d'un processus par lequel une organisation aborde systématiquement les risques associés à ses activités et recherche ainsi des bénéfices durables de ces activités, individuellement et collectivement.

1.2.2. Les objectifs du management des risques :

- Création et la préservation de la valeur : Le management du risque vise à aider les organisations à créer de la valeur tout en maintenant leur valeur actuelle. En d'autres termes, c'est gérer les risques de manière à maximiser les opportunités tout en préservant les actifs et la réputation de l'organisation.
- Amélioration de la performance : Les organisations peuvent améliorer leur performance globale en identifiant, évaluant et gérant les risques. Cela signifie que la gestion des risques peut aider les organisations à atteindre leurs objectifs et à mieux

répondre aux exigences des parties intéressé. Cela peut entraîner une meilleure performance financière, opérationnelle et stratégique.

- Atteinte des objectifs : Les organisations peuvent mieux atteindre leurs objectifs stratégiques et opérationnels grâce à une gestion efficace des risques.
- Pour assurer une gestion efficace des risques à tous les niveaux, la gestion des risques doit être intégrée à la gouvernance et au leadership d'une organisation.

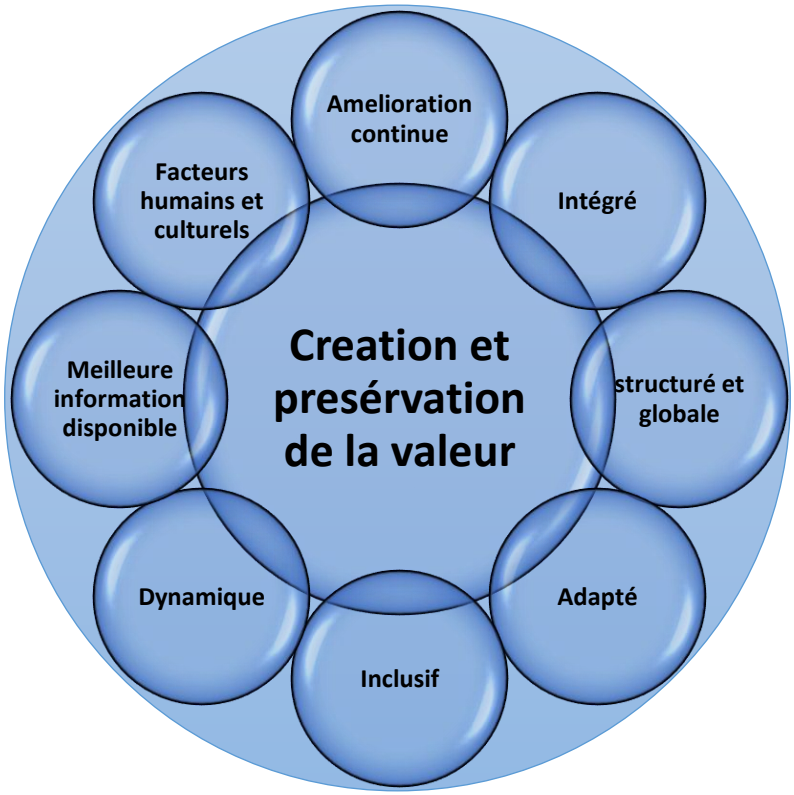
La norme ISO 31000 : 2018 aide les organisations à gérer efficacement les risques pour atteindre leurs objectifs, accroître leur efficacité et augmenter leur valeur ajoutée tout en tenant compte des incertitudes environnementales.

1.2.3. Les principes de management des risques :

La gestion des risques repose sur un certain nombre de principes et diverses tentatives ont été faites pour les définir. La norme internationale ISO 31000 énonce 08 principes de gestion des risques.

a) La gestion des risques doit faire partie intégrante de toutes les activités d'une organisation.
b) Pour obtenir des résultats cohérents, il est important d'avoir une approche structurée et globale de management des risques, adaptée au contexte et aux objectifs de l'organisation.
c) Pour que le management des risques soit efficace, il faut ajuster une stratégie en fonction de la taille, de la complexité et des objectifs de l'entreprise, ainsi que des facteurs externes et internes qui influencent vos opérations. Donc il doit être adaptée à l'organisation et a son environnement.
d) L'implication des parties prenantes au bon moment, permet de mieux gérer les risques en tenant compte de leurs connaissances et de leurs opinions.
e) Le management des risques doit être capable de s'adapter en anticipant, identifiant, reconnaissant et répondant aux nouveaux risques et changements internes et externes à l'organisation.
f) Le management des risques utilise des données passées, présentes et futures pour évaluer les risques.
g) La culture et le comportement des employés ont un impact significatif sur le management des risques à tous les niveaux et étapes. De plus, l'apprentissage et l'expérience améliorent continuellement le management des risques.

Figure 1: *Les principes de management des risques*



Source : (ISO 31000 :2018)

Cette figure illustre les éléments clés nécessaires pour gérer efficacement les risques au sein d'une organisation, tout en garantissant la création et la préservation de la valeur. En intégrant ces principes, on adopte une approche holistique qui permet de maîtriser les risques et d'assurer le maintien et l'augmentation de la valeur au sein de l'organisation.

1.2.4. Processus général de management des risques :

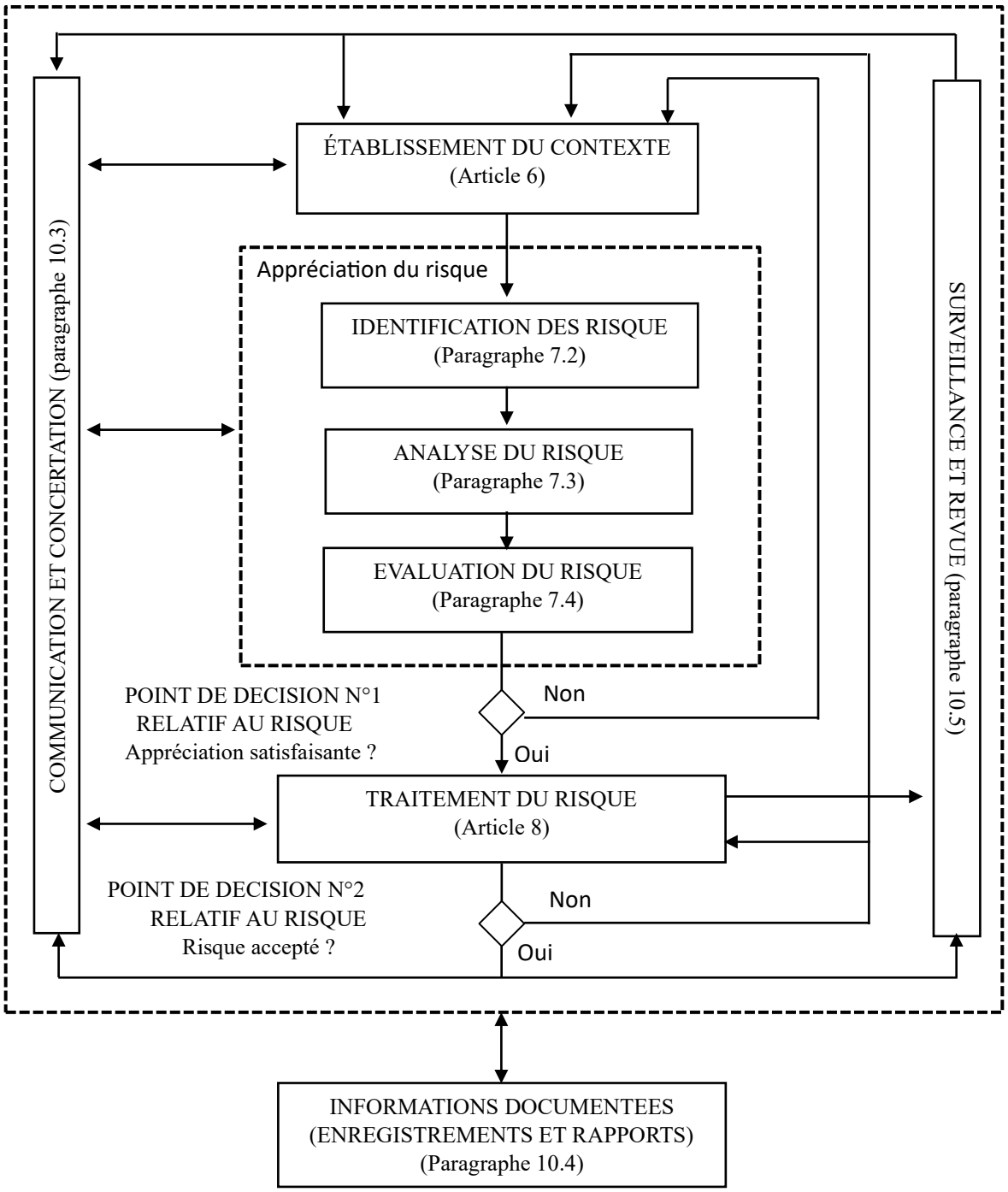
- Définir le contexte : Définir un cadre pour identifier, évaluer et gérer les risques, en tenant compte des objectifs, des contraintes, des parties prenantes et du contexte organisationnel.
- Conseils et communication : Communiquer efficacement les informations sur les risques et consulter les parties prenantes pour obtenir des points de vue divers.
- Enquêter sur les menaces, les vulnérabilités et les opportunités pour identifier les risques, anticiper les problèmes potentiels et développer des stratégies efficaces de gestion des risques.
- L'analyse des risques évalue la probabilité et l'impact des risques sur les ressources d'information. Classer les risques selon leur gravité et leur probabilité à l'aide de méthodes quantitatives et qualitatives.

- Évaluation des risques : comparez les résultats de l’analyse aux critères de risque pour déterminer si le risque est acceptable ou si un traitement est nécessaire.
- Le management des risques implique la mise en œuvre de mesures visant à réduire, transférer, éviter ou accommoder les risques identifiés grâce à l'élaboration de stratégies et de plans d'action appropriés.
- Surveillance et examen : Surveillance continue des risques, analyse des données et amélioration des processus de management des risques.
- Enregistrement et reporting des risques : Les risques identifiés, les décisions prises pour y faire face et les mesures de contrôle prises doivent être documentés.

Il existe deux types du management des risques :

- La gestion préventive des risques : consiste à identifier les risques potentiels avant qu'ils ne surviennent et à les atténuer en prenant des mesures pour éviter ou réduire leur impact. Par exemple, l`analyse AMDEC est utilisée lors du développement de nouveaux produits, de nouveaux processus ou pour répondre à de nouvelles réglementations, ainsi que pour évaluer les fournisseurs ou analyser les tendances
- La gestion réactive des risques consiste à réagir aux risques après leur apparition et à prendre des mesures pour limiter les dommages et assurer la continuité des activités. Cela comprend l’élaboration de plans de gestion de crise et de continuité des activités pour répondre efficacement aux incidents.

Figure 2: *Processus général de management des risques*



Sources : (ISO/IEC 27005)

Cette figure décrit les étapes clés de la gestion des risques dans une organisation. Elle commence par l'établissement du contexte, suivi de l'identification, l'analyse et l'évaluation des risques. Ensuite, les risques sont traités. Le processus comprend des points de décision pour évaluer et accepter les risques, et intègre la communication, la surveillance, et la documentation, formant ainsi un cycle itératif.

1.2.5. Les outils d'analyse des risques :

Il existe différentes méthodes d'évaluation des risques, adaptées à différents secteurs d'activité et types de risque, parmi les méthodes les plus couramment utilisés on trouve :

a) Le modèle ROAM (Resolved, Owned, Accepted, Mitigated)

Le modèle ROAM est un outil que les équipes de projet utilisent pour classer les risques identifiés. Les risques sont classés en quatre groupes distincts :

- "Resolved " : les risques qui peuvent être éliminés ou évités par des actions particulières.
- " owned " : Les risques qui doivent être gérés par les membres de l'équipe qui en ont accepté la responsabilité. Ils sont chargés de mettre en œuvre les mesures nécessaires et de s'assurer qu'elles fonctionnent correctement.
- "Accepted" : Les risques qui ont été acceptés et les conséquences potentielles. En général, il s'agit de risques minimes ou d'un impact limité.
- "Mitigated" : Les risques des actions qui ont déjà été prises pour réduire les chances et les effets.

Les risques sont classés en fonction de leur probabilité de se produire et de leur impact sur le projet. Cette classification est visualisée à l'aide d'un tableau ROAM, qui permet à l'équipe de suivre l'évolution de la gestion des risques.[4]

b) L'analyse par arbre de défaillances (FTA)

Selon la norme CEI 61025, l'analyse par arbre de défaillances est une méthode qui commence par considérer les défaillances dans la fonctionnalité d'un produit ou d'un processus. Puis évaluer systématiquement les échecs en recherchant les causes potentielles individuellement et en identifiant les chaînes causales possibles.

Les résultats sont affichés graphiquement sous forme d'arbre de défaillances à l'aide d'opérateurs logiques pour décrire les combinaisons de modes de défaillance à chaque niveau de l'arbre.

Cette approche nécessite l'expertise d'experts pour identifier les causes possibles d'erreurs.

Les arbres de défaillances aident à identifier la cause première des pannes, à enquêter sur les plaintes et les écarts, à évaluer la manière dont plusieurs facteurs influencent un problème particulier, à développer des programmes de surveillance et à évaluer les risques.

[4] https://www.nutcache.com/fr/blog/modele-roam-gestion-des-risques/

Le résultat est une représentation visuelle des modes de défaillance et une communication efficace des résultats d'analyse à toutes les parties impliquées.

c) La méthode de classification et de filtrage des risques

La méthode de classification et de filtrage des risques est une approche permettant d'évaluer et de hiérarchiser les risques au sein d'un projet, d'un processus ou d'une organisation. Cette méthode consiste à classer les risques selon leur probabilité d'occurrence et leur impact sur les objectifs du projet ou de l'organisation.

Le processus de classification et de filtrage des risques se déroule généralement en plusieurs étapes.

- Identification des risques : Cette étape identifie tous les risques potentiels auxquels le projet ou l'organisation peut être exposé.
- Classification des risques : Une fois les risques identifiés, ils sont classés selon leur nature (risque financier, risque opérationnel, risque stratégique, etc.) et leur impact potentiel sur les objectifs du projet ou de l'organisation du projet.
- Évaluation des risques : Chaque risque est évalué en fonction de sa probabilité d'occurrence et de son impact sur les objectifs. La probabilité peut être divisée en plusieurs niveaux (faible, moyen, élevé) et l'impact peut également être évalué sur une échelle (faible, moyen, élevé).
- Filtrage des risques : Une fois les risques évalués, ils sont filtrés en fonction de leur importance relative. Généralement, les risques les plus importants sont sélectionnés pour une analyse plus approfondie.
- Priorisation des risques : Les risques sélectionnés sont priorisés en fonction de leur importance relative. Cela permet de se concentrer sur les risques les plus importants et de définir les mesures d'atténuation appropriées pour y faire face.

2. L'ANALYSE DES MODES DE DEFAILLENCE, DE LEURS EFFETS ET DE LEURS CRITICITES (AMDEC)

Dans le cadre de notre recherche, nous avons décidé de nous concentrer sur l'analyse des modes de défaillance, de leurs effets et de leur gravité (AMDEC) pour contrôler les risques associés à la sécurité des plateformes numériques. Dans cette partie, nous allons expliquer en détail le concept de l'AMDEC.

2.1. Définition de l'AMDEC :

L'analyse des modes de défaillance, de leurs effets et de leur gravité (AMDEC) est un outil d'analyse inductive qui étudie de manière approfondie les causes potentielles d'erreurs dans un système.

L’association de normalisation AFNOR définit l’AMDEC en étant *« une méthode inductive qui permet de réaliser une analyse qualitative et quantitative de la fiabilité ou de la sécurité d’un système* ».

Cette méthode consiste à étudier systématiquement les pannes potentielles du système, leurs causes et leurs effets sur le fonctionnement global.

Après avoir hiérarchisé les défaillances potentielles sur la base d'une évaluation du degré de risque de défaillance, soit l’importance des mesures prioritaires, les mesures sont initiées et suivies.

L'objectif principal de l'AMDEC est d'identifier les points critiques d'un système, d'un processus ou d'un produit afin que des mesures préventives puissent être prises avant que des pannes ne surviennent.

2.2. L’historique de l’AMDEC

La méthode AMDEC a été développée par la société McDonnell Douglas aux États-Unis en 1966.

Le principe initial était de dresser une liste des composants du produit et de collecter des informations sur les types de pannes possibles, leur fréquence et leurs conséquences.

Cette méthode, appelée FMEA (Failure Modes and Effects Analysis), a été affinée en collaboration avec la NASA et l'industrie de défense pour évaluer l'efficacité du système.

Dans les années 1970, l’industrie automobile, notamment des sociétés telles que Toyota, Nissan, Ford, BMW, Peugeot et Volvo, a largement adopté cette méthode pour améliorer la fiabilité des produits. L’AMDEC s’est depuis étendue à d’autres industries telles que la mécanique, l’électronique, la chimie, l’aérospatiale, le nucléaire et, plus récemment, à l’industrie pharmaceutique et aux secteurs des services.

Cette méthode a permis aux entreprises d'identifier les pannes potentielles et de prendre des mesures préventives pour éviter de futurs problèmes. Cela a également contribué à améliorer la qualité, la sécurité et la fiabilité des produits et services tout en réduisant les coûts associés aux pannes et aux rappels de produits. (Joseph, 1998)

2.3. Les différents types d’AMDEC

Il existe plusieurs types d'AMDEC, dont les plus significatifs sont les suivants (Joseph, 1998) :

a) L’AMDEC produit ou FMEA projet : est une méthode spéciale pour une analyse approfondie de la phase de conception d’un produit ou d’un projet. Lorsqu'un produit est constitué de plusieurs éléments ou composants, appliquez le composant FMEA pour examiner les risques associés à chaque composant individuellement.

L’objectif principal d’une AMDEC produit est d’évaluer et de comprendre l’impact des défauts potentiels du produit sur l’utilisation finale. Cette analyse détaillée permet d'identifier les vulnérabilités du produit en fonction de la conception du produit, nous permettant ainsi de mettre en œuvre des actions correctives et des mesures préventives pour garantir la qualité, la sécurité et la fiabilité tout au long du cycle de vie.

b) L’AMDEC de sécurité : a pour objectif de réduire les risques liés à l’utilisation des moyens de production. Par exemple, il peut être utilisé pour évaluer les risques chimiques associés à l’exposition aux matières premières à différentes étapes d’un processus. Son objectif est d'identifier les dangers potentiels, d'évaluer leur probabilité d'occurrence et leur gravité, et de prendre des mesures préventives pour éviter les accidents et assurer la sécurité des salariés et de l'environnement.

c) L’AMDEC organisation : est une méthodologie appliquée à différents niveaux des processus métiers. Il peut être utilisé pour évaluer et améliorer la gestion, l’information, la production, les ressources humaines, le marketing, la finance et même l’organisation des tâches de travail. Son objectif est d'identifier les points critiques pouvant affecter le bon fonctionnement de l'organisation, d'évaluer les risques associés à ces points critiques et de prendre des mesures préventives pour les gérer.

d) L'AMDEC du service : est une méthode permettant de confirmer si la valeur ajoutée réalisée par le service répond aux attentes du client. Cela garantit également que le processus de prestation de services est sans erreur. L’objectif est d’identifier les points critiques dans le processus de service, d’évaluer les risques associés à ces points critiques et de prendre des mesures préventives pour les gérer.

e) L’AMDEC Processus : est une technique qui peut être appliquée aux processus de fabrication. Ceci est utilisé pour analyser et évaluer la gravité de tous les défauts potentiels du produit pouvant être causés par le processus de fabrication. Cette méthode s'applique également aux postes de travail. Son objectif est d'identifier les erreurs potentielles dans le processus de fabrication, d'évaluer leur gravité et leur probabilité d'apparition et de prendre des mesures préventives pour les éviter.

f) L'AMDEC moyen : est une méthode visant à identifier les déficiences des moyens de production qui affectent directement la productivité d'une entreprise. Cette méthode consiste donc à analyser les pannes potentielles des équipements et à optimiser les opérations de maintenance. Son objectif est de prédire les pannes des

équipements de production, d'évaluer leur gravité et leur probabilité d'apparition et de prendre des mesures préventives pour éviter les pannes.

2.4. Les aspects de la méthode AMDEC

Les techniques AMDEC (analyse des modes de défaillance, de leurs effets et de leur gravité) utilisent des approches à la fois qualitatives et quantitatives.

a) Aspects qualitatifs : Cette partie de l'investigation consiste à répertorier les erreurs potentielles, à identifier les causes de ces erreurs et à évaluer l'impact sur les clients, les utilisateurs et l'environnement interne ou externe. Cela vous aide à comprendre les risques et les conséquences d'un échec.

b) Aspect quantitatif : L'aspect quantitatif de l'AMDEC vise à estimer le risque associé à chaque erreur potentielle. Cela inclut la priorisation des types d'erreurs en fonction de critères tels que l'impact sur le client. Cette évaluation quantitative permet de prioriser les mesures d'atténuation des risques.

