الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MEMOIRE DE FIN D'ETUDES

En vue de l'obtention d'un Master professionnel en

Management Stratégique et Système d'Information

L'intégration de l'intelligence artificielle dans la gestion des risques des systèmes d'information

Cas : Entreprise Nationale des grands travaux pétrolier

(ENGTP)

Élaboré par :

LARABI Ikram

BELATRECHE Inas

Encadré par :

Dr. NACER Loubna

Co-Encadré par :

Dr. SEGHIRI Narimene

Année Universitaire 2024/2025

Résumé

Ce travail de recherche analyse l'intégration de l'intelligence artificielle (IA) dans la gestion des risques des systèmes d'information (SI), avec une application au sein de l'entreprise ENGTP. Dans un contexte où la sécurité des SI représente un enjeu stratégique, l'étude vise à évaluer comment l'IA peut optimiser les pratiques actuelles. Une approche qualitative a été adoptée, reposant sur des entretiens semi-directifs avec trois experts du domaine. Les résultats révèlent que si l'ENGTP applique une méthode structurée fondée sur des référentiels reconnus, les pratiques restent largement manuelles. L'intégration de l'IA est perçue comme un levier pour améliorer la détection des menaces, automatiser les réponses et renforcer la résilience numérique. Ce mémoire propose ainsi des recommandations concrètes pour une gestion proactive et intelligente des risques SI.

Mots clés : Intelligence artificielle, gestion des risques, systèmes d'information, cybersécurité, ENGTP**.**

Abstract

This research work analyzes the integration of artificial intelligence (AI) into information systems (IS) risk management, with a focus on its application within the ENGTP company. In a context where IS security is a strategic concern; the study aims to assess how AI can optimize current risk management practices. A qualitative approach was adopted, based on semi-structured interviews with three IT experts. The findings show that while ENGTP applies a structured method based on recognized frameworks, most practices remain manual. AI is perceived as a key tool to enhance threat detection, automate responses, and strengthen digital resilience. The study provides concrete recommendations for a more proactive and intelligent approach to IS risk management.

Keywords : Artificial intelligence, risk management, information systems, cybersecurity, ENGTP**.**

ملخص

يحلّل هذا العمل البحثي إدماج الذكاء الاصطناعي في إدارة مخاطر أنظمة المعلومات، مع تطبيق عملي داخل المؤسسة الوطنية للأشغال البترولية الكبرى في ظل اعتبار أمن أنظمة المعلومات قضية استراتيجية. هدفت هذه الدراسة إلى تقييم كيفية مساهمة الذكاء الاصطناعي في تحسين الممارسات الحالية. وقد اعتمدنا على منهج نوعي من خلال مقابلات شبه موجهة مع ثلاثة خبراء في المجال. أظهرت النتائج أن الشركة تعتمد منهجاً منظماً مبنياً على معايير معترف بها، إلا أن التطبيق لا يزال يدوياً في الغالب. يُنظر إلى الذكاء الاصطناعي كأداة فعالة لتعزيز الكشف عن التهديدات، وأتمتة الاستجابات، وتعزيز المرونة الرقمية. ويقترح هذا البحث توصيات عملية لاعتماد إدارة ذكية واستباقية لمخاطر أنظمة المعلومات.

الكلمات المفتاحية :الذكاء الاصطناعي، إدارة المخاطر، أنظمة المعلومات، الأمن السيبراني، المؤسسة الوطنية للأشغال البترولية الكبرى.

Remerciement

Je tiens à exprimer ma plus profonde gratitude à celles et ceux qui ont été les piliers de ma force et les sources constantes de mon inspiration tout au long de ce parcours.

À mon cher père, en reconnaissance de ses efforts et de ses sacrifices inestimables. Rien n'a jamais freiné sa volonté de me voir réussir. Merci d'avoir toujours cru en moi et de m'avoir portée, pas à pas, vers mes objectifs.

À ma chère maman, lumière de mon chemin, source intarissable d'amour et de générosité. Merci pour ta tendresse, ton soutien et ton amour inconditionnel, qui m'ont accompagnée à chaque étape de cette aventure.

À mes sœurs adorées – Amina, Hind et Habiba, qui ont partagé avec moi les joies comme les épreuves, qui ont été mon refuge, mes confidentes et mon soutien indéfectible. Merci de m'avoir entourée d'un amour aussi sincère que précieux.

À ma binôme Inès, ainsi qu'à ma Hibouche et Inaam, que le destin a placées sur mon chemin et qui sont devenues bien plus que de simples amies. Vous êtes mes sources de bienveillance et ma force. Merci pour votre précieuse complicité.

À mes amies proches et à mes cousines adorées, en souvenir des meilleurs moments qu'on a partagé ensemble, chacune d'entre vous est chères à mon cœur.

À madame Nacer Loubna et madame Seghiri Narimene, mes encadrantes, je tiens à adresser mes sincères remerciements pour leur accompagnement, et la qualité de leurs conseils.

Enfin, à toutes celles et ceux qui m'ont entourée d'amour et de soutien, par leurs mots, leurs gestes ou simplement leur présence : l'ensemble de ma famille et mes connaissances.

Merci à vous toutes et tous. Ce travail est aussi le vôtre.

Larabi Ikram

Remercîment

Je tiens à exprimer ma plus profonde gratitude à celles et ceux qui ont été les piliers de ma force et les sources constantes de mon inspiration tout au long de ce parcours.

À mes grands-parents, pour leur amour inestimable, leurs prières sincères et leur sagesse. Leur présence rassurante et leurs valeurs ont toujours été une boussole dans ma vie.

À mon cher père, que Dieu lui accorde Sa miséricorde. Ton absence me pèse chaque jour, mais ton souvenir m'accompagne et me donne la force d'avancer. Ce mémoire t'est dédié, papa, avec tout mon amour.

À ma merveilleuse maman, ma lumière, mon roc, ma meilleure alliée. Tu incarnes la force, la tendresse et le courage. Tu as été à la fois mère et père, toujours là, aimante et présente. Je t'aime profondément et je te dédie chaque réussite.

À mon frère Anis, pour ton soutien indéfectible, ta présence discrète mais rassurante, et ta fidélité sans faille. Merci d'être toujours là.

À ma binôme Ikram, pour ta patience, ton sérieux, ta complicité et notre belle collaboration tout au long de ce travail.

À Inaam, ma meilleure amie, ma sœur de cœur. Merci pour ta loyauté, ta lumière, ton écoute et ta force qui m'ont aidée à traverser les hauts comme les bas. Ta présence est un cadeau précieux.

À Hiba, Malak et Lina, mes amies de cœur. Merci pour vos sourires, votre soutien et votre présence constante dans cette aventure.

À ma tante Amina, qui est bien plus qu'une tante : une sœur de l'âme, une confidente, une seconde maman. Ton amour, ton soutien et ta présence m'ont donné une force immense.

À mes autres tantes, mes oncles, mes cousines et cousins, pour leur amour, leurs encouragements et leur tendresse qui ont embelli ce parcours.

Enfin, à toutes celles et ceux qui, par leurs gestes, leurs paroles ou simplement leur présence, ont contribué à faire de ce chemin une aventure exceptionnelle : merci infiniment. Ce mémoire est aussi le vôtre.

Belatreche Inas

Table des matières

Résumé ..... **I**
Remerciement ..... **III**
Table des matières ..... **V**
INTRODUCTION GÉNÉRALE 1
Objectifs de la Recherche 3
Méthodologie 3
Problématique 3
Pertinence de la Recherche 4
Structure du Mémoire 4
CHAPITRE I : REVUE DE LITTERATURE ET CADRE CONCEPTUEL **5**
Section 01 : Revue de littérature 6
1.1 Approche méthodologique de la gestion des risques liés à l'intelligence artificielle : 6
1.2 L'intelligence artificielle dans la gestion des risques des systèmes d'information : ... 8
1.3 Comparaison entre l'étude actuelle et les travaux antérieurs 12
Section 02 : Cadre conceptuel 14
1. La gestion des risques 14
1.1 Le concept du risque 14
1.2 Définition et portée de la gestion des risques 14
1.3 Le cadre de gestion des risques 15
1.4 Importance de gestion des risques 16
1.5 Les étapes du processus de gestion des risques 16
1.6 Typologie des risques 20
1.7 Approche standardisée de la gestion des risques 22
2. Gestion de Risque des systèmes d'information 23
2.1 Définitions et typologies des risques de système d'information 23
2.2 Processus et classification des risques liés aux systèmes d'information 26
2.3 Enjeux et défis de la sécurité des systèmes d'information (SI) 30
2.4 Normes et référentiels dans la gestion des risques SI 31
2.5 Méthodes et Outils d'Analyse des Risques SI 33
2.6 Les critères de choix de méthode de gestion des risques SI 42
3. Intelligence Artificielle appliquée à la Gestion des Risques SI 43
3.1 Définition et technologies pertinentes de l'Intelligence Artificielle 43
3.2 Apports potentiels de l'intelligence artificielle dans l'analyse, la détection et la prédiction des risques liés aux systèmes d'information 45

3.3 Limites et défis d'intégration de l'IA dans la gestion des risques des SI 46
CHAPITRE II : CADRE METHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL 49
Section 01 : cadre méthodologique 50
1.1 Choix du thème 50
1.2 Choix de l'entreprise 51
1.3 Méthode de recherche 51
1.4 Méthodes et techniques de récolte des données 51
1.5 La sélection des interviewés 54
1.6 La construction du guide d'entretien 55
1.7 Le traitement des données 57
Section 02 : Choix de l'organisme d'accueil ……..……..58
1. Présentation de l'entreprise 58
1.1 Historique 59
1.2 Missions de « GTP » 59
1.3 Objectifs de GTP 60
1.4 Activités de l'entreprise 60
1.5 Organigramme de l'entreprise ENGTP 63
1.6 Ressources et politique de l'entreprise 64
1.7 Le système de management intégré QHSE de l'ENGTP 66
1.8 Notoriété de GTP 67
2. ENGTP et la gestion des risques de système d'information : 68
2.1 Contexte du stage 68
2.2 Présentation département d'accueil DSI 69
2.3 État de la sécurité de l'information au sein de l'entreprise 70
2.4 Menaces de sécurité auxquelles fait face l'entreprise 71
2.5 Moyens de protection appliqués par l'entreprise 72
CHAPITRE III : RESULTATS ET DISCUSSIONS 74
Section 01 : Présentation des résultats 75
1. Résultats des entretiens 75
1.1 Analyse descriptive : 75
1.2 Analyse textuelle de données 77
1.2.4 L'analyse thématique : 82
2 La gestion des risques au sein de l'ENGTP : 86
2.1 Processus de gestion des risques SI au sein de l'ENGTP : 86

2.2 Perspective future de la contribution de l'IA à la gestion des risques SI au sein de l'ENGTP : 89
Section 02 : Discussion 93
1. Analyse critique des résultats 93
2. Convergences et divergences avec la littérature 95
CONCLUSION GÉNÉRALE 98
Recommandations stratégiques 99
Limites de la recherche 101
Perspectives 102
BIBLIOGRAPHIE 103
ANNEXES 104

Liste des figures

Figure 1 Processus de gestion des risques 20
Figure 2 les étapes de stratégie de gestion des risques 29
Figure 3 Facteurs externes et interne de gestion des risques 30
Figure 4 la démarche de la méthode EBIOS 36
Figure 5 la logique de construction d'un scénario de risque 37
Figure 6 la démarche de MEHARI 39
Figure 7 La logique de traitement des risques MEHARI 40
Figure 8 phases de la méthode OCTAVE 42
Figure 9 Les techniques de collecte des données 52
Figure 10 Organigramme de l'entreprise ENGTP 64
Figure 11 Architecture Client / Serveur à GTP 66
Figure 12 Structure organisationnelle de la Direction des Systèmes d'Information (DSI) de l'ENGTP 70
Figure 13 information sur les interviewé 76
Figure 14 nuage des mots 78
Figure 15 Synapsie sur le mot "IA" 80
Figure 16 Requête corrélation sur le mot "risque" 81
Figure 17 la matrice des risques de système d'information 88
Figure 18 Apports et risques de l'IA appliquée à la gestion des risques des systèmes d'information 92

Liste des tableaux

Tableau 1 Information sur interviewé 55
Tableau 2 Coefficient de corrélation entre les entretiens 79

Liste des annexes

Annexe 1 matrice d'analyse thématique - partie A – 106
Annexe 2 matrice d'analyse thématique - partie B - 112
Annexe 3 matrice d'analyse thématique - partie c - 115
Annexe 4 matrice d'analyse thématique - partie D - 121
Annexe 5 Fiche d'évaluation du risque brut 122
Annexe 6 Mesures d'atténuation prévues à horizon fin 2024 122
Annexe 7 Évaluation du risque résiduel et acceptabilité 123
Annexe 8 page d'accueil de leurs Site Web 123

Liste des abréviations

IA Intelligence Artificielle

SI Systèmes d'Information

ENGTP Entreprise Nationale des Grands Travaux Pétroliers

RSSI Responsable de la Sécurité des Systèmes d'Information

PMSI Responsable des Projets Systèmes d'Information

DBA Administrateur de Bases de Données

ISMS Information Security Management System (Système de Management de la Sécurité de l'Information)

ISO International Organization for Standardization

IEC International Electrotechnical Commission

ISO/IEC 27001 Norme de management de la sécurité de l'information

ISO/IEC 27005 Norme de gestion des risques liés à la sécurité de l'information

ISO 31000 Norme de management du risque

PDCA Plan-Do-Check-Act (Cycle d'amélioration continue)

RGPD Règlement Général sur la Protection des Données

SMSI Système de Management de la Sécurité de l'Information

MEHARI Méthode Harmonisée d'Analyse des Risques

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité

OCTAVE Operationally Critical Threat, Asset, and Vulnerability Evaluation

CLUSIF Club de la Sécurité de l'Information Français

NLP Natural Language Processing (Traitement Automatique du Langage Naturel)

AI RMF AI Risk Management Framework

NIST National Institute of Standards and Technology

PRA Plan de Reprise d'Activité

PCA Plan de Continuité d'Activité

QHSE Qualité, Hygiène, Sécurité, Environnement

VPN Virtual Private Network

IoT Internet of Things (Internet des Objets)

APT Advanced Persistent Threat

SGBD Système de Gestion de Base de Données

KRI Key Risk Indicator (Indicateur Clé de Risque)

INTRODUCTION GÉNÉRALE

Dans un monde où la digitalisation s'intensifie, les systèmes d'information (SI) jouent un rôle central dans la gestion des données, la prise de décision et le bon fonctionnement des entreprises. Cependant, cette dépendance aux technologies numériques expose les organisations à de nombreux risques : cyberattaques, pannes techniques, erreurs humaines ou encore défaillances organisationnelles. La gestion des risques liés aux SI est ainsi devenue un enjeu majeur, nécessitant des approches toujours plus efficaces pour protéger les infrastructures critiques et garantir la continuité des activités.

Dans ce contexte, l'intelligence artificielle (IA) se positionne comme une technologie prometteuse pour optimiser la gestion des risques SI. Grâce à ses capacités d'analyse avancée, d'apprentissage automatique et de détection en temps réel des menaces, l'IA permet aux entreprises d'anticiper et d'atténuer plus efficacement les risques informatiques. Elle offre également des outils d'automatisation qui facilitent la surveillance des incidents de sécurité et la prise de décision en matière de gestion des risques.

Cette évolution technologique est particulièrement pertinente dans les secteurs complexes, à l'échelle mondiale, de nombreuses entreprises adoptent déjà des outils d'intelligence artificielle pour renforcer la résilience de leurs infrastructures et améliorer leur prise de décision en matière de gestion des risques.

Dans le secteur pétrolier, l'IA est utilisée pour prédire des défaillances d'équipements, détecter des anomalies en temps réel, et optimiser la maintenance des systèmes critiques.

Malgré son potentiel, l'IA reste encore peu exploitée dans ce secteur, où les infrastructures critiques nécessitent une protection renforcée. Elle soulève également des défis, notamment en termes de coût, d'intégration avec les infrastructures existantes, et d'acceptation organisationnelle.

Ces obstacles n'empêchent pas comme même l'intérêt croissant pour ces technologies, qui incite les entreprises à rechercher des solutions adaptées à leurs besoins spécifiques.

Cependant, L'ENGTP, acteur majeur dans ce domaine en Algérie, fait face à des enjeux stratégiques liés à la sécurisation de ses systèmes d'information. Or, l'absence d'une intégration structurée de l'IA dans ses pratiques de gestion des risques.

Objectifs de la Recherche

L'objectif principal de cette étude est d'analyser l'apport potentiel de l'IA dans l'optimisation de la gestion des risques SI et d'examiner les conditions organisationnelles qui facilitent son adoption. Plus spécifiquement, ce mémoire vise à :

- Évaluer l'état actuel de la gestion des risques SI à l'ENGTP afin d'identifier les failles et les points d'amélioration.
- Identifier les limites des méthodes traditionnelles et les défis auxquels l'entreprise fait face dans la gestion des risques.
- Analyser les opportunités offertes par l'intelligence artificielle dans la détection, la prévention et la gestion des risques SI.

Méthodologie

Ce mémoire repose sur une approche qualitative, qui permet de mieux comprendre les enjeux, les défis et les opportunités liés à l'intégration de l'IA dans la gestion des risques SI. La méthodologie adoptée comprend plusieurs étapes :

- Revue de littérature : Analyse des concepts clés liés à la gestion des risques SI et aux apports de l'IA dans ce domaine.
- Entretiens semi-directifs : Recueil de témoignages et d'avis d'experts en cybersécurité et en gestion des risques IT.
- Étude de cas : Analyse de l'environnement de l'ENGTP et de ses pratiques actuelles en matière de gestion des risques SI.

Problématique

Malgré l'émergence de technologies avancées, de nombreuses entreprises industrielles, dont ENGTP, tardent à intégrer pleinement l'intelligence artificielle (IA) dans leurs pratiques de gestion des risques des systèmes d'information (SI). Ce constat soulève une question centrale :

Comment l'intégration de l'intelligence artificielle peut-elle optimiser le processus de gestion des risques SI au sein de l'ENGTP ?

Pour y répondre, nous avons formulé les sous-questions suivantes :

- Quels outils d'IA pourraient être adaptés à l'environnement d'ENGTP ?
- Quels sont les freins organisationnels, humains ou techniques à leur implémentation ?

Pertinence de la Recherche

L'intérêt de cette recherche réside dans le besoin croissant des entreprises d'adopter des stratégies efficaces pour protéger leurs systèmes d'information face aux menaces informatiques de plus en plus sophistiquées. Dans le secteur pétrolier, où la cybersécurité est un enjeu critique, il devient impératif d'explorer des solutions innovantes comme l'IA pour renforcer la résilience et la sécurité des infrastructures numériques.

L'ENGTP, en tant qu'acteur majeur du secteur, pourrait bénéficier de l'intégration de l'IA pour améliorer ses mécanismes de gestion des risques et garantir une protection optimale de ses données et systèmes. Cette étude apporte ainsi une contribution pertinente en examinant comment l'IA peut être appliquée pour optimiser la gestion des risques SI.

Structure du Mémoire

Ce mémoire est structuré en trois chapitres :

- Chapitre 1 : Revue de littérature et cadre conceptuel Présentation des notions clés sur la gestion des risques SI, l'intelligence artificielle et les méthodes d'analyse des risques.
- Chapitre 2 : Cadre méthodologique et contexte organisationnel Explication de la méthodologie adoptée et présentation de l'environnement de l'ENGTP.
- Chapitre 3 : Résultats et discussions Analyse des données collectées et exploration des opportunités et défis liés à l'IA dans la gestion des risques SI.

CHAPITRE I : REVUE DE LITTERATURE ET CADRE CONCEPTUEL

Ce chapitre propose tout d'abord de revisiter de façon critique la littérature existante sur la gestion des risques des systèmes d'information et le potentiel bénéfique de l'intelligence artificielle.

Section 01 : Revue de littérature

Cette section présente une synthèse des principales recherches et travaux antérieurs et études précédentes concernant la gestion des risques des systèmes d'information et l'utilisation de l'intelligence artificielle.

1.1 Approche méthodologique de la gestion des risques liés à l'intelligence artificielle :

Gestion des Risques et Sécurité Informatique

Selon (Al Kurdi, 2024), dans leur article "Cybersecurity and Risk Management Practices and Their Impact on Sustainable Green Operations", la cybersécurité et la gestion des risques sont des déterminants majeurs pour atteindre les objectifs de durabilité opérationnelle. L'étude vise à explorer comment la cybersécurité et la gestion des risques influent sur les pratiques vertes des entreprises de sécurité.

Les auteurs adoptent une méthodologie quantitative, allant du développement d'une étude empirique autour de 77 entreprises de sécurité situées à Sharjah (Émirats arabes unis) et échantillonnées en grappes, à l'évaluation de la cybersécurité sur la continuité d'exploitation et sur la performance environnementale.

Les résultats d'enquête montrent une relation positive significative entre l'implémentation de politiques de cybersécurité (protection des données, contrôle des accès privilégiés et formation des employés) et la réduction des risques opérationnels liés aux cybermenaces, permettant ainsi la continuité des services et une meilleure efficacité écologique.

Les auteurs mentionnent une limite géographique et sectorielle à leur recherche, suggérant d'élargir dans des recherches futures à d'autres secteurs d'activité tels que le secteur industriel ou le secteur des transports.

Normes Internationales pour la Gestion des Risques dans les Systèmes d'Information

Selon (Filali, 2022), dans son article « La norme ISO/IEC 27001 : un levier stratégique pour la sécurité de l'information », la norme internationale ISO/IEC 27001 constitue un cadre structurant pour le renforcement de la sécurité des systèmes d'information. L'objectif

de l'étude est de démontrer comment l'adoption de cette norme contribue à la protection des données, à la conformité réglementaire et à la crédibilité des entreprises.

La méthode utilisée par l'auteur est une méthode normative, de nature qualitative, tirée de l'analyse du référentiel ISO/IEC 27001 et de l'analyse de l'application de la norme dans des environnements organisationnels. Le modèle PDCA est le seul outil proposé pour organiser et structurer le cycle d'amélioration continue de la gestion des risques.

Les résultats montrent que la mise en œuvre de cette norme permet d'assurer la sécurité (confidentialité, intégrité, disponibilité) des informations, la résilience des organisations face aux menaces numériques, la rationalisation de la politique de sécurité, l'identification et la correction des vulnérabilités, (ce qui va dans le sens d'un renforcement de la posture globale des entreprises en matière de cybersécurité).

Méthodes d'Analyse des Risques dans les Systèmes d'Information

D'après (Fakrane, 2020) dans leur publication « Comparaison des méthodes d'analyse des risques pour les systèmes d'information », le management des risques s'appuie sur des démarches strictes visant à repérer, mesurer et gérer les périls pesant sur les ressources numériques des structures. Le but de leur recherche est d'analyser les avantages et les contraintes de trois techniques couramment admises dans le secteur de la sûreté des systèmes d'information : CORAS, ISRAM et MEHARI.

Les auteurs emploient une méthode comparative qualitative fondée sur un examen minutieux des trois approches à travers l'analyse documentaire. CORAS utilise la modélisation UML pour simplifier l'illustration graphique des scénarios de risques, ce qui favorise une meilleure saisie des menaces par toutes les parties intéressées. De son côté, ISRAM adopte une approche quantitative, examinant les risques à travers des sondages axés sur la probabilité de survenance des incidents et leurs conséquences financières. Pour finir, MEHARI, conçu par le CLUSIF, adopte une approche qualitative collaborative répondant aux standards ISO/IEC 27001 et 27005. Elle offre un cadre organisé pour la création de scénarios et l'exécution de plans de traitement appropriés.

Les conclusions avancées à l'issue de l'étude révèlent bien que chaque méthode présente des atouts ciblés en fonction du type d'organisation de la structure considérée, en ce sens que CORAS procure avant tout des outils de communication visuelle, ISRAM des indicateurs de quantification du risque, et MEHARI une approche globale conforme de

structures des référentiels certifiés mondialement, mais suggèrent que la sélection de la méthode appropriée ne peut se faire que selon un niveau de plus grande adéquation avec les véritables besoins de la structure retenue, son niveau de maturité en cybersécurité et les capacités mobilisables pour sa mise en condition.

1.2 L'intelligence artificielle dans la gestion des risques des systèmes d'information :

Intelligence Artificielle et Gestion des Risques

L'article de (Achir, 2024), intitulé « L'intelligence artificielle au service de la gestion des risques » (2024), s'implique que l'introduction des technologies d'intelligence artificielle apparaît comme un levier stratégique pour moderniser et renforcer les dispositifs de gestion des risques dans les organisations contemporaines. L'enjeu de l'article est de démontrer comment des outils comme le Big Data, le Machine Learning ou l'analyse prédictive permettent de mieux anticiper et réagir face aux menaces.

Les auteurs adoptent une méthodologie analytique s'appuyant sur l'étude de l'émergence des technologiques, soulignant les apports concrets de l'IA dans la détection à grande échelle des anomalies, l'amélioration de la prise de décision et de l'automatisation des procédures de surveillance.

Les résultats révèlent que l'IA permet d'augmenter la précision des prévisions et d'offrir aux entreprises des réactions en temps réel face aux risques à caractère opérationnel. Cependant, l'article insiste sur la nécessité de contrôles stricts, soulignant que l'efficacité technologique doit aller de pair avec des mesures de dispositifs de sureté et une gouvernance éthique pour garantir la protection de la confidentialité des données sensibles et la conformité aux Framework règlementaires.

Gestion des risque et intelligence artificielle

Selon ((Hub france, 2024), dans leur article intitulé « Qu'est-ce que la gestion des risques liés à l'intelligence artificielle ? », la gestion des risques liés à l'intelligence artificielle repose sur une approche méthodologique structurée visant à sécuriser l'ensemble du cycle de vie des systèmes d'IA. L'étude s'intéresse particulièrement à la manière d'opérationnaliser cette gestion des risques, notamment dans les systèmes dits à "haut risque", tels que définis par le règlement européen AI Act.

Les auteurs adoptent une méthodologie qualitative basée sur une revue structurée des meilleures pratiques et des normes existantes (telles que les normes ISO/IEC, ou encore les

directives européennes). L'objectif est de proposer une feuille de route permettant aux organisations d'identifier les vulnérabilités, d'évaluer les modèles, de gouverner les données et de mettre en place des mécanismes correctifs.