2.5. La démarche de l'AMDEC :

Le processus AMDEC comprend huit étapes. L'étape préparatoire consiste à collecter les données nécessaires à l'étude, à former un groupe de travail et à préparer les documents, tableaux et logiciels nécessaires.

- Étape 01 : constitution d'un groupe de travail

Pour une analyse AMDEC réussie, il est essentiel de constituer une équipe diversifiée et compétente composée de membres familiers avec les processus étudiés et de représentants de différents départements qui fournissent une vue d'ensemble.

L'équipe doit être multidisciplinaire et dirigée par un animateur formé aux techniques AMDEC.

Pour garantir une analyse réussie, il est important de définir clairement la portée de l'étude et d'assurer la participation de tous les membres.

- Étape 02 : l'analyse fonctionnelle

Cette étape nécessite une compréhension détaillée de toutes les caractéristiques d'un produit ou d'un processus afin d'identifier d'éventuelles erreurs. Des outils tels que des diagrammes fonctionnels, des arborescences de fonctionnalités et des matrices d'exigences sont souvent utilisés pour visualiser les relations entre les fonctionnalités et identifier les fonctionnalités importantes.

L'objectif est de déterminer avec précision le comportement attendu d'un produit ou d'un processus afin d'identifier plus facilement les problèmes potentiels.

- Étape 03 : l’étude qualitative des défaillances

Cette étape identifie tous les défauts possibles, détermine leur nature et leur impact et analyse les causes potentielles et les plus probables. Cette analyse s'appuie sur une analyse fonctionnelle pour prédire les causes et comprendre l'impact de chaque panne.

Le but de cette étape est de considérer tous les scénarios de défaillance, d'évaluer leurs conséquences et d'identifier les causes critiques pour guider les actions correctives.

- Étape 04 : l’étude quantitative

Cette étape s'appuie sur une analyse quantitative basée sur des critères tels que l'apparition de modes de défaillance, leur détectabilité et l'impact sur les clients ou utilisateurs.

Ces critères peuvent être ajustés en fonction du problème.

Une méthode courante d'évaluation des risques consiste à définir un tableau contenant des plages d'indices pour chaque critère et à attribuer des scores aux groupes en fonction de l'expérience antérieure et d'une recherche de consensus.

L'indice de criticité (RPN) est calculé en multipliant les scores obtenus pour l'occurrence, la détectabilité et la gravité de chaque mode de défaillance.

$C = G \times O \times D$

Les modes de défaillance qui présentent un risque élevé, se produisent fréquemment, sont difficiles à détecter et ont des conséquences graves reçoivent des notes plus élevées.

- Étape 05 : La hiérarchisation

Lorsque l’on tente de prédire les problèmes et de trouver des solutions proactives, la principale difficulté réside dans la diversité des problèmes potentiels à prendre en compte. Pour cette raison, il est important de hiérarchiser les erreurs et de classer les types d’erreurs par ordre d’importance. En établissant des priorités sur la base de cette échelle d’importance, il est possible de prioriser les mesures à prendre.

Les types de défauts sont généralement classés en quatre catégories ($C>100$, $100>C>50$, $50>C>20$, $20>C$) en fonction de leur gravité et des mesures préventives à prendre en priorité.

En règle générale, les entreprises fixent le seuil de gravité à 100 pour les produits/processus FMEA et à 16 pour les supports FMEA.

- Étape 06 : la recherche des actions préventives/correctives

Après avoir classé les types de pannes selon leur gravité, le groupe désigne une personne chargée de trouver des mesures préventives ou correctives.

Pour ce faire, il faut utiliser des outils tels que des diagrammes en arête de poisson, l'analyse de Pareto, le brainstorming et le travail d'équipe.

L'objectif est de réduire l'indice d'importance en agissant sur :

- ✓ Probabilité d'occurrence due à des changements dans la conception du produit ou du processus.
- ✓ Probabilité de non-détection en raison de changements dans la conception du processus ou dans le système de contrôle.
- ✓ Gravité de l'impact des erreurs causées par les modifications de conception.

- Étape 07 : Le suivi des actions prises et la réévaluation de criticité

Lorsqu'une action préventive ou corrective est entreprise, un nouvel indice de gravité est calculé de la même manière que l'évaluation initiale. Ce nouvel indicateur, appelé « risque résiduel », permettra d'évaluer l'impact et l'efficacité des mesures prises.

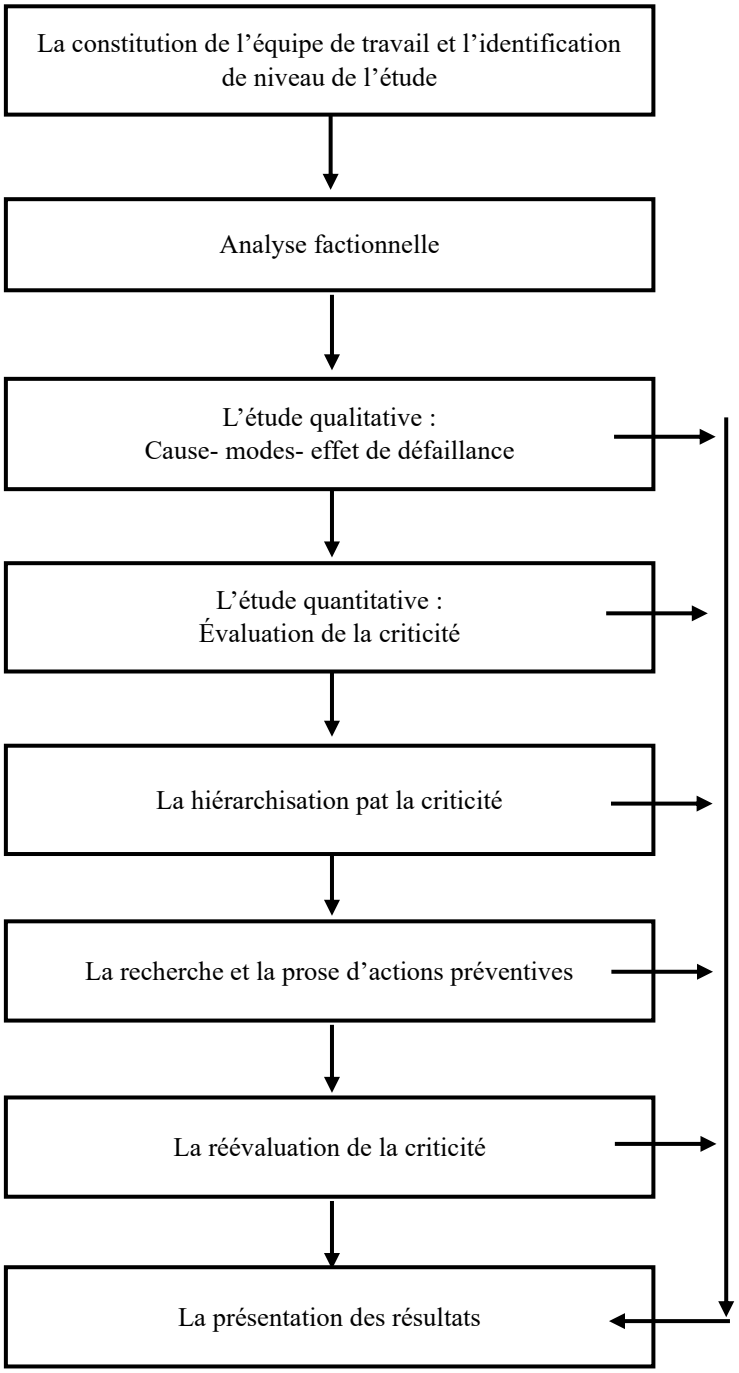
L'objectif est que ce nouvel indicateur tombe en dessous d'un seuil critique établi, ce qui signifie que les mesures ont réduit le risque à un niveau acceptable.

- Étape 08 : la présentation des résultats

Pour faciliter la mise en œuvre de l'AMDEC, les entreprises utilisent des tableaux développés spécifiquement pour le système étudié. Ces tableaux, disposés en colonnes, contiennent les informations dont vous avez besoin pour mener votre recherche.

Les tableaux 1 à 4 montrent comment exécuter le processus FMEA.

Figure 3: *La démarche de l'AMDEC*



Source : Source (Joseph, 1998)

Cette figure décrit le processus de l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. Elle commence par la constitution de l'équipe de travail et l'identification du niveau de l'étude, suivie de l'analyse fonctionnelle. Ensuite, l'étude qualitative identifie les causes, modes et effets de défaillance, tandis que l'étude quantitative évalue la criticité de ces défaillances. La hiérarchisation par criticité permet de classer les défaillances selon leur importance, ce qui conduit à la recherche et à la mise en œuvre d'actions préventives.

La criticité est ensuite réévaluée pour mesurer l'efficacité des actions, et les résultats sont présentés pour communiquer les conclusions de l'étude.

3. La transformation digitale et plateformes digitales

La digitalisation, la révolution du XXI -ème siècle, change notre façon de vivre, de travailler et d'interagir. Elle implique l'utilisation des technologies numériques pour créer, adapter ou améliorer les processus et produits ou l'ensemble du secteur du service. La digitalisation est un phénomène omniprésent car elle change tous les secteurs de l'économie et de la société. Il affecte profondément les modèles commerciaux, les relations clientèles et les formes de communication.

Même si la digitalisation comporte beaucoup de bons côtés, elle pose également des défis, tels que la sécurité, la protection des données ou l'inclusion numérique.

3.1. La transformation digitale :

La digitalisation est un concept relativement récent qui comprend des notions telles que la numérisation et l'informatisable. La digitalisation est basée sur quatre dimensions principales :

L'envergure des changements, l'échelle des transaction informationnelles, la vitesse des flux informatifs et les sources du changement. Par exemple, l'envergure des changements met en question les acteurs historiques dans le commerce du détail. À mesure que le commerce multicanal est en vogue et ses habitudes de consommation évoluent, les acteurs dans la distribution doivent revoir leur modèle d'affaires, leur logistique et, en fait, leur organisation entière.

L'échelle des transactions d'informations sera multipliée par dix et l'interface entre les entreprises et leurs environnements augmentera. Les entreprises doivent répondre aux demandes via les réseaux sociaux et les clients deviennent des influenceurs. Le rythme du changement est également si rapide que les grandes entreprises ne peuvent plus compter sur un avantage concurrentiel. Le cycle du NPD a été raccourci par des discours et a eu un impact énorme sur les médias, la bourse et le commerce.

Les sources du changement sont diverses et la concurrence peut désormais se cacher n'importe où. La numérisation modifie les frontières des entreprises, déstabilisant les ordres établis, les relations avec les parties prenantes et la rapidité avec laquelle les entreprises doivent répondre aux demandes du marché.

3.2. L'historique de la digitalisation :

Ces dernières années, la numérisation a considérablement modifié le comportement des consommateurs. Les nouveaux outils numériques facilitent la vie des consommateurs, leur font gagner du temps et leur offrent une variété de services (Belvaux & Notebaert, 2015)

Avant d'aborder plus en détail la numérisation, il est important de clarifier le terme « numérique ».

Dans leur étude sur la digitalisation de la relation client, Belvaux et Notebaert définissent le digital comme : Au début du triomphe des ordinateurs et d'Internet, le terme « numérique » était préféré à « numérique ». À cette époque, les produits utilisant les nouvelles technologies étaient appelés « numériques ». Ces deux termes sont désormais considérés comme presque synonymes, et le terme « numérique » remplace souvent le terme « numérique » dans le langage marketing. Ceux-ci font référence à toutes les informations codées sous les nombres. (Belvaux & Notebaert, 2015)

Les médias numériques ont changé la façon dont les consommateurs accèdent aux sites Web à tout moment, n'importe où et sur n'importe quel appareil (Bressolles, 2016)

Selon Marc Van Huel, professeur de marketing à HEC Paris, les technologies numériques offrent de nouvelles opportunités de création de valeur, notamment via la vente directe et les intermédiaires. Cela vous permet également de créer un programme de fidélité plus personnalisé.

Du côté des consommateurs, donner une voix publique dans l'espace de consommation peut être source de responsabilisation. Dans l'ensemble, ces changements ont modifié de manière significative de nombreux aspects. (Flores, 2016)

En seulement 10 ans, la popularisation d'Internet a entraîné la digitalisation de l'économie et une véritable révolution pour les entreprises. Cette révolution se caractérise par deux éléments principaux. Tout d'abord, la vitesse : Internet se répand rapidement dans le monde et les smartphones sont devenus le principal moyen d'accès à Internet. Deuxièmement, cela a un impact universel sur le parcours client.

Le numérique impacte non seulement la communication d'entreprise, mais également le marketing, les ventes, la distribution, la gestion de la relation client (CRM) et le service (Sheid, Vaillant, & De Montaigu, 2012)

Aucun secteur de l'économie n'est à l'abri des effets de cette transformation numérique.

3.3. La digitalisation en Algérie :

Ces dernières années, le gouvernement algérien a mis en œuvre un plan ambitieux de numérisation des services publics. Ce changement est déjà visible dans plusieurs régions clés du pays.

Le président Abdelmadjid Tebboune a souligné cet engagement en faveur de la numérisation dans un discours au Parlement en décembre dernier. Le Président a annoncé

que le projet de numérisation du gouvernement devrait être achevé d'ici la fin du premier semestre 2024.

Il a également évoqué d'autres projets importants en cours et souligné l'importance de la numérisation pour l'avenir de l'Algérie.

En 2023, sous la direction du président Tebboune, plusieurs domaines clés ont été modernisés, notamment la justice, la fiscalité, les douanes, la santé et l'identité numérique. Par exemple, le ministère de l'Enseignement supérieur et de la Recherche scientifique a mis en place plus de 46 plateformes numériques pour la formation et la recherche.

Pour coordonner ces efforts, le Haut-commissariat à la numérisation a été créé en septembre et présidé par Mme Meriem Benmorou. Cette agence sera chargée de concevoir la stratégie nationale de numérisation ainsi que de son suivi et de sa mise en œuvre.

En outre, une loi sur la numérisation visant à renforcer la stratégie nationale de numérisation devrait être adoptée au premier trimestre 2024.

Ces mesures démontrent l'engagement de l'Algérie à moderniser les services publics et à promouvoir le développement numérique dans le pays[5].

3.4. Plateformes digitales :

Les plates-formes numériques sont des services qui servent d'intermédiaires pour l'accès à des contenus, informations, services et produits provenant de divers tiers.

Contrairement aux sites Web traditionnels, les plates-formes numériques organisent activement le contenu pour les utilisateurs finaux. Les utilisateurs sont encouragés à interagir et à participer, créant ainsi un écosystème décentralisé dynamique. Ceux-ci fournissent une variété de services supplémentaires et peuvent avoir un impact significatif sur l'activité économique du secteur dans son ensemble. Il favorise les relations entre les différentes parties et contribue à la formation de réseaux de collaboration.

En résumé, les plates-formes numériques deviennent plus que de simples sites Web en permettant la communication entre les parties et en offrant une variété de services supplémentaires.

3.4.1. Évolution et Impact des Plates-formes Numériques dans l'Économie et la Société

Les plates-formes numériques sont apparues dès les débuts d'Internet, mais leur importance a considérablement augmenté au début des années 2000 avec l'émergence de la théorie du « Marché biface ». Cette théorie explique comment les plates-formes peuvent

[5] https://www.aps.dz/sante-science-technologie/149551-2022-annee-de-l-acceleration-de-la-numerisation-en-algerie

faciliter l'interaction entre différents groupes d'utilisateurs, tels que les acheteurs et les vendeurs, en créant un marché où l'offre et la demande correspondent efficacement.

Au fil du temps, les plates-formes numériques deviennent des acteurs importants de l'économie numérique, offrant aux utilisateurs une variété de services et facilitant les interactions dans différents domaines d'activité. Ils ont changé notre vie quotidienne, impactant notre façon de communiquer, de consommer du contenu, d'acheter en ligne, de traiter les paiements, etc.

Les plates-formes numériques ont contribué à réduire les coûts de transaction en simplifiant le processus d'échange et en éliminant les intermédiaires inutiles. Il a également amélioré l'efficacité en permettant des interactions plus rapides en temps réel entre les utilisateurs. En outre, il a favorisé l'innovation en créant de nouveaux modèles économiques et en favorisant la concurrence.

Aujourd'hui, les plates-formes numériques sont omniprésentes dans notre société et jouent un rôle important dans leur adoption massive et dans la facilitation de l'accès aux services et à l'information. Ils sont devenus des acteurs économiques importants dans tous les domaines d'activité, modifiant fondamentalement notre façon de consommer et d'interagir.

3.4.2. Les catégories principales de plates-formes bifaces ou multifaces.

Selon Evans & Schmalensee (Evans & Schmalensee, 2008) il existe 4 catégories principales des plateformes.

- Les plates-formes d'échange en ligne : elles facilitent les échanges de biens ou de services entre particuliers ou entreprises. Par exemple commander un trajet en voiture comme Uber ou commander des produits sur une place de marché. Ces plates-formes simplifient la recherche, la comparaison et l'achat, rendant le trading plus accessible et plus pratique.
- Les plates-formes médiatiques publicitaires, telles Instagram Ads, TikTok Ads, et LinkedIn Ads permettent aux entreprises de diffuser des publicités auprès de leur public cible de manière ciblée et efficace. Par exemple, Les marques de vêtements de sport peuvent utiliser les publicités Instagram pour cibler les utilisateurs intéressés par le fitness et les activités sportives et promouvoir de nouveaux produits de manière à attirer ce public.
- Une plate-forme logicielle fournit aux développeurs et aux utilisateurs des outils et des fonctionnalités qui facilitent le développement et l'utilisation de logiciels. Par exemple, la plate-forme GitHub fournit aux développeurs des outils de contrôle de

version et de collaboration pour les projets de développement de logiciels. De même, la plate-forme Salesforce fournit aux entreprises des outils de gestion de la relation client (CRM) pour gérer efficacement les interactions clients. Ces plates-formes offrent des fonctionnalités importantes pour simplifier et améliorer le processus de développement et d'utilisation de logiciels.

- Une plate-forme de gestion des transactions est un système qui aide les entreprises à traiter les transactions financières et à gérer les transactions de paiement. Par exemple, PayPal est une plate-forme de paiement en ligne largement utilisée par les entreprises et les particuliers pour effectuer des transactions financières en ligne de manière sécurisée.

De même, Square est une autre plate-forme de gestion de transactions qui propose des services de paiement aux petites et moyennes entreprises, notamment des paiements par carte de crédit et des solutions de traitement des paiements mobiles. Ces plates-formes permettent aux entreprises de gérer efficacement les transactions financières et de simplifier le processus de paiement pour leurs clients.

4. Le Management des Risques Cybernétiques :

4.1. La sécurité informatique

La sécurité informatique représente l'ensemble des pratiques, techniques, solutions et ressources déployées dans le but de protéger les systèmes et données numériques d'une entreprise contre les cybermenaces, attaques et risques divers. Son objectif principal est d'assurer la confidentialité, l'intégrité et la disponibilité des informations sensibles. Parmi les outils de sécurité informatique, on retrouve notamment les antivirus, pare-feu, chiffrement des données, contrôles d'accès, mots de passe robustes, etc. Le renforcement des mesures de cybersécurité est essentiel pour prévenir les pertes financières, préserver la réputation de l'entreprise et éviter les sanctions légales ou réglementaires en cas d'incident majeur.

4.1.1. Les objectifs de la sécurité informatique :

La sécurité des données couvre quatre objectifs principaux, et est représentée sous forme d'acronymes (C.I.D.P) :

- **Confidentialité :** vise à empêcher la divulgation d'informations sensibles des personnes non autorisées, au moyen de techniques comme le chiffrement et les contrôles d'accès.
- **Intégrité :** elle garantit que les données n'ont pas été modifiées ou corrompues de manière inappropriée, grâce à des contrôles d'intégrité détectant les changements non autorisés.

- **Disponibilité :** elle assure que les données et systèmes sont accessibles aux utilisateurs légitimes quand ils en ont besoin, impliquant des mesures de tolérance aux pannes, sauvegarde et redondance.
- **Preuve et la non répudiation :** fournissent la capacité de prouver l'origine des données et empêchent quelqu'un de nier avoir envoyé ou reçu des informations, par exemple via les signatures numériques.