Les résultats de l'analyse soulignent que les organisations doivent développer des dispositifs de suivi et d'audit tout au long du cycle de vie des modèles IA, en intégrant des outils de mesure de la qualité des données, d'analyse des biais algorithmiques, et de contrôle de la transparence des décisions. L'étude insiste également sur la nécessité de garantir la conformité réglementaire dans un contexte juridique en évolution rapide. Les auteurs affirment que la mise en place d'une gestion rigoureuse et documentée des risques liés à l'IA constitue un levier stratégique pour renforcer la confiance, la sécurité, et la résilience des systèmes d'information intégrant l'intelligence artificielle.

Gestion des Risques dans les Systèmes d'Information Basés sur l'Intelligence Artificielle

Selon (Badman, 2024), dans son article *"Qu'est-ce que la gestion des risques liés à l'IA ?"* publié par IBM, la gestion des risques liés à l'intelligence artificielle constitue un pilier essentiel pour garantir un usage éthique, sécurisé et conforme des systèmes d'IA. L'objectif principal de l'article est de clarifier les mécanismes permettant d'identifier, d'atténuer et de contrôler les risques associés à l'IA tout au long de son cycle de vie.

L'autrice adopte une approche analytique en s'appuyant sur des études sectorielles (IBM Institute for Business Value, McKinsey) ainsi que sur des cadres réglementaires et normatifs tels que l'AI RMF du NIST, la loi européenne sur l'IA, les normes ISO/CEI et le décret présidentiel américain. Elle identifie quatre grandes catégories de risques : les risques liés aux données, aux modèles, aux opérations, et les risques éthiques et juridiques.

Les résultats montrent que, bien que 72 % des entreprises utilisent l'IA, seuls 24 % des projets d'IA générative sont considérés comme sécurisés. L'article met en lumière les vulnérabilités courantes (attaques adverses, biais algorithmiques, dérives de modèles) et insiste sur l'importance d'une gouvernance proactive pour renforcer la transparence, la conformité réglementaire et la confiance du public.

L’article recommande aux entreprises d’adopter une approche intégrée de la gestion des risques en s’appuyant sur des outils comme IBM Watsonx. governance pour assurer un contrôle continu, automatisé et éthique de leurs systèmes d’IA.

Analyse des Risques de Cybersécurité dans les Systèmes avec Composants d'Intelligence Artificielle

(Camacho, 2024) dans l'article « AI-driven Risk Management in Cybersecurity: A Simulation-Based Framework », soulignent que l’intégration des technologies d’intelligence artificielle dans les systèmes d’information complexifie les dynamiques de vulnérabilités et impose aux organisations de repenser leurs modèles traditionnels de gestion des risques. La recherche a pour objectif de proposer un modèle d’analyse des risques de cybersécurité adapté aux environnements intégrant l’IA.

La méthodologie est qualitative et expérimentale, reposant sur la simulation de scénarios de cyberattaques et l’expérimentation de défaillances algorithmiques. Le cadre d’analyse proposé prend en compte les menaces intentionnelles (attaques adverses), les erreurs systémiques (bugs, biais, dérives), et la résilience des systèmes face aux incidents.

Les conclusions mettent en évidence l'importance d'une gouvernance solide, fondée sur des critères de sécurité, et préconisent l'utilisation du Cadre de Gestion des Risques d'IA (AIRMF) en tant qu'instrument de gestion. Ce dernier offrirait la possibilité d'incorporer des processus de suivi continu, de transparence algorithmique et de stratégies de récupération, garantissant ainsi la crédibilité des systèmes d'information face aux dangers associés à l'IA. L'étude détermine que c'est uniquement une gestion proactive, organisée et réglementée des risques liés à l'IA qui peut assurer la sécurité numérique des entreprises sur le long terme.

L’intelligence artificielle comme levier de résilience : Vers une gestion prédictive des risques et une continuité opérationnelle accrue

(Odeh, 2023)Démontrent que l’intelligence artificielle joue un rôle crucial dans la prévision des divers risques et dans le maintien de la continuité des activités. Dans leur article intitulé: « The Role of Artificial Intelligence in Predictive Risk Assessment and Business Continuity » (Risks, 12, 19), les auteurs s’appuient sur une méthodologie quantitative de type transversal. Ils ont réalisé une collecte d’informations sur 360

techniciens pour en examiner l'impact du développement de différents modules de l'IA dans le domaine de la gestion des risques.

Leurs résultats montrent que les technologies de l'IA augmentent significativement l'efficacité du processus de gestion des risques et la résilience organisationnelle. En fait, le traitement automatique du langage naturel (NLP) permet à la fois d'accélérer et d'améliorer la précision des évaluations de risques, alors que l'intégration de l'IA dans les plans de réponse aux incidents réduit fortement les arrêts et facilite le rétablissement en cas d'imprévu. Les auteurs recommandent ainsi aux organisations d'investir dans les compétences en IA, notamment en NLP, en analyse de données, en maintenance prédictive et en planification des crises répondant aux besoins d'automatisation et d'anticipation.

L'intelligence artificielle au service de la gestion de projet : une approche exploratoire entre automatisation et compétences humaines

Selon (Soravito, 2023) dans l'article intitulé « Artificial Intelligence and Project Management », l'intelligence artificielle (IA) est perçue comme une technologie innovante susceptible d'influencer profondément la société et le monde des affaires. L'étude s'inscrit dans une perspective qualitative, adoptant une approche exploratoire visant à comprendre comment l'IA peut être intégrée dans les pratiques de gestion de projet.

L'auteure de l'étude, Giorgia Soravito, s'appuie sur une analyse documentaire approfondie et une réflexion critique pour évaluer les effets potentiels de l'IA sur la performance des entreprises et la gestion des projets. Bien qu'il ne s'agisse pas d'une recherche quantitative fondée sur des données statistiques ou des expérimentations, l'étude explore de manière systématique les apports de l'IA dans un contexte managérial complexe. Les résultats montrent que l'IA permet aux chefs de projet d'accroître leur efficacité et d'automatiser certaines tâches tout en soulignant que la nature unique et spécifique des projets peut constituer un obstacle à l'automatisation complète. L'étude révèle également que malgré les avancées technologiques, les compétences humaines – telles que le leadership, l'éthique, et la coordination interdisciplinaire – demeurent essentielles dans la gestion de projet.

Ainsi, cette recherche met en évidence la complémentarité entre l'intelligence artificielle et les compétences humaines, tout en anticipant une transformation progressive du rôle des managers à l'ère numérique.

Vers une cybersécurité proactive : apport et limites de l'intelligence artificielle dans la gestion des risques SI

Selon (Kunle-Lawanson O. , The role of AI in information security risk management, 2022; Kunle-Lawanson T. , 2022) l'intelligence artificielle (IA) occupe une position centrale dans la gestion des risques qui pèse sur la sécurité des systèmes d'information compte tenu de ses capacités avancées de détection des menaces, d'analyse prédictive et de réponse automatisée. Son article dans le World Journal of Advanced Engineering Technology and Sciences, à visée qualitative a pour objectif d'explorer comment l'IA peut non seulement succéder aux anciennes approches en matière de cybersécurité, mais également implanter une posture proactive dans la sauvegarde des actifs numériques. L'auteur souligne plusieurs technologies majeures de l'IA, machine learning, deep learning, natural language processing (NLP), analyse comportementale, analyse prédictive, à usage dans les secteurs sensibles tels que la finance, la santé ou la défense. Grâce à ces technologies, les entreprises peuvent mieux prévoir les attaques, réduire les faux positifs, blender l'automatisation des protocoles de sécurité, et soulever la résilience de leur environnement numérique. En revanche, l'étude signale également des limites notables : coûts exorbitants, enjeux de la vie privée, complexité technique, et la nécessité de conserver un contrôle humain pour éviter une possible dérive algorithmique. Des cas d'étude dans les secteurs bancaire, hospitalier Le recours aux études de cas en banque, à l'hôpital et à l'administration démontre l'impact bénéfique de l'IA sur la gestion des risques.

En conclusion, l'auteur plaide pour un recours hybride à l'IA et à l'expertise humaine, en faveur d'une cybersécurité plus robuste, contextualisée et éthique, pour mieux faire face à la sophistication des menaces numériques.

1.3 Comparaison entre l'étude actuelle et les travaux antérieurs

L'étude actuelle confirme les constats établis par Achir et Douari (2024), qui soulignent l'apport de l'IA en matière de détection des anomalies et d'aide à la décision dans la gestion des risques. En effet, les entretiens réalisés avec les responsables de l'ENGTP révèlent une ouverture progressive à l'intelligence artificielle comme levier d'assistance technique, notamment dans le traitement de configurations, l'analyse de vulnérabilités ou la consultation de recommandations techniques. Cela rejoint également les travaux de

Odeh et al. (2023), qui démontrent que l'IA peut significativement améliorer la réactivité et la résilience des dispositifs de sécurité.

Cependant, contrairement aux résultats quantitatifs de Odeh et al. (2023) ou Kunle-Lawanson (2022), qui montrent une intégration avancée de l'IA dans les secteurs sensibles (santé, finance, défense), l'étude actuelle met en évidence une adoption encore limitée, souvent ponctuelle, à l'ENGTP. Cette divergence s'explique notamment par des facteurs contextuels : un cadre réglementaire algérien encore flou, la sensibilité des données manipulées, et des ressources humaines ou techniques insuffisamment préparées à l'usage de l'IA dans un environnement industriel à haute criticité.

De plus, contrairement à ce que préconisent des auteurs comme Badman (2024) ou Camacho et al. (2024) – qui plaident pour une gouvernance IA robuste encadrée par des référentiels comme l'AI Act ou le NIST RMF – les pratiques à l'ENGTP restent informelles et peu alignées sur ces standards internationaux. Les méthodes comme MEHARI ou EBIOS sont connues mais rarement mises en œuvre, ce qui illustre un écart entre la théorie académique et la réalité opérationnelle.

Enfin, bien que plusieurs études (ex. Fakrane & Regragui, 2020) insistent sur l'importance de formaliser une approche méthodologique outillée, l'étude actuelle montre que les pratiques internes reposent sur des outils simples (Excel, observation terrain) mais restent pragmatiques, souples et ancrées dans l'expérience des responsables. Cela révèle un besoin de structuration progressive, à condition que celle-ci respecte les contraintes locales et les capacités internes.

Section 02 : Cadre conceptuel

Dans cette section, il s'agit de définir les notions clés mobilisées dans cette étude, en commençant par le concept central de la gestion des risques.

1. La gestion des risques

Cette session a été conçue spécialement pour accompagner les premières nations dans cette démarche. Il met à disposition une série d'outils pour initier une réflexion collective autour de la notion de risque et pour soutenir le leadership – tant politique qu'administratif – dans l'élaboration de stratégies de prévention et d'atténuation.

1.1 Le concept du risque

Le risque a été défini comme : la possibilité que les résultats attendus d'un projet ou d'un investissement ne se réalisent pas comme prévu et génèrent des conséquences indésirables à son promoteur » (Josée, 2004) (Turcotte, 2010). Les méthodes de gestion des risques quantitatives sont nombreuses (T, 2010) de même que celles qualitatives (Emblemsvåg Jan, 2006) .
Le concept du risque est vaste. Il est utilisé dans pratiquement tous les domaines possibles. Dépendamment du contexte dans lequel il est employé, sa signification peut varier. On parle de risques financiers, de risques économiques, de risques de projet, de risques de pays, etc.

Le risque désigne la possibilité qu'un événement imprévu et défavorable surviennent, avec un impact potentiel sur les activités d'une organisation. Il s'agit d'un élément fondamental à prendre en compte, car il permet de se préparer à des situations qui pourraient compromettre l'atteinte des objectifs.

Anticiper les risques, c'est réfléchir aux scénarios négatifs possibles et mettre en place des actions pour en limiter les conséquences. Ce processus constitue le cœur de ce que l'on appelle la gestion des risques.

1.2 Définition et portée de la gestion des risques

« La gestion du risque est un processus coordonné pour diriger et contrôler les activités d'une organisation en matière de risque. » (ASSOCIATIONS, CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES, 2003)

Les risques varient en nature et en gravité. Certains sont bénins et faciles à maîtriser, alors que d'autres peuvent avoir de lourdes répercussions sur le fonctionnement de l'organisation. La gestion des risques permet d'identifier, de classifier et de traiter ces différents types de menaces de manière structurée.

Même si l'on ne peut jamais prédire exactement quand ou si un événement risqué surviendra, il est possible, à partir de l'expérience acquise et d'une analyse rigoureuse, de repérer les scénarios plausibles et d'en estimer les effets potentiels. Cette démarche repose sur une évaluation systématique de la probabilité d'occurrence et de l'impact de ces événements.

Ainsi, la gestion des risques correspond à l'ensemble des processus, outils et mécanismes permettant de détecter les menaces, d'anticiper leur survenue et de mettre en place des mesures adaptées pour les surveiller et y faire face. Elle est d'autant plus efficace lorsqu'elle est intégrée à tous les niveaux de l'organisation et alignée avec sa vision, ses priorités et ses objectifs stratégiques.

1.3 Le cadre de gestion des risques

Un cadre de gestion des risques est un système structuré couvrant un ensemble de politiques, de méthodologies et d'échelonnements formalisés, avec pour objectif de créer une démarche harmonisée et exhaustive dans la découverte, l'évaluation et le traitement des risques. Cette démarche systématique permet de porter la gestion des risques d'harmonie avec les objectifs stratégiques et opérationnels de l'organisation. Lorsque ce cadre est déployé de manière holistique à l'échelle d'une entité, il prend alors la forme d'une « gestion intégrée des risques » ou d'une « gestion des risques organisationnels » (également désignée sous le terme anglo-saxon Enterprise Risk Management – ERM). (nations, 2016)

L'adoption des principes directeurs et des instruments méthodologiques que ce référentiel donne aux organisations, les administrations locales et les gouvernements autochtones et des Premières Nations la possibilité d'appréhender de manière précise les menaces potentielles et les opportunités inscrites dans leurs activités. Ce dispositif leur permet non seulement d'estimer de manière scientifique les conséquences liées à ces risques, mais également à concevoir et mettre en place des mécanismes de mitigation appropriés. Une telle approche contribue in fine à accroître la résilience institutionnelle et à faciliter la réalisation des orientations stratégiques définies par les instances décisionnelles.

1.4 Importance de gestion des risques

Dans ce titre met l'accent sur la valeur ajoutée d'une gestion structurée et systématique des risques :

- Elle favorise une gestion proactive plutôt que réactive.
- Elle permet à l'organisation de réduire les incertitudes, de protéger ses actifs, ses ressources humaines, ses connaissances, et sa réputation.
- Elle améliore la résilience, c'est-à-dire la capacité de l'organisation à résister à des chocs et à se rétablir.
- Elle aide à l'alignement entre les stratégies, les processus, la culture et la structure de l'organisation.

« La gestion des risques est une composante essentielle du management, qui soutient l'atteinte des objectifs et la performance durable de l'organisation. » (ASSOCIATIONS, CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES, 2003)

La gestion des risques est le processus qui permet aux gestionnaires informatiques d'équilibrer les coûts opérationnels et économiques des mesures de protection et d'obtenir des gains en capacité de mission en protégeant le besoin de "mission".

Le chef d'une unité organisationnelle doit s'assurer que l'organisation dispose des capacités nécessaires pour accomplir sa mission. Ces responsables de mission doivent déterminer les capacités de sécurité que leurs systèmes informatiques doivent avoir pour fournir le niveau de soutien à la mission souhaité face aux menaces réelles. La plupart des organisations ont des budgets serrés pour la sécurité informatique ; par conséquent, les dépenses en sécurité informatique doivent être examinées aussi minutieusement que les autres décisions de gestion. Une méthodologie de gestion des risques bien structurée, lorsqu'elle est utilisée efficacement, peut aider la direction à identifier les contrôles appropriés pour fournir les capacités de sécurité essentielles à la mission.

1.5 Les étapes du processus de gestion des risques

La gestion des risques repose sur un ensemble d'étapes interdépendantes qui s'inscrivent dans une logique itérative et dynamique. Loin d'être linéaire ou figée, cette démarche s'adapte en fonction du contexte organisationnel, des parties prenantes impliquées, ainsi que de l'évolution des menaces et opportunités. Le processus est conçu pour être

applicable à tout type d'organisation, quel que soit son secteur d'activité, et il permet d'instaurer une culture du risque proactive et structurée.

1. L'établissement du contexte

Avant même de commencer à identifier les risques, il est indispensable de bien comprendre l'environnement dans lequel l'organisation évolue. Cette première étape vise à définir le cadre global de la gestion des risques, tant du point de vue interne (structure organisationnelle, culture, processus, ressources) qu'externe (réglementations, marché, partenaires, environnement technologique).

Il s'agit également de déterminer les objectifs du processus de gestion des risques : quels résultats sont attendus ? À quelle échelle (stratégique, opérationnelle, projet) la gestion des risques sera-t-elle appliquée ? Par ailleurs, il est essentiel de fixer les critères d'évaluation des risques (gravité, fréquence, acceptabilité), ainsi que les rôles et responsabilités des différents acteurs impliqués.

L'établissement du contexte permet ainsi d'aligner la démarche de gestion des risques sur la stratégie de l'organisation et de garantir sa pertinence et son efficacité. (ASSOCIATIONS, CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES, 2003)

2. L'identification des risques

Une fois le cadre établi, la phase d'identification consiste à détecter l'ensemble des événements potentiels, incertains mais susceptibles d'avoir un effet — positif ou négatif — sur l'atteinte des objectifs. Cette étape implique une exploration rigoureuse des sources de risques, des vulnérabilités existantes, ainsi que des menaces internes et externes.

Dans le cas des systèmes d'information, cela peut concerner les cyberattaques, les pannes matérielles ou logicielles, les défaillances humaines, ou encore les risques liés à la confidentialité des données. L'identification peut s'appuyer sur plusieurs techniques telles que les brainstormings, les interviews, les audits, l'analyse des incidents passés, ou l'utilisation de check-lists sectoriels.

Cette étape constitue la base du processus : un risque non identifié ne pourra jamais être traité.

3. L’analyse des risques

Après avoir identifié les risques, il est nécessaire de les analyser en profondeur. Cela consiste à examiner, pour chaque risque, la probabilité qu’il se réalise ainsi que l’impact qu’il pourrait produire. L’objectif est d’en comprendre la nature, les causes, les conséquences, les interactions avec d’autres risques et les facteurs aggravants ou atténuants. (ASSOCIATIONS, 2003)

L’analyse peut être qualitative, en classant les risques selon des critères prédéfinis, ou quantitative, en leur attribuant une valeur chiffrée (coût estimé, fréquence, niveau de perturbation). Elle permet également de représenter graphiquement les risques (par exemple via une matrice de criticité) afin de faciliter leur compréhension et leur priorisation.

4. L’évaluation des risques

Étroitement liée à l’analyse, l’évaluation vise à déterminer si les risques identifiés et analysés sont acceptables ou non, au regard des critères définis précédemment. Il s’agit de prioriser les risques selon leur criticité, c’est-à-dire en fonction de leur gravité et de leur probabilité combinée.

Cette priorisation permet de concentrer les efforts sur les risques les plus menaçants pour l’organisation, tout en identifiant ceux qui peuvent être tolérés ou nécessitent simplement une surveillance. C’est également à ce stade que les arbitrages stratégiques se font : quels risques devons-nous traiter en priorité ? Lesquels pouvons-nous assumer ou transférer ? (27005, 2018)

5. Le traitement des risques

Une fois les risques évalués, il faut décider des actions à mettre en œuvre pour les maîtriser. Quatre grandes stratégies de traitement sont possibles :

- Éviter le risque : cesser ou modifier l’activité à l’origine du risque ;
- Réduire le risque : diminuer sa probabilité de survenue ou ses conséquences (ex. : mises à jour de sécurité, redondance des serveurs, contrôles d’accès) ;
- Transférer le risque : déléguer sa gestion à un tiers (assurances, sous-traitance) ;
- Accepter le risque : en assumer les conséquences si celui-ci reste dans les limites acceptables.

Le choix de traitement doit être cohérent avec les ressources disponibles, les priorités stratégiques, et les attentes des parties prenantes. Il nécessite souvent un plan d'action structuré, assorti de délais, d'indicateurs de suivi et de responsables désignés.

6. La surveillance et la révision

Le monde étant en constante évolution, les risques ne sont jamais figés. Il est donc impératif d'assurer une surveillance continue de la situation, afin de détecter l'apparition de nouveaux risques, la modification de ceux existants, ou encore l'inefficacité des mesures mises en place.

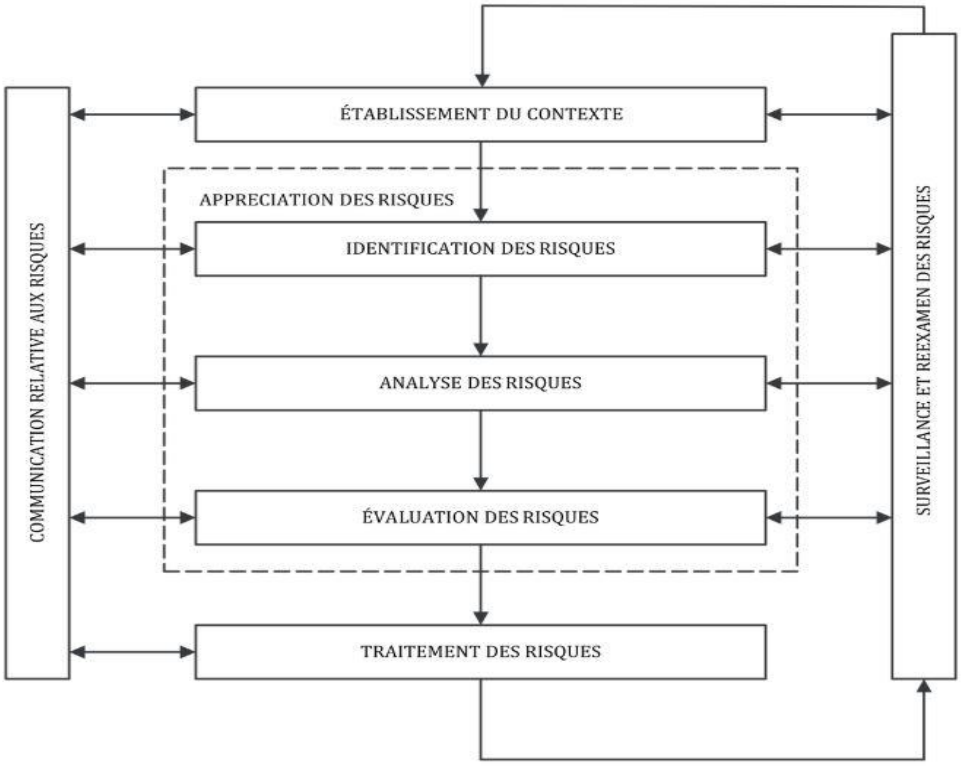
Cette surveillance repose sur des indicateurs de performance, des audits internes, des retours d'expérience et des mises à jour régulières du registre des risques. Une bonne gestion des risques est donc évolutive et adaptative, capable de s'ajuster aux changements internes et aux mutations de l'environnement. (27005, 2018)

7. La communication et la consultation

Tout au long du processus, il est indispensable de communiquer activement avec toutes les parties prenantes, internes comme externes. La communication permet d'assurer une compréhension partagée des enjeux, d'expliquer les choix effectués, de renforcer l'adhésion aux plans de traitement, et de favoriser une culture du risque.

La consultation, quant à elle, vise à impliquer les personnes concernées à chaque étape du processus, notamment celles disposant d'une expertise ou d'une responsabilité sur les sujets abordés. Cela contribue à renforcer la pertinence et l'efficacité des actions menées.

Figure 1 : Processus de gestion des risques



Source : (27005, 2018).

1.6 Typologie des risques

Dans le cadre d'un processus structuré de gestion des risques, l'étape d'identification nécessite une catégorisation claire des menaces potentielles auxquelles une organisation peut être confrontée. Cette catégorisation, communément appelée *typologie des risques*, constitue une base essentielle pour orienter les choix méthodologiques, prioriser les actions de traitement, et adapter les dispositifs de surveillance. Elle permet d'appréhender la diversité des risques en fonction de leur origine, de leur nature ou encore de leurs effets attendus sur les objectifs de l'organisation.

1.6.1 Typologie fonctionnelle des risques organisationnels : (ZAGRÉ, 2016)

En complément de la distinction interne/externe, une typologie fonctionnelle peut être établie selon les domaines d'impact. On recense généralement les catégories suivantes :

Risques stratégiques : Ils concernent la direction à long terme de l'organisation. Ils peuvent résulter de décisions mal alignées sur les évolutions du marché, d'un positionnement inadapté, ou d'un défaut d'anticipation de ruptures structurelles.

Risques financiers : Ils touchent aux flux monétaires, à la solvabilité, au financement ou encore à la gestion des actifs. Ils incluent également les risques de fraude, de variation des taux ou de change.

Risques opérationnels : Relatifs au fonctionnement quotidien de l'organisation, ces risques résultent de défaillances de processus, de systèmes ou de personnes. Ils peuvent perturber la chaîne de valeur et engendrer des pertes immédiates.

Risques technologiques et liés aux systèmes d'information : En forte croissance, ces risques englobent les cyberattaques, les interruptions de service, les pertes de données, ou encore l'obsolescence des infrastructures numérique.

Risques réglementaires et de conformité : Ils découlent de la non-conformité aux exigences légales, normatives ou sectorielles. Ils peuvent entraîner des sanctions juridiques Financière ou réputationnelles.

Risques liés à la réputation : Ils résultent d'événements affectant l'image de l'organisation auprès de ses parties prenantes. Ils peuvent être déclenchés par une crise médiatique un scandale ou un défaut de communication.

Risques environnementaux ou naturels : Ceux-ci incluent les catastrophes naturelles, les pandémies ou les conséquences du changement climatique. Bien qu'externes, ils doivent faire l'objet d'une planification rigoureuse.