4.1.2. Types de sécurité informatique :

- **La cybersécurité :** a pour objectif de sécuriser les infrastructures et actifs informatiques connectées au réseau internet. Elle met en place des mesures de protection contre les cybermenaces et attaques extérieures visant les systèmes de réseaux, les équipements informatiques (serveurs, ordinateurs, etc.) ainsi que les données numériques transitant ou stockées sur ces environnements en ligne.
- **La sécurité des terminaux ou "Endpoint" :** consiste à mettre en place des mesures de protection sur les appareils informatiques tels que les ordinateurs de bureau, portables, smartphones et tablettes afin de les prémunir contre les logiciels malveillants, accès non autorisés et autres attaques informatiques. Ces terminaux connectés au réseau de l'entreprise représentent des vecteurs d'attaque potentiels s'ils ne sont pas correctement sécurisés.
- **La sécurité du cloud :** elle vise à assurer la protection de l'environnement informatique infonuagique et des ressources qui y sont déployées contre les diverses cybermenaces. Cela englobe la sécurisation de l'infrastructure cloud sous-jacente (serveurs, réseaux, stockage, etc.) ainsi que la mise en défense des services cloud, applications et données sensibles hébergés dans le cloud. Des contrôles et outils de sécurité spécifiques au cloud permettent de détecter et contrer les attaques, fuites de données, accès non autorisés et autres risques pouvant impacter la confidentialité, l'intégrité et la disponibilité des environnements cloud.
- **La sécurité des applications :** consiste à mettre en œuvre des mesures pour réduire les vulnérabilités dans les logiciels et applications, afin de prévenir le vol, la fuite ou l'altération non autorisée des données et du code source. Cela passe par des pratiques de développement sécurisé, les tests de sécurité, le contrôle d'accès et le chiffrement tout au long du cycle de vie applicatif.
- **La sécurité des conteneurs :** consiste à protéger de manière continue les conteneurs applicatifs, leur cycle de vie complet (construction, déploiement,

approvisionnement), leur infrastructure d'orchestration et leur chaîne d'approvisionnement contre les différentes cybermenaces pouvant les compromettre.

- **La sécurité IoT :** se concentre sur la protection, la surveillance et l'atténuation des menaces visant les réseaux d'objets connectés à Internet qui collectent, stockent et partagent des données. Elle vise à sécuriser l'ensemble de l'écosystème IoT, des appareils aux plateformes cloud de gestion, contre les accès non autorisés, les failles de sécurité et les cyberattaques.

4.2. Les risques associés à la sécurité informatique

Les menaces pour la sécurité informatique peuvent être classées en deux grandes catégories : les perturbations ou nuisances système d'une part, et les cyberattaques ciblées d'autre part. Les perturbations système englobent les incidents temporaires causés par des défaillances matérielles, des pannes réseau ou des bogues logiciels, entraînant des interruptions d'activité et potentiellement des pertes financières ainsi que des dommages d'image pour l'entreprise. Cependant, la protection contre les cyberattaques représente un enjeu encore plus critique. La majorité de ces attaques malveillantes visent spécifiquement à accéder de manière illicite aux données confidentielles d'une organisation ou à les dérober. Parmi les cybermenaces les plus répandues, on peut citer :

- **Menaces persistantes avancées (APT) :** les APT sont des cyberattaques sophistiquées et insidieuses où un attaquant parvient à s'infiltrer et rester caché durablement au sein des systèmes d'une cible spécifique. Soigneusement préparées, elles exploitent les failles pour contourner la sécurité et dérober furtivement des données sensibles sur le long terme, sans éveiller les soupçons. Leur grande discrétion et persistance les rendent très difficiles à détecter et contrer.
- **Les logiciels malveillants ou "malwares" :** sont des programmes conçus dans un but malicieux, représentant une menace majeure en cybersécurité. Les principaux types incluent les virus, ransomwares, enregistreurs de frappe, chevaux de Troie, vers et spywares. Ils exploitent les failles pour s'introduire dans les systèmes, corrompre les données, voler des informations ou prendre le contrôle des équipements infectés.[6]
- **Phishing** : Le phishing, également connu sous le nom d`hameçonnage, est une technique de cybercriminalité qui consiste à envoyer des courriels frauduleux pour inciter les gens à divulguer des informations personnelles ou financières.

[6] https://www.crowdstrike.fr/cybersecurity-101/malware/types-of-malware/

- **Attaque de déni de service (DDoS) :** est une attaque qui utilise de fausses requêtes pour perturber le réseau. Cela empêche les utilisateurs autorisés d'utiliser des services courants tels que l'accès à des sites Web et à des comptes en ligne. Les attaques DDoS (Distributed Denial of Service) sont similaires, mais elles utilisent plusieurs ordinateurs infectés pour lancer l'attaque, ce qui les rend plus difficiles à éliminer[7].

4.2.1. Les bonnes pratiques en matière de sécurité informatique :

La sécurité informatique est bien plus qu'un simple problème informatique et sa solution ne repose pas uniquement sur des solutions techniques. Les organisations doivent prendre en compte les politiques, procédures et technologies utilisées dans toutes les fonctions de l'organisation pour mettre en œuvre une stratégie de cybersécurité optimale**.**

Les méthodes de cybersécurité les plus efficaces intègrent des ressources humaines avancées avec des technologies alternatives telles que l'intelligence artificielle (IA), l'apprentissage automatique (ML) et d'autres formes d'automatisation intelligente pour détecter les activités anormales de cybersécurité et optimiser les temps de réponse et de remédiation. Ces stratégies doivent intégrer les éléments suivants :

- Appelé EDR (Endpoint Detection and Response) : Une activité malveillante sur les appareils finaux est détectée et analysée par cette solution. Cela permet à l'équipe de protection de se concentrer sur la résolution du problème.
- MDR (Managed Detection and Response) : le service de cybersécurité exploite à la fois la technologie et l'expertise humaine pour détecter les menaces, surveiller les systèmes et répondre aux incidents. Son principal avantage est la capacité de détecter précocement les cybermenaces et de limiter leur impact sans augmenter le nombre de personnes embauchées pour la sécurité.
- Réponse aux incidents : est un processus conçu pour prévenir, détecter et arrêter les violations de sécurité des données et récupérer les systèmes concernés. La manière la plus courante d'y parvenir consiste à développer une stratégie de réponse aux incidents qui décrit les étapes et les procédures à suivre en cas de problème de sécurité.
- Antivirus de nouvelle génération (NGAV) : exploite l'intelligence artificielle, la surveillance comportementale, les algorithmes d'apprentissage automatique et exploite l'atténuation pour prédire et prévenir toutes les menaces de sécurité connues et inconnues.

[7] https://www.crowdstrike.fr/cybersecurity-101/it-security/

- Tests d'intrusion : est une simulation d'attaque réelle conçue pour évaluer la capacité d'une organisation à détecter et à répondre aux cyberattaques.

Conclusion du chapitre :

Nous avons vu dans ce chapitre que le risque est un facteur inhérent à toute plateforme numérique en ligne. Les cybermenaces peuvent survenir à tout moment et impacter gravement leur fonctionnement et leur sécurité. C'est pourquoi une gestion rigoureuse des risques liés à la cybersécurité est primordiale.

La gestion des risques pour les plateformes en ligne est une activité coordonnée visant à identifier, évaluer et traiter les risques numériques de manière à assurer leur disponibilité, leur intégrité et la protection des données sensibles face aux changements constants des menaces.

En adoptant les bonnes pratiques et méthodologies telles que l'AMDEC, les responsables des plateformes en ligne renforcent leur posture de cybersécurité, assurent la continuité des services numériques et préservent la confiance des utilisateurs face à la recrudescence des cyberattaques.

CHAPITRE 2 :
METHODOLOGIE DE RECHERCHE ET CONTEXTE ORGANISATIONNEL

Nous avons structuré ce chapitre en deux parties distinctes. La première partie se concentre sur la présentation de l'organisme d'accueil, la deuxième partie sur la méthodologie de recherche et l'approche de collecte et traitement des données.

Section 1 : méthodologie de recherche

La méthodologie de recherche fait référence à la manière dont une étude est réalisée pour obtenir des résultats significatifs et fiables sur un sujet particulier. En abordant les techniques et procédures utilisées pour collecter, analyser et interpréter les données afin d'atteindre les objectifs de recherche.[8]

1.1. Posture épistémologique :

Le choix du positionnement épistémologique des chercheurs est important car il influence directement les stratégies qu'ils utilisent pour produire des connaissances scientifiques solides et valides. Grâce à un positionnement épistémologique, les chercheurs définissent des concepts sur la nature des connaissances et la réalité de ce qu'ils étudient, qui guident leur choix de méthodologie, leur approche de collecte et d'analyse des données et l'interprétation des résultats.

Depuis son introduction en français en 1907, le terme "épistémologie" est devenu couramment utilisé. A. Lalande (1962) souligne que *: « Le mot anglais epistemology est très fréquemment employé pour désigner ce que nous appelons en français « théorie de la connaissance » ou « gnoséologie »*, il tient à préciser aussi qu'on *« doit distinguer l'épistémologie de la théorie de la connaissance, bien qu'elle en soit l'introduction et l'auxiliaire indispensable, en ce qu'elle étudie la connaissance en détail et à posteriori, dans la diversité des sciences et des objets plutôt que dans l'unité de l'esprit. ».*

Ainsi, Jean Piaget (1957) donne une définition large de l'épistémologie, l'envisageant comme : *« L'étude de la constitution des connaissances valables »*

L'épistémologie pose trois questions fondamentales **:** *« Qu'est-ce que la connaissance ? (La question gnoséologique), Comment est-elle constituée ou engendrée ? (La question méthodologique) Comment apprécier sa valeur ou sa validité ? (La question éthique)».* (Jean-Louis, 2007)

De ce fait, le dictionnaire philosophique l'épistémologie fait référence à l'étude de la science, son objectif est d'analyser, d'étudier et de critiquer tous les domaines scientifiques (mathématiques, chimie, biologie, physique, médecine, etc.), notamment en critiquant leurs

[8] https://www.voxco.com/fr/blog/methodologie-de-recherche/

méthodes et leurs découvertes, peut être pratiquée dans divers domaines, notamment la philosophie, l'histoire, la sociologie et même les sciences cognitives.[9]

L'épistémologie des sciences examine si ce que disent les scientifiques est vrai et comment leurs idées se comparent à la vie quotidienne des gens et aux idées de la philosophie.

Ben Aissa (2001) a expliqué dans son article que toute méthodologie de recherche commence par une curiosité de comprendre ou d'expliquer un phénomène, ou une volonté de résoudre un problème identifié. Selon lui, trois facteurs influencent le choix méthodologie de recherche, sont : la vision philosophique du chercheur, les objectifs de la recherche et les aspects techniques de sa mise en œuvre.

Il existe trois principaux paradigmes épistémologiques sont : le positivisme, le constructivisme et l'interpretativisme. Ces derniers sont importants car ils représentent les traditions de recherche établies dans un domaine particulier, ils comprennent des théories, des approches, des modèles, des cadres, des résultats de recherche et des méthodes acceptés.

a) **Le positivisme :**

Le paradigme positiviste repose sur l'idée que les faits réels peuvent être observés de manière empirique et expliqués par une analyse logique. Il défend les principes du raisonnement déductif et de la vérification empirique des hypothèses afin de les accepter ou de les réfuter. Le positivisme nous permet d'expliquer et de prédire le comportement de phénomènes réels et de découvrir la vraie nature des choses principalement par des méthodes déductives.

b) Le constructivisme :

Dans ce paradigme, la réalité émerge des intentions, des valeurs, des expériences et des perceptions humaines, et non des lois naturelles par lesquelles la réalité est « construite ».

Le paradigme constructiviste affirme que le chercheur et le sujet de recherche sont interconnectés et que leur interaction produit des connaissances. Selon cette perspective, la réalité n'est pas absolue et dépend de l'expérience du chercheur. Cela signifie qu'il n'existe pas une réalité unique, mais plusieurs réalités construites par des individus ou des groupes et qui peuvent évoluer au fil du temps.

Ce paradigme repose sur l'idée que la connaissance est générée par les capacités cognitives humaines. En adoptant le constructivisme, nous cherchons à expliquer plutôt qu'à prédire les phénomènes.

---

[9] https://www.linternaute.fr/dictionnaire/fr/definition/epistemologie/

c) L’interpretativisme *:*

L'interprétivisme est ainsi appelé parce qu'il repose sur l'interprétation et la description subjectives d'une situation à partir des expériences et des représentations du chercheur, et il ne présuppose pas l'existence d'un « objectif » mais influence plutôt notre perception du monde.

Pour l’interprétativisme et le constructivisme, la connaissance ne consiste plus à représenter fidèlement la réalité extérieure, mais plutôt à trouver des manières d’agir qui correspondent à une compréhension du monde.

Plutôt que de tenter d'expliquer le comportement de manière objective, ce paradigme cherche à comprendre la signification du comportement, ses raisons et les expériences subjectives qui y sont associées, en tenant compte du contexte et de son évolution au fil du temps.

Tableau 3: *Positions épistémologiques des paradigmes positiviste, interprétativiste et constructivisme.*

	Le positivisme	L'interpretativisme	Le constructivisme
Quel est le statut de la connaissance ?	- Hypothèse réaliste. - Il existe une essence propre à l'objet de connaissance.	- Hypothèse relativiste. - L'essence de l'objet ne peut être atteinte.	- Hypothèse relativiste. - L'essence de l'objet ne peut être atteinte (constructivisme modéré) ou n'existe pas (constructivisme radical)
La nature de la « Réalité »	- Indépendance du sujet et de l'objet. - Hypothèse déterministe. - Le monde est fait de nécessités.	- Dépendance du sujet et de l'objet. - Hypothèse intentionnaliste. - Le monde est fait de possibilités.	- Dépendance du sujet et de l'objet. - Hypothèse intentionnaliste. - Le monde est fait de possibilités.
Comment la connaissance est-elle engendrée ?	- La découverte. - Recherche formulée en termes de « pour quelles cause… ».	- L'interprétation. - Recherche formulée en termes de « pour quelles motivations des acteurs… ».	- La construction. - Recherche formulée en termes de « pour quelles finalités… ».
Le chemin de la connaissance scientifique	- Statut privilégié de l'explication.	- Statut privilégié de la compréhension.	- Statut privilégié de la construction.
Quelle est la valeur de la connaissance ?	- Vérifiabilité.	- Idéographie.	- Adéquation.
Les critères de validité	- Conformabilité. - Réfutabilité.	- Empathie (révélatrice de l'expérience vécu par les acteurs).	- Enseignabilité.

Source : (Perret & Florence, 2014)

Notre étude adopte une perspective interprétativiste et une démarche inductive, reposant sur des observations empiriques plutôt que sur des cadres théoriques existants. Cette approche nous permet de saisir les subtilités et les dynamiques uniques de chaque contexte, en mettant l'accent sur les perceptions et les actions des personnes concernées.

Face à la rareté et à la fragmentation des recherches sur le management des risques en sécurité numérique, notre objectif est de participer à la littérature en explorant l'utilisation de l'AMDEC chez **DEVLOG**. En intégrant cette technique à notre enquête, nous espérons dévoiler les approches et les opinions des experts de **DEVLOG** en matière de risques, afin de renforcer la sécurité des plateformes numériques et d'enrichir la recherche académique avec une vision plus globale et contextuelle de management des risques.

1.2. Présentation de la méthodologie de recherche : une recherche qualitative basée sur la recherche action.

La recherche qualitative consiste à recueillir des données verbales permettant une démarche interprétative. (Aubin-Auger, et al., 2008)

La recherche qualitative est un type de méthode de recherche qui cherche à explorer, comprendre et expliquer les significations, les expériences et les perceptions d'individus ou de groupes dans un contexte spécifique.

Elle utilise diverses sources de données qualitatives telles que des observations, des analyses de documents, des entretiens, des images ou des vidéos, etc. (Kohn & Christiaens, 2014)

Pour Imbert (2010), la recherche qualitative au niveau épistémologique adopte une approche holistique, immédiate, directe et interprétative pour comprendre l'objet d'étude et pour explorer et comprendre la nature du phénomène étudié.

L'objectif de la recherche qualitative est de développer des concepts qui nous aident à comprendre les phénomènes sociaux dans des contextes naturels plutôt qu'expérimentaux. Elle met l'accent sur le sens, les expériences et les perspectives de tous les participants.

Dans notre étude, nous avons décidé d'utiliser la recherche-action comme méthode de recherche. Cette approche a été spécifiquement choisie pour contribuer à la maîtrise des risques pour les clients de **DEVLOG**, en particulier pour le projet **DERMACARE** car étant un projet de plateforme numérique dédiée aux produits cosmétiques bio et aux consultations dermatologiques en ligne, nécessite une attention particulière à la sécurité de ses plateformes numériques.

Pour ce faire, nous allons appliquer l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) afin d'identifier, d'évaluer et de prioriser les risques potentiels liés à la sécurité des plateformes numériques. En impliquant activement les parties prenantes.

La recherche-action repose sur l'idée que l'action et l'expérience créent des connaissances et que la valeur de ces connaissances réside dans leur efficacité pratique.

Cependant, il est important de noter que la recherche-action est encore relativement peu pratiquée et peut limiter la richesse et la variété des connaissances générées. Cette méthode est une approche où la théorie et la pratique interagissent et où les concepts théoriques sont continuellement affinés grâce à l'expérimentation pratique.

Contrairement à la recherche traditionnelle, dans la recherche-action, le chercheur participe activement à changer la réalité de ce qui est étudié. (Morvan, 2013)

La RA est une *« recherche dans laquelle les auteurs de recherches et les acteurs sociaux se trouvent réciproquement impliqués : les acteurs dans la recherche et les auteurs dans l'action »* (Desroche, 1982) cité par (Morin, 1985). Le terme acteur désigne ici ceux qui interviennent spécifiquement dans la situation, comme les travailleurs sociaux, mais aussi les bénéficiaires de services.

Selon Desroche, il existe trois niveaux de recherche-action qui définissent les actions du chercheur, la relation avec le sujet et les objectifs de la recherche : la recherche-action explicative, la recherche-action appliquée et la recherche-action participative.

Tableau 4: *Positionnement du chercheur et des acteurs à partir des travaux de Desroches.*

	Expliquée	**Appliquée**	**Impliquée**
Degré d'engagement des acteurs et chercheurs	La recherche est faite sur les acteurs et est définie par les chercheurs.	La recherche est faite pour les acteurs sur une proposition des chercheurs.	La recherche est définie et réalisée par les acteurs et les chercheurs.
Démarche méthodologique	Démarche hypothético-déductive.	Démarche hypothético-déductive. Un type d'application choisi par le chercheur.	Démarche inductive
Exemple de recueil de données	Observation	Observation participante	Participation observante
Résultat	Production de connaissances concernant les acteurs (recherche des causes et des effets d'une action).	Applications pour pourvoir à des politiques d'actions, d'éducation, de planification, d'aménagement, recommandations de pratiques efficientes (« bonnes pratiques »)	Transformation des pratiques, émancipation des acteurs, transformation de l'environnement (changement social/ sociétal)

Source : (Clavreull & Albuquerque, 2020)

Ce tableau présente trois approches de recherche en sciences sociales, selon le niveau d'implication des acteurs et des chercheurs, l'approche méthodologique, la collecte de données et les résultats :

- Les études expliquées sont réalisées sur des acteurs et définies par des chercheurs selon une approche hypothético-déductive, qui utilise les observations comme exemple de collecte de données pour mieux comprendre les acteurs.
- Les études appliquées sont réalisées pour les acteurs à partir des suggestions du chercheur, et sont également hypothético-déductive, mais utilisent l'observation participante pour collecter des données, en utilisant des applications au choix du chercheur, et générer des recommandations d'applications pratiques et de bonnes pratiques.
- Les études impliquées sont définies et réalisées conjointement par les acteurs et les chercheurs, suivant une approche inductive de collecte de données avec participation observationnelle, dans le but de transformer la pratique, de libérer les sujets et de provoquer un changement social.
- Nous avons choisi la recherche-action, qui combine la recherche empirique avec des mesures concrètes pour améliorer la performance des pratiques et du système. Notre démarche vise à améliorer notre compréhension des risques liés à la sécurité des plateformes numériques et à proposer des solutions concrètes pour les gérer. Nous apprécions une coopération étroite avec les parties prenantes concernées. Dans ce contexte, l'AMDEC joue un rôle central dans notre approche, nous permettant d'identifier, d'évaluer et de prioriser les risques et d'apporter des solutions pour assurer la sécurité des plateformes numériques.

1.3. Les méthodes et outils de collecte des données

Pour aborder de manière exhaustive les enjeux de sécurité des plateformes digitales, plusieurs méthodes de collecte de données ont été employées.