Risques humains et sociaux : Ils sont liés à la gestion du personnel, à la motivation, au climat social, au recrutement ou au maintien des compétences critiques. Un risque RH peut se traduire par une baisse de productivité ou un turnover élevé. (ZAGRÉ, 2016)

1.6.2 Les risques perçu comme opportunité

Dans une vision plus moderne et élargie du management du risque, notamment soutenue par les référentiels ISO, le risque n'est pas uniquement perçu comme une menace à écarter. Il est également envisagé comme un facteur d'opportunité, dans la mesure où il peut conduire à des bénéfices, s'il est bien anticipé et exploité. Cette vision bidimensionnelle (négative/positive) du risque renforce l'idée que le rôle du management du risque est de favoriser la prise de décision en contexte incertain, et pas uniquement de protéger l'organisation contre les aléas défavorables. (31000, 2018)

1.7 Approche standardisée de la gestion des risques

Dans un contexte marqué par l'incertitude, la complexité des environnements organisationnels et la mondialisation des échanges, la gestion des risques est devenue une fonction stratégique incontournable. Donc, on va découvrir la standardisation qu'elle répondre à cette nécessité

La norme ISO 31000 : (31000, 2018)

L'Organisation internationale de normalisation (ISO) a élaboré une norme de référence universelle : l'ISO 31000, dont la première édition date de 2009 et qui a été actualisée en 2018. En France, elle est reprise sous l'intitulé NF ISO 31000 : Management du risque – Principes et lignes directrices.
Contrairement aux normes à vocation certifiante, ISO 31000 n'a pas pour objectif d'imposer un système rigide. Il s'agit d'un cadre non prescriptif, fondé sur des principes et lignes directrices applicables à toute organisation, indépendamment de sa taille, de son secteur d'activité ou de sa structure juridique. Elle vise ainsi à guider les entités dans l'élaboration d'un dispositif de gestion des risques intégré, proportionné et adapté à leur propre contexte.

Ce positionnement découle de sa genèse : dès 2005, sous l'impulsion du Japon et avec l'appui de l'Australie, du Royaume-Uni et de la France, un consensus s'est formé autour de l'idée de créer une norme générique, dépourvue d'exigences contraignantes, et non destinée à une finalité de certification. Cette approche souple a été maintenue dans les versions ultérieures, y compris dans la révision majeure de 2018.

- **Fondements et objectifs de la norme**

La finalité première de l'ISO 31000 est de permettre aux organisations de créer et de protéger la valeur en les aidant à prendre de meilleures décisions, à atteindre leurs objectifs et à renforcer leur résilience. Elle repose sur une série de principes fondamentaux, parmi lesquels:

- L'intégration du management du risque à toutes les activités de l'organisation ;
- Une démarche structurée, exhaustive et dynamique ;
- L'adaptation au contexte interne et externe de chaque organisation ;
- L'inclusion des parties prenantes dans une logique participative ;

- La prise en compte de facteurs humains, culturels et informationnels ;
- L'amélioration continue des pratiques de gestion des risques. (31000, 2018)

Ces principes servent de socle conceptuel à l'ensemble du dispositif de gestion des risques. Ils soulignent notamment que la gestion du risque n'est pas une fonction isolée, mais qu'elle doit être pleinement intégrée dans les processus décisionnels et les structures de gouvernance.

- **Un cadre de référence structurant**

La norme ISO 31000 propose un cadre organisationnel complet, structuré autour de trois piliers : les principes, le cadre (framework), et le processus. Ce cadre vise à garantir l'efficacité, la cohérence et l'adaptabilité du management des risques à tous les niveaux :

Le cadre (framework) permet d'intégrer le management du risque dans la gouvernance globale, avec l'implication de la direction générale, la clarification des rôles, la mobilisation des ressources et l'évaluation régulière du dispositif.
Le processus quant à lui est itératif, et se décline en plusieurs étapes : communication et consultation, établissement du contexte, évaluation des risques (identification, analyse, évaluation), traitement des risques, suivi et revue, enregistrement et communication des résultats.

Ce processus peut être appliqué à différents niveaux : stratégique, opérationnel, projet, programme, etc.

2. Gestion de Risque des systèmes d'information

Dans le but de maîtriser la gestion des risques des systèmes d'information, il convient, dans un premier temps, de définir les notions essentielles et de repérer les différentes catégories de risques se rapportant à cette gestion.

2.1 Définitions et typologies des risques de système d'information

Pour mieux comprendre la nature des risques liés aux systèmes d'information, il convient d'en définir d'abord les fondements.

2.1.1 Définition du système d'information

Le SI est l'ensemble des ressources (matériels, logiciels, données, procédures, humains…) Structurés pour acquérir, traiter, mémoriser, transmettre et rendre disponible l'information (sous forme de données, textes, sons, images…) dans et entre les organisations. (Reix, 1995) Le SI est avant tout une organisation des ressources destinée à traiter l'information soit pour produire, soit pour piloter. Ces ressources sont organisées pour : (Rivière, 2017)

Collecter l'information : enregistrer une information (support papier, informatique…) avant son traitement

- Mémoriser l'information (stockage) : conserver, archiver (utilisation ultérieure ou obligation légale)
- Traiter l'information : effectuer des opérations (calcul, tri, classement, résumé…)
- Diffuser l'information : transmettre à la bonne personne (traiter et afficher une information après traitement) .....

Donc, un système d'information (SI) désigne l'ensemble des dispositifs humains, organisationnels et technologiques mis en œuvre au sein d'une organisation dans le but de collecter, traiter, stocker et diffuser l'information nécessaire à son bon fonctionnement. Il ne se limite pas à une infrastructure informatique, mais constitue un système global intégrant plusieurs composantes interdépendantes : les données (structurées ou non), les technologies (matériel, logiciels, réseaux), les processus de traitement de l'information, les utilisateurs (internes ou externes), ainsi que les règles de gouvernance qui encadrent son usage. (Châtelain & Roche, 2000)

Véritable levier de pilotage et de performance, le système d'information joue un rôle central dans l'automatisation des processus métiers, le soutien à la prise de décision, la circulation fluide de l'information et l'alignement stratégique de l'organisation. Dans un contexte de transformation numérique accélérée, marqué par l'essor du cloud computing, de l'intelligence artificielle ou encore de l'Internet des objets, un SI efficace doit concilier innovation, sécurité, interopérabilité et évolutivité. Il devient ainsi un facteur déterminant de compétitivité et de résilience pour les organisations contemporaines, quels que soient leur secteur d'activité ou leur taille.

2.1.2 Définition du Risque des Systèmes d'Information

Le risque est défini comme un événement ou un aléa pouvant survenir et créant des dommages

Plus ou moins considérable. en gestion des systèmes d'information (SI), un risque peut être décrit comme la probabilité qu'une menace exploite une vulnérabilité, entraînant ainsi un impact négatif sur les actifs informationnels de l'organisation.

2.1.3 Objectif de la Gestion des Risques SI

La gestion des risques SI concerne l'identification, l'évaluation et le traitement des risques liés à l'usage, à la possession et à l'adoption des technologies de l'information au sein d'une organisation.

Elle vise à assurer la confidentialité, l'intégrité et la disponibilité des informations, ainsi qu'à réduire les menaces liées aux cyberattaques et aux failles de sécurité.

2.1.4 Typologies des Risques SI

Les risques liés aux systèmes d'information (SI) peuvent être classés selon plusieurs catégories, en fonction de leur nature, de leur origine et de leur impact potentiel sur l'organisation :

Risques informatiques : Ils concernent les menaces techniques telles que les intrusions non autorisées, les fuites de données, les virus, les ransomwares ou d'autres formes de cyberattaques pouvant compromettre la sécurité, la confidentialité et l'intégrité des données.

Risques opérationnels : Ils résultent de dysfonctionnements internes, notamment des pannes d'équipements, des erreurs humaines, des défauts de maintenance ou une mauvaise configuration des systèmes.

Risques stratégiques : Ces risques apparaissent lorsqu'il y a un mauvais alignement entre les systèmes d'information et les objectifs stratégiques de l'entreprise. Une stratégie numérique inadaptée peut freiner l'innovation ou compromettre la compétitivité.

Risques de conformité : Ils concernent le non-respect des réglementations, normes ou politiques en vigueur, telles que l'**ISO 27001**, l'**ISO 27005**, ou d'autres exigences

nationales, régionales ou internationales en matière de sécurité des SI et de protection des données.

Risques juridiques de non-conformité légale : Ces risques peuvent découler de la violation de lois locales, régionales ou internationales, incluant des obligations liées à la cybersécurité, à la protection des données personnelles (ex. RGPD), ou aux obligations contractuelles spécifiques à certains secteurs d'activité.

Risques d'atteinte à la réputation : Un incident majeur affectant les systèmes d'information peut porter gravement atteinte à l'image de l'entreprise ou, dans certains cas, nuire à la réputation du secteur ou du pays, notamment dans un contexte géopolitique sensible ou fortement médiatisé. (ZAGRÉ, 2016)

2.2 Processus et classification des risques liés aux systèmes d'information

2.2.1 Les étapes de gestion des risques des systèmes d'information

La gestion des risques appliquée aux systèmes d'information repose sur un ensemble de méthodes et de bonnes pratiques visant à identifier, analyser, traiter et surveiller les menaces susceptibles de compromettre la sécurité, l'intégrité, la disponibilité ou la confidentialité des actifs informationnels d'une organisation. Ce processus est fondamental dans un environnement numérique en constante évolution, où les risques technologiques deviennent de plus en plus complexes, interconnectés et difficiles à anticiper.

Le processus de gestion des risques SI peut être décliné en étapes principales, chacune jouant un rôle clé dans la protection et l'optimisation du système d'information (Intervalle, 2024)

1. **Identification des risques** La première phase de la démarche consiste à recenser de manière exhaustive l'ensemble des menaces susceptibles de porter atteinte à la sécurité des systèmes d'information, qu'il s'agisse de leur intégrité, de leur disponibilité ou de la confidentialité des données. Parmi les menaces les plus courantes, on peut citer les cyberattaques (phishing, ransomware, DDoS), les pannes techniques, les erreurs humaines ou encore les fuites de données.

Une fois ces menaces identifiées, il convient de procéder à une analyse approfondie des vulnérabilités présentes au sein de l'infrastructure. Cela comprend l'évaluation des failles techniques (systèmes non mis à jour, configurations faibles), organisationnelles (absence

de procédures ou de contrôles) et humaines (manque de sensibilisation ou de formation). L'objectif est de déterminer comment et dans quelles conditions ces vulnérabilités pourraient être exploitées par des acteurs malveillants ou par des défaillances internes.

2. **Évaluation des risques** Chaque risque identifié doit ensuite faire l'objet d'une analyse qualitative ou quantitative, reposant sur deux axes principaux :

La probabilité d'occurrence, estimée à partir de l'historique des incidents, des tendances sectorielles ou de l'environnement technologique ;

L'impact potentiel peut être d'ordre financier (pertes économiques), opérationnel (interruption de service), juridique (sanctions pour non-conformité) ou réputationnel (perte de confiance des parties prenantes).

Cette évaluation permet de prioriser les risques selon leur niveau de criticité, facilitant ainsi la prise de décision sur les actions à engager en priorité. (Intervalle, 2024)

3. **Traitement et atténuation des risques** Sur la base de l'évaluation réalisée, l'organisation doit mettre en œuvre des mesures de traitement adaptées aux risques jugés inacceptables. Ces mesures peuvent être de différentes natures :

Techniques : installation de pare-feux, systèmes de détection d'intrusion, solutions de chiffrement des données, contrôles d'accès ;

Organisationnelles et administratives : définition de politiques de sécurité, élaboration de procédures internes, sensibilisation et formation du personnel ;

Physiques : sécurisation des locaux informatiques, contrôle des accès physiques, vidéosurveillance.

L'objectif est de réduire l'exposition au risque soit en diminuant la probabilité d'apparition, soit en limitant les conséquences potentielles.

4. **Surveillance continue et réévaluation** La gestion des risques ne saurait se limiter à une intervention ponctuelle. Elle nécessite une vigilance constante à travers un système de monitoring en temps réel, capable de détecter rapidement toute anomalie, toute faille émergente ou tout comportement suspect.

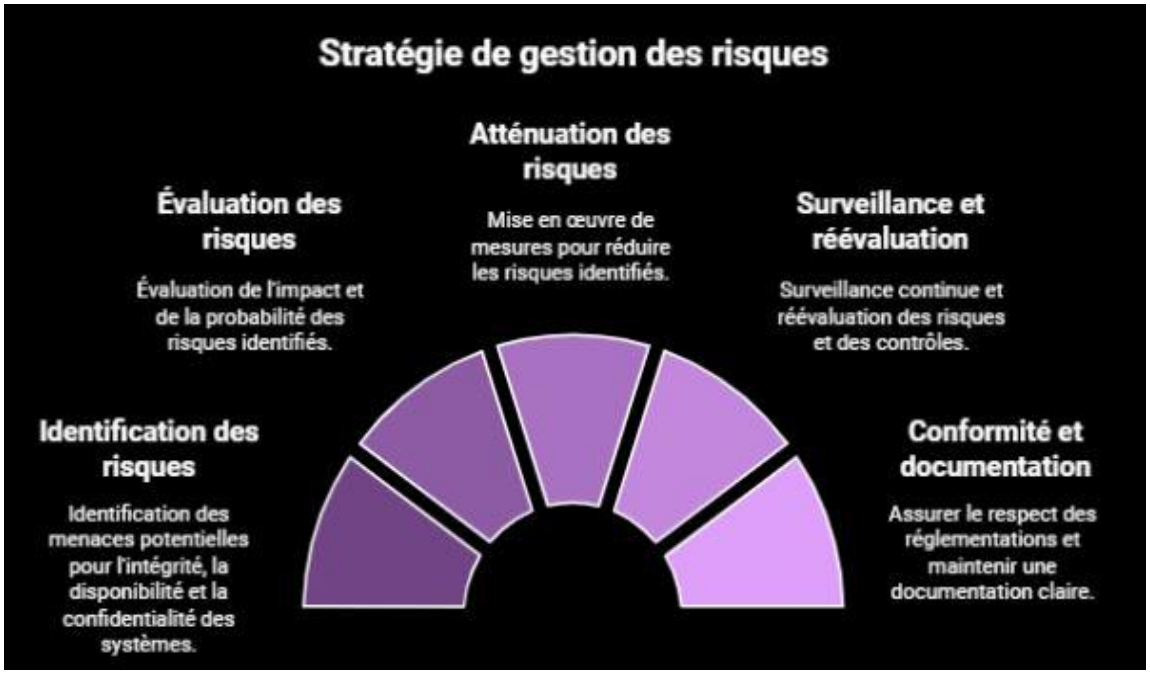
Il est également essentiel de mettre en place une réévaluation périodique des risques et des dispositifs de sécurité existants. Cette révision régulière permet d'ajuster la stratégie de gestion des risques aux évolutions technologiques, aux changements organisationnels ou encore aux nouvelles obligations réglementaires.

5. **Conformité réglementaire et documentation** Un aspect fondamental de la gestion des risques en environnement numérique réside dans le respect des cadres juridiques et normatifs applicables. Les organisations doivent veiller à être en conformité avec les réglementations en vigueur, telles que le Règlement Général sur la Protection des Données (RGPD) ou la norme ISO/CEI 27001, portant sur les systèmes de management de la sécurité de l'information (SMSI). (Intervalle, 2024)

Par ailleurs, il est impératif de maintenir une documentation rigoureuse et complète retraçant toutes les étapes du processus : de l'identification des risques à leur traitement, en passant par les décisions stratégiques, les contrôles mis en place, et les plans d'amélioration continue. Une telle documentation favorise la transparence, la traçabilité, et la cohérence des actions, tout en facilitant les audits internes et externes.

En intégrant cette approche méthodique dans leur stratégie globale, les organisations renforcent leur résilience face aux menaces numériques, tout en assurant la protection durable de leurs actifs critiques et la conformité aux exigences réglementaires.

Figure 2 les étapes de stratégie de gestion des risques



Source : (Intervalle, 2024).

2.2.2 Classification des risques

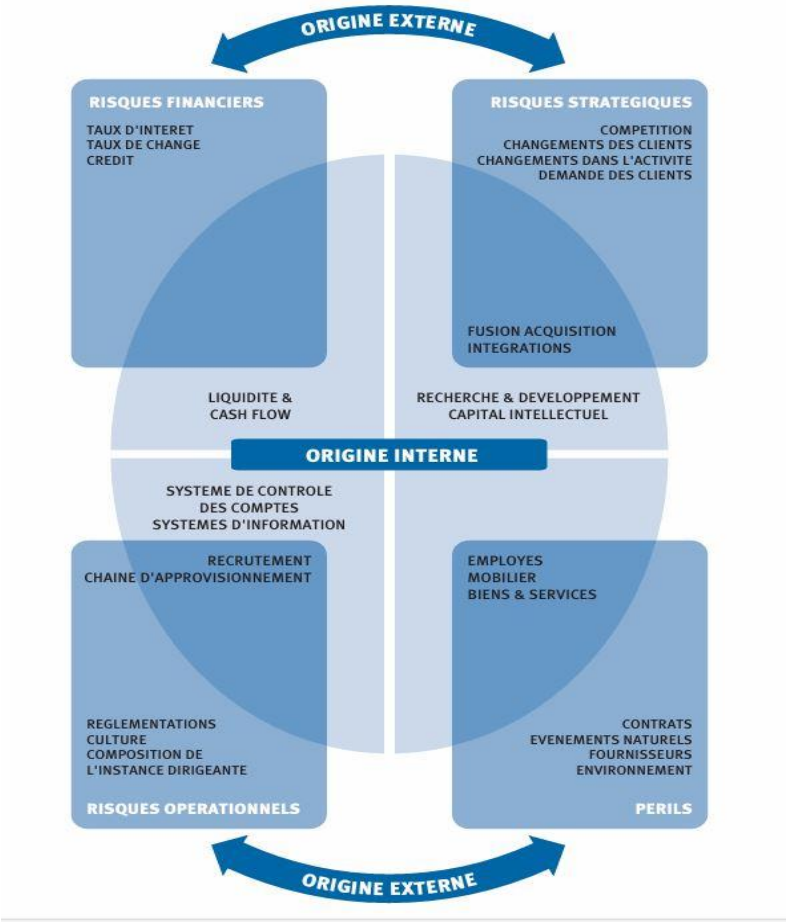
Pour mieux appréhender les risques auxquels une organisation peut être confrontée, il est utile de les classer selon leur source et leur nature.

Les risques internes générés au sein même de l'organisation, sont généralement liés à ses processus, à ses ressources humaines, à sa gouvernance, ou encore à ses systèmes technologiques. Ils peuvent résulter d'une mauvaise coordination, d'erreurs humaines, de faiblesses organisationnelles ou de défaillances techniques.

Les risques externes proviennent de l'environnement dans lequel évolue l'organisation. Ils peuvent être d'ordre économique, réglementaire, technologique, environnemental ou géopolitique, et sont souvent plus difficiles à maîtriser. Leur impact peut être amplifié par la mondialisation des échanges et la complexité des chaînes de valeur actuelles.

Cette distinction permet de déterminer le degré de contrôle que l'organisation peut exercer sur les risques identifiés, et oriente ainsi les stratégies de gestion. (ASSOCIATIONS, 2003)

Figure 3 Facteurs externes et interne de gestion des risques



Source : (ASSOCIATIONS, 2003).

2.3 Enjeux et défis de la sécurité des systèmes d'information (SI)

Avant d'aborder les défis à relever, il est essentiel de présenter les enjeux majeurs liés à la sécurité des systèmes d'information

2.3.1 Enjeux de la sécurité des SI

Les systèmes d'information jouent un rôle central dans les entreprises, et leur sécurité est essentielle pour :

- Protéger la confidentialité, l'intégrité et la disponibilité des données.
- Assurer la continuité des activités face aux cyberattaques et incidents techniques.
- Respecter les réglementations (ex. : RGPD, ISO 27001) , la Loi 18-07 et le RNSI 2021 en Algérie.
- Éviter les pertes financières et atteintes à la réputation en cas de violation des données.

2.3.2 Défis de la sécurité des SI

Les entreprises rencontrent plusieurs défis dans la sécurisation de leurs SI :

Complexité croissante des infrastructures IT

- Multiplication des points d'entrée avec l'IoT et le cloud.
- Difficultés à maintenir une architecture sécurisée sur plusieurs environnements.

Cyber menaces de plus en plus sophistiquées

- Attaques ciblées (phishing avancé, ransomwares, menaces persistantes avancées - APT).
- Nécessité d'une surveillance continue et d'une réponse rapide aux incidents.

Manque de sensibilisation et d'expertise

- L'erreur humaine reste une cause majeure des failles de sécurité.
- Besoin de formations pour renforcer la culture de la cybersécurité.

Conformité réglementaire et gestion des risques

- Respect des standards de sécurité (Fatna, 2023)
- Mise en place de plans de continuité d'activité et de reprise après sinistre.

Intégration de l'intelligence artificielle

- Automatisation de la détection et de l'analyse des cybermenaces.
- Difficultés à interpréter certains modèles d'IA pour la cybersécurité.

2.4 Normes et référentiels dans la gestion des risques SI

Pour garantir une approche précise et acceptée internationalement de la gestion des risques sur les systèmes d'information, il convient de s'appuyer sur des normes acceptées internationalement. Dans cette section, nous couvons deux référentiels qui sont l'ISO 27001 et l'ISO/IEC 27005, et décrivons ce que ces documents exposent, ainsi que les éléments clés utilisés pour établir une gestion des systèmes de sécurité durable et pérenne. (Louisot, 2022).

2.4.1 Norme ISO 27001 et son Rôle dans la Gestion des Risques IT

- ISO 27001 :2018 est une norme internationale qui définit les exigences pour un Système de Management de la Sécurité de l'Information (ISMS).

- Elle aide les organisations à : Identifier les risques liés à la sécurité de l'information, Mettre en place des mesures de contrôle pour atténuer ces risques, Maintenir une surveillance continue pour améliorer la gestion des risques IT.

- L'ISO 27001 fournit un cadre permettant d'évaluer les risques et de les traiter en fonction de leur impact potentiel.

- Processus de Gestion des Risques selon ISO 27001 :

1. Identification des risques : Recenser les menaces internes et externes (cyberattaques, erreurs humaines, défaillances techniques).
2. Analyse et évaluation : Estimer l'impact et la probabilité d'occurrence des risques.
3. Traitement des risques : Élaborer des stratégies de mitigation (éviter, réduire, transférer ou accepter le risque).
4. Surveillance et amélioration continue : Mettre en place un Plan-Do-Check-Act (PDCA) pour assurer une gestion efficace. (Fatna, 2023)

2.4.2 Norme ISO/IEC 27005

La norme ISO/IEC 27005 représente un standard internationalement apprécié pour la gestion des risques en matière de sécurité de l'information autrement dit, un référentiel méthodologique pour la gestion des risques en sécurité de l'information.

Cette norme, publiée par l'ISO (Organisation Internationale de Normalisation), a pour objectif d'accompagner l'implémentation d'un Système de Management de la Sécurité de l'Information (SMSI) en conformité avec la norme ISO/IEC 27001, en privilégiant une approche axée sur les risques.

Elle propose une série de lignes directrices permettant aux organisations de mettre en œuvre un processus structuré et cohérent d'identification, d'analyse, d'évaluation, de traitement, de suivi et de communication des risques susceptibles d'affecter les actifs informationnels. La norme s'adresse à l'ensemble des acteurs impliqués dans la gouvernance de la sécurité, qu'il s'agisse de responsables métiers, de décideurs, de techniciens, ou de parties prenantes externes.

L’un des principaux intérêts de la norme ISO/IEC 27005 réside dans sa souplesse d’application. Elle n’impose pas une méthodologie unique, mais autorise l’organisation à choisir la méthode d’analyse des risques la plus adaptée à son contexte (approche qualitative, quantitative ou semi-quantitative). Elle insiste également sur la nécessité de définir clairement les critères d’acceptabilité du risque, en tenant compte des objectifs stratégiques et opérationnels de l’organisation. (27005, 2018)

Enfin, cette norme s’inscrit dans une logique d’intégration avec d’autres référentiels tels que ISO/IEC 27001 (exigences pour un SMSI) et ISO/IEC 27002 (bonnes pratiques de sécurité). Elle constitue ainsi un outil essentiel pour renforcer la résilience des systèmes d’information, améliorer la maîtrise des menaces numériques, et assurer une conformité réglementaire durable.

2.5 Méthodes et Outils d'Analyse des Risques SI

L'analyse des risques des systèmes d'information est essentielle pour identifier, évaluer et traiter les menaces potentielles. Plusieurs méthodes ont été développées pour structurer cette analyse. Parmi les plus reconnues figurent MEHARI, OCTAVE et EBIOS. Chacune offre une approche spécifique en fonction des besoins organisationnels. (ANSSI, Guide d’hygiène informatique, 2017)

2.5.1 EBIOS Risk Manager

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) constitue une approche méthodologique française dédiée à l'évaluation et à la gestion des risques associés à la sécurité des systèmes d'information. Initialement élaboré par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), EBIOS offre une approche structurée pour l'analyse des risques, définissant les exigences en matière de sécurité, les menaces pesant sur les actifs essentiels et les méthodes appropriées de traitement.

Son actualisation, nommée EBIOS Risk Manager, propose une approche recontextualisée aux réalités du numérique d’aujourd’hui (interconnexion des systèmes, complexité croissante des écosystèmes métiers et techniques, rapidité d’évolution des menaces cyber) afin d’assister les organisations à concevoir, évaluer et faire évoluer un dispositif de sécurité qui corresponde à leurs enjeux stratégiques en considérant ainsi la nature dynamique de leur environnement de menace.

L'un des principes de base d'EBIOS Risk Manager consiste à replacer la menace au centre de l'analyse, non pas uniquement à partir des vulnérabilités techniques, mais également à partir des intentions des assaillants, de leurs capacités et de leurs cibles potentielles. En opposition à la vision traditionnelle de la sécurité, centrée sur les vulnérabilités internes, cette méthode est construite d'un point de vue attaquant, et repose donc sur la construction de scénarios de risques crédibles et réalistes, modélisant la chaîne d'attaques qu'un adversaire pourrait mettre en œuvre pour porter atteinte aux actifs critiques d'une organisation.

EBIOS est structurée en cinq ateliers méthodologiques successifs, permettant une construction progressive et cohérente du diagnostic de sécurité. Le premier atelier, dit *Cadrage et contexte*, a pour fonction de définir les contours de l'étude, en identifiant les missions sensibles, les actifs essentiels à protéger, ainsi que les dépendances stratégiques internes et externes. Cette étape ancre l'analyse dans les réalités métier de l'organisation, en tenant compte de son périmètre opérationnel, de ses priorités, mais aussi des contraintes juridiques ou techniques. (ANSSI, 2017)

Les étapes de la méthode EBIOS:

Le deuxième atelier, appelé *Sources de risque et objectifs visés*, consiste à dresser le portrait des acteurs susceptibles de constituer une menace. Ces derniers peuvent être très variés : cybercriminels organisés, groupes étatiques, hacktivistes, concurrents malveillants ou encore menaces internes (employés ou sous-traitants). L'analyse s'intéresse à leurs motivations, leurs ressources techniques, et leur capacité à cibler certains actifs. Comme le précise l'ANSSI, cette phase vise à comprendre "les objectifs visés par les attaquants, leurs motivations et leurs modes opératoires privilégiés" (ANSSI, 2017) .

Le troisième atelier, dédié aux *scénarios stratégiques*, permet d'imaginer des chemins d'attaque exploitant l'écosystème de l'organisation. Il s'agit de relier une source de menace à un événement redouté, à travers des vecteurs comme un partenaire mal sécurisé, un fournisseur critique ou une infrastructure exposée. Cette étape apporte une vision macroscopique des menaces pesant sur l'organisation et met en lumière les fragilités de son environnement global.

Dans la continuité, le quatrième atelier, dit *Scénarios opérationnels*, traduit les scénarios stratégiques en actions techniques concrètes. On y décrit les méthodes d'attaque plausibles

: hameçonnage, exploitation de failles, compromission d'identifiants, intrusion via objets connectés, etc. Cette étape vise à cartographier précisément les vulnérabilités susceptibles d'être exploitées dans la réalité.

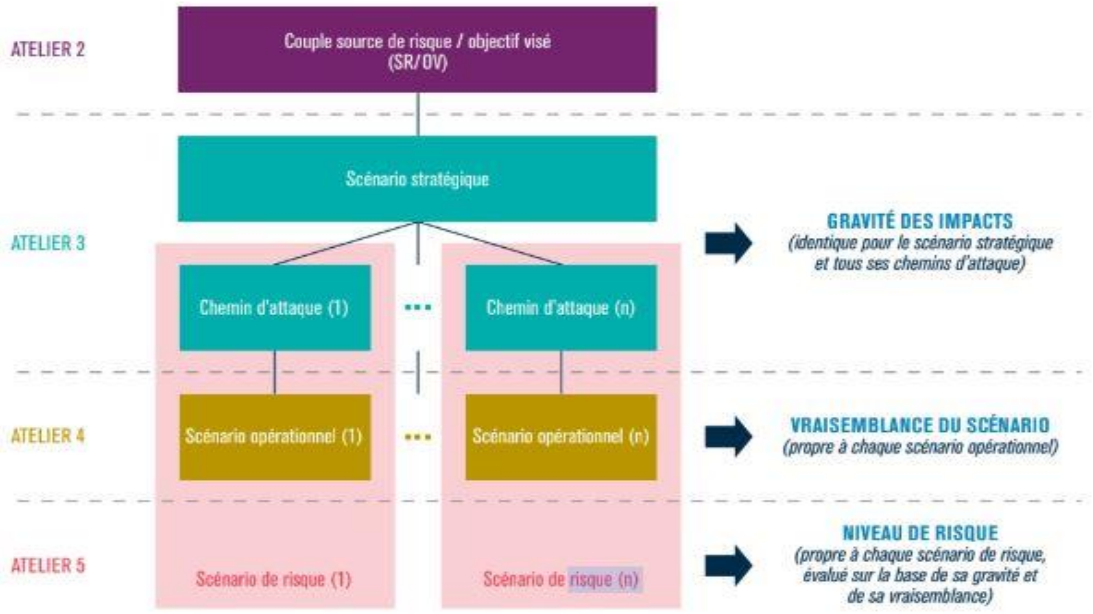
Le cinquième et dernier atelier, centré sur les *mesures de sécurité*, consiste à proposer des dispositifs de protection adaptés aux risques identifiés. Ces contre-mesures peuvent être préventives (durcissement des systèmes, segmentation réseau, formation), détectives (systèmes de surveillance, logs), ou réactives (plans de réponse aux incidents, PRA/PCA). L'objectif est de prioriser les mesures selon leur efficacité et leur adéquation avec les ressources de l'organisation.

L'un des points forts d'EBIOS Risk Manager est sa souplesse d'adaptation. Elle peut être mobilisée pour des projets spécifiques (mise en production d'un service cloud, refonte d'un SI), pour des analyses sectorielles (sécurité de la chaîne logistique, RGPD, etc.), ou à l'échelle globale d'un système d'information. Elle est en parfaite cohérence avec les principes de la norme ISO/IEC 27005, ce qui en fait un outil compatible avec les démarches de certification ou de mise en conformité réglementaire.

Pour l'ANSSI, "EBIOS Risk Manager permet de lier étroitement sécurité et stratégie d'entreprise, en partant des enjeux métiers et en remontant vers les menaces susceptibles de les compromettre" (ANSSI, 2017) .(Cette approche intégrée fait d'EBIOS un véritable levier de gouvernance, en facilitant la prise de décision, l'arbitrage des ressources de cybersécurité, et la communication entre les différents acteurs de l'organisation.

Finalement, EBIOS Risk Manager se présente comme une manière de penser clairement systémiquement et organiquement au risque de cyber sécurité, en lien avec l'enjeu majeur de la transformation numérique. Il donne aux organisations un cadre rigoureux afin d'anticiper les attaques, de mieux maîtriser leur surface d'exposition, de renforcer durablement leur résilience au risque face à la menace cyber.

Figure 4 la démarche de la méthode EBIOS



Source : (ANSSI, 2018).

2.5.2 La méthode MEHARI

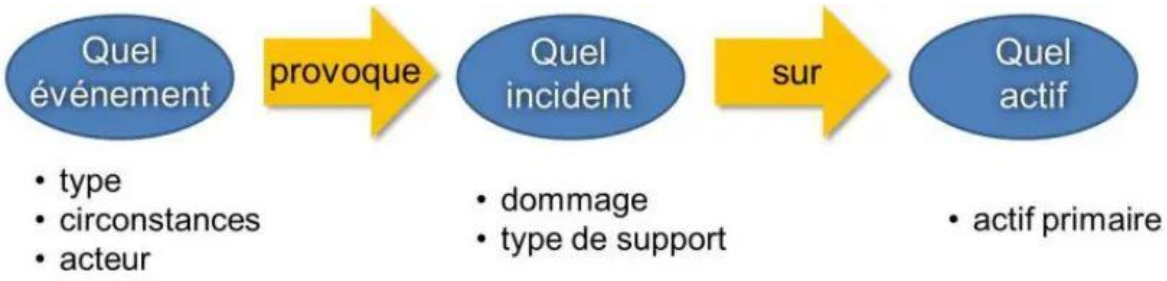
La méthode MEHARI (Méthode Harmonisée d'Analyse des Risques) est une méthodologie complète dans le domaine de la sécurité des systèmes d'information, mise au point par le CLUSIF (Club de la sécurité de l'information français). Sa version de 2010, fondée sur une formalisation rigoureuse et appuyée sur des bases de connaissances, garantit l'adéquation avec des démarches internationales, comme les normes ISO/IEC (27005, 2018)et ISO/IEC 27005:2008. L'intérêt de MEHARI est de permettre à des organismes d'avancer dans l'édification de leur gestion du risque par une prise en compte intégrée de préoccupations stratégiques, techniques et organisationnelles.

MEHARI, comme son nom l'indique, s'intéresse à la sécurité de l'information, c'est-à-dire aux systèmes informatiques par eux-mêmes et à toute une diversité d'information, qu'elle soit numérique, analogique, écrite, etc. (clusif, s.d.)

Dans ce cadre, la mission de MEHARI ne consiste pas seulement à détecter les situations à risque, et à estimer leur ampleur. Elle suppose aussi d'identifier les actions pour faire descendre le risque à un niveau convenable à travers des scénarios préétablis. Ces scénarios permettent de représenter de manière structurée les incidents potentiels pouvant

affecter les actifs critiques de l'organisation. Le schéma ci-dessous résume la logique de construction d'un scénario de risque

Figure 5 la logique de construction d'un scénario de risque



Source : (Les fondamentaux de Méhari, s.d.)**.**

MEHARI, qui se propose également de se concentrer sur le niveau de qualité et d'efficacité requis pour l'application des mesures, affirme au fond une règle première, qui vaut pour tous ses modules : il ne faut jamais minimiser un risque.

Les étapes de la méthode MEHARI :

La méthode MEHARI consiste donc en une démarche articulée en trois grandes phases : la phase préparatoire, la phase opérationnelle d'analyse des risques puis celle de planification et de traitement des risques. Dans chaque phase, un certain nombre d'étapes sont décrites et associées à des outils et livrables permettant de traiter les risques d'une manière complète. (CLUB DE LA SECURITE DE L'INFORMATION FRANçAIS, 2010)

a. Phase préparatoire :

La préparation à l'évaluation des risques consiste à situer cette évaluation dans un contexte organisationnel général. Le premier objectif de la phase de préparation est donc de prendre en compte le contexte stratégique, technique et organisationnel.

En effet, il s'agit de structurer la position de l'entité sur son marché, de prendre en considération les contraintes juridiques et réglementaires, tout en intégrant les objectifs de la politique de sécurité de l'information. Dans le domaine technique, il est nécessaire de procéder à une cartographie des systèmes d'information, de réaliser la documentation des architectures (réseaux, systèmes, applicatives) et d'identifier les fournisseurs critiques. L'analyse organisationnelle repose sur l'analyse de la structure hiérarchique, des responsabilités internes relatives à la sécurité et des processus de prise de décision

correspondant à l'organisation des plans d'action. (CLUB DE LA SECURITE DE L'INFORMATION FRANçAIS, 2010)

Une fois bien précisé le contexte qui précède, la démarche engagée consiste alors à délimiter rigoureusement la mission, en précisant à la fois le champ technique (recteurs de systèmes, genres de médias.) et organisationnel (activités mais aussi services ou filiales concernés par l'étude). Il est à ce stade également souhaitable de constituer un comité de pilotage devant encadrer le processus.

Cette phase se conclut finalement par la définition des paramètres techniques requis pour l'analyse, sous forme de : cadre des niveaux d'acceptabilité des risques (qui spécifie des limites de tolérance), cadre des expositions naturelles (ou potentialités intrinsèques aux risques), puis cadres d'évaluations des impacts et potentialités résiduels permettant d'apprécier les risques en fonction de divers scénarios. (CLUB DE LA SECURITE DE L'INFORMATION FRANçAIS, 2010)

b. Phase opérationnelle d'analyse des risques

Lors de la deuxième étape du travail, trois éléments principaux sont pris en compte : la catégorisation des actifs, l'évaluation des services de sécurité et l'estimation des risques. L'évaluation des enjeux commence par la mise en place d'une échelle de valeurs affectées aux dysfonctionnements potentiels de chacune des activités professionnelles, qui doit répondre à la difficulté à mesurer la gravité potentielle des atteintes à la confidentialité, à l'intégrité, à la disponibilité ou à la conformité.

Cette échelle sert pour la classification des actifs et doit permettre d'évaluer, pour chaque catégorie d'actifs (services, données, infrastructures, etc.), le potentiel d'impact maximal d'un dysfonctionnement. On utilise des grilles standardisées (T1, T2, T3) pour évaluer selon l'intensité de la menace, un score de gravité pour chaque bien de 1 (impact modeste) à 4 (impact sévère).

Parallèlement, une évaluation de la situation des services de sécurité est effectuée, pouvant concerner jusqu'à 14 aspects, comme la protection des sites, la gestion des identités, la sécurité des réseaux..., dans le but d'évaluer le niveau actuel des mesures de protection et donc les éléments susceptibles de réduire les risques.

Finalement, l'approche repose sur le choix de scénarios appropriés dans la base de données MEHARI (environ 800 scénarios possibles), avant de les évaluer selon leur sévérité. Cette

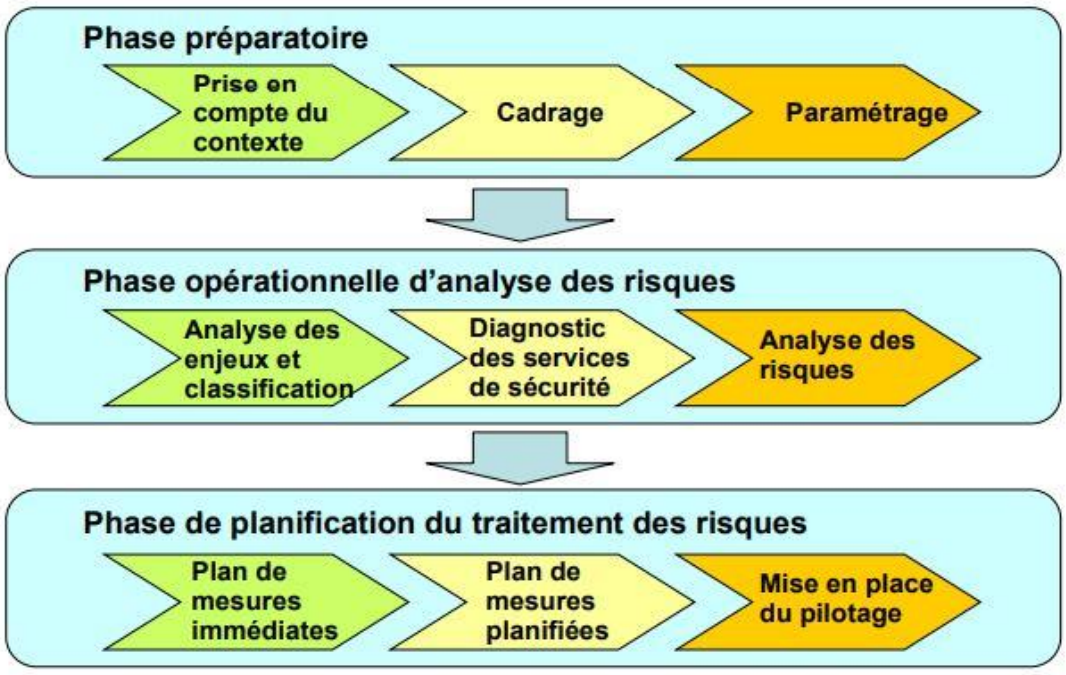
évaluation regroupe « impact intrinsèque », « exposition naturelle » et les conclusions du diagnostic de sécurité. Cela facilite la distinction entre les risques résiduels (risques post-mesures) et les risques intrinsèques (risques pré-mesures), ce qui permet de hiérarchiser les actions à entreprendre. (FRANÇAIS, 2010)

c. Phase de planification et de gestion des risques

L'étape finale vise à convertir les résultats de l'analyse en actions concrètes et gérables. Initialement, les risques considérés comme intolérables (habituellement de gravité 4) sont gérés en priorité par le biais d'actions immédiates. Ces mesures peuvent rechercher la diminution du risque (grâce à une meilleure maîtrise technique ou organisationnelle), son évitement, son transfert (par exemple : à travers une assurance), ou son acceptation si le coût de gestion s'avère excessif.

Ainsi, MEHARI souligne la nécessité d'une gestion permanente par le biais d'indicateurs clés de risque (KRI - Key Risk Indicators), de tableaux de bord et de révisions périodiques et continues des risques résiduels et mesures en cours, favorisant l'avancement d'un système de gestion des risques. (CLUB DE LA SECURITE DE L'INFORMATION FRANçAIS, 2010)

Figure 6 la démarche de MEHARI



Source : (FRANÇAIS, MEHARI 2010, 2011).

- **Application de la méthode MEHARI pour l'évaluation des risques :**

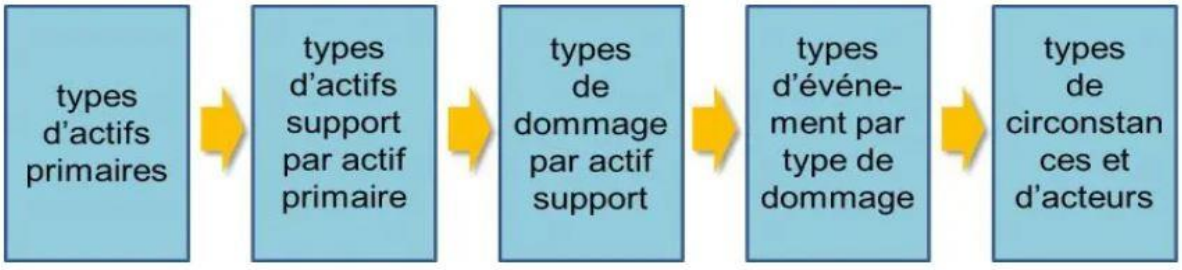
Pour l'évaluation des risques liés à l'informatique, la méthode MEHARI s'inscrit dans une démarche d'analyses et de classifications soit systématique, soit rigoureuse, soit orientée en fonction du domaine d'activité. Le risque est alors à la fois repéré, classé en fonction de sa gravité et des mesures propres à éviter son occurrence, mais aussi et surtout suivi au moyen des décisions prises.

L'analyse commence alors par l'établissement des enjeux commerciaux relatifs à la sécurité de l'information, c'est-à-dire, l'identification des activités critiques de l'organisation et agréées d'exigences spécifiques attachées à la confidentialité, à l'intégrité, à la disponibilité et à la conformité. Chaque information est ensuite examinée en fonction de la portée des effets, en cas de manquement à ces normes, facilitant ainsi la classification des actifs selon leur importance.

La phase d'analyse des risques proprement dite, vient alors, une fois les menaces identifiées, l'utilisation de scénarios de menaces, pré-formatées dans le répertoire de connaissances de MEHARI, pour reproduire des incidents probables. Chaque incident valide le lien entre une catégorie d'actif, une vulnérabilité et une menace, par une évaluation du potentiel de dommage possible et de la probabilité d'occurrence, considérée a priori avant intervention. Ce qui permet de prendre en compte toutes les combinaisons potentielles.

L'image ci-dessous présente cette suite logique :

Figure 7 La logique de traitement des risques MEHARI



Source : (clusif, s.d.).

L'étape suivante consiste à évaluer les services de sécurité existants, en important dans l'analyse que l'on fait du degré de protection déjà pris en charge (gestion des accès, sauvegarde de données, gestion de l'identité, …) et leur efficience réelle à corriger les

risques. Ceci finalement, nous permet d'atteindre une évaluation des risques résiduels (ceux qui demeurent par rapport aux mesures de sécurité déjà mises en place).

Un des points forts de MEHARI est sa capacité à quantifier les écarts de risque entre risque initial et risque résiduel, de manière à objectiver les décisions de traitement. Les risques les plus élevés (niveau 4) sont intégrés dans des plans d'action immédiat, les autres pouvant être intégrés dans une planification stratégique de la sécurité, en balance avec les ressources disponibles, les délais et les priorités métier.

Enfin, MEHARI promeut un pilotage dynamique du risque à l'aide d'indicateurs clés (KRI), de tableaux de bord, et de revues régulières, garantissant ainsi l'amélioration continue du dispositif de sécurité, ainsi qu'une meilleure résilience face aux menaces managériales évolutives. (FRANÇAIS, 2011)

2.5.3 La méthode OCTAVE

OCTAVE est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Une fois ces derniers identifiés, la méthode permet de mesurer les menaces et les vulnérabilités pesant sur eux.

Les trois étapes subséquentes détaillées dans OCTAVE suivent l'examen graduel des trois segments des notions de gestion des risques exposées précédemment :

La première phase (perspective organisationnelle) consiste à repérer les ressources informatiques essentielles, les risques liés et les exigences de sécurité correspondantes.

La phase 2 (perspective technique) vise à déceler les failles de l'infrastructure (celles-ci, une fois associées aux menaces, engendrent le risque).

La phase 3 de la méthode décline le développement de la stratégie de sécurité et sa planification (protection et plan de réduction des risques). (Etiévant, 2006)

Figure 8 phases de la méthode OCTAVE

Source : (Etiévant, 2006).

2.6 Les critères de choix de méthode de gestion des risques SI

La sélection d'une méthode de gestion des risques des systèmes d'information repose sur des critères stratégiques garantissant son efficacité opérationnelle et son intégration dans l'organisation. Cette section précise les indicateurs à apprécier suivantes :

- L'origine géographique de la méthode, la culture du pays jouant beaucoup sur le fonctionnement interne des entreprises et leur rapport au risque.
- La langue de la méthode, il est essentiel de maîtriser le vocabulaire employé
- La qualité de la documentation
- La compatibilité avec une norme nationale ou internationale
- Le coût de la mise en œuvre
- La quantité de moyens humains qu'elle implique et la durée de mobilisation
- La taille de l'entreprise à laquelle elle est adaptée
- Le support de la méthode par son auteur, une méthode abandonnée n'offre plus la possibilité de conseil et de support de la part son éditeur
- Sa popularité, une méthode très connue offre un réservoir de personnels qualifiés pour la mettre en œuvre. (Amina, 2020/2021)

3. Intelligence Artificielle appliquée à la Gestion des Risques SI

Dans un cadre où les SI sont de plus en plus compliqués et exposés à toute une série de risques, la IA apparaît en tant que solution inusitée pour l'accroissement de la résilience organisationnelle. L'IA assemble un ensemble de méthodes, telles que le Machine Learning (apprentissage automatique), le Deep Learning (apprentissage profond), et le Traitement Automatique du Langage Naturel (NLP), qui permettent aux systèmes informatiques d'apprendre en fonction des données, de faire des reconnaissances de modèles et d'interagir de manière intelligente avec leur monde. Appliquée à la gestion des risques SI, l'IA offre des apports significatifs dans l'analyse, la détection et la prédiction des incidents. Grâce au machine Learning, les entreprises peuvent détecter des anomalies en temps réel, prédire des pannes ou intrusions potentielles, et établir des profils de risques évolutifs. Par exemple, dans le domaine de la cybersécurité, l'IA est utilisée pour identifier des comportements suspects, bloquer des attaques automatiquement et renforcer la vigilance face aux menaces émergentes. De plus, les capacités prédictives de l'IA permettent d'anticiper des défaillances système ou des erreurs humaines à fort impact

3.1 Définition et technologies pertinentes de l'Intelligence Artificielle

Pour bien appréhender les apports de l'intelligence artificielle, il convient tout d'abord d'en définir clairement le concept.

3.1.1 Définition de l'intelligence artificielle (IA)

L'intelligence artificielle est une branche de l'informatique qui cherche à développer des systèmes capables de reproduire l'intelligence humaine. Cela regroupe un éventail de méthodes et de théories qui permettent à un système d'apprentissage automatique de percevoir son environnement, d'acquérir des connaissances à partir de données, de raisonner, de prendre des décisions et parfois même d'agir par lui-même. L'intelligence artificielle peut se présenter sous différents aspects, comme la reconnaissance de la parole, la vision informatique, les systèmes expertes ou encore les aides virtuelles. Elle s'appuie sur divers champs tels que l'apprentissage automatique (machine Learning), le traitement du langage naturel et les réseaux de neurones, et trouve son application dans de nombreux secteurs comme la santé, la finance, l'industrie et même les transports. (Pastre, 1999/2000).

3.1.2 Définition de l'Intelligence Artificielle appliquée à la gestion des risques des systèmes d'information (SI)

L'intelligence artificielle (IA) désigne un ensemble de technologies capables de simuler l'intelligence humaine, en apprenant à partir de données, en prenant des décisions et en résolvant des problèmes complexes. Dans le contexte de la gestion des risques des systèmes d'information, l'IA joue un rôle de plus en plus central.

En effet, les environnements numériques actuels sont caractérisés par une complexité croissante, une multiplication des flux de données, et une intensification des menaces informatiques. Dans ce cadre, l'IA se révèle particulièrement efficace pour renforcer les mécanismes de sécurité. Elle permet d'automatiser la détection d'anomalies, de prédire des comportements suspects, et de réagir rapidement face à des cyberattaques potentielles.

Ce potentiel repose notamment sur la capacité de l'IA à traiter d'importants volumes de données en temps réel, à identifier des modèles invisibles à l'œil humain, et à ajuster ses réponses de manière autonome. Ainsi, l'IA offre une nouvelle dimension à la gestion des risques SI, en rendant les systèmes plus résilients, plus réactifs et plus intelligents face aux menaces internes et externes. (Pastre, 1999/2000)

3.1.3 Technologies pertinentes en Intelligence Artificielle pour la gestion des risques SI

Dans le cadre de la gestion des risques des systèmes d'information, plusieurs technologies d'intelligence artificielle se révèlent particulièrement pertinentes. Parmi elles, on retrouve l'apprentissage automatique (Machine Learning), l'apprentissage profond (Deep Learning), le traitement automatique du langage naturel (NLP), ainsi que d'autres approches avancées.

Le Machine Learning regroupe des algorithmes capables d'apprendre à partir de données historiques pour détecter des modèles, identifier des comportements inhabituels et anticiper certains types de menaces. Il existe plusieurs formes d'apprentissage :

- **L'apprentissage supervisé**, qui repose sur des données étiquetées pour entraîner un modèle à faire des prédictions précises ;
- **L'apprentissage non supervisé**, qui permet de découvrir des schémas cachés ou des anomalies dans des données non structurées ;

- **L’apprentissage par renforcement**, où le système apprend par essais-erreurs afin d’optimiser ses décisions au fil du temps.

Le Deep Learning, quant à lui, s’appuie sur des réseaux de neurones artificiels très profonds et est particulièrement efficace pour le traitement d’images, de sons ou de grandes bases de données complexes. Il améliore la capacité de détection des menaces complexes ou furtives.

Enfin, le NLP (Natural Language Processing) est utilisé pour analyser les flux d’informations textuelles, comme les e-mails, les logs systèmes ou les messages réseaux, afin de détecter des signes d’attaques, de fraudes ou de tentatives d’hameçonnage.

Comme mentionné dans l’article, *« parmi les techniques d'IA largement utilisées en cybersécurité figurent l'apprentissage supervisé, l'apprentissage non supervisé, l'apprentissage par renforcement et l'apprentissage profond »* (Kunle-Lawanson O. , 2022)

Ces technologies, combinées à des capacités de traitement en temps réel, permettent aujourd’hui de construire des systèmes de défense beaucoup plus intelligents, proactifs et adaptatifs face aux risques pesant sur les systèmes d’information.