1.3.1. L'observation

Lors de la collecte de données d'observation, les chercheurs effectuent des observations directes limitées des processus et des comportements au sein d'une organisation. Cette méthode permet d'obtenir des données factuelles basées sur des observations, par opposition aux données verbales pouvant être sujettes à interprétation. (Thietart, R, & All, 2017)

L'observation peut être réalisée de manière participative, dans laquelle le chercheur s'intègre dans l'environnement observé, ou de manière non participante, dans laquelle il reste à l'extérieur.

a) La grille d'observation

La grille d'observation qu'on a développée a été conçue pour fournir une analyse détaillée des pratiques et des outils de sécurité utilisés par l'entreprise d'accueil, avec un focus sur la maitrise des risques associés à la sécurité des plateformes numériques. Les observations ont porté sur les procédures de sécurité mises en œuvre au sein de l'entreprise, l'utilisation des outils de sécurité informatique et la sensibilisation à la sécurité. (ANNEXE A)

1.3.2. Les entretiens :

« L'entretien de recherche est un procédé d'investigation scientifique, utilisant un processus de communication verbale, pour recueillir des informations, en relation avec le but fixé. » (BOUTIN, 2018)

Les entretiens de recherche sont une technique de collecte de données informationnelles. Cette méthode permet de collecter et d'analyser un certain nombre de facteurs : points de vue, attitudes, émotions et points de vue de la personne interrogée.
Il existe 3 types d'entretien sont les suivant :[10]

a) L'entretien directif :

La structure de l'entretien directif, aussi appelée entrevue normalisée, est rigoureuse, assurant ainsi des conditions d'interrogation équitables pour tous les participants. Cette méthode stricte simplifie la comparaison des résultats. Les interrogations sont fréquemment précises et fermées, offrant ainsi des réponses par "oui" ou "non" ou des choix multiples, ce qui rend également l'analyse statistique des réponses plus facile. Cette méthode présente des bénéfices tels que la préparation préalable des questions par l'intervieweur, ce qui rassure l'interviewé. Cependant, elle présente également des limites, telles que l'incapacité de l'intervieweur à approfondir un sujet ou à établir un lien de confiance lors d'une discussion.

b) L'entretien non directif (ouvert) :

Également appelé « entretien libre », se caractérise par l'absence de questions prédéfinies ou de structure définie. L'intervieweur propose un sujet général et n'intervient que pour

[10] https://www.scribbr.fr/methodologie/entretien-recherche/

relancer la conversation et inciter l'interviewer à approfondir. L'enquêteur a une attitude d'écoute, de compréhension et de neutralité.

L'avantage de cette méthode est qu'elle permet à l'enquêter de s'exprimer librement et de développer ses idées. Il offre la possibilité de découvrir de nouvelles hypothèses au cours du processus d'échange.

Cependant, cet entretien peut s'écarter de l'objectif initial car la personne interrogée peut donner des développements qui ne répondent pas à la question initiale. Par conséquent, l'enquêteur doit veiller à recentrer la discussion si nécessaire, ce qui peut entraîner un stress supplémentaire pour le chercheur.

c) **L'entretien semi-directif :**

Également appelés « entretiens qualitatifs » ou « entretiens approfondis », reposent sur des questions généralement ouvertes. Cela donne la possibilité de poser de nouvelles questions si la personne interrogée soulève des aspects inconnus.

Pour mener ce type d'entretien, l'intervieweur doit préparer les questions à l'avance, les classer par sujet, dans un ordre raisonnable, et être capable de poser de nouvelles questions au cours du processus d'entretien.

Toutefois, les chercheurs ne sont pas obligés de poser toutes les questions dans l'ordre prévu ou dans une formulation particulière. Au contraire, il s'agit de donner aux répondants la liberté de s'exprimer en utilisant leurs propres mots et en abordant les sujets dans l'ordre qui leur semble naturel. Les chercheurs ramènent simplement la discussion au but lorsqu'elle va trop loin et posent des questions de suivi aux moments appropriés et de manière naturelle. (Van Campenhoudt, Quivy, & Marquet, 2006)

Tableau 5: *les caractéristiques des trois types d'entretiens.*

Entretien directif	Entretien semi-directif	Entretien non directif
Discours non continu qui suit l'ordre des questions posées.	Discours par thèmes dont l'ordre peut être plus ou moins déterminé selon la réactivité de l'interviewé.	Discours continu.
Questions préparées à l'avance et posées dans un ordre bien précis.	Quelques points de repéré (passage obligés) pour l'interviewer.	Aucune question préparée à l'avance.
Information partielle et réduite.	Information de bonne qualité, orientée vers le but poursuivi.	Information de très bonne qualité, mais pas nécessairement pertinente.
Information recueille rapidement ou très rapidement.	Information recueille dans un laps de temps raisonnable.	Durée de recueil d'informations non prévisible.
Inférence assez faible.	Inférence modérée.	Inférence exclusivement fonction de mode de recueil.

Source : (J.-M & Roegiers, 1996)

Dans le cadre de notre étude visant à gérer les risques liés à la sécurité des plateformes numériques, nous avons choisi les entretiens semi-directifs pour deux raisons principales. Premièrement, il permet de collecter un large éventail d'informations sans être trop contraint en termes de spécifications détaillées des besoins décisionnels et des résultats attendus. De plus, l'utilisation d'un guide d'entretien vous aidera à maintenir la conversation sur la bonne voie et vous assurera de répondre à toutes les questions importantes.

a) Guide d'entretien

Comme mentionné au paravent, nous allons aborder un guide d'entretien qui vise à approfondir notre recherche, structuré de manière à recueillir des informations pertinentes. Ce guide est destiné aux professionnels et experts du domaine de la sécurité digitale, les questions de guide ont été conçues de la manière suivante :

- <u>Une première rubrique :</u>

Questions générales : pour mieux comprendre le profil des participants.

- Une deuxième rubrique :

Questions spécifiques sur les pratiques de gestion des risques en matière de sécurité digitale : en mettant l'accent sur l'identification des risques, les méthodes d'évaluation, les outils utilisés, les défis rencontrés, les adaptations aux tendances émergentes, la réaction en cas d'incident et les recommandations pour renforcer la sécurité.

Ces différentes rubriques ont été développées pour répondre à nos questions de recherche.

Notre engagement a respecté la confidentialité des réponses et à utiliser les informations uniquement à des fins scientifiques renforce la rigueur et l'éthique de notre étude. (ANNEXE B)

b) **Argumentation de choix d'échantillon**

Le choix de l'échantillon pour notre recherche s'est porté sur quatre employés de l'entreprise **DEVLOG**, où se déroule le stage. Cette décision a été guidée par les contraintes organisationnelles, notamment la taille de l'équipe de développement qui est composée uniquement de ces quatre individus.

La similarité des réponses fournies par les développeurs a permis d'atteindre une saturation des données, ce qui signifie que l'échantillon était suffisamment représentatif pour permettre une analyse pertinente des risques de sécurité. Ainsi, même restreint, cet échantillon a été jugé adéquat pour les besoins de l'étude.

Tableau 6: *Sélection des interviewés*

	Poste	**Jour d'entretien**	**Durée**	**L'endroit de l'entretien**
R. F	Développeur web	02/05/2024	40 Min	DEVLOG
S. L	Co-gérante / développeur web	05/05/2024	45 Min	DEVLOG
R. B	Designer	05/05/2024	20 Min	DEVLOG
I. C	Co-fondateur/ Manager général / développeur web	09/05/2024	50 Min	DEVLOG

Source : élaborer par nous-mêmes.

Le tableau ci-dessus répertorie les entretiens menés pour notre étude, axés sur la maitrise des risques liés à la sécurité des plateformes numériques.

Il résume les initiales de la personne interrogée, son rôle au sein de **DEVLOG**, la date et la durée de l'entretien, ainsi que la pertinence de ses réponses par rapport au sujet de recherche.

1.4. Traitement des données

Après la collecte des données, une phase de traitement rigoureuse a été mise en place. Nous avons utilisé le logiciel NViVO 11 pour analyser qualitativement les données recueillies, et l'outil AMDEC pour évaluer et gérer les risques identifiés.

1.4.1. NVIVO 11

Pour analyser les résultats de notre enquête à l'aide d'un guide d'entretien, nous adopterons une approche de méthodes mixtes, combinant deux méthodologies complémentaires. Tout d'abord, pour la première partie du guide, nous avons choisi l'analyse sémantique. Cela implique un traitement manuel des données collectées, au cours duquel nous examinons les réponses des participants en profondeur, analysant les mots et les phrases à la recherche d'idées, de concepts et de significations. Cette approche nous permettra de capter la richesse des réponses et de comprendre les nuances des points de vue exprimés par les personnes interrogées.

Pour la deuxième partie de ce guide, nous utiliserons le logiciel NVIVO 11.

NVIVO 11 est un outil spécialisé dans l'analyse de données qualitatives, offrant des capacités avancées pour la gestion, l'exploration et l'analyse de données textuelles. Dans cet exemple, nous utilisons principalement NVIVO 11 pour effectuer une analyse statistique sur des données textuelles et générer des nuages de mots. Cette visualisation nous permettra de mettre en évidence les termes les plus fréquemment mentionnés dans les réponses des participants, offrant ainsi un aperçu visuel des principaux thèmes et sujets abordés lors des entretiens.

En combinant ces deux méthodes, nous serons en mesure d'acquérir une compréhension approfondie et nuancée des données collectées au cours de l'enquête, en tirant parti des aspects qualitatifs et quantitatifs des réponses des participants.

1.4.2. AMDEC

Nous développons une matrice AMDEC pour identifier et évaluer les risques potentiels liés à la sécurité des plateformes numériques. Cette matrice s'affiche sous forme de tableau à plusieurs colonnes, comme suit :

- **Opérations ou activités :** Cette colonne comprend diverses opérations ou activités liées à la sécurité de la plateforme numérique qui seront analysés.
- **Les contraintes :** cette colonne contient conditions ou des limites imposées au système, au composant ou au processus qui peuvent influencer sa performance
- **Mode de défaillance :** cette colonne répertorie les modes de défaillance ou les risques possibles pour chaque opération ou activité. C'est la réponse à la question de base « Qu'est-ce qui pourrait aller mal ? ».
- **Effet potentiel :** Cette colonne traite l'impact potentiel de chaque mode de défaillance. C'est la réponse à la question « Quels pourraient être les effets entraînés par ce mode de défaillance potentielle ? ».
- **Causes possibles *:*** Cette colonne identifie les causes possibles pour chaque mode de défaillance. C'est la réponse à la question « « Quelles pourraient être les causes à l'origine de ce mode de défaillance potentielle ? ».
- **Gravité de l'impact :** cette colonne évalue la gravité de l'impact potentiel sur une échelle de 1 à 5. (1 est le moins grave et 5 est le plus grave). C'est la réponse à la question « Quelle est la gravité relative des effets ? ».
- **Fréquence :** Cette colonne évalue la fréquence à laquelle chaque mode de défaillance se produit sur une échelle de 1 (très rare) à 5 (très courant). « Quelle est la probabilité relative d'apparition des causes ? ».
- **Détection :** Cette colonne évalue la capacité à détecter chaque mode de défaillance s'ils se produisent sur une échelle de 1 à 5 (1 détection très haute et 5 détection très faible).
- **Criticité :** Cette colonne calcule le niveau de risque en multipliant la gravité, la fréquence et l'indice de détection. Cela permet de prioriser les actions à entreprendre en fonction du risque.

  $C = (G \times F \times D)$
- **Plan d'action :** cette colonne recommande des mesures (correctives / préventives) concrètes pour contrôler et éliminer les sources de défaillance.
- **Responsabilité :** Cette colonne établit les responsables de chaque action.
- **Evaluation :** Cette colonne évalue la nouvelle criticité de chaque mode de défaillance après la mise en place des actions préventives pour chaque mode de défaillance.

- **Observation :** Cette colonne détaille les observations de chaque mode de défaillance après leur traitement par les plans d'action correspondants.

Tableau 7: *échelle d'évaluation de la Détection, Fréquence, et Gravité.*

Echelle	Critère		
	Gravité (G)	Fréquence (F)	Détection (D)
5	Catastrophique	Très fréquent	Indétectable
4	Critique	Fréquent	Difficilement détectable
3	Grave	Probable	Détectable
2	Mineur	Rare	Facilement détectable
1	Négligeable	Très rare	Evident

Source : élaboré par nous même

Ce tableau fournit une échelle de notation de 1 à 5 pour les trois principaux critères de l'analyse AMDEC : détection, fréquence et gravité. Ces critères sont essentiels pour identifier, évaluer et prioriser les types de défaillances dans un système ou un processus. En organisant cette évaluation, cette table facilite l'identification des priorités et l'élaboration de plans d'action pour réduire les risques et améliorer la fiabilité et la sécurité des systèmes analysés.

Conclusion de la section

La méthodologie de notre recherche combine une approche qualitative basée sur la recherche-action avec des techniques de collecte de données telles que l'observation et les entretiens semi-directifs. Cette approche nous permet de comprendre en profondeur les défis de la sécurité des plateformes numériques et d'apporter des recommandations pratiques pour améliorer la gestion des risques, en mettant particulièrement en lumière l'efficacité de l'outil AMDEC.

Section 2 : contexte organisationnel

Dans cette section, nous vous proposons une présentation de l`organisme d'accueil basée sur nos propres observations. Nous avons également bénéficié de l'assistance du manager et consulté le site web de l'entreprise pour compléter notre analyse. Cette approche nous a permis de fournir une vue d'ensemble précise et détaillée de l'organisation.

2.1. Présentation de l'entreprise

Le nom de l'organisme d'accueil : DEVLOG

L'adresse : cité Djillali N 21 RDC, Staoueli-Alger

Contact : 07.99.11.25.06

Site : https://devlog.dz/

Depuis sa fondation en 2019, **DEVLOG** s'est distinguée comme une start-up dynamique en Algérie. Spécialisée dans le développement d'applications informatiques innovantes, la société propose des solutions standard ainsi que sur mesure pour répondre aux besoins spécifiques de ses clients, dans des secteurs aussi variés que les services aux entreprises et aux collectivités, l'artisanat, les professions libérales, le tourisme, le domaine médical et la formation professionnelle, entre autres.

L'objectif principal de **DEVLOG** est de fournir des solutions informatiques précises, performantes, créatives et adaptées aux exigences des professionnels les plus exigeants en matière informatique, en mettant l'accent sur une approche personnalisée. Certaines solutions visent des processus complexes nécessitant une flexibilité et une adaptabilité exceptionnelles, tandis que d'autres sont conçues pour les petites entreprises ou entrepreneurs individuels à la recherche de services abordables et faciles à utiliser.

Grâce à sa compréhension fine des besoins de ses clients, **DEVLOG** s'efforce continuellement d'offrir des services sur-mesure et de qualité. L'entreprise accorde une grande importance à la compréhension approfondie et nuancée des besoins complexes de chaque client, analysés avec précision et délicatesse.

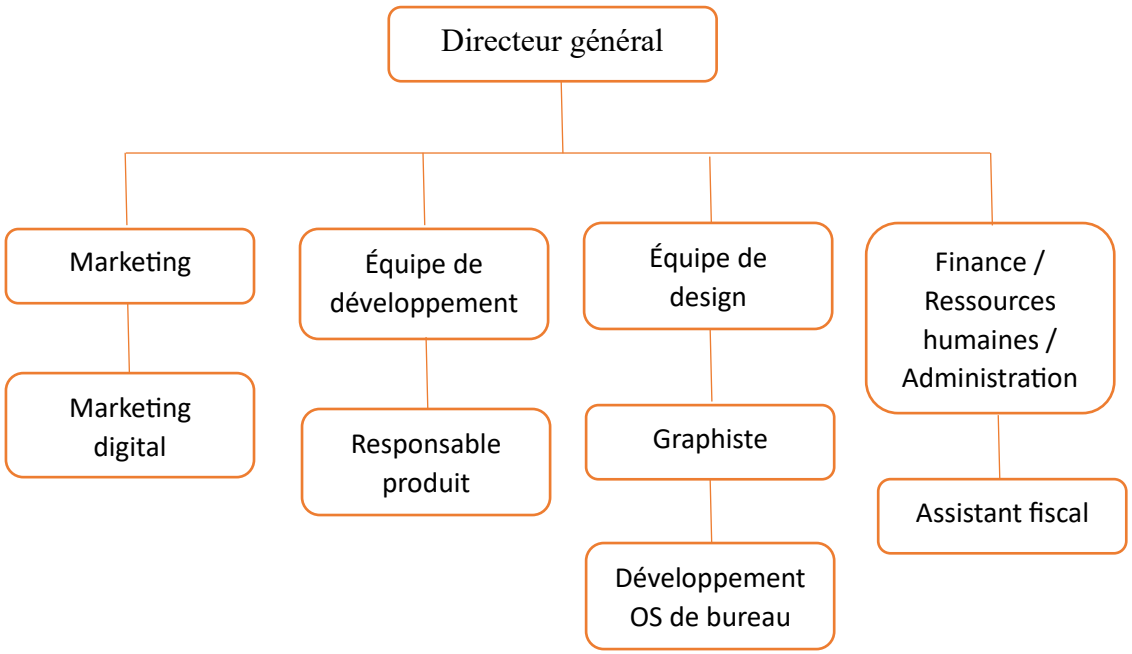
Cette approche attentive et méticuleuse a conduit **DEVLOG** à gagner la confiance de nombreux clients de premier plan, qu'ils évoluent dans le secteur public avec des réglementations strictes ou dans le secteur privé avec des défis changeants. Ainsi, l'entreprise se positionne adroitement comme le partenaire privilégié et adaptable pour toute

organisation souhaitant extraire et exploiter pleinement le potentiel inattendu de la technologie dans diverses applications afin d'atteindre ses objectifs commerciaux avec sagacité.

2.2.Organigramme de l'entreprise :

Cet organigramme représente la structure hiérarchique de l'entreprise.

Figure 4: *organigramme de l'entreprise.*



Source : document interne de l'entreprise

L'organigramme de l'entreprise, basé sur un document interne, présente une structure hiérarchique claire sous la direction du Directeur général, qui supervise quatre branches principales.

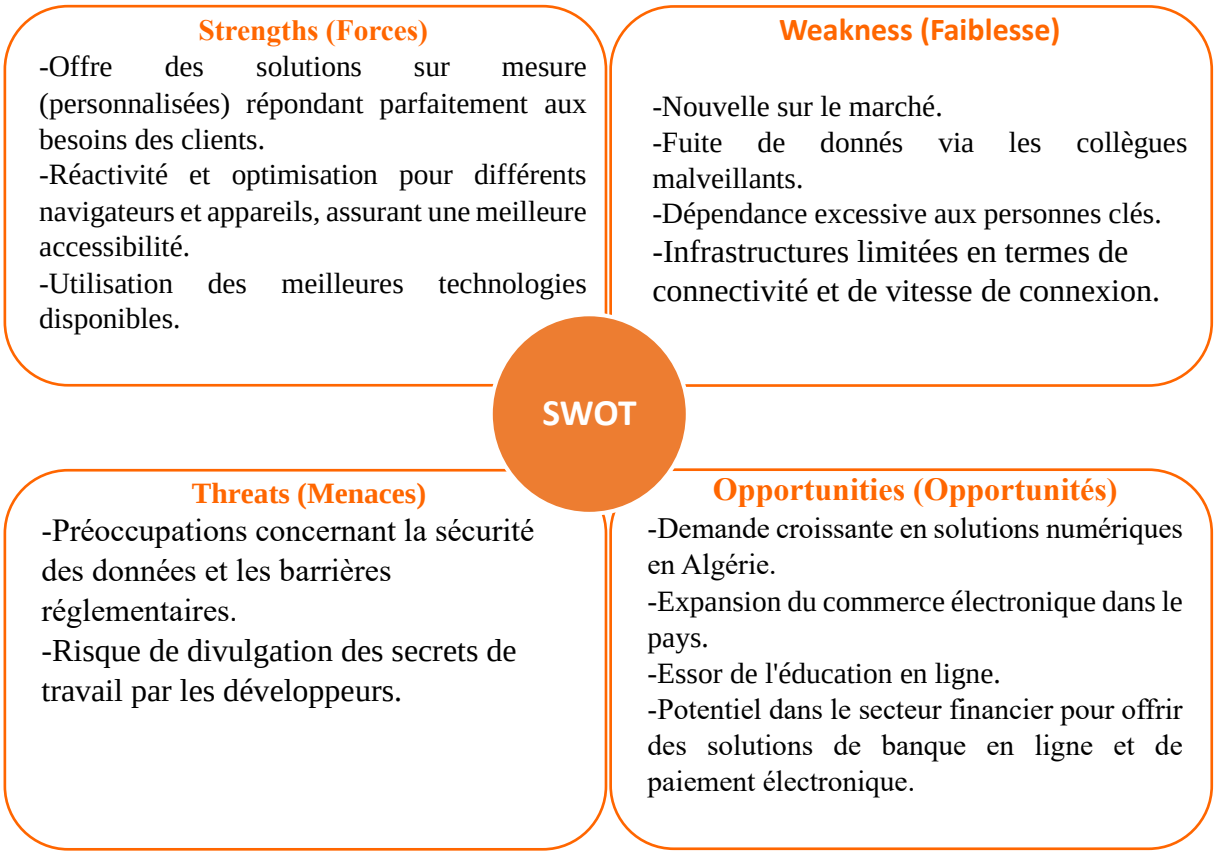
- Le département Marketing inclut une sous-division dédiée au marketing digital, responsable des stratégies publicitaires en ligne et de la gestion des réseaux sociaux.
- L'équipe de développement est dirigée par un Responsable produit, essentiel pour coordonner le développement des produits et assurer la communication entre les équipes techniques et commerciales.
- L'équipe de design comprend un graphiste chargé de la création visuelle et une fonction de développement des systèmes d'exploitation pour les postes de travail.
- Enfin, le département Finance/Ressources humaines/Administration inclut un assistant fiscal, chargé de la gestion des aspects fiscaux et comptables de l'entreprise.