3.2 Apports potentiels de l’intelligence artificielle dans l’analyse, la détection et la prédiction des risques liés aux systèmes d’information

L’intelligence artificielle (IA) s’impose aujourd’hui comme un levier stratégique majeur dans l’optimisation des systèmes de gestion des risques. Sa capacité à traiter des volumes massifs de données en temps réel, à identifier des modèles complexes et à détecter des comportements inhabituels en fait un outil puissant pour renforcer la sécurité et la résilience des systèmes d’information.

Premièrement, l’IA permet l’analyse approfondie de données hétérogènes issues de multiples sources, telles que les fichiers journaux (logs), les bases de données ou encore les flux de communication réseau. Grâce à ses algorithmes avancés, elle est capable d’extraire des signaux faibles et de mettre en lumière des corrélations souvent indétectables par les méthodes traditionnelles.

Deuxièmement, l’IA contribue à la détection proactive des incidents de sécurité, en identifiant automatiquement des anomalies ou des comportements suspects. Par exemple, les algorithmes de Machine Learning peuvent apprendre à reconnaître des modèles

d'activité typiques, et signaler toute déviation comme une potentielle menace interne ou externe.

Enfin, l'intelligence artificielle joue un rôle clé dans la prédiction des risques. En s'appuyant sur des historiques d'incidents et sur des modèles prédictifs, les systèmes intelligents peuvent anticiper certains types de défaillances ou d'attaques avant qu'ils ne surviennent, ce qui améliore considérablement la réactivité des équipes informatiques.

Comme le souligne l'article scientifique : *« L'IA peut traiter de vastes ensembles de données afin d'identifier des modèles, de détecter des anomalies et d'améliorer les capacités de détection des menaces. Les techniques de Machine Learning sont particulièrement efficaces pour analyser de grandes quantités de données et identifier des menaces qui pourraient échapper aux méthodes classiques. »* (Kunle-Lawanson O. , 2022)

3.3 Limites et défis d'intégration de l'IA dans la gestion des risques des SI

Bien que l'intelligence artificielle (IA) représente une avancée significative dans la gestion des risques liés aux systèmes d'information, son intégration soulève de nombreuses problématiques techniques, économiques, éthiques et réglementaires. Ces défis doivent être examinés avec attention afin de garantir une adoption maîtrisée et responsable.

3.3.1 Obstacles techniques : coût élevé et complexité d'intégration

L'intégration de l'IA dans les systèmes de gestion des risques SI implique des investissements technologiques et humains importants. Sur le plan technique, le développement et le déploiement de solutions d'IA nécessitent des infrastructures spécifiques telles que des serveurs puissants, des capacités de stockage élevées, et des plateformes logicielles avancées. Ces technologies doivent être capables de traiter en temps réel de très grandes quantités de données issues des systèmes d'information.

De plus, l'exploitation de ces technologies requiert une main-d'œuvre hautement qualifiée, notamment des data scientistes, des ingénieurs en cybersécurité, et des experts en machine learning. Cette double exigence (infrastructure + compétences) engendre des coûts très élevés, souvent inaccessibles pour les petites et moyennes entreprises (PME).

"The process of using AI for information security can be resource-consuming. Sophisticated hardware, high-performance processors and data storage systems are

needed… These costs can be prohibitively expensive for many smaller organizations.” (Kunle-Lawanson O. , 2022)

La complexité technique est également un frein : la mise en œuvre de systèmes d’IA performants demande une compréhension approfondie des fondements de l’intelligence artificielle, de la cybersécurité, mais aussi des enjeux organisationnels. Or, il existe un manque de profils hybrides possédant ces compétences transversales, ce qui ralentit l’adoption de ces technologies.

“To implement AI in information security, you need to know much more than just information security – machine learning, data analysis, foundations of AI, and AI ethics… there is a skill gap in the cybersecurity workforce.” (Kunle-Lawanson O. , 2022)

3.3.2 Défis éthiques et réglementaires

L’autre grande limite à l’intégration de l’IA concerne les considérations éthiques et juridiques. Les systèmes d’IA utilisés dans la sécurité des SI reposent sur l’analyse massive de données personnelles ou sensibles (comportements, connexions, communications, géolocalisation, etc.). Ce traitement soulève des enjeux cruciaux en matière de respect de la vie privée, de transparence des décisions algorithmiques et de conformité aux réglementations comme le RGPD (Règlement Général sur la Protection des Données) en Europe, ou HIPAA aux États-Unis dans le secteur de la santé.

“Machine learning models and other AI technologies are data-hungry… The collection, storage, and processing of such high volumes may raise privacy concerns when the information is personal or sensitive… adhering to privacy laws and regulations such as GDPR, HIPAA.”. (Kunle-Lawanson O. , The role of AI in information security risk management, 2022)

L'usage de l’IA pour surveiller les comportements des utilisateurs ou des employés peut aussi être perçu comme intrusif, voire contraire aux droits fondamentaux. Cette surveillance automatisée peut générer un sentiment de contrôle excessif, nuire au climat de confiance au sein des organisations et poser des risques réputationnels.

“By using AI to track employee behavior, we might risk colliding with individual privacy rights… organizations must ensure that they handle this data responsibly and transparently to preserve trust.” (Kunle-Lawanson O. , 2022).

Par ailleurs, le manque de transparence des algorithmes (souvent qualifiés de "boîtes noires") complique leur adoption dans un cadre réglementé où les décisions doivent être justifiables et auditables.

CHAPITRE II : CADRE METHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

Avant d'aborder notre analyse empirique, nous avons dans le premier chapitre posé les fondations théoriques et conceptuelles de notre travail, en examinant la gestion des risques des systèmes d'information et les apports potentiels de l'intelligence artificielle dans un contexte organisationnel complexe. Cette revue de littérature nous a permis de cerner les normes, référentiels et méthodes classiques utilisés dans le domaine, tout en identifiant les limites auxquelles font face les grandes entreprises industrielles.

Dans ce deuxième chapitre, nous allons présenter la méthodologie adoptée pour mener à bien cette étude (section 1). Nous détaillerons les choix de recherche, les outils de collecte des données, ainsi que les techniques d'analyse utilisées. L'objectif est de décrire précisément le cadre dans lequel notre enquête a été menée, en justifiant chacun des choix méthodologiques retenus.

Nous consacrerons également une partie à la présentation de l'ENGTP, entreprise d'accueil dans laquelle notre stage a été réalisé et qui constitue le terrain de notre étude (section 2). Ce cadre nous a permis d'observer concrètement les pratiques de gestion des risques SI et d'interroger les responsables concernés sur les perspectives d'intégration de solutions d'intelligence artificielle.

Enfin, nous exposerons les outils mobilisés – notamment les entretiens semi-directifs, l'analyse documentaire et l'observation – et les critères ayant guidé la sélection des participants à l'enquête. Ce dispositif méthodologique nous a permis de recueillir des données riches et contextualisées, indispensables à une compréhension fine des enjeux de sécurité numérique et à l'identification des leviers d'optimisation basés sur l'IA.

Section 01 : cadre méthodologique

Cette section présente les différentes étapes méthodologiques suivies, à commencer par le choix du thème.

1.1 Choix du thème

Le thème de cette recherche porte sur l'intégration de l'intelligence artificielle dans la gestion des risques des systèmes d'information, une problématique d'actualité dans un contexte de transformation numérique accélérée. Face à l'évolution constante des menaces informatiques, les entreprises doivent renforcer leurs capacités à anticiper, détecter et gérer efficacement les risques liés à leurs systèmes d'information.

À travers cette étude, nous visons à analyser l'apport potentiel de l'IA dans l'optimisation des processus de gestion des risques SI, tout en identifiant les conditions organisationnelles favorables à son adoption dans un environnement industriel stratégique. Ce sujet s'inscrit pleinement dans la continuité des enseignements reçus en management stratégique, systèmes d'information et data, et répond à un besoin réel d'innovation sécuritaire, face à la montée en complexité des menaces numériques.

1.2 Choix de l'entreprise

ENGTP (Entreprise Nationale de Grands Travaux Pétroliers) a été choisie comme terrain d'étude en raison de son rôle stratégique dans le secteur énergétique et de sa forte dépendance aux systèmes d'information. Évoluant dans un environnement technique complexe, l'entreprise est confrontée à divers risques numériques, ce qui rend la gestion des risques SI essentielle à la continuité de ses activités.

1.3 Méthode de recherche

La recherche a été conduite selon une approche qualitative, centrée sur l'analyse approfondie d'un phénomène organisationnel complexe : l'intégration de l'intelligence artificielle dans la gestion des risques des systèmes d'information. Selon Mays et Pope (1995), l'objectif de la recherche qualitative est de développer des concepts permettant de comprendre les phénomènes sociaux dans leur contexte naturel, en mettant l'accent sur les significations, les expériences vécues et les points de vue des participants.

Cette méthode est particulièrement pertinente pour explorer les pratiques, les perceptions et les défis rencontrés par les professionnels de l'ENGTP dans le domaine de la sécurité des SI. Elle permet également de saisir les enjeux stratégiques et techniques liés à l'introduction de l'IA, en tenant compte des spécificités de l'environnement industriel, des contraintes réglementaires et des réalités opérationnelles de l'entreprise.

1.4 Méthodes et techniques de récolte des données

Méthode :

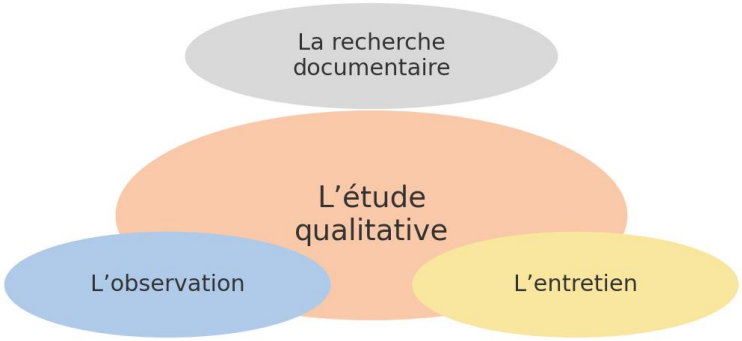
Selon Pinto & Grawitz (1971), une méthode désigne « un ensemble d'étapes utilisées par une discipline pour parvenir aux vérités qu'elle cherche à établir ». Dans la même logique, Raynal & Rieunier (1998) soulignent que la méthode correspond à une structuration codifiée des techniques et des moyens employés pour atteindre un objectif précis. Notre

recherche a donc suivi une méthode qualitative rigoureuse, visant à explorer en profondeur les pratiques de gestion des risques des systèmes d'information, ainsi que les opportunités d'intégration de l'intelligence artificielle dans une entreprise industrielle telle que l'ENGTP.

Technique :

Comme le définit Nguapitshi Kayongo (2009), une technique est un ensemble de moyens concrets mobilisés dans un contexte donné pour mener à bien une enquête. Dans le cadre de notre travail, nous avons utilisé les techniques suivantes :

Figure 9 Les techniques de collecte des données



Source : élabore par nous-même

1.4.1 La recherche documentaire

La recherche documentaire a constitué une étape préliminaire essentielle, permettant d'asseoir notre cadre théorique. Elle a consisté en une exploration systématique de documents spécialisés (normes, guides, rapports techniques, articles scientifiques, mémoires, documents internes de l'ENGTP) afin de cerner les pratiques en matière de gestion des risques SI, les normes ISO applicables (ISO/IEC 27001, ISO/IEC 27005, ISO 31000), ainsi que les apports potentiels de l'IA dans ce domaine.

Nous avons consulté :

- Des ouvrages spécialisés disponibles à la bibliothèque de l'École Nationale Supérieure de Management (ENSM),
- Des articles issus de bases de données comme ASJP, SNDL et Scholarvox,

- Des rapports internes de l'ENGTP (procédures SI, politiques de sécurité, documentation des outils).

Cette phase a permis de construire les axes de réflexion, de concevoir le guide d'entretien, et de comparer les données empiriques avec les standards théoriques.

1.4.2 L'observation

L'observation directe a été rendue possible grâce à notre stage pratique au sein de la direction des systèmes d'information de l'ENGTP. Cette immersion a permis de recueillir des informations empiriques sur :

- Les processus de gestion des risques en place,
- L'environnement technique et organisationnel,
- Les outils utilisés pour la sécurité des SI,
- Les comportements des agents face aux incidents ou aux menaces potentielles.

L'observation a offert une vue globale et réaliste de l'état des lieux, facilitant l'identification de certaines dissonances entre les procédures prévues et les pratiques réelles.

1.4.3 Les entretiens semi-directifs

Pour compléter les données documentaires et les observations, nous avons mené une série de trois entretiens semi-directifs avec des profils clés au sein de l'ENGTP : responsables SI, ingénieurs développement, experts réseaux, et chef de département sécurité.

Ces entretiens visaient à :

- Recueillir leurs expériences et perceptions sur la gestion actuelle des risques,
- Explorer les limites des méthodes traditionnelles,
- Évaluer leur ouverture et leur vision quant à l'introduction de l'intelligence artificielle dans les systèmes de sécurité.

Les entretiens ont été menés de manière progressive au fil des visites effectuées durant le stage, chaque session abordant une partie spécifique du guide d'entretien thématique (Annexes 1 à 4). Cette approche a permis non seulement de préparer à l'avance certaines réponses, mais aussi de laisser place à la découverte de nouveaux éléments au fur et à

mesure des échanges. Le guide d'entretien a servi de fil conducteur pour structurer les discussions autour de cinq grandes rubriques clés :

1. Gestion des risques SI.
2. Outils et méthodes utilisés.
3. IA et sécurité informatique.
4. Enjeux stratégiques.
5. Propositions d'amélioration.

Les propos recueillis ont ensuite été analysés à l'aide d'une grille d'analyse thématique, permettant de faire émerger les convergences et divergences entre les répondants, tout en reliant leurs témoignages au cadre théorique.

1.5 La sélection des interviewés

Durant notre stage à l'ENGTP, nous avons mené trois entretiens avec des professionnels occupant des fonctions clés dans les systèmes d'information. Les personnes interrogées sont : le Responsable de la Sécurité des Systèmes d'Information (RSSI), le Responsable des Projets SI (PMSI) et un Administrateur de Bases de Données (DBA).

Ces échanges nous ont permis de collecter des données qualitatives précises sur les pratiques de gestion des risques, les outils utilisés, et la perception de l'intelligence artificielle dans ce contexte. Leurs réponses ont offert une vision concrète et professionnelle du fonctionnement de l'entreprise, en lien avec notre sujet d'étude.

Tableau 1: Information sur les interviewés

Interviewé	Diplôme	Pote de travail	Expérience
Responsable 01	Ingénieur d'état en Informatique	Responsable sécurité de système d'information	19 ans
Responsable 02	Ingénieur d'état Inf.	Chef de projet Systèmes informatiques	15 ans
Responsable 03	Ingénieur d'état Inf.	Administrateur bases de données	25 ans

Source : élaboré par nous-même.

1.6 La construction du guide d'entretien

1.6.1 Structure

Le guide d'entretien que nous avons élaboré dans le cadre de notre mémoire est structuré en quatre grandes parties, chacune portant sur des aspects clés liés à la gestion des risques SI et à l'intégration de l'intelligence artificielle dans le contexte de l'entreprise ENGTP. L'objectif est de couvrir de manière exhaustive l'état actuel, les pratiques méthodologiques, les perspectives d'innovation, ainsi que la vision stratégique des professionnels interrogés.

Thème A : Gestion des risques des systèmes d'information

Cette première partie vise à comprendre la politique actuelle de gestion des risques SI au sein de l'ENGTP. Elle aborde :

- Les pratiques générales et les outils utilisés pour l'identification, l'évaluation et la mise à jour des risques,
- Les types de risques les plus fréquents rencontrés (cybermenaces, pannes, erreurs humaines, etc.),
- Les normes et référentiels appliqués (tels que ISO 27001 ou ISO 31000) pour structurer la gestion des risques.

Thème B : Outils et méthodes d'analyse des risques

Ce thème est centré sur l'utilisation des méthodes d'évaluation des risques SI, en particulier les cadres comme MEHARI, EBIOS et OCTAVE. Il permet d'identifier :

- Les outils réellement utilisés par l'entreprise,
- Les raisons de leur adoption (ou non),
- Les avantages et limites perçus de ces approches dans le contexte spécifique d'une entreprise industrielle.

Thème C : L'intelligence artificielle appliquée à la gestion des risques

Cette section interroge les répondants sur leur perception et leur expérience en matière d'IA, notamment :

- L'existence ou non d'initiatives liées à l'IA dans la sécurité des SI,
- Leur vision sur l'apport potentiel de l'IA pour la détection et la prévention des risques,
- Les obstacles rencontrés dans son adoption (compétences, budget, culture d'entreprise),
- Les conditions favorables à son intégration (accompagnement, sensibilisation, investissement...).

Thème D : Vision stratégique et prospective

Enfin, cette dernière partie vise à comprendre la projection des professionnels sur l'évolution de la gestion des risques SI. Elle explore :

- Leur vision sur l'avenir de la cybersécurité,
- Les leviers stratégiques envisagés pour anticiper et gérer les menaces émergentes.

1.6.2 Difficultés rencontrées dans la construction du guide d'entretien

La conception du guide d'entretien a représenté une étape déterminante mais non dénuée de difficultés. L'un des principaux défis a été de trouver un juste équilibre entre la précision des questions et la clarté des thématiques abordées. Il était nécessaire de formuler des questions à la fois suffisamment ouvertes pour encourager l'expression libre des répondants, tout en gardant une cohérence avec les objectifs de recherche et les axes du mémoire.

Une autre difficulté notable a concerné l'adaptation du contenu aux spécificités de l'étude de cas ENGTP. Bien que le guide s'appuie sur des cadres théoriques généraux liés à la gestion des risques et à l'intelligence artificielle, il a fallu veiller à contextualiser les formulations pour qu'elles correspondent à la réalité du secteur pétrolier et aux pratiques propres à l'organisation. Ce travail d'ajustement s'est aussi accompagné d'une volonté de conserver une certaine transférabilité : autrement dit, les questions devaient rester exploitables dans d'autres contextes similaires, notamment pour des entreprises industrielles confrontées à des problématiques de cybersécurité et de transformation numérique.

Enfin, la multiplicité des angles abordés (management des risques, IA, normes ISO, stratégie SI…) a exigé une structuration rigoureuse, afin de ne pas surcharger l'entretien tout en assurant une couverture complète des dimensions du sujet.

1.7 Le traitement des données

Cette approche permet d'examiner en profondeur les données collectées, en mettant en évidence les thèmes et motifs essentiels

1.7.1 Analyse de contenu

Pour examiner les données qualitatives obtenues lors des entretiens, nous avons choisi d'utiliser la méthode d'analyse de contenu, qui offre une interprétation méthodique, organisée et neutre des propos des participants. Cette approche est particulièrement appropriée pour notre recherche, car elle cherche à identifier les motifs récurrents, les représentations et les perceptions associées à notre thématique.

L'analyse de contenu repose sur un processus de codification thématique, consistant à identifier, regrouper et interpréter les unités de sens à partir des verbatims collectés. Cette approche permet de faire émerger des tendances significatives, d'explorer les convergences et divergences entre les répondants, et d'apporter une lecture approfondie du contexte organisationnel.

Pour analyser les entretiens réalisés, nous avons utilisé le logiciel NVivo14, un outil très utile pour ce type de recherche qualitative. Il nous a aidé à mieux organiser les données recueillies, à créer des catégories thématiques en lien direct avec notre problématique, et à

repérer plus facilement les idées ou notions qui revenaient souvent dans les réponses. Grâce à NVivo14, il a aussi été possible de faire le lien entre les propos des participants et les concepts abordés dans notre cadre théorique, ce qui a renforcé la cohérence de notre analyse.

L'utilisation du logiciel NVivo a contribué à améliorer la fiabilité et la traçabilité de l'analyse, tout en offrant une meilleure lisibilité des résultats à travers des fonctions de cartographie, de synthèse et de requêtes textuelles.

Section 02 : Présentation de l'organisme d'accueil

Dans cette section, nous présentons le contexte organisationnel de l'étude à travers une brève introduction de l'entreprise ENGTP

1. Présentation de l'entreprise

L'Entreprise Nationale des Grands Travaux Pétroliers (ENGTP) est une filiale à 100 % du groupe SONATRACH, spécialisée dans la réalisation de projets industriels majeurs dans les secteurs des hydrocarbures, de l'énergie, et plus récemment de l'hydraulique et des énergies renouvelables. Fondée le 19 février 1989, ses actions étaient détenues d'une part par la société mère à 51% et d'autre part par la Société de Gestion de participation à 49% jusqu'au 13 Décembre 2005 où toutes ses actions sont détenues à 100 % par Sonatrach.

Elle est aujourd'hui un acteur clé de l'industrie pétrolière et gazière en Algérie, son capital social est actuellement de 2.790.000.000 DA. Son Objet social est l'étude et la réalisation des projets d'installation matérielle notamment dans les domaines des hydrocarbures, de l'hydraulique, de l'énergie, de l'agroalimentaire, des matériaux de construction et des industries s'y rapportant, à l'intérieur du territoire et à l'étranger. La maintenance d'installations industrielles en exploitation. La formation dans ce domaine de soudage, contrôle et activités annexes.

Le siège social de l'entreprise est basé à Réghaïa (Alger), et son organisation couvre l'ensemble du territoire national à travers six unités régionales implantées à Réghaïa, Arzew, Skikda, Hassi Messaoud, Hassi R'mel et In Amenas. L'entreprise dispose d'un parc de plus de 8 500 équipements et d'un effectif important, ce qui lui confère une forte capacité opérationnelle dans les zones industrielles du nord et les régions productives du sud.

ENGTP est également engagée dans une dynamique de diversification stratégique, notamment à travers la construction de centrales solaires et de stations de dessalement d'eau de mer. Son Centre de soudure et d'expertise à Arzew constitue un pôle technique essentiel, dédié à la formation, au contrôle qualité, à la métrologie et aux essais spécialisés.

D'autre part, l'entreprise affirme sa dimension stratégique par la conclusion de partenariats de haut niveau, comme le contrat EPC signé avec le Groupement TFT (Sonatrach – Total Energies) pour le développement du champ gazier de TFT dans le bassin d'Illizi.

1.1 Historique

L'Entreprise Nationale des Grands Travaux Pétroliers (ENGTP) trouve ses origines en 1968 sous le nom d'ALTRA, société d'économie mixte affiliée à Sonatrach. Elle devient filiale à 100 % en 1972, avant d'être restructurée en 1980 par décret pour devenir une entreprise socialiste à caractère économique.

Depuis, ENGTP a connu plusieurs évolutions structurelles et organisationnelles majeures. Elle passe en société par actions en 1989, étend ses directions opérationnelles et centrales dans les années 1990, et adopte progressivement une organisation divisionnaire géographique afin de mieux répondre aux exigences du terrain.

En parallèle, son capital social et son chiffre d'affaires ont connu une croissance importante, atteignant 10 milliards de dinars en 2003. Cette dynamique de développement s'est accompagnée de la création de nouvelles directions (logistique, maintenance, catering, audit, qualité), marquant une volonté d'adaptation stratégique, d'élargissement des compétences internes et de professionnalisation de la gouvernance.

1.2 Missions de « GTP »

- Études et la réalisation des projets d'installations matérielles dans le domaine des hydrocarbures et des industries s'y rapportant.
- Etudes générales industrielles, résolution des problèmes technico-économiques et expertise.
- Contrôle et réception de tous matériaux, matériels et installations industrielles.
- La réalisation des grands ensembles industriels dans le domaine des Hydrocarbures et des industries se rapportant à son objet.
- La formation des hommes.

- Réalisation de réseaux de collectes et désertes d'Hydrocarbures liquides et gazeux et des installations de surfaces y afférents.

1.3 Objectifs de GTP

Les objectifs que cherche à atteindre GTP sont :

- Le développement et l'amélioration de la rentabilité de ces activités.
- La fidélisation de sa clientèle.
- Une exploitation de toutes les opportunités offertes par la mondialisation tant au niveau national qu'international.
- La pénétration des marchés extérieurs.
- L'augmentation de son chiffre d'affaires et de sa part de marché.

1.4 Activités de l'entreprise

- Etudes, procurement, supervision, essais et mise en service d'installations industrielles.
- Génie-civil et bâtiments industriels (travaux et terrassements généraux de fondations des équipements, de VRD…).
- Génie-mécanique (préfabrication et montage de structure métallique de tuyauteries d'équipements statiques ou dynamiques…).
- Génie-électrique (installation d'équipements électriques et d'instrumentations, étalonnage et montage des instruments …).
- Canalisation (topographique, bardage de tubes, soudage et contrôle, testes hydrostatiques et protection cathodiques).
- Soudage (procèdes SMA W, GTA W, GMA W, FCA W, SA W).
- Contrôle (non destructif par rayons x, rayons Gamma et destructif par compression, traction, pliage, résilience et macrographie).
- Traitement thermique.
- Maintenance industrielle (intervention préventive par la mise à disposition d'équipes d'entretien ou curative par la remise en état d'équipements ou d'organes d'une usine en exploitation). Ses différents domaines d'intervention sont :
    - Secteur Hydrocarbures.
    - Secteur Chimie et Pétrochimie.
    - Secteur Energie Electrique.
    - Secteur Agroalimentaire.

- Secteur Matériaux de Construction.

Principales réalisations en Algérie :

Secteur Hydrocarbures :

1978 : Centre de stockage et distribution à Remchi, Tébessa, Ghardaïa, Sétif et Saida.
1979 : Raffinerie à Hassi Messaoud 1 200 000 T / AN.
1979/1988 : Station de pompage, compression et injection Gaz et Eau (Hassi Messaoud).
1979/1991 : Centre Emplisseurs GPL à Touggourt, Sétif, Tiaret, Bouira, Khroub et Blida (de 1 200 à 2 400 bouteilles / heures).
1981 : Unité d'optimisation de pétrole brut.
1982/1986 : Unité traitement de Gaz (Hassi R'mel, Hassi Messaoud).
1993 : Unité de Reforming Catalytique à Skikda 50 000 T/AN.
1995 : Unité de traitement et de recyclage de G.N à Hamra 1 500 000 T/AN GPL Condensât.
Usine de récupération assistée de pétrole (Rhourd EL Baguel).
Unité d'extraction GPL (Rhourd Nouss).
Unité de traitement de GPL (Hassi Messaoud).
Unité de traitement de Gaz (Alrar).
Revamping (Hassi Messaoud).
Unité de traitement de Gaz (TFT).
Module zéro et une phase B (Hassi R'mel).
Station de traitement de Gaz (Ourhoud).

Secteur Chimie et Pétrochimie :

1969 : Complexe Acide Nitrique et Ammoniaque à Arzew.
1980 : Unités Complexes Engrais à Annaba.
PEHD (Skikda).

Secteur Energie

1980/1990 : Centrale Thermoélectrique I et II à Mers-El-Hadjadj 168 MGW x 5.
1988 : Centrales à Gaz Hassi Messaoud, 3 x 26 MGW, centrale Hassi R'mel 3 x 25 MGW, centrale à Tiaret 3 x 110 MGW.
Centrales Electriques (Jijel 1993, Adrar 1994).

Secteur Matériaux de construction (Cimenterie)

1975 : Montage des équipements de Mefteh 1 000.000 T/AN.
1978 : Montage des équipements de Ain Kebira 1 000.000 T/AN.

Activité permanente

Réseaux de Collectes et Dessertes (Hassi Messaoud, In Amenas et Hassi R'mel).

Pour propre compte

1975/1980 : Étude et Réalisation du siège social de l'entreprise à Réghaia.
1975/1983 : Étude et Réalisation d'une base vie permanente, d'une capacité de 362 lits à Hassi Messaoud

Principales réalisations à l'Étranger :

Ayant acquis une solide expérience dans le domaine des études et des réalisations de la construction, l'entreprise a exporté ses services vers la Mauritanie, le Mali, le Maroc et le Yémen.

Mauritanie

- Réalisation à Nouakchott d'un centre enfûteur de stockage et d'emplissage de bouteilles GPL, clé en main, puis extension 600 bouteilles / heure 1986-1988.
- Extension et rénovation de la raffinerie de Nouadhibou 1986-1988.
- Montage de deux unités de dessalement d'eau de mer.

Maroc

- Réalisation des travaux de montage de la centrale électrique de TANTAN 3x33 MGW 1992.

Mali

- Réalisation d'une étude technico-économique de dépôts de stockage de produits pétroliers à Tombouctou, Gao, Kayes, Mopti et Sikasso.

Yémen

- Réalisation d'infrastructures 1993.

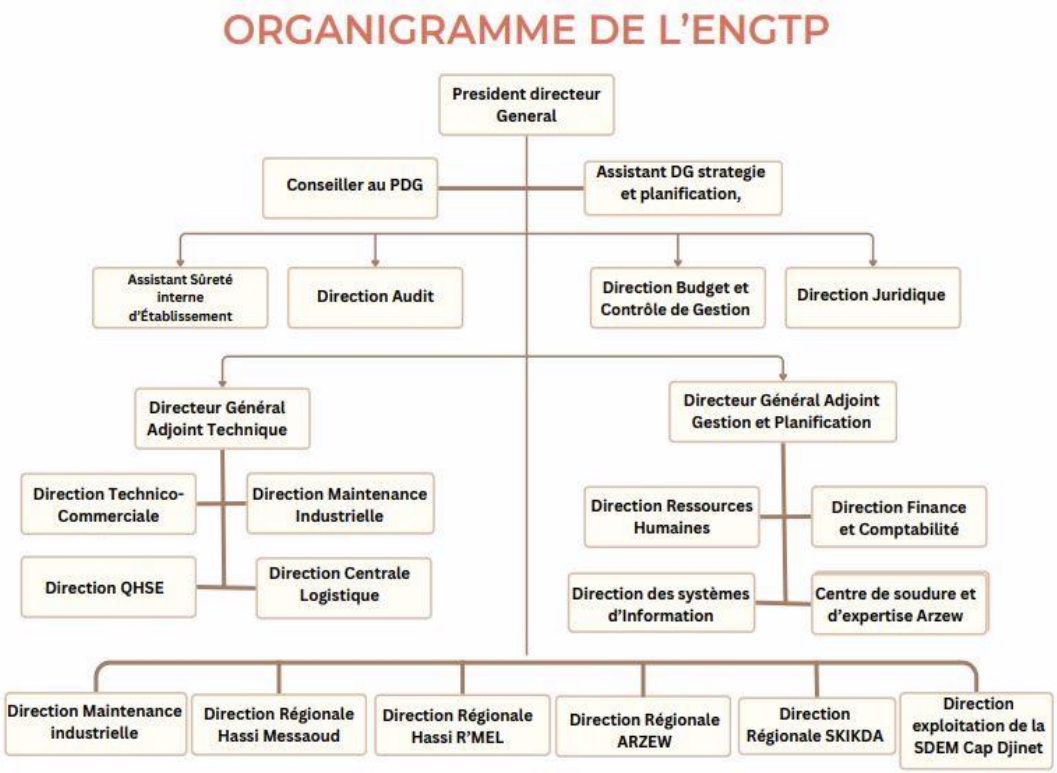
1.5 Organigramme de l'entreprise ENGTP

L'organigramme de l'Entreprise Nationale de Génie Civil et Bâtiment (ENGTP) révèle le caractère hiérarchique de l'organisme et le découpage fonctionnel et régional, qui le structure. C'est ainsi qu'il y a à la tête de l'établissement un Président Directeur Général (PDG), assisté de plusieurs directions stratégiques et de fonctions support. On est notamment sous le contrôle du PDG :

- Un Conseiller au PDG, Un Assistant à la stratégie et à la planification, Une Direction Audit, Une Direction Juridique Une Direction du Budget et Contrôle de gestion
- Les directions opérationnelles sont réunies sous l'autorité de deux Directeurs Généraux Adjoints (Technique, et Gestion & Planification) sous l'autorité desquelles on regroupe :
- Maintenance industrielle, Technique commerciale, Systèmes d'information, Logistique, Finance et Comptabilité, Ressources Humaines, QHSE (Qualité Hygiène Sécurité Environnement)
- Et des centres régionaux et d'exploitation (Hassi Messaoud, Arzew, Skikda, Cap Djinet…).

Cette structuration permet une gouvernance efficiente de l'établissement qui a des activités complexes tout en assurant, sur le territoire national, une couverture territoriale cohérente. La Direction des Systèmes d'Information, notamment, joue un rôle central dans la gestion des technologies de l'information et notamment dans la gestion du risque SI, qui est au cœur du mémoire.

Figure 10 Organigramme de l'entreprise ENGTP



Source : document fournis par l'entreprise

1.6 Ressources et politique de l'entreprise

1.6.1 Humaines

L'entreprise GTP emploie en moyenne 7800 agents, dont les principaux domaines d'activité sont les suivant :

- La Réalisation : 54%,
- La Maintenance Industrielle : 15%,
- La logistique : 13%,
- Gestion :7%,
- Catering : 9%,
- Sécurité : 2%.

1.6.2 Matérielles

GTP dispose de :

- Un atelier de soudage.

- Des ateliers de Tuyauterie.
- Des Laboratoires de Contrôle Destructif et Non Destructif.
- D'un parc matériel roulant de 3000 équipements, dans les principaux domaines ci-après:
- Le Terrassement et Génie Civil.
- Le soudage et contrôle.
- Le Levage (Grue de 18 T à plus de 300T).
- Politique Qualité et Environnement : De renommée internationale prouvée, GTP est certifiée ISO 9001/2000 depuis 2004.

1.6.3 Les données

L'entreprise dispose d'une base de données centrale contenant l 'ensemble des données et des bases de données régionales sont identiques à celle centrale mais ne sont accessibles en mode mise à jour que pour les données de la région concernée. Les bases de données sont installées sur des serveurs : Un serveur central d'entreprise et des serveurs régionaux.

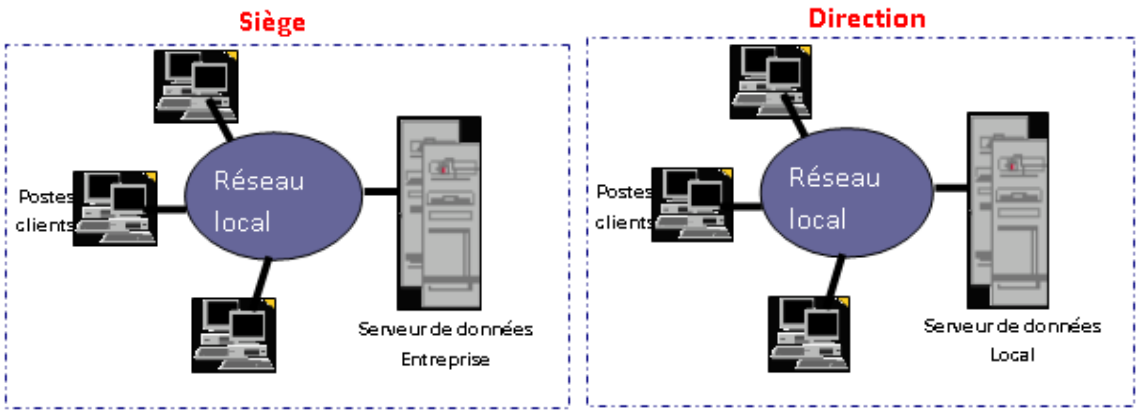
Les postes de travail qui ont accès aux bases de données sont reliés aux serveurs à travers des réseaux locaux. Ces postes de travail sont appelés Clients par rapport aux Serveurs. C'est le mode Client / Serveur.

L'accès aux bases de données se fait à travers des applications développées par le centre informatique et installées sur les postes Clients conformément au schéma suivant :

Des postes clients et un serveur de données entreprise au niveau siège interconnecté via un réseau local.

Des postes clients et un serveur de données régional implantés au niveau de chacune des quatre directions régionales interconnectés via des réseaux locaux

Figure 11 Architecture Client / Serveur à GTP



Source : Fourni par l'entreprise.

1.6.4 Les traitements

Les bases de données régionales sont mises à jour de deux manières différentes :

- En local pour les différents mouvements effectués dans la région, par les services informatiques de l'entreprise, après les traitements de consolidation.
- La mise à jour des bases de données permet de visualiser la situation des produits et des charges de l'ensemble des centres de frais de l'entreprise à travers la production d'états et de rapports synthétiques mis à la disposition des managers.

1.7 Le système de management intégré QHSE de l'ENGTP

Dans une optique d'excellence opérationnelle et afin de s'aligner aux standards internationaux, l'Entreprise Nationale de Grands Travaux Pétroliers (ENGTP) a mis en place un Système de Management Intégré QHSE (Qualité, Hygiène, Sécurité, Environnement) fondé sur les principes de l'amélioration continue.

L'entreprise est certifiée ISO 9001 depuis 2004, dans une démarche visant l'intégration progressive de l'ensemble de ses activités dans un processus de progrès continu. Consciente des enjeux économiques et humains liés à son secteur, ENGTP place la santé de ses collaborateurs, la sécurité de ses installations et la préservation de l'environnement au cœur de ses priorités.

Consciente de l'importance de l'alignement sur des standards internationaux, ENGTP a entrepris une démarche de conformité avec la norme ISO 27001, la référence mondiale en matière de sécurité des systèmes d'information.

L'entreprise a lancé les procédures nécessaires pour l'obtention de cette certification, en adaptant ses systèmes d'information, sa politique de sécurité et ses méthodes de protection aux exigences de cette norme. Elle a obtenu la certification ISO 27001 en 2010, pour une durée de trois ans. Cependant, ENGTP n'a pas poursuivi le processus de renouvellement de cette certification. En effet, la norme ISO 27001 n'est pas permanente ; elle requiert des audits réguliers et un renouvellement périodique afin de garantir que l'organisation maintient le niveau requis de conformité.

Du fait de la nature de ses activités (chantier, soudure, levage, manutention, transport, utilisation de produits chimiques et de sources radioactives), ENGTP a très tôt pris conscience des risques auxquels sont exposés ses travailleurs. C'est pourquoi elle a instauré un Système de Management de la Santé et de la Sécurité au Travail, initialement certifié OHSAS 18001 en 2013.

Dans une dynamique d'amélioration continue, l'entreprise a ensuite opéré une transition vers un Système de Management Intégré conforme aux normes ISO 9001:2015 (Qualité), ISO 14001:2015 (Environnement) et ISO 45001:2018 (Santé et Sécurité au Travail).

Cette transition a été formalisée avec succès à travers l'audit réalisé du 18 au 27 mars 2019 par Vinçotte International Algérie, suivi de la certification par l'organisme international INTERTEK Total Quality Assured, reconnu à l'échelle mondiale.

En 2022, ENGTP a renouvelé ses certifications après un audit de recertification mené du 27 février au 3 mars, couvrant plusieurs structures de l'entreprise. Ce renouvellement confirme l'engagement fort de la direction générale ainsi que l'implication active de l'ensemble des travailleurs dans la consolidation du statut de leader de l'entreprise dans son domaine d'activité.

1.8 Notoriété de GTP

La liste des réalisations de GTP est longue à énumérer tant l'entreprise a été leader dans le domaine de la construction de grands ensembles industriels dans le secteur des hydrocarbures. Sa notoriété est donc bel et bien établie au sein du secteur.

L'entreprise a toujours honoré ses engagements et a tiré des satisfactions de reconnaissances de ses partenaires en sus de résultat financiers. Dans le domaine des reconnaissances pourraient être citées :

- Attestation de satisfaction de l'entreprise Naftal pour les études, la réalisation et la mise en route de centres enfûteurs effectués par GTP.
- Attestation de satisfaction faite par le groupement TFT « Sonatrach-Total-Repsol » pour la construction du projet : développement du champ de gaz de TFT, réalisé par GTP.
- Attestation de reconnaissance faite par Sonarco / Kellogg GTP sur la satisfaction de la productivité déployée et le succès du projet.

- **Coordonnées du siège**

Localisation : BP 09 Zone industrielle, Réghaia –Alger,
Tél 1 : +213(0) 23 96 51 00 à 05
Tél 2 : +213(0) 23 96 50 32 / 33
Email : info@engtp.com
Site web : www.engtp.com

2. ENGTP et la gestion des risques de système d'information :

2.1 Contexte du stage

Dans le cadre de ma formation, j'ai intégré le département informatique du siège de Réghaïa. Ce département joue un rôle essentiel dans le bon fonctionnement de l'infrastructure numérique de l'entreprise. Il est chargé notamment de la gestion du parc informatique, du support aux utilisateurs, de la sécurité des systèmes d'information ainsi que du développement et de la maintenance des applications internes.

Face à la complexité croissante des systèmes d'information et aux menaces de plus en plus sophistiquées auxquelles ils sont confrontés (intrusions, piratages, sinistres, logiciels malveillants, etc.), la sécurité informatique est devenue un enjeu stratégique majeur pour ENGTP.

Durant notre stage, on a découvert l'organisation informatique d'une grande entreprise industrielle, et on a assisté à la gestion quotidienne des systèmes d'information, et de contribuer à diverses missions techniques, en lien avec l'amélioration de la performance et

de la sécurité des outils numériques. Nous avons pu observer que malgré l'existence de moyens matériels et logiciels de protection (antivirus, pare-feux, chiffrement, contrôle d'accès, etc.), des vulnérabilités subsistent, notamment en matière de sensibilisation des utilisateurs, de gestion proactive des incidents et de veille stratégique.

C'est dans ce contexte que s'inscrit ma réflexion sur l'opportunité d'intégrer l'intelligence artificielle dans la gestion des risques des systèmes d'information. L'IA pourrait permettre à ENGTP de passer d'une approche principalement réactive à une approche prédictive et automatisée de la sécurité, en renforçant la détection des anomalies, l'analyse comportementale, l'anticipation des menaces et la prise de décision rapide en cas d'incident.

Ce stage nous a offert un terrain d'observation concret et riche, à travers lequel nous avons pu confronter la théorie à la réalité du terrain, et réfléchir à des pistes d'amélioration réalistes et adaptées au contexte de l'entreprise.

2.2 Présentation département d'accueil DSI

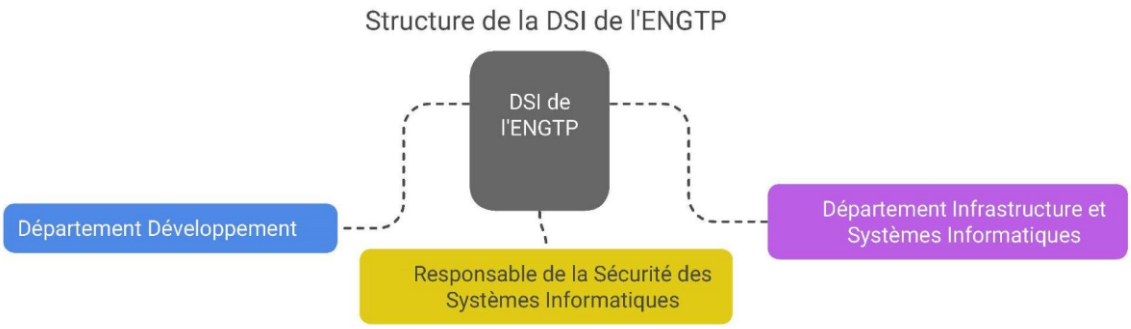
La Direction des Systèmes d'Information (DSI) de l'Entreprise Nationale de Grands travaux Pétroliers (ENGTP) rattachée au directeur général adjoint joue un rôle stratégique dans le bon fonctionnement et la modernisation des outils informatiques de l'entreprise. Elle a pour mission principale de garantir la disponibilité, la sécurité et la performance des systèmes d'information.

La DSI de l'ENGTP est structurée autour de deux départements complémentaires : le département Développement et le département Infrastructure et Systèmes Informatiques. Le département Développement est chargé de la conception, du développement et de la maintenance de l'ensemble des applications internes utilisées par les différents services de l'entreprise.

Ce département veille à adapter les solutions logicielles aux besoins métiers, en garantissant leur évolutivité et leur performance. De son côté, le département Infrastructure et Systèmes Informatiques assure la gestion du parc informatique, la maintenance matérielle et logicielle des équipements, la gestion du réseau, ainsi que le support utilisateur à travers le service helpdesk.

En parallèle, un responsable de la sécurité des systèmes informatiques supervise la mise en œuvre des politiques de sécurité, veille à la protection des données sensibles et à la résilience des infrastructures face aux menaces numériques.

Figure 12 Structure organisationnelle de la Direction des Systèmes d'Information (DSI) de l'ENGTP



Source : fourni par l'entreprise.

2.3 État de la sécurité de l'information au sein de l'entreprise

- La place de la sécurité de l'information dans l'organisation

ENGTP fait partie des rares entreprises algériennes à avoir institutionnalisé une fonction dédiée à la sécurité des systèmes d'information. Elle dispose en effet d'un service spécialisé appelé Service des Systèmes d'Information, composé d'un chef de service et de plusieurs spécialistes en systèmes d'information et en informatique.

Au sein de ce service, un responsable de la sécurité des systèmes d'information (RSSI) est chargé d'assurer la sécurité des postes informatiques, des équipements numériques, des informations sensibles et des ressources critiques à l'échelle du service mais aussi de toute l'entreprise.

- Politique de sécurité de l'information

ENGTP a adopté une politique de sécurité de l'information claire et bien définie, reposant sur des règles et des principes précis. Cette politique est publiée en ligne sur le site officiel de l'entreprise, accessible à l'ensemble des employés afin de favoriser la sensibilisation et l'adhésion de tous.

- Sensibilisation de la direction et des employés

Malgré les efforts importants consacrés à la sécurité informatique, tant sur le plan matériel, humain que technique, on observe que la prise de conscience de la direction vis-à-vis des menaces informatiques reste relativement faible. De même, la culture de la sécurité chez les employés n'atteint pas le niveau escompté.

Dans la pratique, la sécurité est surtout appliquée sur le plan physique (sécurité périmétrique) et technique (logiciels de protection, systèmes de sécurité sur serveurs, etc.). En revanche, la veille stratégique et la sensibilisation réelle à l'importance des menaces informatiques demeurent cantonnées au Service des Systèmes d'Information, qui s'efforce d'améliorer la culture de la sécurité au sein de l'entreprise.

2.4 Menaces de sécurité auxquelles fait face l'entreprise

Comme toute grande entreprise, l'ENGTP est confrontée à diverses menaces, qu'elles soient physiques (vols, catastrophes naturelles, etc.) ou techniques (piratage, logiciels malveillants, accès non autorisés, etc.). Parmi les incidents enregistrés, on peut citer :

2.4.1 Menaces physiques

- Intrusions non autorisées : Cela désigne toute personne, connue ou inconnue, qui accède au site de l'entreprise sans autorisation préalable. Une telle intrusion représente un danger pour la sécurité de l'organisation.
- Vol d'équipements : L'entreprise a déjà été victime d'actes de vol, lors desquels des intrus ont pénétré illégalement sur ses sites pour dérober du matériel appartenant à l'entreprise.
- Catastrophes naturelles : Un seul cas a été enregistré, touchant une de ses unités, et ayant causé des pertes matérielles.

2.4.2 Menaces techniques

- Accès non autorisé aux systèmes d'information : Il s'agit de tentatives d'accès aux équipements ou aux systèmes de l'entreprise par des individus non habilités, que ce soit des employé interne ou des personne externe (hackers).
- Piratage informatique : L'entreprise a subi une attaque de type piratage externe, perpétrée par un amateur, ayant causé des dégâts mineurs.

Spams et vers informatiques : ENGTP, comme beaucoup d'autres entreprises, n'a pas échappé aux menaces de logiciels malveillants tels que les vers. Pour y faire face, l'entreprise a mis en œuvre ouvre plusieurs mesures, notamment : Des actions correctives, Le réglage des paramètres de sécurité, La conduite d'enquêtes internes, Le renforcement de la sécurité périmétrique, Le changement des mots de passe, Et d'autres actions préventives.

2.5 Moyens de protection appliqués par l'entreprise

Les protections mises en œuvre par ENGTP sont à la fois matérielles et logicielles :

2.5.1 Protection matérielle

Elle vise à protéger le site et les équipements physiques par divers dispositifs, parmi lesquels :

- Contrôle des accès via un poste de sécurité à l'entrée, encadré par de nombreux agents chargés de filtrer toute entrée dans les locaux.
- Port de badges obligatoires distinguant les employés, les visiteurs et les stagiaires.
- Accompagnement des visiteurs par un agent de sécurité jusqu'aux zones autorisées.
- Utilisation de cartes magnétiques pour accéder à certaines zones.
- Vidéo-surveillance : Des caméras sont installées dans tous les espaces internes et externes.
- Interdiction d'accès aux véhicules non autorisés, seuls ceux des employés sont admis.
- Systèmes de ventilation spécifiques pour les salles contenant des équipements et serveurs sensibles, nécessitant des conditions climatiques précises.
- Sécurisation renforcée des équipements critiques, placés dans des espaces dédiés.
- Centre de secours : L'entreprise dispose d'un centre informatique de secours équipé de systèmes d'information, utilisable en cas de sinistre majeur.

2.5.2 Protection logicielle

Cette protection repose sur des programmes et des dispositifs technologiques destinés à sécuriser les systèmes d'information, notamment :

- Antivirus : L'entreprise n'utilise pas de logiciels piratés, elle investit dans des solutions antivirus originales et certifiées.
- Anti spams : pour filtrer les courriers indésirables.

- Pare-feux matériels : ENGTP utilise des dispositifs physiques dédiés à la protection réseau, plutôt que de simples logiciels.
- Chiffrement : Toutes les informations sensibles échangées (en interne ou avec des entités externes sont cryptées.
- VPN (réseau privé virtuel) et sauvegarde de secours : Pour sécuriser les connexions et garantir la continuité des activités.
- Sauvegarde régulière des données, tant en interne qu'en externe, avec mises à jour fréquentes des logiciels de sécurité.
- Renouvellement périodique des mots de passe, ou après tout incident de sécurité.

Ce chapitre a permis de poser les fondations méthodologiques de notre étude ainsi que de contextualiser l'environnement organisationnel dans lequel elle s'inscrit. À travers une approche qualitative fondée sur des entretiens semi-directifs, nous avons justifié nos choix méthodologiques en lien avec l'objectif de compréhension approfondie des pratiques de gestion des risques des systèmes d'information.

L'analyse du contexte de l'ENGTP, entreprise stratégique du secteur pétrolier en Algérie, a permis de mieux cerner les enjeux spécifiques liés à la sécurité de l'information. La présentation de la Direction des Systèmes d'Information (DSI), des dispositifs de sécurité en place ainsi que des principales menaces identifiées constitue une base solide pour l'analyse des données dans le chapitre suivant.

Ainsi, ce cadre méthodologique rigoureux et cette immersion dans le contexte réel de l'ENGTP nous permettront d'évaluer de manière pertinente les pratiques actuelles de gestion des risques SI et d'envisager l'apport potentiel de l'intelligence artificielle dans ce domaine.

CHAPITRE III :
RESULTATS ET DISCUSSIONS

Ce chapitre présente les résultats des entretiens semi-directifs réalisés avec trois acteurs clés du système d'information de l'ENGTP : le Responsable de la Sécurité des Systèmes d'Information (RSSI), le Responsable des Projets SI (PMSI), et l'Administrateur de Bases de Données (DBA). L'objectif de cette enquête est de dresser un diagnostic des pratiques actuelles de gestion des risques SI, d'identifier les perceptions des professionnels sur les enjeux critiques de sécurité, et d'évaluer l'intérêt potentiel de l'intelligence artificielle (IA) dans ce domaine. Les réponses recueillies reflètent des pratiques vécues en situation de travail et sont confrontées à des références théoriques issues de la littérature, notamment en matière de méthodes d'analyse des risques, de normes ISO, de gouvernance et de maturité organisationnelle.

La structure de ce chapitre se scinde en deux sections : la première est consacrée à l'examen de l'existant à travers une analyse thématique des entretiens, tandis que la seconde présente une discussion critique des résultats, en les confrontant aux bonnes pratiques internationales et au potentiel contributif de l'IA dans ce domaine de recherche majeur.

Section 01 : Présentation des résultats

Dans cette section, nous procéderons à une analyse détaillée des résultats des observations et entretiens réalisés auprès des employés, en explorant divers aspects de leur perception du processus de gestion des risques de système d'information en intégrant l'intelligence artificielle.

1. Résultats des entretiens

Les entretiens menés auprès des responsables SI (RSSI, PMSI, DBA) de l'ENGTP ont permis de dégager une vision globale de la stratégie actuelle de gestion des risques.