Cet organigramme illustre la répartition des rôles et la collaboration entre les différentes fonctions sous la supervision du Directeur général.

2.3. Analyse SWOT de l'entreprise DEVLOG :

Pour mieux comprendre la position actuelle de l'entreprise et ses perspectives futures, une analyse SWOT a été réalisée.

Figure 5: *matrice SWOT de l'entreprise*



Source : Elaboré par nous-même sur la base d'une collaboration avec les responsables.

Cette analyse SWOT permet de mieux comprendre les points forts et les défis de l'entreprise, tout en identifiant les opportunités à exploiter et les menaces à surveiller.

2.4. Le workflow de l'entreprise :

a. Analyser les besoins :

- Diagnostiquer finement les situations commerciales complexes au travers d'une analyse approfondie des données factuelles afin de cerner précisément les enjeux et défis uniques à chaque client.

- Identifier méthodiquement les domaines dans lesquels l'entreprise pourrait apporter, une valeur ajoutée significative et sur mesure, en ciblant les leviers d'actions prioritaires.

b. Formuler des solutions adaptées :

- Proposer des pistes de transformation stratégiques adaptées et personnalisées aux besoins spécifiques du client.
- Définir clef en main les priorités opérationnelles du client pour orienter de manière pragmatique nos recommandations.
- Modéliser sous forme de schémas ou plans d'actions les idées forces afin de faciliter leur appropriation et leur mise en œuvre.

c. Stratégie d'action :

- Elaboration d'un plan détaillé pour mettre en place les recommandations et mettre en œuvre la stratégie d'action.
- Surveillance continue de l'évolution, suivi des progrès et ajustement du plan si nécessaire pour atteindre les objectifs fixés.

d. Suivi et analyse des performances :

- Evaluation des résultats obtenus par rapport aux objectifs établis, avec analyse des résultats.
- Utilisation des analyses pour orienter les recommandations à venir et améliorer les processus, en vue de préparer les éléments futurs.

2.5. Les différents services proposés par l'entreprise :

- **Création graphique :** la création du logo à la conception des éléments de communication **DEVLOG** propose des visuels qui captent l'attention, séduisent, créent l'envie et suscitent la consommation. Un beau contenu visuel.
- **Application web :** Ils sont une agence web experte dans la création de sites Internet en Algérie. Ils conçoivent des sites Web efficaces et fonctionnels. En effet, le web est le moyen le plus efficace pour communiquer. C'est pourquoi leur agence propose de démarquer les entreprises grâce à un web design créatif optimisé pour le référencement.
- **Application mobile :** leurs ingénieurs développent des fonctionnalités sur-mesure pour apporter de la valeur à la société. Ils développent des applications (conception, ergonomie, design d'interface, développement mobile, web et desktop, tests et publication).

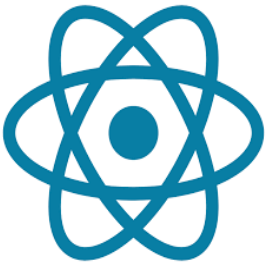
- **Logiciel métier** : conception de solutions logicielles sur mesure pour optimiser l'efficacité de des entreprises en fonction de leurs processus métier.
- ***Site vitrine :*** élaboration de sites web informatifs et séduisants afin de présenter de manière professionnelle les entreprises, leurs produits ou leurs services.
- ***ERP :*** **DEVLOG** conçoit des solutions ERP (Entreprise Ressources Opérationnels) sur mesure, intégrant harmonieusement les processus opérationnels pour une efficacité maximale.

2.6. Les technologies utilisées :

○ JavaScript

JavaScript, souvent abrégé en « JS », est un langage de script léger et orienté objet, principalement connu pour son utilisation sur les pages web. Cependant, il est également utilisé dans de nombreux environnements en dehors des navigateurs web, tels que Node.js, Apache CouchDB et même Adobe Acrobat. Le code JavaScript est interprété ou compilé à la volée (JIT) et repose sur le concept de prototype pour la programmation orientée objet. Il dispose d'un typage faible et dynamique, ce qui lui permet de prendre en charge plusieurs paradigmes de programmation, notamment la programmation fonctionnelle, impérative et orientée objet.

○ React



React est une bibliothèque JavaScript open-source développée par Facebook, utilisée pour créer des interfaces utilisateur interactives et dynamiques. Plutôt que de se concentrer sur des modèles MVC traditionnels, React se concentre sur la construction de composants réutilisables. Il utilise un concept appelé le DOM virtuel pour améliorer les performances en minimisant les manipulations directes du DOM. React favorise un style de programmation déclaratif, où les développeurs décrivent comment l'interface utilisateur devrait se comporter et React se charge de mettre à jour l'interface utilisateur en fonction des changements d'état de manière efficace. Cela rend le code plus prévisible et plus facile à comprendre, ce qui en fait un choix populaire pour le développement d'applications web modernes.

- **Dart**

Dart est un langage de programmation open-source développé par Google, principalement utilisé pour le développement d'applications mobiles et web. Il se distingue par sa syntaxe claire et concise, inspirée de langages tels que C et JavaScript, ce qui le rend relativement facile à apprendre pour les développeurs venant d'autres langages. Dart est également connu pour sa performance élevée, grâce à son compilateur just-in-time (JIT) et son compilateur ahead-of-time (AOT), qui permettent d'exécuter du code Dart à des vitesses comparables à celles du langage natif. Dart est souvent utilisé avec le framework Flutter, qui permet de créer des interfaces utilisateur multiplateformes élégantes et réactives. Cette combinaison de Dart et Flutter en fait une option attrayante pour le développement d'applications mobiles et web modernes, offrant une productivité élevée et des performances exceptionnelles.

- **Flutter**

Flutter est un framework open-source développé par Google pour créer des applications multiplateformes, notamment pour Android, iOS, Windows, Mac, Linux et le web à partir d'un seul codebase. Il se distingue par sa capacité à produire des interfaces utilisateur fluides, réactives et esthétiques grâce à sa conception basée sur des widgets personnalisables. Flutter utilise le langage de programmation Dart, qui offre des performances élevées grâce à son compilateur just-in-time (JIT) et son compilateur ahead-of-time (AOT). Grâce à sa hot reload, les développeurs peuvent voir instantanément les changements apportés au code, ce qui accélère le processus de développement et facilite le débogage. Flutter est largement adopté pour le développement d'applications mobiles et web en raison de sa productivité élevée, de sa performance élevée et de sa capacité à offrir une expérience utilisateur de haute qualité sur différentes plateformes.

- **Firebase**

Firebase est une plateforme de développement d'applications mobiles et web développée par Google. Elle propose une gamme de services backend, notamment l'authentification des utilisateurs, la base de données en temps réel, le stockage de fichiers, l'hébergement web, les fonctions cloud, l'analyse, la messagerie cloud, etc. Firebase est connu pour sa facilité d'utilisation et sa capacité à fournir une infrastructure backend puissante sans nécessiter de configuration complexe. Il est largement utilisé pour développer des applications évolutives et réactives, offrant aux développeurs les

outils nécessaires pour créer des applications de haute qualité rapidement et efficacement. Firebase s'intègre également parfaitement avec d'autres produits Google, ce qui en fait une solution attrayante pour les développeurs souhaitant créer des applications multiplateformes modernes et performantes.

- **Node.JS**

Node.js est un environnement d'exécution JavaScript côté serveur, basé sur le moteur JavaScript V8 de Google Chrome. Il permet aux développeurs d'utiliser JavaScript pour écrire des applications côté serveur, en plus de son utilisation traditionnelle côté client dans les navigateurs web. Node.js est apprécié pour sa rapidité et son efficacité, en partie grâce à son architecture basée sur des événements non bloquants, qui permet à de nombreuses opérations d'être exécutées de manière asynchrone. Cela le rend particulièrement adapté pour les applications web en temps réel, les API RESTful, les serveurs de messagerie et d'autres types d'applications réseau. Node.js est également largement utilisé avec des frameworks tels que Express.js pour simplifier le processus de développement web. Grâce à son écosystème de modules NPM (Node.js Package Manager), Node.js offre une grande variété de packages prêts à l'emploi pour étendre les fonctionnalités de base de Node.js et accélérer le développement d'applications.

- **Google cloud**

Google Cloud est une plateforme de services en ligne de Google qui permet de stocker des données, d'héberger des applications et de gérer des ressources informatiques. Elle propose des outils pour créer et déployer des applications, analyser des données, et utiliser l'intelligence artificielle, tout en fournissant une infrastructure sécurisée et évolutive.

- **Mongo DB**

MongoDB est une base de données populaire qui stocke les données sous forme de documents au format JSON, ce qui facilite leur manipulation et leur organisation. Elle est souvent utilisée pour les applications nécessitant une gestion agile des données, offrant une grande flexibilité pour évoluer avec les besoins des applications.

2.7. Projets réalisés par l'entreprise :

- **TRACkMED (Solution de traçabilité bio nettoyage)**

TrackMed est une application web spécifiquement conçue pour faciliter la traçabilité du bionettoyage dans les établissements de santé français, avec pour objectif d'améliorer l'efficacité et la conformité des processus.

La plateforme intuitive garantit un contrôle précis et un suivi rigoureux de l'exécution et le respect des protocoles et règle d'hygiène établis par l'agence régionale de santé (ARS) et la direction générale de la santé (DGS). (ANNEXE C)

- **AACDHB (Association Algérienne De Chirurgie Digestive & Hépatobiliaire)**

AACDHB est une association active dans le domaine medical, plus precisement dans le secteur de la chirurgie. Elle édite une revue trimestrielle appelée "Algerian Journal of Surgery" (AJS), dont le rédacteur en chef est le Pr Abdelkrim Anou. L'association invite les professionnels et les chercheurs à contribuer à la revue en soumettant des articles, des cas cliniques, des vidéos, etc.

Leur site web constitue une plateforme centralisée pour les actualités de l'association et les événements à venir. Il offre également la possibilité aux personnes intéressées de soumettre leur demande d'adhésion en ligne. L'entreprise valorise les retours des utilisateurs et invite les visiteurs à partager leurs suggestions, remarques et critiques pour améliorer le site, qui est conçu pour être évolutif en fonction des besoins de la communauté. L'association a collaboré avec la société "SITTEM", spécialisée dans l'événementiel, pour la conception professionnelle de son site web. En résumé, cette entreprise est un acteur dynamique dans le domaine de la chirurgie, cherchant à promouvoir la recherche et le partage de connaissances tout en offrant une plateforme interactive pour ses membres et les professionnels intéressés. (ANNEXE D)

- **AIC B2B (Algeria Invest Conference)**

AIC B2B constitue une plateforme web et mobile sur mesure, méticuleusement conçue pour fournir une assistance complète aux participants de l'évènement « Algeria Invest Conference » en matière d'organisation et de suivi de leurs rencontres professionnelles de type B2B. (ANNEXE E)

- **LF**

DEVLOG a développé avec succès une plateforme de facturation et de gestion commerciale robuste et personnalisée. Leur solution hautement fonctionnelle intègre la gestion complète des processus commerciaux, depuis la création et l'envoi de factures

jusqu'au suivi des paiements et à la génération de rapports financiers détaillés. Avec une interface conviviale, cette plateforme vise à optimiser l'efficacité opérationnelle des entreprises, en leur permettant de gérer facilement leurs transactions, d'automatiser les tâches administratives et de prendre des décisions éclairées grâce à une meilleure visibilité sur leur performance financière. (ANNEXE F)

- **MenuCraft**

MenuCraft révolutionne le secteur de la restauration avec sa solution digitale sur mesure qui élimine les contraintes des menus traditionnels. Fini les coûts d'impression, les mises à jour saisonnières ou le nettoyage, cette plateforme permet une édition facile en ligne, affichant le menu actuel de manière hygiénique, sans germes ni erreurs. Avec cette solution, la restauration moderne et hygiénique est à portée de clic. (Annexe 07)

- **DERMACARE**

DERMACARE est une plateforme en ligne qui agit comme un intermédiaire entre les clients, les dermatologues et les fournisseurs de produits cosmétiques bio. Elle propose à la vente une variété de produits cosmétiques bio tout en offrant des consultations dermatologiques en ligne.

Conclusion du chapitre

Ce chapitre a exposé l'organisation interne de **DEVLOG** et la méthodologie utilisée pour étudier les risques liés à la sécurité des plateformes numériques. Il a souligné l'importance de comprendre la structure et les processus internes pour identifier et gérer efficacement les risques. En explorant diverses méthodes de recherche et d'analyse, il a établi une base solide pour l'évaluation des risques et a préparé le terrain pour les discussions et recommandations à venir.

CHAPITRE 3 : RESULTATS ET DISCUSSION

Section 1 : résultats de l'étude qualitative

Dans cette section, nous partageons les résultats de notre étude. Nous avons collecté les données en observant et en discutant avec différentes personnes lors d'entretiens. Ces résultats nous aident à comprendre la sécurité des plateformes digitales et à voir comment gérer les risques de manière efficace.

1. Collecte de données

1.1. Déroulement de l'observation :

Au sein de l'entreprise de développement, nous avons bénéficié d'une immersion encadrée par des experts. Cette expérience nous a permis d'observer le processus de création de sites web et d'applications, tout en acquérant des compétences d'identification et d'évaluation des risques liés à la sécurité informatique. Nous avons également utilisé l'outil Figma pour concevoir des maquettes, y compris celle de la plateforme "**DERMACARE**" pour un client. Ces expériences pratiques nous ont sensibilisés aux défis uniques de la sécurité dans le développement web, renforçant ainsi notre compréhension des mesures de gestion des risques.

1.2. Déroulement des entretiens :

Nous avons mené une étude qualitative basée sur des entretiens semi-directifs avec des intervenants dans le domaine du développement web au sein de l'entreprise **DEVLOG** à Staoueli.

Nous avons réalisé des entretiens avec quatre répondants, couvrant l'ensemble des employés de **DEVLOG**. Nous leur avons posé trois questions générales et huit questions spécifiques sur les pratiques de la maitrise des risques liés a la sécurité informatique.

Cependant, il est important de noter que l'un des interviewé a été exclu sur la majorité des questions car il était un designer et n'avait pas les connaissances nécessaires dans ce domaine.

Les entretiens ont joué un rôle crucial dans notre collecte d'informations sur les différents aspects de la sécurité des plateformes digitales. Ils nous ont permis d'identifier plusieurs risques potentiels et de recueillir des informations sur les mesures préventives déjà en place pour les atténuer.

2. Interprétation des résultats depuis NVIVO 11

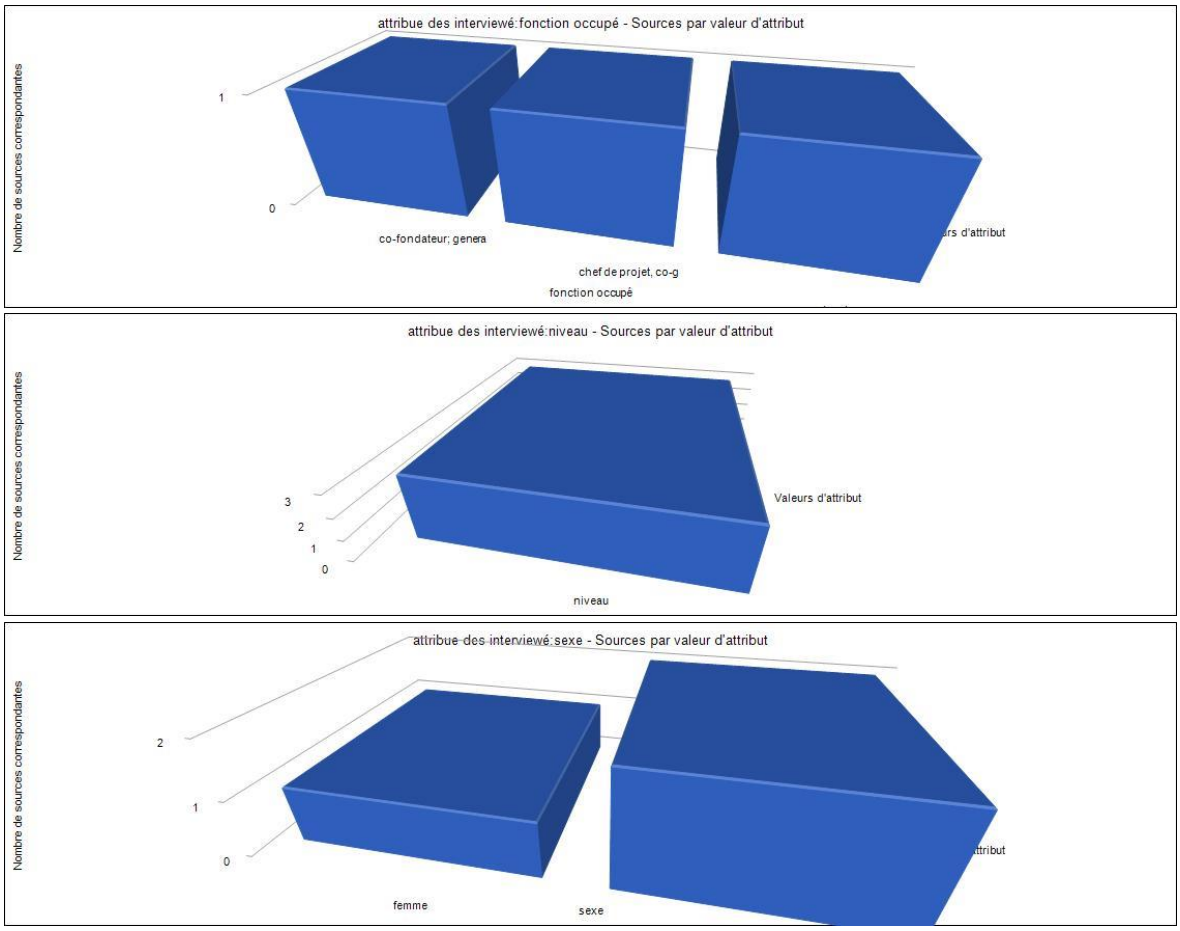
Pour analyser efficacement les résultats des entretiens, nous avons structuré cette section en deux volets principaux. Le premier volet présente une analyse globale des entretiens, incluant la description de l'échantillon et une étude du nuage de mots. Le

deuxième volet se concentre sur l'analyse des différents thèmes abordés dans le guide d'entretien.

2.1. Description de l'échantillon :

Afin de mieux connaitre notre échantillon nous avons réalisé quelques illustrations générées par l'outil d'analyse NVIVO 11.

Figure 6: *Informations personnelles des interviewés*



Source : Informations personnelles des interviewés

L'étude inclut une diversité de fonctions, y compris des co-fondateurs et des chefs de projet, offrant ainsi une vision complète des pratiques de gestion des risques liés à la sécurité des plateformes digitales. Cette variété permet d'analyser les différentes perspectives et approches en matière de sécurité. Par exemple, les co-fondateurs peuvent apporter des insights stratégiques, tandis que les chefs de projet peuvent offrir des retours sur la mise en œuvre des mesures de sécurité.

En incluant des participants des deux sexes, l'étude bénéficie d'une perspective variée en termes de genre, ce qui enrichit l'analyse. Cette approche multidimensionnelle permet de

mieux comprendre les perceptions et les pratiques de gestion des risques, et de proposer des ajustements ciblés pour améliorer la sécurité des plateformes digitales.

2.1.1. Analyse du nuage de mots :

Cette figure générée par NVIVO 11 représente un nuage de mots mettant en évidence les termes les plus fréquents dans les entretiens. Elle permet de visualiser et de souligner le sujet de recherche ainsi que la problématique abordée à travers les questions des entretiens. La taille de chaque mot est proportionnelle à sa fréquence d'apparition dans les discussions.

Figure 7: *nuage de mots*

Source : générer par NVIVO 11

Dans notre nuage de mots, "sécurité" est le terme le plus proéminent, apparaissant 86 fois. Cela indique que le concept de sécurité est central dans la discussion, reflétant notre concentration sur la manière dont la sécurité des plateformes digitales est perçue et gérée par les parties prenantes.

Les mots "digitales" et "risque" reviennent respectivement 36 et 34 fois. Cela montre que notre étude s'est focalisée sur les aspects numériques et les risques associés, soulignant l'importance de comprendre et de gérer les vulnérabilités dans les environnements numériques.

Le terme "gestion" apparaît 24 fois, indiquant que la gestion des risques est un élément clé de notre recherche. Cela montre notre intérêt pour les stratégies et les méthodes utilisées pour atténuer les risques identifiés.

Le mot "plateforme" revient 22 fois, ce qui signifie que les plateformes digitales sont au cœur de notre étude. Nous avons examiné comment elles sont structurées, utilisées et protégées contre les menaces potentielles.

Le mot "menace" apparaît 23 fois, soulignant les défis et les dangers auxquels ces plateformes sont confrontées. Cela est crucial pour comprendre les mesures nécessaires pour renforcer leur sécurité.

Ces résultats indiquent que notre étude se concentre principalement sur la sécurité des plateformes digitales, la gestion des risques et les menaces, soulignant l'importance de ces éléments pour améliorer la résilience et la fiabilité des systèmes numériques.

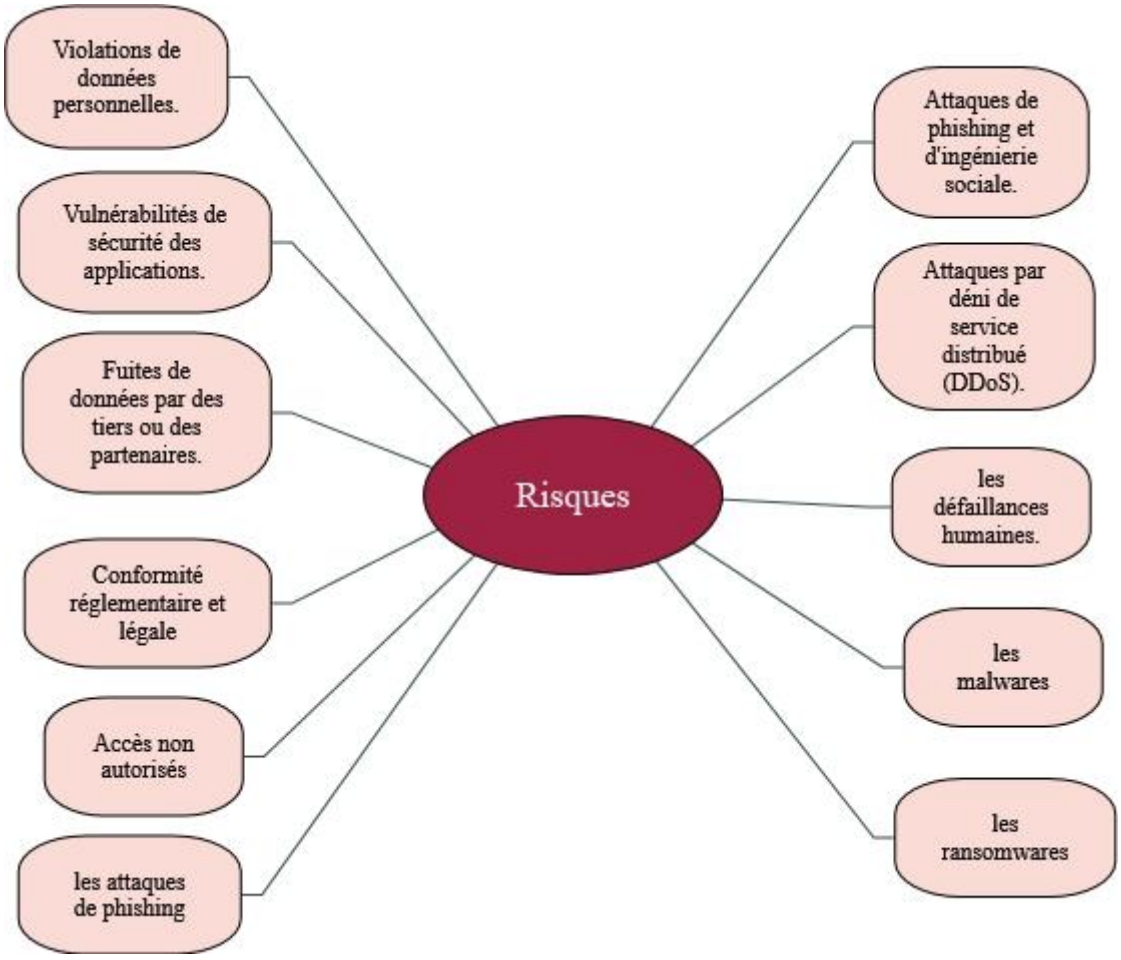
2.2. L'analyse des résultats des différents axes traités dans l'entretien

Pour analyser les axes, nous avons adopté une démarche en deux étapes. Tout d'abord, nous avons utilisé des graphiques générés par NVIVO11 pour illustrer les résultats, rendant les données plus claires et compréhensibles. Ensuite, nous avons synthétisé les réponses des interviewés dans des tableaux, permettant de regrouper et de comparer les informations de manière structurée et concise. Cette approche combinée facilite une interprétation approfondie et une meilleure compréhension des thèmes principaux abordés dans le guide d'entretien.

- **Les risques :**

Pour analyser les risques liés à la sécurité de la plateforme **DERMACARE** identifiés lors des entretiens, une carte mentale a été conçue pour regrouper et visualiser de manière systématique les divers risques relevés. Cette approche permet d'identifier les risques techniques, ainsi que les obstacles liés à la sécurité et à la fiabilité du système. En examinant ces risques de manière structurée, **DEVLOG** peut élaborer des stratégies de gestion des risques ciblées pour renforcer la sécurité et la performance de la plateforme **DERMACARE.**

Figure 8: *Carte mentale des risques identifiés sur la plateforme* ***DERMACARE.***



Source : élaboré par nous-même sur la base du logiciel NVIVO 11

Cette figure illustre les divers risques liés à la sécurité des plateformes digitales, englobant les violations de données personnelles, les vulnérabilités des applications, les fuites de données par des tiers, la non-conformité réglementaire, les accès non autorisés, ainsi que les attaques de phishing, d'ingénierie sociale et par déni de service distribué (DDoS). Elle inclut également les défaillances humaines, les malwares et les ransomwares, soulignant l'importance d'une gestion proactive pour minimiser ces menaces et protéger les informations sensibles et les systèmes informatiques.

2.2.2. Le management des risques :

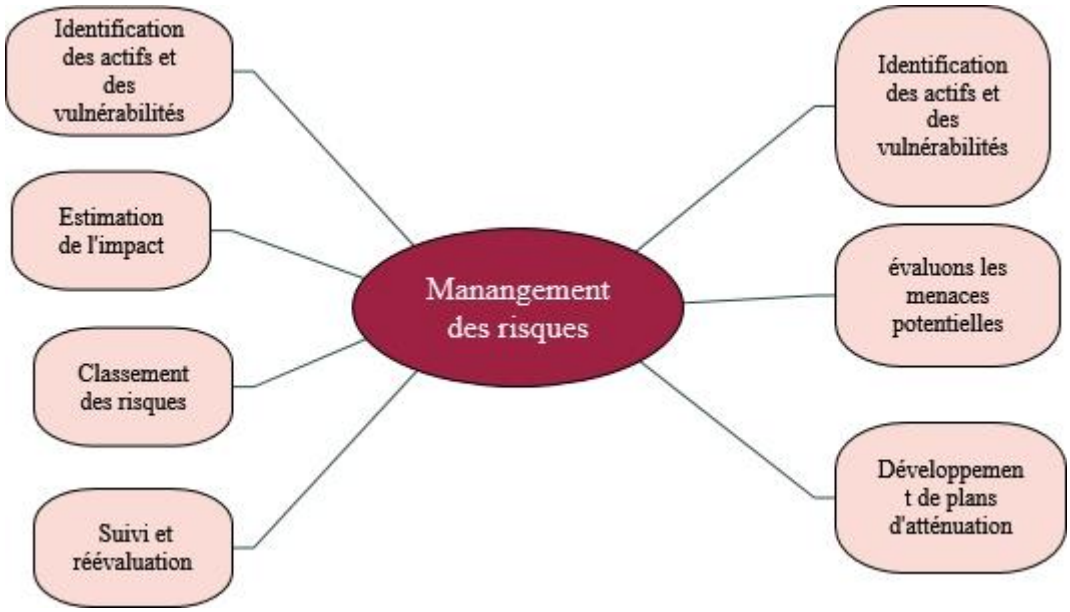
Pour analyser la maitrise des risques liés à la sécurité des plateformes par **DEVLOG**, trois cartes mentales ont été créées. De plus, nous avons élaboré nous-mêmes un tableau des verbatims pour renforcer les résultats de ces cartes mentales. Cette approche permet de mieux comprendre les priorités en matière de gestion des risques liés à la sécurité des

plateformes, comme la protection des données sensibles, la prévention des cyberattaques, les logiciels de surveillance des réseaux, ou encore les solutions de gestion des vulnérabilités.

En conséquence, elle guide les futures actions de management des risques de **DEVLOG** en fonction des besoins réels, garantissant ainsi une sécurité renforcée et une maitrise des risques plus efficace. (ANNEXE H)

La première carte se concentre sur le management des risques, illustrant comment **DEVLOG** évalue et classe les différents risques.

Figure 9: *Carte mentale de la gestion des risques par DEVLOG*

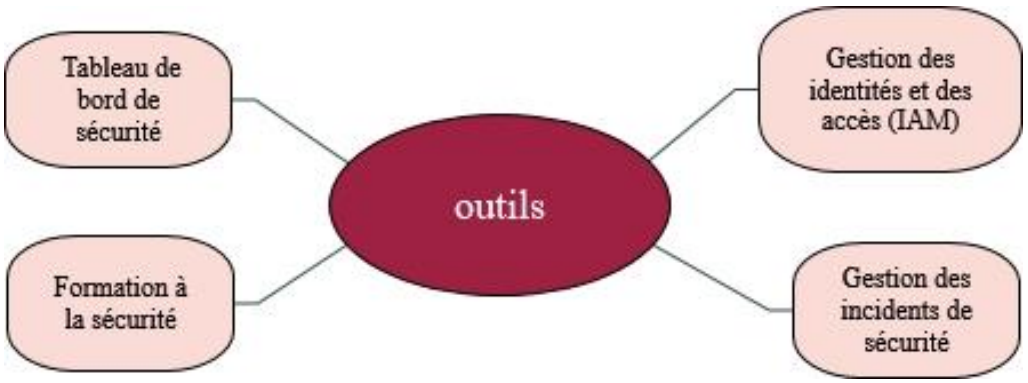


Source : élaboré par nous-même sur la base du logiciel NVIVO 11

Cette figure illustre le processus de management des risques en matière de sécurité des plateformes digitales. Il comprend l'identification des actifs et des vulnérabilités, l'estimation de l'impact, le classement des risques, le suivi et la réévaluation des risques, ainsi que l'évaluation des menaces potentielles et le développement de plans d'atténuation. Ces étapes sont essentielles pour une gestion efficace des risques, permettant de protéger les systèmes informatiques contre les diverses menaces.

La deuxième carte regroupe les outils que **DEVLOG** utilise dans le management des risques, offrant un aperçu clair des ressources et des technologies déployées.

Figure 10: *Carte mentale des outils utilisés dans le management des risques par* ***DEVLOG***

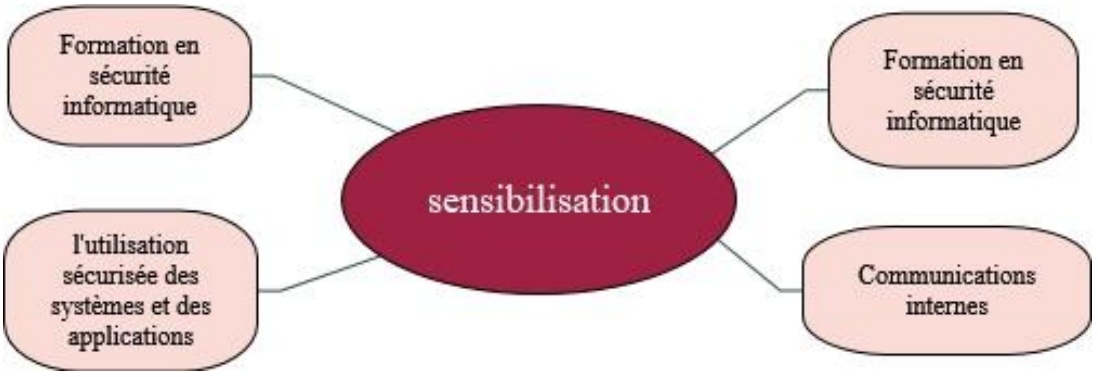


Source : élaboré par nous-même sur la base du logiciel NVIVO 11

Cette figure présente les différents outils utilisés pour renforcer la sécurité des plateformes digitales. Elle inclut le tableau de bord de sécurité, la formation à la sécurité, la gestion des identités et des accès (IAM), ainsi que la gestion des incidents de sécurité. Ces outils sont essentiels pour surveiller les systèmes, former le personnel, contrôler les accès et réagir efficacement aux incidents de sécurité, contribuant ainsi à une protection globale des infrastructures numériques.

Enfin, la troisième carte aborde la sensibilisation des employés, mettant en lumière les stratégies mises en place pour renforcer la culture de sécurité au sein de l'entreprise.

Figure 11: *Carte mentale de la sensibilisation des employés à la sécurité par* ***DEVLOG***



Source : élaboré par nous-même sur la base du logiciel NVIVO 11

Cette figure, issue des entretiens avec les personnels de DEVLOG et générée par NVivo 11 après l'encodage des nœuds, met en évidence les composantes essentielles de la sensibilisation en matière de sécurité informatique. Les résultats montrent que cette

sensibilisation repose sur un équilibre entre formation continue et communication efficace, visant à renforcer la sécurité des systèmes et applications utilisés par l'entreprise.

2.2.3. Interprétation générale des résultats générés par NVIVO 11

L'étude menée auprès des employés de **DEVLOG** met en lumière leur forte implication et leur engagement envers la sécurité des plateformes digitales. Les entretiens ont révélé que la sécurité est une préoccupation centrale, avec des discussions approfondies sur les risques, leur gestion, et les menaces liées aux plateformes digitales. Les employés sont conscients de l'importance de protéger les données sensibles et de prévenir les cyberattaques.

L'utilisation de NVIVO 11 pour l'analyse des entretiens a permis de mettre en évidence les principaux termes et concepts discutés, tels que la sécurité, les risques, la gestion, et les menaces. Ces résultats ont aidé à identifier les principaux domaines d'intérêt et à orienter les discussions vers des solutions et des actions concrètes pour renforcer la sécurité des plateformes digitales.

En résumé, cette étude souligne l'importance accordée par **DEVLOG** à la sécurité des plateformes digitales, en mettant en avant les efforts déployés pour gérer les risques et renforcer la culture de sécurité au sein de l'entreprise. Ces résultats pourraient guider les futures actions de gestion des risques de **DEVLOG**, garantissant ainsi une sécurité renforcée et une gestion des risques plus efficace.

3. La mise en place de l'AMDEC

Étape 01 : constitution de l'équipe de travail

L'équipe chargée de cette analyse était composée de

- AKHROUF Aicha et OUALI Racha.
- Manager de **DEVLOG**.
- Chef de projet.
- Un développeur web.
- Un designer.

Le but de l'étude était d'analyser les risques relatifs à la sécurité des plateformes digitales et d'élaborer une matrice AMDEC au niveau de l'entreprise **DEVLOG**, pour son client **DERMACARE**.

Etape 02 : étude qualitative des défaillances

Nous avons mené une étude qualitative sur les risques potentiels liés à la sécurité des plateformes digitales. L'objectif de cette étude était d'identifier les risques, c'est-à-dire les défaillances potentielles susceptibles d'apparaître et d'affecter la sécurité de ces plateformes.

Cette analyse a été réalisée en combinant diverses sources d'informations. Nous avons conduit des entretiens avec différents acteurs économiques de l'entreprise, notamment les responsables et les chefs de projets. Ces entretiens nous ont permis de recueillir des informations précieuses sur les éventuelles défaillances et les risques associés.

Les risques identifiés sont :

- Violations et fuites de données personnelles et sensibles, accès non autorisés, vulnérabilités de sécurité des applications et des logiciels.
- Attaques de phishing et d'ingénierie sociale.
- La rencontre de bugs.
- Les risques judicaires.
- Risques budgétaires.
- Les menaces internes, telles que les employés malveillants ou négligents.

Etape 03 : appréciation des défaillances

Après avoir identifié les risques potentiels liés à la sécurité des plateformes, nous sommes passées à leur évaluation. Pour cela, nous avons calculé leur criticité selon la formule : (C = G x F x D), et en utilisant une échelle allant de 1 à 5. Comme présentés dans la première section du chapitre précédent.

Tableau 8: *les intervalles de criticité des risques en fonction de la fréquence, de la gravité et de la détection.*

Intervalle de Criticité	Fréquence	Gravité	Détection	Justification
1 à 8	1 à 2	1 à 2	1 à 2	Le premier intervalle (de 1 à 8) correspond à une combinaison des critères variant de (1*1*1) à (2*2*2).
9 à 27	2 à 3	2 à 3	2 à 3	Le deuxième intervalle (de 9 à 27) couvre les valeurs de (2*2*2) à (3*3*3).
28 à 64	3 à 4	3 à 4	3 à 4	Le troisième intervalle (de 28 à 64) représente les niveaux de (3*3*3) à (4*4*4).
65 à 125	4 à 5	4 à 5	4 à 5	Le quatrième intervalle (de 65 à 125) englobe les valeurs de (4*4*4) à (5*5*5).

Source : Elaboré par nous-mêmes.

Les intervalles des risques ont été établis en fonction des niveaux de chaque critère : fréquence, gravité et détection. Ainsi, le premier intervalle (de 1 à 8) correspond à une combinaison des critères variant de (1*1*1) à (2*2*2). Le deuxième intervalle (de 9 à 27) couvre les valeurs de (2*2*2) à (3*3*3). Le troisième intervalle (de 28 à 64) représente les niveaux de (3*3*3) à (4*4*4), et enfin, le quatrième intervalle (de 65 à 125) englobe les valeurs de (4*4*4) à (5*5*5). Cette classification permet de mieux évaluer et prioriser les risques en fonction de leur criticité.

Etape 4 : la hiérarchisation

Après le calcul de la criticité de chaque mode de défaillance, nous avons pu les hiérarchiser afin de déterminer des actions préventives ou correctives prioritaires pour chaque mode de défaillance. Les principaux risques identifiés sont :

- Les menaces internes, telles que les employés malveillants ou négligents : Avec une criticité de 60, ce risque est le plus élevé.
- Violations et fuite de données personnelles et sensible, Vulnérabilités de sécurité des applications et des logiciels, Accès non autorisés : Avec une criticité de 40.
- Incapacité à payer les abonnements de sécurité pour sa plateforme : Avec une criticité de 40.
- Risques judiciaires : avec une criticité de 27.
- Attaques de phishing, les ransomware et les malwares : avec une criticité de 20.
- La rencontre des bugs : avec une criticité de 15.

Tableau 9: *Échelle de priorité.*

Niveau de risque évalue	Définition de risque	Acceptabilité
1≤ C≤ 8	Risque acceptable	Acceptable sans aucune mesure
9≤ C ≤27	Risque Modérer	Acceptable avec les mesures prises
28≤ C ≤ 64	Risque indésirable	Non acceptable : mesure de gestion des risques à moyen terme
65 ≤ C ≤ 125	Risque inacceptable	Non acceptable : Mesures urgentes de contrôle des risques

Source : élaborer par nous-mêmes

Estimation générale :

Cette estimation se fond sur une échelle de cinq niveaux pour estimer la fréquence, la gravité, ainsi que la capacité de détection, comme mentionné dans la section une du chapitre précédent. Voici une interprétation de chaque dimension :

- Gravité :

1 : négligeable, 2 : mineur, 3 : grave, 4 : critique, 5 : catastrophique

- Fréquence :

1 : très rare, 2 : rare, 3 : probable, 4 : fréquent, 5 : très fréquent

- Détection :

1 : évident, 2 : facilement détectable, 3 détectable, 4 : difficilement détectable, 5 : indétectable.

Etape 05 : la recherche des actions préventives / correctives

Pendant notre étude, nous avons pris des mesures préventives pour réduire les risques, surtout quand leur fréquence est élevée ou leur gravité importante. Notre but était de diminuer les chances de dysfonctionnement et d'atténuer les risques non détectés. Les actions correctives et préventives ont été définies en fonction du niveau de risque de chaque défaillance identifiée, avec des propositions venant de tous les développeurs après les entretiens. Cette approche a permis d'utiliser les connaissances de chaque membre de l'équipe pour décider des actions à prendre. Les mesures recommandées visaient spécifiquement les causes probables des défaillances identifiées.

Etape 06 : le suivie et la réévaluation de la criticité

Dans le cadre de notre recherche, des mesures ont été mises en œuvre pour atténuer les risques, en particulier ceux qui sont fréquents ou graves. L'objectif principal était de minimiser les risques de défaillance et de non-détection. Suite aux entretiens avec l'ensemble des développeurs, des solutions correctives et préventives ont été élaborées, proportionnellement au niveau de risque associé à chaque anomalie détectée. Cette méthode a permis de capitaliser sur l'expertise collective de l'équipe afin de déterminer les mesures à appliquer. Les interventions suggérées étaient conçues pour adresser directement les causes potentielles des défaillances identifiées.