Pour apprécier convenablement le travail d'interview, cette section est scindée en deux parties fondamentales. La première partie s'attèle à une vue d'ensemble des entretiens, avec la caractérisation de l'échantillon et un coup d'œil sur l'analyse lexique et textuelle alors que la seconde partie s'attaque à la recherche thématique des différents thèmes traités par le guide d'entretien.

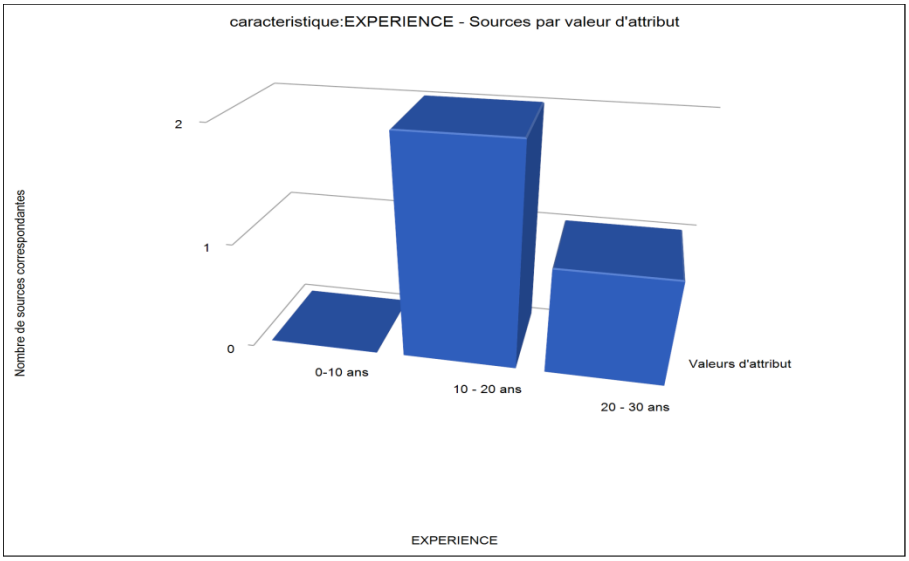
1.1 Analyse descriptive :

L'analyse descriptive est une méthode d'exploration des données qui vise à résumer, organiser et présenter de manière claire les principales caractéristiques d'un corpus ou d'un

ensemble d'informations recueillies. Elle repose généralement sur des outils statistiques simples (moyennes, fréquences, écarts-types, etc.) ou sur des représentations graphiques (tableaux, graphiques, nuages de mots) afin de dégager les tendances générales, les régularités et les particularités du matériau étudié, sans chercher à établir de relation de cause à effet.

L'échantillon mobilisé dans cette étude se compose de trois experts occupant des postes stratégiques dans la gestion des systèmes d'information de l'ENGTP, à savoir : un Responsable de la Sécurité des Systèmes d'Information (RSSI), un Responsable de Projets SI (PMSI), et un Administrateur de Base de Données (DBA). Tous ont participé à des entretiens semi-directifs visant à recueillir des perceptions approfondies sur les pratiques actuelles et les perspectives d'intégration de l'intelligence artificielle dans la gestion des risques SI.

Figure 13 information sur les interviewés



Source : généré par NVivo 14.

La variable « expérience professionnelle » a été mobilisée comme indicateur clé pour apprécier la diversité des profils interrogés. Comme le montre le graphique ci-dessous, l'échantillon couvre deux tranches d'ancienneté : deux répondants présentent une expérience comprise [entre 10 et 20 ans], tandis qu'une autre affiche [entre 20 et 30 ans] de pratique. Aucun participant ne relève de la catégorie des [moins de 10 ans] d'expérience.

Ce constat témoigne d'une forte capitalisation en matière de savoir organisationnel, de mémoire institutionnelle et de maturité professionnelle. En effet, le fait que les répondants

disposent tous de plus d'une décennie d'expérience dans le domaine SI garantit une qualité analytique élevée**.**

Les réponses recueillies s'appuient à la fois sur une connaissance empirique des risques opérationnels et sur une vision stratégique des enjeux de sécurité à long terme. Cette double expertise permet de recueillir des témoignages profondément ancrés dans la réalité du terrain, enrichis par des années d'expérience, tout en offrant une lecture pertinente des limites et des opportunités du dispositif actuel de gestion des risques. Elle ouvre également la voie à des pistes d'optimisation concrètes et réalisables, notamment par l'intégration de technologies émergentes comme l'intelligence artificielle. Ainsi, la qualité et la diversité de cet échantillon garantissent une analyse approfondie et nuancée, indispensable pour traiter un sujet aussi complexe et évolutif que l'optimisation de la gestion des risques SI par l'IA.

1.2 Analyse textuelle de données

L'analyse textuelle consiste à examiner les discours recueillis à travers les entretiens dans le but d'identifier les structures linguistiques, les régularités lexicales et les usages terminologiques propres aux participants. Elle permet de mettre en évidence les termes les plus fréquemment employés, les cooccurrences significatives, ainsi que les thématiques dominantes, en offrant ainsi une première lecture descriptive des contenus avant toute interprétation approfondie.

1.2.1 L'approche lexicale :

L'approche lexicale permet d'explorer les fréquences d'occurrence des mots dans le corpus des entretiens afin de mettre en évidence les termes dominants. Elle constitue une première étape d'analyse, offrant une lecture synthétique des discours recueillis et révélant les concepts clés, les préoccupations récurrentes ainsi que les champs thématiques les plus mobilisés par les répondants.

Le nuage de mots met en évidence les termes les plus récurrents dans les entretiens, notamment : Risques, gestion, sécurité, systèmes, projet, méthodes, données, utilisateurs, intelligence artificielle, informations, industrielles, prévention, etc.

Figure 14 nuage des mots

Source : générer par nous-mêmes avec NVivo 14.

Ce nuage confirme visuellement que le thème central tourne autour de la gestion des risques des systèmes d'information.

1.2.2 L'approche linguistique :

L'approche linguistique est une méthode d'analyse qualitative qui s'intéresse à la manière dont le langage est utilisé dans un corpus de textes ou de discours. Pour en dégager les intentions, les représentations et les structures argumentatives des locuteurs. Cette approche permet de mieux comprendre les mécanismes de communication, les stratégies discursives et les rapports de sens présents dans les entretiens ou les productions écrites.

L'objectif de cette approche est de décrypter les choix de formulation et les structures langagières utilisées par les interviewés afin d'interpréter leurs logiques argumentatives mobilisées face aux enjeux de gestion des risques et à l'intégration de l'intelligence artificielle.

Une analyse de la corrélation lexicale entre les trois entretiens a été réalisée afin de mesurer la similarité des réponses en termes de vocabulaire utilisé par les différents professionnels interrogés. Le résultat de coefficients de corrélation de Pearson **c**alculé, se présente dans le tableau suivant :

Tableau 2 Coefficients de corrélation entre les entretiens

Source A	Source B	Coefficient de corrélation
Responsable 02	Responsable 01	0,923564
Responsable 03	Responsable 02	0,871714
Responsable 03	Responsable 01	0,851397

Source : élaboré par nous-même avec NVivo14.

Les résultats montrent un fort niveau de cohérence lexicale entre les participants :

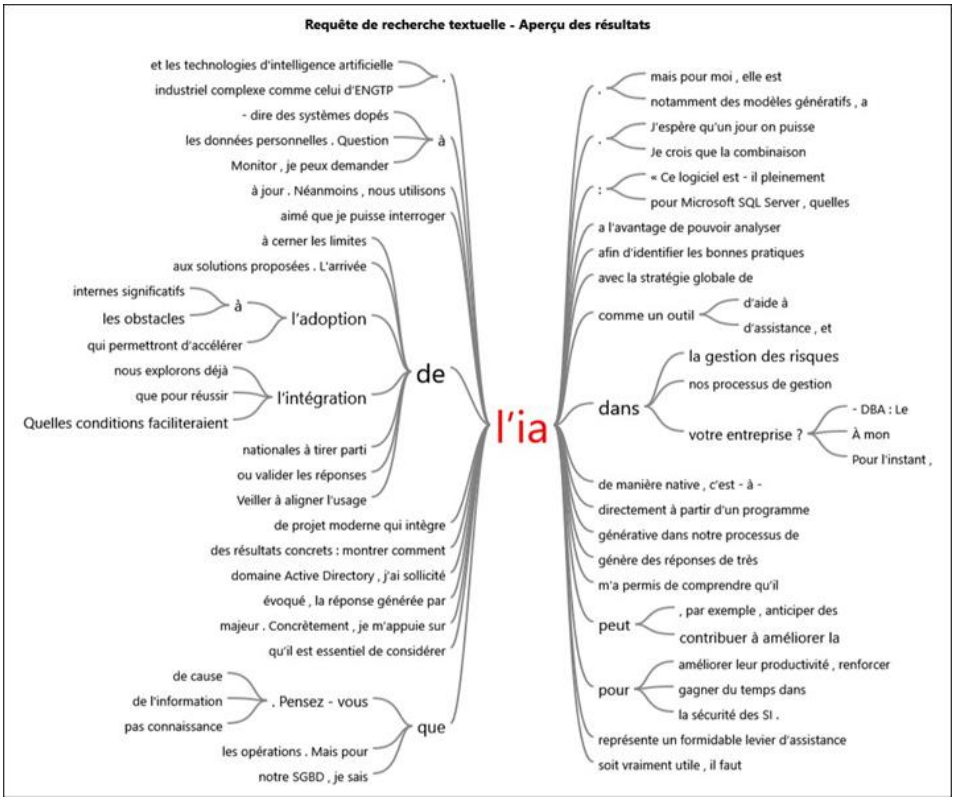
- L'entretien 02 et l'entretien 01 présentent une corrélation de 0,92, ce qui traduit une très forte similarité dans les idées abordées et les termes employés.
- L'entretien 03 est également proche des deux premiers avec des corrélations de 0,87 avec l'entretien 02 et 0,85 avec l'entretien 01.

Cette analyse renforce la validité des résultats thématiques, en montrant que malgré des fonctions différentes, les répondants partagent une vision commune des enjeux liés à la gestion des risques SI et à l'apport potentiel de l'intelligence artificielle.

1.2.3 Cartographie cognitive :

Afin d'approfondir l'analyse du contenu des entretiens, une cartographie cognitive permet de représenter visuellement les concepts évoqués par les participants et les liens entre eux. À travers la méthode Synapsie, cette approche met en lumière les idées dominantes et leur organisation mentale sur deux mots clés majeurs de cette recherche : "IA" et "risque"

Figure 15 Synapsie sur le mot "IA"

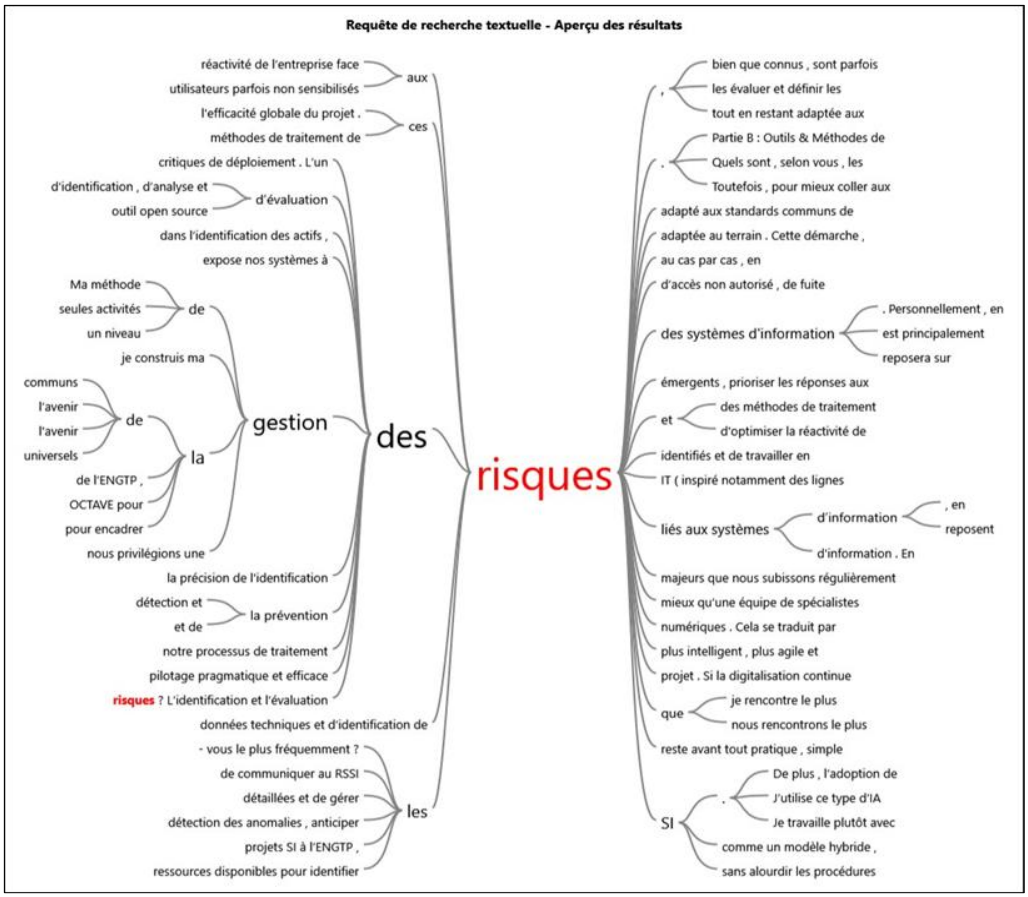


Source : Résultat du logiciel NVivo 14.

L'arbre de mots généré autour du mot "IA" révèle une utilisation fréquente du terme dans des contextes liés à l'aide à la décision, à l'automatisation, et à la gestion des menaces. Selon les données recueillies il retrouve des formulations comme : "l'IA peut anticiper certains incidents", "nous utilisons l'IA générative pour valider des configurations techniques", "l'IA permet de gagner du temps dans le traitement des vulnérabilités".

Ces occurrences confirment la perception de l'intelligence artificielle comme un outil stratégique au service de la sécurité et de la performance organisationnelle.

Figure 16 Requête corrélation sur le mot "risques"



Source : Résultat du logiciel NVivo 14.

La requête centrée sur le mot "risque" met en évidence des préoccupations récurrentes liées à la cybersécurité, aux erreurs humaines, aux défaillances techniques, et aux contraintes réglementaires. Les extraits suivants ont été particulièrement représentatifs :"le plus grand risque reste la compromission des mots de passe", "il est difficile d'évaluer le risque d'incompatibilité entre les systèmes", "l'IA aide à anticiper les scénarios de risque avant qu'ils ne se matérialisent".

Cette analyse montre que le terme "risque" est souvent associé à des enjeux techniques et organisationnels, en lien direct avec la gestion des systèmes d'information, et que son évaluation reste un élément clé de la stratégie de sécurité.

1.2.4 L'analyse thématique :

Dans cette étude, l'approche thématique a été guidée par les objectifs de recherche définis en amont, et les entretiens ont été codés manuellement, puis analysés à l'aide du logiciel NVivo14.

Il permet d'identifier les idées clés, les points de convergence et de divergence entre les participants. Chaque thème a été construit à partir des unités de sens récurrentes dans les discours des trois participants interrogés : le Responsable de la sécurité des systèmes d'information (RSSI), le Responsable des projets SI (PMSI) et l'Administrateur de bases de données (DBA). (Annexe 1-2-3)

Cette section présente les résultats selon les grands axes thématiques identifiés, en croisant les différentes perceptions exprimées et en contextualisant les réponses dans l'environnement spécifique de l'entreprise. L'interprétation s'appuie à la fois sur les extraits significatifs et sur l'analyse transversale des profils, afin de dégager une compréhension approfondie des enjeux actuels et des leviers d'amélioration.

Thème A : Gestion des risques SI

Les différentes méthodes de gestion des risques SI se sont révélées au travers des entretiens effectués, bien que certaines lignes directrices commencent à s'esquisser.
Le premier responsable (RSSI) porte attention sur le mode de gestion fondé sur une approche organisée ayant pour objectifs de détecter les actifs à protéger, leur vulnérabilité face à des risques, de définir un ordre préférentiel pour les actions correctives précises à exécuter. Il précise que l'approche repose toujours sur un tronc commun de moyens techniques fondés sur l'utilisation de moyen disparate (antivirus, pare-feux et cryptage) mais également de processus internes de type questionnaires d'auto-évaluation. Mais il met également en avant que cette approche demeure fondamentalement réactive et postule davantage de systèmes de prévision. Comme il le souligne : « Nous concentrons d'abord nos efforts sur les éléments les plus sensibles de notre SI... mais notre approche reste majoritairement réactive, axée sur la détection et la correction post-incident. »

Le deuxième responsable (PMSI) est plus orienté dans l'opérationnel : priorité est donnée à l'expérience accumulée sur les projets antérieurs. Le questionnaire de recensement d'analyse des risques à l'aide d'un simple outil comme Excel est réalisé sur la base des

besoins du terrain. Il indique : « Ma méthode de gestion des risques reste avant tout pratique, simple et adaptée au rythme des projets que je pilote. »

Il insiste sur la flexibilité comme facteur clé de succès dans un contexte industriel mouvant : « Mon objectif est d'être réactif et pratique, sans m'enfermer dans une méthode formelle. » La recherche est fortement orientée vers une identification pragmatique des risques projet en lien avec le travail de logistique, de coordination, ou de gestion des retards.

Le troisième responsable (DBA), enfin, se penche précisément sur la question du risque de la sécurité dans les systèmes d'information. Le résultat de sa contribution prend la forme d'un signalement du risque lié à la gestion des bases de données, principalement en matière de sauvegardes non effectives ou d'attribution abusive de droits d'accès. Il l'explique en précisant qu'il transmet aux RSSI ses alertes : « Mon focus maximal est sur la donnée personnelle contenue dans la base de données. J'essaie de prendre en considération tous les risques applicables et de les communiquer au RSSI. » dans une démarche de signalement coopératif et non stratégique.

Thème B : Outils & Méthodes de gestion des risques

Les entretiens réalisés révèlent une absence d'application systématique des méthodes formelles telles que MEHARI, EBIOS ou OCTAVE dans la gestion des risques des systèmes d'information à l'ENGTP. Toutefois, chacun des participants développe une approche spécifique, plus souple, adaptée au contexte organisationnel de l'entreprise.

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) indique que l'entreprise n'applique pas formellement ces méthodes, bien qu'il connaisse bien la méthode EBIOS. Il la considère adaptée au contexte des risques IT modernes grâce à sa capacité à dérouler des scénarios de risques, mais souligne que son application rigoureuse nécessite des ressources humaines spécialisées, ce qui représente une contrainte dans l'environnement de l'ENGTP. Il précise que l'approche actuelle repose sur une méthode personnalisée qu'il décrit comme suit : « J'utilise une méthode assez épurée et personnalisée. La séquence est la suivante : Identification – Évaluation – Traitement – Réévaluation. » Le Responsable des Projets SI (PMSI) confirme ne pas recourir à ces méthodes formelles, préférant une gestion empirique et réactive, fondée sur l'expérience de terrain. Il insiste sur la nécessité de flexibilité dans les projets, justifiant le choix d'une méthode maison, intégrée dans ses

outils quotidiens comme Excel, et adaptée à la complexité opérationnelle et aux imprévus. L'Administrateur des bases de données (DBA) adopte la méthode utilisée par le RSSI, ce qui insiste sur la coordination hiérarchique : « Je me contente de communiquer au RSSI les risques identifiés et de travailler en collaboration avec lui sur les traitements et révisions ». Reflète une approche centralisée et hiérarchique dans la définition de la stratégie de gestion des risques au sein de la DSI.

Dans l'ensemble, ce thème met en évidence une absence d'appropriation des méthodes standards, compensée par des pratiques internes, adaptées et allégées, mieux ajustées aux ressources limitées et aux réalités organisationnelles d'une entreprise industrielle. Il reflète aussi un besoin latent de structuration, qui pourrait, à l'avenir, justifier une formalisation progressive autour d'un cadre plus normé.

Thème C : L'intégration de l'intelligence artificielle dans la gestion des risques des systèmes d'information

À travers l'analyse des entretiens, il ressort que l'intelligence artificielle (IA) commence à prendre une place notable dans les pratiques de gestion des risques SI au sein de l'ENGTP, même si son intégration reste encore à un stade exploratoire.

Le Responsable de la sécurité des systèmes d'information (RSSI) affirme utiliser l'IA, notamment des outils d'IA générative, dans le cadre de ses missions. Il cite l'exemple d'un serveur Windows pour lequel il a sollicité l'IA afin d'obtenir des recommandations techniques en matière de sécurité (ex. durcissement, limitation des privilèges, etc.). Pour lui, l'IA constitue un outil d'aide à la décision, permettant de gagner du temps et d'améliorer la qualité des mesures proposées. Toutefois, il insiste sur le fait que ces recommandations sont toujours validées par des experts internes, et que l'humain reste au centre de la décision. Il souligne également l'importance du respect des lois algériennes, notamment l'interdiction d'externaliser certaines données vers des plateformes étrangères.

De son côté, le Responsable des projets SI (PMSI) explique qu'il utilise l'IA principalement pour vérifier la compatibilité des solutions proposées avec l'infrastructure existante. Il considère que cela lui fait gagner un temps précieux dans l'évaluation des fournisseurs et dans la préparation des déploiements. Il évoque aussi l'idée d'un futur outil

de gestion de projet intégrant l'IA de manière native, ce qui améliorerait le suivi des risques et l'automatisation de certaines tâches.

Quant à l'Administrateur de base de données (DBA), il précise que son usage de l'IA concerne surtout la conformité réglementaire, notamment la loi 18-07 sur la protection des données personnelles. Il trouve l'IA très utile pour ajuster des configurations techniques en lien avec la sécurité des bases de données, même s'il regrette de ne pas disposer d'une solution IA interne capable de dialoguer directement avec ses systèmes. Il espère qu'un jour, l'IA pourra aller plus loin, jusqu'à générer des architectures sécurisées et rédiger automatiquement des procédures adaptées.

En conclusion, bien que les usages de l'IA restent encore limités à des tâches ponctuelles ou exploratoires, les trois acteurs interrogés reconnaissent sa valeur ajoutée dans la gestion des risques SI. Les avis convergent sur la nécessité de l'intégrer de manière progressive, tout en respectant la sécurité, la confidentialité et la réglementation locale. Cette ouverture à l'IA reflète une volonté d'adapter les pratiques internes aux évolutions technologiques actuelles.

Thème D : Vision stratégique

Les propos recueillis révèlent un consensus autour du potentiel transformateur de l'intelligence artificielle dans le domaine de la gestion des risques SI. Deux des trois répondants expriment une perception clairement positive de l'IA, soulignant son rôle dans l'anticipation des incidents, la détection rapide des anomalies et la rationalisation des décisions. Ils associent l'IA à une modernisation inévitable des dispositifs de sécurité, notamment face à la complexité croissante des infrastructures numériques.

Cependant, un répondant adopte une posture plus prudente**,** insistant sur les limites de l'IA et les risques d'une dépendance excessive aux outils automatisés. Ce point de vue invite à envisager une intégration équilibrée, où l'IA viendrait en appui des experts humains sans les remplacer.

En somme, les discours traduisent une ouverture générale à l'innovation, tout en soulignant l'importance de maîtriser les enjeux techniques, éthiques et organisationnels liés à l'IA.

2 La gestion des risques au sein de l'ENGTP :

L'observation approfondie du système de gestion des risques des systèmes d'information au sein de l'ENGTP a permis de reconstituer une démarche structurée, fondée sur des standards reconnus de gestion des risques, combinant évaluation qualitative et modélisation visuelle à travers des matrices de criticité. Cette méthode repose sur une succession logique d'étapes allant de l'identification des menaces jusqu'à la formulation de recommandations finales.

2.1 Processus de gestion des risques SI au sein de l'ENGTP :

D'après les entretiens menés avec les responsables du système d'information ainsi que les observations réalisées tout au long de notre stage au sein de l'ENGTP, il ressort que le processus de gestion des risques suit une démarche relativement structurée. Cette sous-section détaille les principales étapes observées

2.1.1 Identification des menaces et analyse de la vulnérabilité

Chaque scénario de risque est d'abord formalisé à travers une menace clairement identifiée, par exemple : panne de serveur physique, vulnérabilités connues non corrigées ou accès non autorisé aux bases de données. Pour chaque cas, une étude de vulnérabilité est menée afin de déterminer les failles potentielles exploitées par ces menaces. Cette première étape repose sur l'expertise du personnel technique (RSSI, DBA, chef de projet SI), mais également sur des référentiels internes documentés.

2.1.2 Évaluation du risque inhérent (avant mesure de sécurité)

Les risques identifiés sont évalués en fonction de deux dimensions principales : la vraisemblance, qui désigne la probabilité d'occurrence de la menace, et l'impact, c'est-à-dire les conséquences potentielles sur le système d'information en cas de survenue. Chacune de ces dimensions est notée sur une échelle de 1 à 5. Le produit de ces deux valeurs permet d'obtenir un niveau de risque inhérent. Ce dernier est ensuite positionné dans une matrice de criticité, comme la montre (l'Annexe 5-6).

2.1.3 Définition de la stratégie de gestion des risques

Une fois le niveau de risque inhérent établi, l'organisation déploie une stratégie adaptée pour y faire face. Cette stratégie repose sur l'une des quatre options classiques de traitement des risques. Il peut s'agir d'une acceptation du risque, lorsque celui-ci est jugé

mineur ou tolérable, ou bien d'une réduction du risque, en mettant en œuvre des mesures techniques ou organisationnelles visant à en atténuer la probabilité ou les effets. Une autre alternative consiste à transférer le risque, notamment à travers une couverture assurantielle. Enfin, dans certains cas, l'évitement du risque est privilégié, ce qui implique la suppression pure et simple de la source de danger.

2.1.4 Mise en place de mesures d'atténuation

Pour les risques nécessitant un traitement, des mesures d'atténuation sont déployées. Celles-ci peuvent inclure :

- Des redondances matérielles et logicielles,
- Des sauvegardes automatisées,
- Des mises à jour de sécurité (patch management),
- L'utilisation de solutions de sécurité telles que WSUS ou antivirus professionnels.