Etape 07 : la présentation des résultats

Les résultats de notre analyse sont présentés sous forme de tableau AMDEC.

Tableau AMDEC (ANNEXE I)

Dans le cadre de notre projet, nous avons réalisé une analyse AMDEC pour le client DERMACARE de l'entreprise DEVLOG.

Nous avons identifié 6 modes de défaillance et 9 causes potentielles qui peuvent les affecter.

Sur la base de ces analyses, nous avons pu calculer le niveau de la criticité pour chaque mode de défaillance, et nous avons trouvé :

Tableau 10: *Classification de l'acceptabilité des risques*

0 Risques inacceptables	65≤ C ≤ 125
4 Risques indésirables	28≤ C ≤ 64
2 Risques modérers	9≤ C ≤27
0 Risques acceptables	1≤ C≤ 8

Source : élaborer par nous-même

Après avoir évalué la criticité de chaque mode de défaillance, nous avons élaboré des plans d'action pour chacun d'eux, en tenant compte du responsable de chaque plan. Nous avons formulé un ensemble total de 10 recommandations d'actions préventives/correctives. L'objectif principal de cette étape était de réduire l'impact de la criticité et de prévenir les risques potentiels. Ces recommandations ont été établies lors de la création de la matrice le 28 avril 2024. Après avoir mis en œuvre les plans d'action, comprenant à la fois des actions correctives et préventives pour chaque mode de défaillance, nous avons réévalué la criticité de chacun de ces modes. Cette réévaluation a été effectuée suite à des discussions avec les chefs de projet. En conséquence, nous avons reclassé les modes de défaillance en fonction de leur nouvelle criticité comme suit :

Tableau 11: *réorganisation les modes de défaillance en fonction de leur criticité*

0 Risques inacceptables	28≤ C ≤ 64
2 Risques indésirables	28≤ C ≤ 64
4 Risques modéré	9≤ C ≤27
0 Risques acceptables	1≤ C≤ 8

Source : élaborer par nous-même

Cette réévaluation nous permet d'avoir une vision actualisée de la criticité des modes de défaillance, ce qui facilite une meilleure priorisation et nous permet de prendre les mesures nécessaires pour les maîtriser de manière adéquate.

Evaluation de l'efficacité du plan d'actions :

Le tableau ci-dessous compare la classification des risques en fonction de leur criticité avant et après la mise en place du plan d'actions.

***Tableau 12**: analyse comparative des criticités.*

Criticité	Avant le plan d'action	Apres le plan d'action
Risque acceptable	0	0
Risque Modérer	2	4
Risque indésirable	4	2
Risque inacceptable	0	0

Source : élaborer par nous-même

En évaluant l'efficacité de nos plans d'action, nous avons réussi à réduire le nombre de risques indésirables de 4 à 2 en prenant des mesures immédiates pour les ramener à un niveau modéré, comme recommandé. Nous avons également constaté une augmentation des risques modérés, passant de 2 à 4. Cette progression est due à notre capacité accrue à contrôler et gérer ces risques grâce aux mesures préventives et correctives que nous avons mises en œuvre. Ces résultats montrent notre engagement et notre efficacité dans la réduction de la criticité des risques liés à nos plateformes digitales. Ils témoignent également de la valeur ajoutée de nos actions préventives et correctives, qui ont contribué à renforcer la sécurité et la fiabilité de nos systèmes numériques.

Section 2 : Discussion

La maîtrise des risques liés à la sécurité des plateformes digitales est devenue cruciale pour garantir la confiance des utilisateurs et la pérennité des entreprises (Smith et al., 2021). Pour cette étude, nous avons pris **DERMACARE** comme exemple afin d'analyser les mesures de sécurité nécessaires pour protéger les données sensibles des utilisateurs, en tenant compte des enseignements tirés de l'expérience de **DEVLOG**. Une matrice AMDEC a été élaborée pour identifier, évaluer, et proposer des actions concrètes de gestion des risques de sécurité spécifiques aux plateformes digitales.

L'analyse des données chez **DEVLOG**, obtenues grâce aux entretiens menés avec l'ensemble des employés, met en lumière l'importance accordée à la sécurité des plateformes digitales. Cette préoccupation centrale reflète l'engagement de l'entreprise envers le management des risques liés à la sécurité. Les termes liés aux aspects numériques et aux risques associés reviennent fréquemment, soulignant l'accent mis sur la compréhension et la gestion des vulnérabilités dans les environnements numériques. Ces résultats mettent en évidence l'importance de ces éléments pour améliorer la résilience et la fiabilité des systèmes numériques chez **DEVLOG**.

Lors de la mise en œuvre de notre démarche de management des risques, nous avons inclus des mesures correctives et préventives, telles que la sensibilisation et la formation du personnel contre les cyberattaques. Cette stratégie est en accord avec les conclusions des recherches menées par Hijji, M., Al-Saati, M., & Alzoubi, D. (2022), qui ont démontré l'efficacité du cadre CAT pour sensibiliser et former les employés aux menaces de cybersécurité, notamment celles basées sur l'ingénierie sociale.

Les conclusions de Jain, A. K., Sahoo, R., & Kaubiyal, P. (2021) démontrent la disponibilité de solutions pour protéger les utilisateurs. En analysant des études scientifiques, des rapports et des études de cas, leur étude qualitative avait pour but d'identifier les tendances et les problèmes de sécurité et de confidentialité dans ces réseaux. Ces résultats rejoignent nos propres résultats, soulignant la nécessité de mener une étude qualitative pour identifier les risques associés à la sécurité des plateformes numériques, afin de mieux comprendre ces risques potentiels et de mettre en place des solutions appropriées, qu'il s'agisse d'actions préventives ou correctives.

Lors de notre étude Dans le cadre de management des risques, il est crucial de mettre en œuvre des actions préventives pour réduire l'occurrence de risques potentiels. Cela s'aligne avec les résultats de Bourreau, M., & Perro, F. (2020) qui soulignent la nécessité d'une régulation préventive pour éviter des effets néfastes sur la concurrence et la société.

En utilisant l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC), nous avons pu identifier, évaluer et prioriser les risques potentiels dans notre processus de gestion de la sécurité des plateformes. Ces résultats confirment les affirmations de Joseph (1998) concernant l'efficacité de l'AMDEC pour anticiper les problèmes, mettre en place des mesures préventives et améliorer la qualité et la fiabilité des produits et des processus, ce qui contribue à renforcer la sécurité.

L'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC), définie par l'Association française de normalisation (Afnor), est une méthode inductive permettant d'analyser qualitativement et quantitativement la fiabilité ou la sécurité d'un système. Elle consiste à examiner de manière systématique les défaillances potentielles des systèmes, ainsi que leurs causes et leurs conséquences sur le fonctionnement global. En hiérarchisant ces défaillances en fonction de leur niveau de risque (leur criticité), des actions prioritaires sont déclenchées et suivies pour les traiter. Grâce à la réalisation de l'AMDEC, nous avons pu réaliser à la fois une analyse quantitative et qualitative de nos modes de défaillance, ce qui nous a permis de prioriser les risques et de réduire la probabilité d'occurrence des causes de défaillance. Nous avons également mis en place des mesures préventives pour atténuer les risques identifiés, conformément aux recommandations de l'Afnor.

Nous reconnaissons que l'application de l'outil AMDEC joue un rôle important dans la protection des plateformes en ligne contre les Cyber-menaces en garantissant la confidentialité. Cette constatation s'aligne avec des recherches antérieures d'Edu, Agoyi, & Agozie (2021) qui soulignent l'importance pour les institutions financières d'adopter des méthodes efficaces de gestion des risques, comme l'AMDEC et la FTOPSIS, pour sécuriser leurs plateformes en ligne et protéger leurs données et leurs systèmes. En utilisant l'AMDEC, nous avons pu identifier les risques liés à la cybersécurité tels que les vulnérabilités, les bugs et les fuites de données, et mettre en place des actions pour protéger les données des clients. Cela s'aligne avec les conclusions de Bays, Ruas Oliveira, Pilla Barcellos, Paschoal Gaspary et Roberto Mauro Madeira (2015) qui ont souligné l'importance de protéger les données et les services dans les environnements de virtualisation des réseaux. Ils ont également mis en évidence des risques tels que l'accès non autorisé, les attaques de type "DoS" et la divulgation de données sensibles, ainsi que la nécessité de prendre des mesures efficaces pour réduire ces risques.

Dans le cadre de notre étude, nous avons mené une analyse des risques spécifiques à la sécurité des plateformes digitales de **DERMACARE**, un client important de **DEVLOG**.

Notre démarche a permis d'identifier les risques potentiels auxquels **DERMACARE** pourrait être confronté, notamment les vulnérabilités des systèmes, les bugs logiciels et les fuites de données. Pour évaluer l'impact et la criticité de ces risques, nous avons pris en considération des critères tels que la fréquence, la gravité et la détection. Enfin, nous avons recommandé l'AMDEC comme l'outil le plus adapté pour répondre aux besoins spécifiques de sécurité des plateformes digitales de **DERMACARE**, en tenant compte de son partenariat avec **DEVLOG**. Ces résultats ont été essentiels pour proposer des solutions adaptées à **DERMACARE** afin de garantir la sécurité de sa plateforme digitale.

En conclusion, notre étude est cohérente avec les recherches antérieures mettant en avant l'importance de l'AMDEC pour une gestion efficace des risques. Elle souligne la nécessité de mettre en place des plans d'action correctifs et préventifs afin de corriger les risques identifiés et de minimiser leur impact potentiel.

CONCLUSION GENERALE

Dans cette étude, notre objectif principal était d'adresser la question de la sécurité des plateformes digitales chez **DEVLOG**, en mettant en lumière le cas de **DERMACARE**. Nous avons cherché à recommander un outil adapté pour protéger efficacement cette plateforme contre les menaces potentielles, tout en fournissant des conseils utiles aux responsables de la sécurité.

La recherche a été structurée en trois chapitres. Le premier a examiné la littérature pertinente, suivi d'un cadre conceptuel définissant les fondements de la gestion des risques en matière de sécurité des plateformes numériques. Le deuxième chapitre, divisé en deux sections, a détaillé l'approche méthodologique et présenté la méthodologie de recherche, basée sur une étude qualitative de recherche-action. La deuxième section a décrit **DEVLOG** et ses services. Enfin, le troisième chapitre a présenté les résultats de notre étude qualitative, accompagnés d'une discussion approfondie et de recommandations.

Les entretiens avec les employés de **DEVLOG** ont souligné l'importance de la sécurité des plateformes digitales, mettant en évidence la nécessité de comprendre et de gérer les vulnérabilités numériques.

Malgré les défis rencontrés, comme le manque d'un système documentaire, le manque de sensibilisation, le temps limité de l'étude, un petit échantillon de l'entreprise, la nouveauté du sujet avec le manque d'articles pertinents, la digitalisation et l'ouverture à la culture des plateformes, ainsi que notre position extérieure au domaine informatique, notre recherche montre que l'AMDEC est essentielle pour une gestion efficace des risques liés à la sécurité des plateformes digitales.

Malgré ces obstacles, notre étude offre une contribution significative en proposant des recommandations concrètes pour renforcer la sécurité de **DERMACARE** et des plateformes similaires chez **DEVLOG**. Les perspectives de cette recherche sont vastes et prometteuses.

Premièrement, il serait intéressant d'approfondir l'étude des risques liés à la sécurité des plateformes digitales dans d'autres entreprises, afin de comparer les pratiques et les outils utilisés. Cela permettrait de développer des recommandations plus générales et applicables à un large éventail d'organisations.

Deuxièmement, étant donné l'importance croissante de la digitalisation, il serait pertinent d'explorer davantage les implications de la sécurité des plateformes numériques dans d'autres secteurs d'activité, tels que la santé, l'éducation ou les services publics. Cette expansion de l'étude permettrait d'identifier les défis spécifiques à chaque domaine et de proposer des solutions adaptées.

Troisièmement, l'évolution constante des technologies et des menaces en matière de sécurité numérique nécessite une veille continue et des mises à jour régulières des pratiques et des outils de gestion des risques. Une perspective future de cette recherche pourrait donc consister à suivre l'application des recommandations formulées et à ajuster celles-ci en fonction des nouvelles tendances et des nouveaux défis rencontrés par les organisations.

Enfin, cette recherche pourrait également ouvrir la voie à des collaborations interdisciplinaires, en associant des experts en sécurité informatique, en gestion des risques et en digitalisation pour élaborer des approches intégrées et holistiques de la sécurité des plateformes numériques.

Perspectives, limites et obstacles de notre étude :

Malgré les défis rencontrés, tels que le manque d'un système documentaire, de sensibilisation, le temps limité de l'étude, un petit échantillon de l'entreprise, la nouveauté du sujet avec le manque d'articles pertinents, la digitalisation et l'ouverture à la culture des plateformes, ainsi que notre position extérieure au domaine informatique, notre recherche montre que l'AMDEC est essentielle pour une gestion efficace des risques liés à la sécurité des plateformes digitales. Notre étude offre des recommandations concrètes pour renforcer la sécurité de DERMACARE et des plateformes similaires chez DEVLOG, malgré ces obstacles. En termes de limites, l'étude se concentre sur DEVLOG, une entreprise algérienne de développement web, et sur la plateforme DERMACARE, son client, rendant les résultats et recommandations spécifiques au contexte algérien. Menée sur une période de trois mois, cette contrainte temporelle limite la profondeur et l'étendue des données analysées. S'appuyant sur les témoignages des quatre employés de DEVLOG, représentant 100 % de l'entreprise, la généralisation des résultats pourrait être restreinte. Focalisée sur la sécurité des plateformes digitales, l'étude exclut d'autres aspects pertinents de la cybersécurité tels que les infrastructures matérielles ou les réseaux de communication.

LA BIBLIOGRAPHIE

A., L. (1962). *Vocabulaire technique et critique de la philosophie* (9ème édition ed.). Paris: PUF.

Aissa, B. (2001). *Quelle méthodologie de recherche appropriée pour une construction de la recherche en gestion ?* .: Conférence de l'AIMS.

ALAOUI, M., & DHIBA, Y. (2022). *Le management des risques : cadre théorique* (Vols. Volume 3, Issue 1-1 (2022)). maroc: International Journal of Accounting, Finance, Auditing, Management and Economics. doi:https://doi.org/10.5281/zenodo.5910114

Ankit Kumar Jain, Ranjan Sahoo, S., & Kaubiyal, J. (2021). *Online social networks security and privacy: comprehensive review* (Vol. 7). India: Complex & Intelligent Systems. doi: 10.1007/s40747-021-00409-7

Aubin-Auger, I., Mercier, A., Baumann , L., Lehr-Drylewicz, A., Imbert, P., & Letriliart, L. (2008). *Introduction à la recherche qualitative.* .: Exercer : La revue française de médecine générale.

Aven, T., & Ortwin , R. (2010). *Risk Management and Governance: Concepts, Guidelines and Applications.* New York: springer. doi:10.1007/978-3-642-13926-0

Bahamid, R. A., & Doh, S. (2017). *A review of risk management process in construction projects of developing countries* (Vol. 271). Johor Bahru, Malysia : IOP Publishing Ltd. doi:10.1088/1757-899X/271/1/012042

Bays, L. R., Ruas Oliveira, r., Pilla Barcellos , M., Paschoal Gaspary, L., & Roberto Mauro Madeira, E. (2015). *Virtual Network Security: Threats, Countermeasures, and Challenges* (Vol. 6). Porto Alegre,Brazil: Journal of Internet Services and Applications. doi:10.1186/s13174-014-0015-z

Belvaux, B., & Notebaert, J. (2015). *Crosscanal et Omnicanal - la digitalisation de la relation client,.* Paris: Collection Management sup.

Benhayoun-Sadafiyine, L., & Boughzala, I. (2020). *Caractérisation des risques liés à l'utilisation des technologies digitales pour une transformation digitale réussie : Une étude exploratoire.* Marrakech: 25ème Conférence de l'Association Information & Management.

Bhathal, G. S., & singh, A. (2019). *Big Data: Hadoop framework vulnerabilities, security issues and attacks* (Vols. 1-2 (2019) 100002). Punjab, India: Array Journal. doi: https://doi.org/10.1016/j.array.2019.100002

Bourreau, M., & Perro, a. (2020). *Plateformes numériques : réguler avant qu'il ne soit trop tard* (Notes du conseil d'analyse économique 2020/6 (n° 60) ed.). paris: Éditions Conseil d'analyse économique. doi:10.3917/ncae.060.0001

BOUTIN, G. (2018). *L'entretien de recherche qualitatif.* Presses de l'Université du Québec.

Bressolles, G. (2016). *Le marketing digital* (2ème édition ed.). Paris: Dunod.

Camélia, B. (2018). *la gestion d'un contrat d'assurance incidence avec recours cas CAAR,.* université MOULOUD MAMMERI DE TIZI-OUZOU,: Mémoire de fin d'etude.

Chaimaa, A., & DOUARI , A. (2024). *Le management du risque à l'ère de l'émergence de l'intelligence* (Vol. 5 Numero 1). Maroc: Revue Française d'Economie et de Gestion.

Clavreull, H., & Albuquerque, S. (2020). *LA RECHERCHE-ACTION, UNE DÉMARCHE MÉTHODOLOGIQUE POUR RENFORCER LA PRATIQUE* (Vols. Volume 6, Numéro 1). France: CARAFE, la Communauté pour l'Avancement de la Recherche Appliquée Francophone en Ergothérapie. doi:10.13096/rfre.v6n1.172

Croom, S. (1999). *Research Methodology in operation management.* Eden Seminar, Brussels, February.: Cité par Ben Aissa, H. (2001). Quelle méthodologie de recherche appropriée pour une construction de la recherche en gestion ? Conférence de l'AIMS.

Desroche, H. (1982). *Les auteurs et les acteurs. La recherche coopérative comme recherche-action.* Archives de Sciences sociales et de la Coopération et du Développement,.

Edu, A. S., Agoyi , m., & Agozie, d. (2021). *Digital Security Vulnerabilities and Threats Implications for Financial Institutions Deploying Digital Technology Platforms and Applications* (PeerJ Computer Science ed., Vol. 7). Nicosia, Chypre.: PeerJ. doi:10.7717/peerj-cs.658

Edu, A. S., AGOYI, M., & AGOZIE, D. (2021). *Digital Security Vulnerabilities and Threats Implications for Financial Institutions Deploying Digital Technology Platforms and Applications* (PeerJ Computer Science ed., Vol. 7). Nicosia, à Chypre.: PeerJ. doi:10.7717/peerj-cs.658

Evans, D., & Schmalensee, R. (2008). *Markets with two-sidedplatforms.* Competition Law and policy : ABA Secton of Antitrust Law.

Flores, L. (2016). *Mesurer l'efficacité du marketing digital.* paris: Dunod.

Glenn, B. &. (2009). *Document Analysis as a Qualitative Research Method.* 9(2): Qualitative Research Journal. doi:https://10.3316/QRJ0902027

Hijji, M., & Alam, G. (2022). *Cybersecurity Awareness and Training for Online-Working-Based Employees.* Basel, Switzerland: sensors. doi:. https://doi.org/10.3390/s22228663

Hijji, M., & Gulzar , A. (2021). *Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees.* (s. akleylek, Ed.) Basel, Switzerland: PeerJ Comput. Sci. doi:10.7717/peerj-cs.658

HOPKIN, P. (2010). *Fundamentals of Risk Management Understanding, evaluating and implementing effective risk management.* londre: Kogan Page Limited.

Imbert, G. (2010). *L'entretien semi-derictif : à la frontière de la santé publique et de l'anthropologie.* 3(102): Recherche en soins infirmiers. doi:https://doi.org/10.3917/rsi.102.0023

J.-M, D. K., & Roegiers, X. (1996). *Méthodologie du recueil d'informations, Fondements des méthodes d'observations, dequestionnaires, d'interviews et d'études de documents.* (3 éme édition ed.). Paris: De Boeck Université.: Méthodes en sciences humaines.

Jean, P. (1957). *Encyclopédie de la pléiade.* Paris: PUF.

Jean-Louis, L. M. (2007). *Les épistémologies constructivistes* (3ème édition ed.). Que sais-je n° 2969 Paris 1995: PUF.

Joseph, K. (1998). *L'AMDEC.* Centre d'étude en qualité totale: école des hautes études commerciales, .

Kohn, L., & Christiaens, W. (2014). *Les méthodes de recherches qualitatives dans la recherche en soins de santé : Apports et croyances* (Éditions De Boeck Supérieur ed.). France: Reflets et perspectives de la vie économique, LIII, 2014/4. doi:10.3917/rpve.534.0067

Kremer, S., Ludovic, M., Didier , R., & Vincent, R. (mai 2019). *Cybersécurité.* France: Inria white book.

MATRADI, S., & MOUNIR, Y. (2023). *Évaluation de l'intégration de l'approche par les risques au vu de la norme ISO 9001-2015 : cas d'une grande entreprise* (Vols. Volume 4, Issue 6-2 (2023)). Agadir, Maroc: International Journal of Accounting, Finance, Auditing, Management and Economics. doi: https://doi.org/10.5281/zenodo.10436977

Mohamed Mouda, Djebabra, M., & Saadi, S. (2013). *Apport de l'AMDEC informationnelle pour l'amélioration des procédures industrielles.* Batna, Algérie: Laboratoire de Recherche en Prévention Industrielle.

Morin, A. (1985). *Critères de « scientificité » de la recherche-action.* Revue des sciences de l'éducation. doi:10.7202/900478ar

Morvan, A. (2013). *Recherche-action.* Paris : GIS Démocratie et Participation: Casillo (dir.), Dictionnaire critique et interdisciplinaire de la participation.

Perret, V., & Florence , A.-P. (2014). *Méthodes de recherche en management.* Dunod.

Sharma, J. K., & Kurien, D. (2017). *Perceived Risk in E-Commerce: A Demographic Perspective* (Issue 1 ed., Vol. Volume XXXIV). Perceived Risk in E-Commerce: A Demographic Perspective: Perceived Risk in E-Commerce: A Demographic Perspective.

Sheid, F., Vaillant, R., & De Montaigu, G. (2012). *Le marketing digital : Développer sa stratégie à l'ère numérique.* Paris: Editions Eyrolles.

Souria, H., BEAHIMI , M., & DJOUZI, Z. (2022). *Les facteurs influençant l'intention d'achat du consommateur sur les plateformes digitales* (Special edition sur la conférence scientifique internationale sur l'économie des plateformes digitales - opportunités et défis ed., Vol. 09). alger: la Revue Le Manager,.

Souria, H., BRAHIMI, M., & DJOUZI, Z. (2022). *Les facteurs influençant l'intention d'achat du consommateur sur les plateformes digitales* (Special edition sur la conférence scientifique internationale sur l'économie des plateformes digitales - opportunités et défis ed., Vol. 09). alger: la Revue Le Manager.

Thietart, R, A., & All, e. (2017). *Méthodes de recherche en management.* Dunod.

Thompson, M. P., Zimmerman, T., Mindar, D., & Taber, M. (2016). *Risk Terminology Primer: Basic Principles and a Glossary for the Wildland Fire Management Community.* fort collins, colorado: U.S. Department of Agriculture, Forest Service, Rocky Mountain Research Station à Fort Collins.

Van Campenhoudt, L., Quivy, R., & Marquet, J. (2006). *Manuel de recherche en sciences sociales.* Dunod, Éd.

Zina, H. S. (2022). *Les facteurs influençant l'intention d'achat du consommateur sur les plateformes digitales* (Special edition sur la conférence scientifique internationale sur l'économie des plateformes digitales - opportunités et défis ed., Vol. 09). alger : la Revue Le Manager.

Webographie :

https://www.kaspersky.fr/about/press-releases/2023_la-derniere-etude-de-kaspersky-revele-que-malgre-une-legere-baisse-en-2022-le-probleme-des-stalkerwares-reste-un-phenomene-mondial

https://cybersecuritymag.africa/creation-ecole-nationale-cybersecurite-algerie

http://www.ineris.fr/

https://www.nutcache.com/fr/blog/modele-roam-gestion-des-risques/

https://www.nutcache.com/fr/blog/modele-roam-gestion-des-risques/

https://www.nutcache.com/fr/blog/modele-roam-gestion-des-risques/

https://www.voxco.com/fr/blog/methodologie-de-recherche/

https://www.linternaute.fr/dictionnaire/fr/definition/epistemologie/

https://www.scribbr.fr/methodologie/entretien-recherche/

ANNEXES

ANNEXE-A : grille d'observation

Catégorie d'observation	Critère d'évaluation
Identification des risques	Identification des Violations de données personnelles. Identification des Attaques de phishing et d'ingénierie. Identification des Vulnérabilités de sécurité des applications.
L'évaluation des risques	L'identification de tous les actifs informatiques et les données sensibles sur leur plateformes digitales, ainsi que les vulnérabilités potentielles qui pourraient compromettre leurs sécurités. L'évaluation des menaces potentielles auxquelles les plateformes digitales pourraient être confrontées, telles que les cyberattaques, les violations de données ou les erreurs humaines. Estimation de l'impact : estimons l'impact financier, opérationnel et réputationnel que chaque menace pourrait avoir sur l'organisation en cas d'exploitation réussie. Évaluation de la probabilité : l'évaluation de la probabilité que chaque menace se matérialise, en tenant compte de facteurs tels que la fréquence des attaques similaires dans le secteur, les mesures de sécurité actuellement en place et les tendances du paysage des menaces.
Mesures de prévention et de protection	Tableau de bord de sécurité : l'utilisation des tableaux de bord de sécurité pour surveiller en temps réel l'état de sécurité de plateformes digitales, en affichant des indicateurs clés de performance (KPI) tels que le nombre d'incidents de sécurité, les tentatives d'attaques détectées et les niveaux de conformité aux Normes de sécurité. Gestion des identités et des accès (IAM) : l'utilisation des solutions IAM pour contrôler et gérer les droits d'accès des utilisateurs à nos plateformes digitales, en veillant à ce que seules les personnes autorisées puissent accéder aux ressources sensibles. Veillant à ce que seules les personnes autorisées puissent accéder aux ressources.
Personnel et formation	Offrir une formation en sécurité informatique à Leur personnel pour les sensibiliser aux meilleures pratiques de sécurité, telles que la création de mots de passe forts, la détection des attaques de phishing et la protection des données sensibles.
Gestion des incidents de sécurité	Établir des procédures pour gérer leurs incidents de sécurité de manière efficace, y compris la notification des parties prenantes concernées, la collecte d'informations sur l'incident, la restauration des systèmes affectés et l'analyse post-incident pour prévenir de futures occurrences.
Communication et sensibilisation	L'utilisons des canaux de communication internes tels que les e-mails, les bulletins d'information et les affichages pour diffuser des informations sur les dernières menaces de sécurité, les mises à jour de politique et les conseils pratiques pour rester en sécurité en ligne.

Suivie et amélioration	Effectuer des évaluations régulières des risques : la Réalisation des évaluations régulières des risques pour identifier les menaces potentielles et les vulnérabilités spécifiques au secteur d'activité, en tenant compte des dernières tendances et des meilleures pratiques en matière de sécurité. Renforcer la sécurité des applications : la mise en place des mesures de sécurité robustes dès la conception et tout au long du cycle de vie des applications, avec l'utilisation des pratiques telles que le développement sécurisé, la gestion des vulnérabilités et les tests de sécurité réguliers.

ANNEXE B - GUIDE D'ENTRETIEN.

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
École Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي
المدرسة الوطنية العليا للمناجمنت
القليعة

Guide d'entretien

Nous sommes OUALI Racha et AKHROUF Aicha, étudiantes en master 2 en entrepreneuriat et management de projet a l'école nationale supérieure de management.
Dans le but d'enrichir notre recherche qui porte sur « la maîtrise des risques liés a la sécurité des plates-formes digitales », nous aimerions vous poser quelques questions, mais avant de commencer, nous tenons à vous signaler les éléments suivants :
Acceptez-vous que cet entretient soit enregistré, sachant que vos réponses seront utilisées uniquement dans un cadre scientifique pour notre de recherche et ne seront partagés avec personne d'autre.

Questions générales :

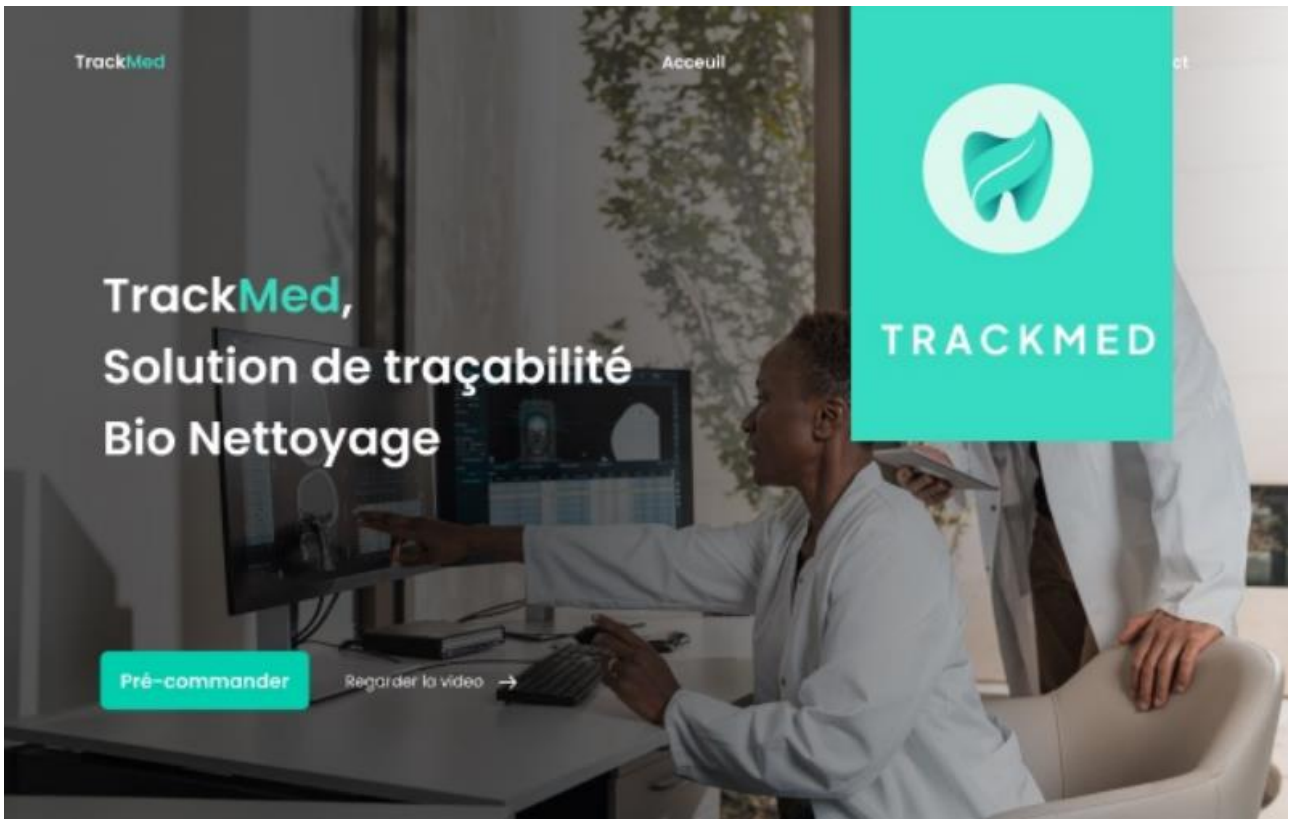
- Pourriez-vous vous présenter ?
- Parlez-nous de votre parcours académique et professionnel
- Pourriez-vous décrire votre rôle et vos responsabilités au sein de votre organisation, et nous présenter brièvement cette dernière ?

Questions sur les pratiques de la gestion des risques :

- Pourriez-vous identifier les principaux risques auxquels les plates-formes digitales sont exposées en termes de sécurité ?
- Comment votre organisation évalue-elle et classe-t-elle les risques liés à la sécurité des plateformes digitales ?
- Quels outils et méthodes utilisez-vous pour évaluer et gérer les risques de sécurité des plateformes digitales ?
- Quels défis rencontrez-vous dans la mise en place de mesure de sécurité pour prévenir les risques liés aux plateformes digitales ?
- Comment votre entreprise s'adapte-t-elle aux tendances émergentes en matière de sécurité des plateformes digitales pour améliorer sa gestion des risques ?
- Comment réagissez-vous en cas de violation de sécurité ou d'incident cybernétique ?
- Comment sensibilisez-vous le personnel aux pratiques de sécurité et à la gestion des risques liés à la sécurité des plates-formes digitales ?
- Quelles sont vos recommandations pour renforcer la sécurité des plateformes digitales et améliorer la gestion des risques dans votre secteur d'activité ?

Nous vous remercions sincèrement pour avoir pris le temps de partager vos précieux conseils et recommandations. N'hésitez pas a ajouter toute autre point que vous jugez pertinent pour enrichir notre compréhension.

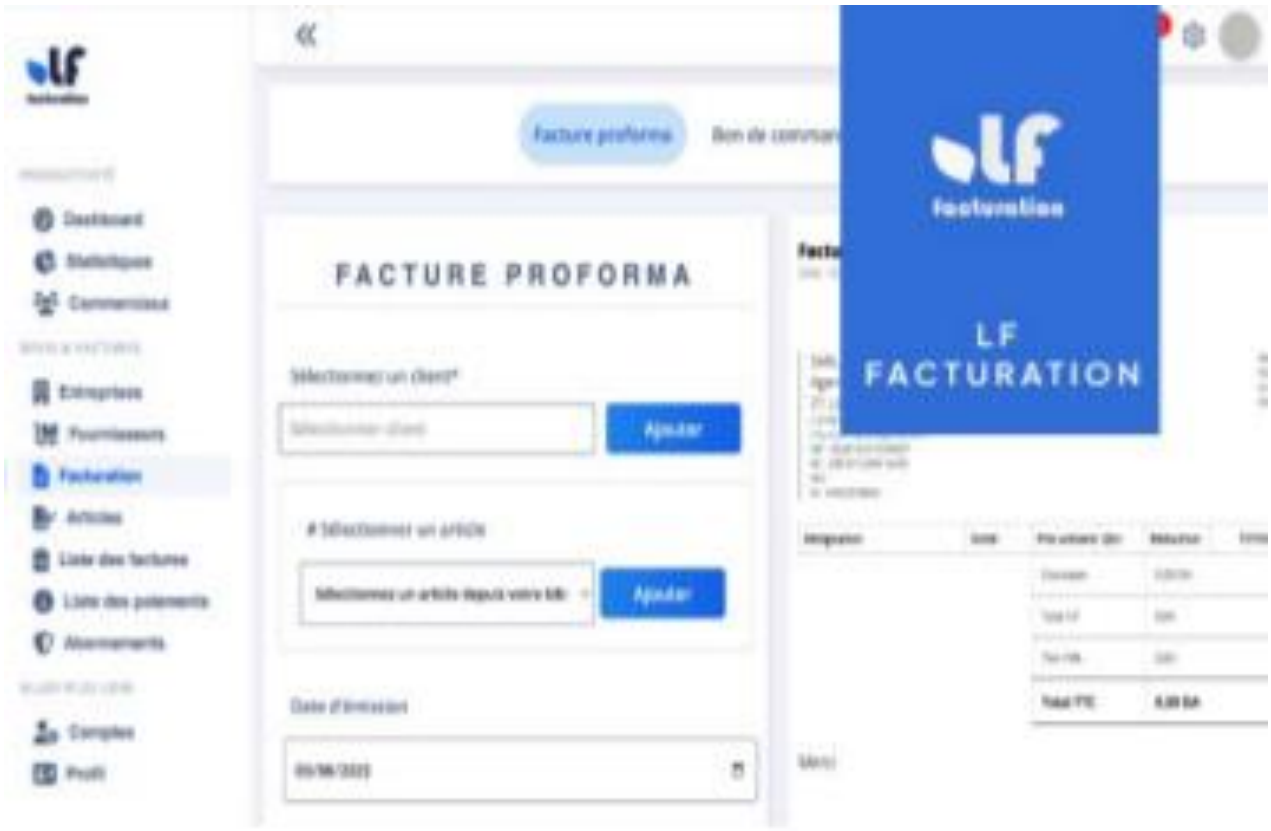
ANNEXE C - TRACKMED.



ANNEXE D – AACDHB.

ANNEXE E – AIC.

ANNEXE F – LF.



ANNEXE G – MENUCRAFT.

ANNEXE H – TABLEAU DES VERBATIMS

Thème		Réponses des interviewé
Risque		*« Les plateformes digitales doivent faire face à pas mal de risques niveau sécurité. D'abord, t'as les violations de données perso, où des infos sensibles peuvent se faire pirater. Ensuite, y'a les attaques de phishing et d'ingénierie sociale, où les gens se font avoir et filent leurs infos confidentielles. Les applis ont souvent des failles de sécurité que les hackers adorent exploiter. Les attaques DDoS, c'est quand des mecs inondent une plateforme de trafic pour la rendre inaccessible. Et puis, faut faire gaffe aux fuites de données via des partenaires ou des tiers, parce que même si ta sécu est béton, les infos partagées peuvent se retrouver vulnérables ». (Employé 01)* *« Les principales menaces pour la sécurité des plates-formes digitales incluent les cyberattaques, les vulnérabilités logicielles, les accès non autorisés, les fuites de données, l'ingénierie sociale, les insuffisances des mesures de sécurité et les menaces internes » (Employé 03).*
Management des risques	Évaluation et classification des risques	*« Nous évaluons les risques liés à la sécurité des plateformes digitales en effectuant des analyses de vulnérabilité, des audits de sécurité et des évaluations des menaces. En fonction de ces évaluations, nous classons les risques en fonction de leur gravité et de leur probabilité d'occurrence ». (Employé 03)*
	Les outils	*« Alors, pour sécuriser nos plateformes, on a plusieurs trucs. D'abord, un tableau de bord de sécurité qui surveille en temps réel les incidents et tentatives d'attaques. Ensuite, on utilise des solutions IAM pour contrôler les accès et s'assurer que seules les personnes autorisées accèdent aux infos sensibles. On fait aussi de la formation en sécurité pour notre staff, pour qu'ils sachent créer des mots de passe solides, repérer le phishing et protéger les données. Et enfin, on a des procédures pour gérer les incidents de sécurité, comme prévenir les parties concernées, réparer les systèmes et analyser pour éviter que ça se reproduise ». (Employé 01)*
	Sensibilisation	*« Nous organisons régulièrement des séances de sensibilisation sur la sécurité informatique, mettons en place des programmes de formation en ligne et envoyons des rappels périodiques sur les meilleures pratiques en matière de sécurité. De plus, nous intégrons des éléments de sécurité dans les processus de formation et d'intégration des nouveaux employés ». (Employé 02)*

ANNEXE I – AMDEC.

Activité	Contrainte	Défaillance	Cause	Effet	G	P	D	C	Plan d'action	G'	P'	D'	C'	Responsa-ble	Observation
Sécurité interne	Comportement humain	Employés malveillants ou négligents	Négligence du personnel, personnel non formé et non sensibilisé	Interruption des services, mauvaise gestion des accès, perte de confiance des clients	5	4	3	60	Formation en sécurité informatique, communications internes, renforcement des clauses contractuelles avec accès limités. contrats spécifiques pour prévenir la divulgation d'informations sensibles	5	2	3	30	Chef de projet	Augmentation de la sensibilisation et des compétences Renforcement de la confiance des clients

Gestion des données personnelles et sensibles.	Les hackers font évoluer leurs cyberattaques très rapidement.	Violation. Fuite de données. Vulnérabilité.	Failles de sécurité. erreurs de Configuration. Mises à jour non appliquées.	Fraude et vol d'identité. Violation de la vie privée. Perte de données. Perturbation des services. Impact sur les opérations commerciales.	5	2	4	40	Gestion des identités et des accès : utilisation de solutions IAM, authentification à deux facteurs	5	2	3	30	Développeur web	Réduction des incidents de sécurité
Gestion budgétaire	Client à budget limité	Incapacité à payer les abonnements de sécurité	Budget insuffisant, tarif de l'abonnement dépasse le budget du client	Moins de ressources pour la surveillance et la détection des menaces, retard dans la mise à jour des systèmes, vulnérabilité de la plateforme	5	4	2	40	Optimisation des ressources existantes, clarification des priorités et des attentes du client	5	2	2	20	Developpeur web	Identification et élimination des coûts superflus

Protection des plateformes	Les cybermenaces évoluent constamment	Attaques de phishing, ransomware et malwares	Pratiques de sécurité inadéquates, politiques de mot de passe faibles, mauvaise configuration	Perte de confidentialité, vol d'informations personnelles et financières, dysfonctionnement de la plateforme	4	1	5	20	Sensibilisation continue des utilisateurs sur les bonnes pratiques de sécurité	4	1	5	20	Chef de projet	Moins de dysfonctionnements et interruptions de service
Conformité réglementaire	Évolutions constantes des réglementations	Risque judiciaire	Apparition de nouvelles lois	Sanctions financières, poursuites judiciaires	3	3	3	27	Abonnement à des entreprises spécialisées dans la veille réglementaire	3	2	2	12	Entreprise de sous-traitance	Amélioration de la conformité réglementaire
Développement de logiciels	Défis de programmation : script complexe nécessitant des modifications	Rencontre de bugs	Erreurs de programmation	Altération ou suppression de données, attaques potentielles, mise en œuvre de mesures de sécurité plus difficile	5	3	1	15	Surveillance des alertes et notifications des services d'hébergement, mises à jour régulières des serveurs	5	2	1	10	Chef de projet	Réduction du nombre de bugs