2.1.5 Évaluation du risque résiduel

Après la mise en place des mesures d'atténuation, une seconde évaluation est conduite afin de mesurer le risque résiduel (post-traitement). Comme pour l'évaluation initiale, le niveau de vraisemblance et l'impact sont à nouveau notés, et une seconde matrice est construite (figure droite), permettant de visualiser le déplacement du risque vers une zone de criticité inférieure.

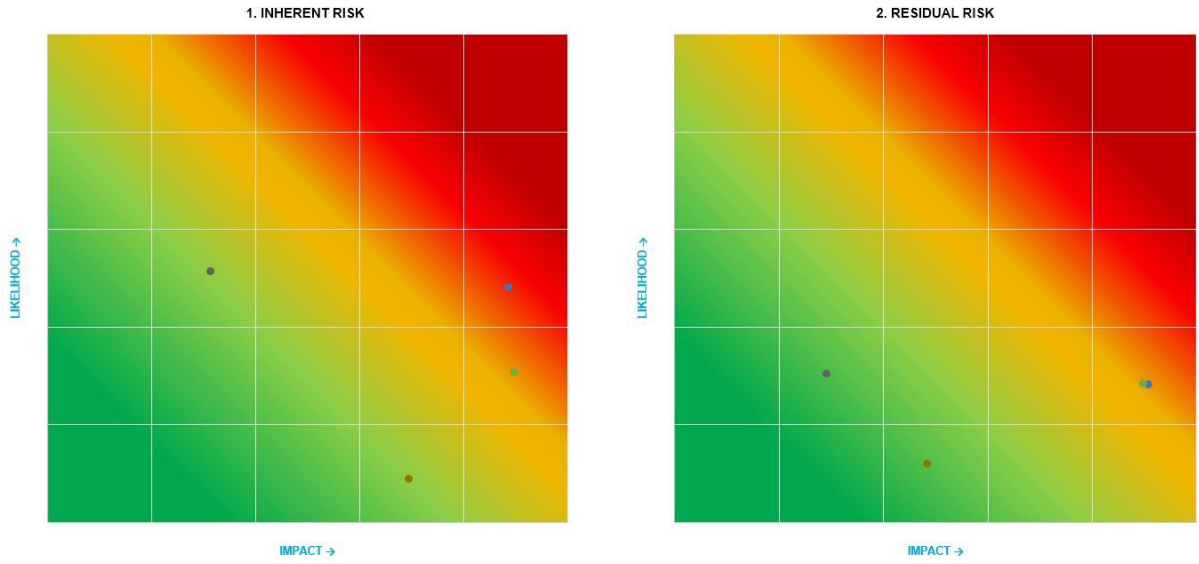
2.1.6 Recommandations finales et documentation

Chaque fiche de risque se conclut par des remarques et recommandations émises par les évaluateurs dans le but de renforcer la résilience du système d'information. Ces suggestions portent généralement sur des actions concrètes telles que l'accélération des mises à niveau technologiques, le renforcement des audits de sécurité, ou encore l'adoption d'outils d'analyse prédictive. Elles peuvent également inclure des perspectives d'évolution, notamment l'intégration de l'intelligence artificielle pour automatiser la détection des anomalies ou pour optimiser la hiérarchisation des vulnérabilités. L'ensemble de ce processus est consigné dans un tableau structuré (sous format Excel), assurant à la fois la traçabilité des décisions prises et une visualisation claire de l'exposition aux menaces, à travers des matrices de criticité codées par couleur.

2.1.7 Analyse visuelle des matrices de risques

Les deux matrices ci-dessous illustrent de manière synthétique la transition du risque inhérent (avant traitement) vers le risque résiduel (après mise en œuvre des mesures d'atténuation). Elles constituent un outil fondamental dans le pilotage de la gestion des risques SI au sein de l'ENGTP.

Figure 17 la matrice des risques de système d'information



Source : Document fourni par l'entreprise.

La matrice des risques inhérents, située à gauche, révèle plusieurs occurrences dans les zones rouge et orange, traduisant un niveau de criticité allant d'élever à très élevé. Ces situations concernent essentiellement des risques techniques, notamment des pannes matérielles affectant les serveurs physiques, des vulnérabilités logicielles non corrigées, ainsi qu'une redondance insuffisante des services critiques, ce qui accentue l'exposition globale du système aux défaillances.

La matrice des risques résiduels, présentée à droite, montre un déplacement marqué des occurrences vers les zones vertes et jaune clair, traduisant une baisse significative du niveau de criticité. Cette évolution témoigne de l'efficacité des mesures d'atténuation mises en place, telles que l'implémentation de sauvegardes automatiques et redondantes, l'utilisation d'outils centralisés de gestion des mises à jour comme WSUS, ainsi que l'activation de processus de reprise d'activité (PRA) en environnement virtualisé.

L'utilisation de ces matrices s'avère essentielle à plusieurs égards. Elles permettent d'abord une visualisation rapide du niveau de risque associé à chaque menace identifiée, facilitant ainsi l'évaluation globale de l'exposition du système. Elles constituent également un outil d'aide à la décision pour hiérarchiser les actions de sécurisation à entreprendre. Par ailleurs, elles offrent un support solide pour justifier les choix stratégiques auprès de la direction et des auditeurs. En somme, ces représentations illustrent que le processus d'évaluation et de traitement des risques liés aux systèmes d'information à l'ENGTP repose sur une approche rigoureuse, progressive et mesurable, en cohérence avec les principes de bonne gouvernance IT.

2.2 Perspective future de la contribution de l'IA à la gestion des risques SI au sein de l'ENGTP :

L'analyse du processus de gestion des risques SI observé à l'ENGTP – notamment à travers les grilles d'évaluation issues du fichier Excel et les matrices de criticité – met en lumière une démarche systématique mais largement manuelle, fondée sur l'expertise humaine pour identifier les menaces, estimer leur vraisemblance, et proposer des stratégies d'atténuation. Si cette approche présente l'avantage d'être contextualisée et adaptée à l'environnement opérationnel, elle demeure limitée par les biais cognitifs, l'exhaustivité subjective et la capacité humaine à anticiper des menaces complexes ou émergentes. C'est à ce niveau que l'intégration de l'intelligence artificielle se révèle particulièrement stratégique.

D'après la discussion avec le RSSI de l'ENGTP, je conçois l'avenir de la gestion des risques des systèmes d'information non plus comme un processus cyclique ponctuel, mais comme un écosystème intelligent et auto-adaptatif, fondé sur l'exploitation avancée de l'intelligence artificielle (IA).

- **Aide à l'identification des risques émergents**

L'un des apports majeurs de l'IA réside dans sa capacité à détecter proactivement des risques que l'humain ne peut identifier immédiatement. Grâce à des algorithmes de machine learning et d'analyse comportementale, elle peut repérer des signaux faibles dans les systèmes, souvent précurseurs d'incidents plus graves. Cela comprend l'analyse des journaux d'événements, des historiques d'incidents, et des comportements inhabituels des utilisateurs ou des machines.

Exemple **:** En analysant les logs d'accès à une base de données RH, l'IA identifie une séquence d'interrogations inhabituelles à des horaires atypiques. Bien qu'aucune alerte n'ait été déclenchée par les systèmes classiques, l'IA propose d'évaluer cette activité comme un risque potentiel, contribuant ainsi à la détection anticipée d'un accès malveillant.

- **Détection intelligente et en temps réel des menaces**

Grâce à l'intégration de solutions IA basées sur la machine learning supervisé et non supervisé, leur système serait capable d'analyser en temps réel des volumes massifs de journaux systèmes, de flux réseau, de tentatives de connexions et de comportements utilisateurs.

Exemple : Un agent IA est déployé sur les serveurs du DataCenter RH. Une nuit, il détecte une tentative d'authentification répétée provenant d'un poste interne compromis. L'IA reconnaît une séquence suspecte de commandes et alerte automatiquement le SOC, évitant ainsi une élévation de privilège non autorisée.

- **Utilisation du NLP pour le traitement automatisé des signaux faibles**

En s'appuyant sur des outils de traitement du langage naturel (NLP), le système pourrait lire et interpréter des flux externes tels que :

- Bulletins de sécurité (ex. CERT, MITRE).
- Discussions sur des forums spécialisés ou dark web.
- Articles techniques et rapports d'incidents mondiaux.

Ces informations seraient automatiquement corrélées à l'infrastructure, pour anticiper des menaces encore inconnues dans le contexte mais détectées ailleurs, et générer des alertes préventives contextualisées.

Exemple : Un module NLP repère une alerte critique concernant une vulnérabilité « 0-day » affectant une version spécifique de Tomcat utilisée dans les applications internes ENGTP. Le système génère automatiquement une alerte avec un ticket prioritaire à l'équipe exploitation pour vérification et patch immédiat.

- **Cartographie cognitive et classification dynamique des actifs**

À l'aide de l'IA, le système établirait une cartographie dynamique des actifs IT, en catégorisant automatiquement les composants selon leur niveau de criticité, leur

dépendance métier, et leur exposition. Ce système apprendrait au fil du temps quelles ressources sont les plus sensibles à la sécurité (serveurs RH, bases de données financières, etc.).

Ainsi, une menace détectée sur un serveur exposé publiquement serait automatiquement jugée plus prioritaire si elle touche un actif classé critique dans cette cartographie.

Exemple : L'IA met à jour automatiquement une carte des interconnexions entre les serveurs du département financier, identifie les flux critiques, et place ces actifs en « haute sensibilité ». Lorsqu'un incident touche une passerelle utilisée dans ce périmètre, la réponse est immédiatement classée en priorité 1.

- **Simulation intelligente et prédictive des scénarios d'attaque**

À travers des modèles prédictifs, notre IA pourrait exécuter des scénarios de compromission simulés en continu, afin de tester la résilience du système sans perturber les opérations (cyber range virtuel). Elle pourrait ainsi nous avertir que :

« Si l'attaque de type ransomware ciblait la base X avec les configurations actuelles, les sauvegardes les plus récentes exploitables datent de 12 jours. »

Ce niveau d'anticipation nous permettrait de passer d'une posture défensive à une posture proactive et préventive.

Exemple : L'IA simule une attaque de type phishing ciblant le personnel comptable. Elle identifie qu'aucun plan de remédiation automatique n'est en place si le poste infecté accède à la base de données des paiements. Cette simulation permet d'ajuster immédiatement la stratégie de sauvegarde et de cloisonnement.

- **Orchestration automatisée de la réponse**

Enfin, l'IA jouerait un rôle clé dans la réduction des délais de réaction, en automatisant certaines actions selon des scénarios validés :

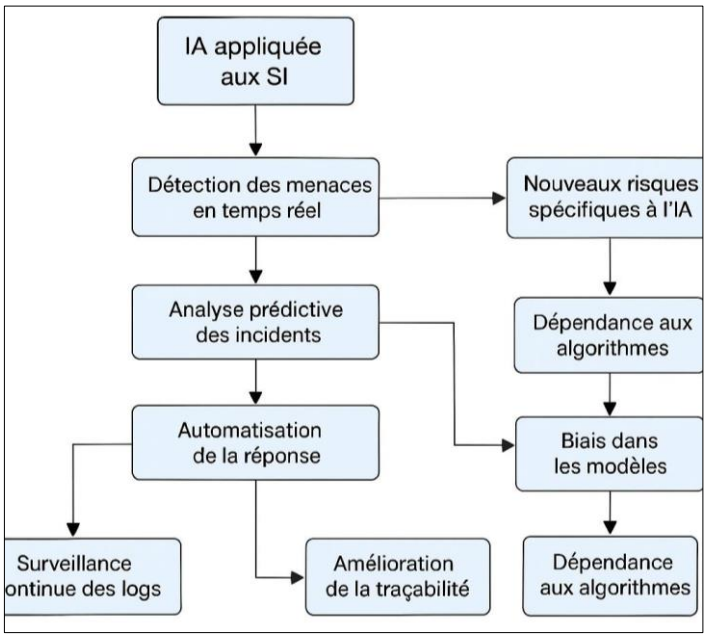
- Isolement réseau d'un terminal compromis.
- Réinitialisation de comptes à privilèges suspects.
- Notification contextuelle aux équipes concernées.

Chaque action serait documentée, traçable, et auditable, tout en laissant la possibilité d'une supervision humaine pour les cas sensibles.

Exemple : Lors d'un test d'intrusion, une anomalie réelle est détectée sur un poste utilisateur du site de Hassi Messaoud. Le système isole immédiatement le poste, notifie l'équipe sécurité, et déclenche un processus automatisé de changement des mots de passe pour les comptes à privilèges, tout en conservant une trace complète pour audit.

Pour conclure, l'intégration de l'intelligence artificielle dans les systèmes d'information transforme profondément les mécanismes de gestion des risques. La figure ci-dessous illustre les principales contributions de l'IA dans ce domaine, en mettant en évidence à la fois les apports fonctionnels et les risques induits.

Figure 18 Apports et risques de l'IA appliquée à la gestion des risques des systèmes d'information



Source : Elaboré par nous-même.

Section 02 : Discussion

1. Analyse critique des résultats

Les résultats obtenus à travers les observations, l'analyse des matrices de risques et les entretiens réalisés avec les responsables du système d'information à l'ENGTP montrent que la gestion des risques SI est bien présente, mais qu'elle repose encore sur des méthodes classiques, souvent manuelles et peu automatisées.

La première limite identifiée concerne l'absence d'outils intelligents ou automatisés capables d'anticiper ou de détecter certaines menaces de façon dynamique. En effet, l'évaluation des risques se fait à travers des grilles sur Excel, où chaque risque est noté selon sa vraisemblance et son impact. Même si cette méthode permet d'avoir une idée claire des niveaux de criticité, elle reste dépendante du jugement humain et ne permet pas toujours de voir venir des menaces plus discrètes ou complexes.

Ensuite, bien que les personnes interrogées (RSSI, PMSI, DBA) disposent d'une longue expérience et d'une bonne connaissance du terrain, l'entreprise n'exploite pas pleinement les normes et référentiels internationaux comme ISO 27005 ou MEHARI.

Les outils sont parfois cités, mais leur application n'est pas toujours formalisée, ce qui peut créer un écart entre la théorie et la pratique.

D'un autre côté, les entretiens ont révélé un intérêt réel pour l'intelligence artificielle, même si celle-ci n'est pas encore intégrée de manière structurée. Par exemple, certains responsables ont mentionné avoir utilisé des outils comme Chat GPT pour obtenir des conseils techniques ou tester certaines configurations. Cela montre que l'IA commence à susciter de la curiosité, mais qu'elle n'est pas encore vue comme une solution de gestion de risque à part entière.

L'intégration de l'intelligence artificielle dans la gestion des risques SI pourrait apporter de nombreux avantages concrets. Elle permettrait notamment d'analyser de manière automatisée les données de sécurité afin d'identifier des comportements suspects ou inhabituels, souvent imperceptibles pour un analyste humain. De plus, l'IA pourrait détecter certaines failles ou vulnérabilités avant qu'elles ne soient exploitées, renforçant ainsi la capacité de prévention de l'organisation. Grâce au traitement automatique du

langage naturel (NLP), elle serait également en mesure d'exploiter des informations issues de sources externes (rapports, flux d'actualité, alertes de cybersécurité, etc.) pour affiner l'évaluation des menaces. Enfin, elle pourrait contribuer à hiérarchiser les risques en fonction de leur criticité réelle, en intégrant les spécificités contextuelles propres à l'organisation, ce qui améliorerait la prise de décision stratégique en matière de sécurité.

Il ressort de cette analyse que l'ENGTP a déjà des bases solides en matière de gestion des risques SI, mais qu'il reste beaucoup à faire pour passer à une approche plus moderne, plus intelligente et plus prédictive. L'intelligence artificielle représente une vraie opportunité d'évolution, à condition de lever certains freins liés à l'organisation, à la formation des équipes, et à la disponibilité des ressources techniques.

Un autre point important ressort également de l'analyse : l'absence de cadre réglementaire spécifique à l'intelligence artificielle en Algérie, en particulier dans les entreprises publiques comme l'ENGTP. Cette situation représente un obstacle majeur à l'intégration de l'IA dans les pratiques de gestion des risques. En effet, sans lois claires encadrant l'usage de l'IA, les responsables hésitent à déployer des outils intelligents, notamment par crainte de violer des règles implicites de confidentialité ou de sécurité.

De plus, les données traitées dans le secteur pétrolier sont souvent sensibles ou stratégiques, et concernent directement les intérêts de l'État. Cela implique une prudence supplémentaire lorsqu'il s'agit d'automatiser des processus d'analyse ou de déléguer à des algorithmes des tâches critiques. Sans garanties juridiques solides, il est difficile de faire confiance à des systèmes qui fonctionnent parfois comme des « boîtes noires », sans transparence sur les critères de décision.

Ainsi, le manque de réglementation nationale sur l'usage de l'IA dans le domaine de la sécurité des systèmes d'information, combiné à la sensibilité des données gouvernementales, freine l'adoption de ces technologies au sein de l'ENGTP. Cela montre que l'intégration de l'intelligence artificielle ne dépend pas uniquement des moyens techniques, mais aussi du cadre juridique et de la volonté politique de soutenir l'innovation de manière sécurisée.

2. Convergences et divergences avec la littérature

L'analyse des résultats obtenus à travers l'étude de cas de l'ENGTP montre plusieurs points de convergence avec les recherches théoriques traitées dans la revue de littérature, notamment en ce qui concerne les bénéfices attendus de l'intelligence artificielle dans la gestion des risques SI. Comme l'ont souligné Achir et Douari (2024), l'IA permet de renforcer les dispositifs de sécurité en offrant une détection rapide des menaces, une meilleure prise de décision, ainsi que l'automatisation des procédures. Cette vision est partagée par certains responsables de l'ENGTP, qui voient dans l'IA un levier potentiel pour anticiper les incidents et automatiser certaines tâches répétitives.

De plus, les propos des acteurs interrogés rejoignent ceux de Camacho et al. (2024), qui insistent sur l'importance d'une gouvernance structurée pour intégrer l'IA dans la gestion des risques. À l'ENGTP, même si l'IA n'est pas encore utilisée à grande échelle, les responsables reconnaissent la nécessité de l'encadrer dans un cadre organisationnel clair et sécurisé, ce qui rejoint les recommandations du AI Risk Management Framework (NIST) évoqué dans la littérature.

Cependant, certaines divergences importantes apparaissent entre les constats de la littérature et la réalité observée sur le terrain. Alors que de nombreux travaux mettent en évidence l'adoption croissante de l'intelligence artificielle dans des secteurs critiques tels que la santé, la finance ou encore l'énergie, les résultats de notre enquête montrent que son usage au sein de l'ENGTP demeure marginal, voire inexistant dans la gestion quotidienne des risques SI. Cette situation s'explique par plusieurs facteurs propres au contexte algérien. D'abord, l'absence de réglementation claire encadrant l'usage de l'IA crée une zone d'incertitude juridique, freinant toute initiative structurée. Ensuite, la nature hautement stratégique des données traitées, liées aux intérêts de l'État, rend les responsables particulièrement prudents quant à l'automatisation des traitements. À cela s'ajoute un retard relatif dans la transformation digitale du secteur public, qui limite la capacité d'accueil de technologies avancées. Par ailleurs, les coûts associés à la mise en œuvre de l'IA – qu'il s'agisse des investissements en matériel, en logiciels ou en formation – constituent un obstacle majeur. Enfin, l'intégration d'une IA performante impliquerait de rassembler, traiter et harmoniser de grandes quantités de données issues de divers départements, un processus exigeant en temps et en ressources humaines, risquant de perturber les autres priorités stratégiques de l'entreprise.

Enfin, contrairement à certaines études optimistes (comme Odeh et al., 2023), les professionnels interrogés à l'ENGTP expriment des réserves quant à la mise en œuvre concrète de ces technologies, notamment en raison des coûts élevés, du manque de compétences internes spécialisées, et du besoin de garder un contrôle humain sur les décisions de sécurité.

En résumé, si les apports théoriques de l'IA en gestion des risques sont bien connus et partagés dans le discours, leur application reste encore très partielle sur le terrain, en particulier dans les entreprises publiques opérant dans des secteurs stratégiques comme l'énergie. Ce décalage entre la théorie et la pratique souligne l'importance d'adapter les recommandations internationales aux réalités locales, tout en renforçant les bases réglementaires et organisationnelles nécessaires à l'innovation.

Ce chapitre a mis en lumière les pratiques actuelles de gestion des risques SI à l'ENGTP, principalement manuelles et fondées sur l'expertise humaine. Bien que structurée, cette approche montre des limites face aux menaces complexes. Les entretiens révèlent un fort intérêt pour l'IA, perçue comme un levier pour renforcer la détection, la prévention et l'automatisation. Toutefois, son intégration reste freinée par des contraintes juridiques, techniques et organisationnelles. L'avenir passe par une adoption progressive, encadrée et alignée sur les besoins de l'entreprise.

CONCLUSION GÉNÉRALE

Dans un contexte où la sécurité des systèmes d'information est devenue une priorité stratégique, en particulier dans les entreprises publiques opérant dans des environnements sensibles comme l'ENGTP, la question de l'intégration de l'intelligence artificielle dans les dispositifs de gestion des risques s'impose avec de plus en plus d'acuité. L'évolution rapide des menaces, la complexité croissante des infrastructures informatiques, ainsi que la nécessité d'une réactivité renforcée, amènent les organisations à repenser leurs approches traditionnelles.

Cette recherche s'est donc inscrite dans cette dynamique, avec pour objectif principal d'évaluer les pratiques actuelles de gestion des risques SI à l'ENGTP, tout en explorant le potentiel offert par l'IA pour améliorer ces dispositifs. Pour y parvenir, une approche qualitative a été adoptée, reposant sur des entretiens semi-directifs menés auprès de trois responsables du système d'information de l'entreprise (Responsable de la Sécurité des Systèmes d'Information, un Responsable de Projets SI, et un Administrateur de Base de Données). Cette méthodologie nous a permis de recueillir des perceptions concrètes du terrain et de les croiser avec les enseignements de la littérature spécialisée, à l'aide notamment de l'outil d'analyse NVivo.

Les résultats issus de cette étude ont permis de dégager plusieurs constats significatifs, à la croisée des observations de terrain, des entretiens réalisés et de l'analyse documentaire. Il ressort tout d'abord que l'ENGTP dispose d'un processus structuré de gestion des risques des systèmes d'information, reposant principalement sur l'expérience des responsables SI, sur l'utilisation d'outils classiques tels que les grilles d'évaluation Excel, ainsi que sur des référentiels reconnus comme la norme ISO 31000 ou la méthode EBIOS. Toutefois, ces normes ne sont pas encore pleinement appliquées dans leur intégralité, ce qui rend le dispositif encore partiellement empirique et réactif, parfois au détriment d'une anticipation systématique des menaces. La démarche suivie est bien séquencée, allant de l'identification des menaces à l'évaluation du risque résiduel, avec des mesures d'atténuation adaptées, mais le tout reste fortement dépendant de l'intervention humaine.

Un second résultat essentiel concerne la perception de l'intelligence artificielle par les professionnels interrogés. Bien que son intégration dans les pratiques actuelles soit encore limitée, l'IA est perçue très favorablement comme un levier d'amélioration des dispositifs existants. Elle est considérée comme un outil capable de renforcer la détection des anomalies, de faciliter le traitement de grandes quantités de données, d'accélérer la prise de

décision, et de simuler des scénarios de risques complexes que l'analyse humaine ne peut anticiper seule. Certains responsables ont d'ailleurs déjà expérimenté l'IA générative pour obtenir des recommandations techniques contextualisées, ce qui montre une volonté d'exploration et d'innovation. Toutefois, cette ouverture s'accompagne de plusieurs freins identifiés, parmi lesquels l'absence d'un cadre juridique spécifique à l'IA en Algérie, la sensibilité des données stratégiques traitées dans un environnement industriel comme celui de l'ENGTP, les coûts d'implémentation élevés, ainsi que le manque de ressources internes formées à ces nouvelles technologies. Ces résultats soulignent ainsi un potentiel d'évolution réel, mais qui nécessite une structuration plus poussée, des investissements ciblés et une volonté stratégique claire pour que l'intelligence artificielle puisse s'intégrer de manière efficace et sécurisée dans la gestion des risques des systèmes d'information.

Recommandations stratégiques

À la lumière des résultats, il apparaît clairement que l'intégration de l'intelligence artificielle dans le processus de gestion des risques SI à l'ENGTP représente une opportunité significative d'évolution. Toutefois, cette intégration ne peut se faire que dans le cadre d'une démarche structurée, progressive et adaptée au contexte organisationnel, juridique et technique de l'entreprise. Les recommandations suivantes s'appuient à la fois sur les observations de terrain, les entretiens réalisés et les apports théoriques abordés dans le cadre de cette recherche.

- **Élaborer une stratégie d'intégration claire et encadrée**

La première étape consiste à définir une vision stratégique formalisée de l'usage de l'intelligence artificielle dans la sécurité des systèmes d'information. Cette stratégie devrait être portée par la direction générale, en lien avec la DSI, et reposer sur des objectifs mesurables : réduction des délais de détection, amélioration de la couverture des vulnérabilités, automatisation de certaines tâches récurrentes, etc.

Elle doit également intégrer les contraintes juridiques spécifiques au secteur public et industriel algérien, notamment les restrictions liées à la loi 18-07 sur la protection des données personnelles, ainsi que l'interdiction d'externaliser des données sensibles hors du territoire.

- **Lancer des projets pilotes ciblés à faible criticité**

Avant une adoption à grande échelle, il est recommandé de commencer par des cas d'usage spécifiques et maîtrisables, tels que l'analyse automatique des journaux de sécurité à l'aide d'un SIEM intelligent, la détection d'anomalies de connexion sur les serveurs internes, ou encore l'optimisation des stratégies de sauvegarde via des recommandations issues de l'IA. Ces expérimentations doivent être encadrées par des indicateurs clairs d'évaluation de la performance, notamment le temps de réponse, la qualité des alertes générées et le niveau de fiabilité des résultats obtenus.

- **Renforcer la gouvernance des données**

Une intelligence artificielle ne peut fonctionner de manière efficace que si elle s'appuie sur des données fiables, normalisées et rigoureusement structurées. Il devient donc essentiel de désigner un responsable chargé de la qualité et de la gouvernance des données, de centraliser les informations critiques au sein d'une base sécurisée, et de mettre en place des règles strictes d'accès et d'anonymisation des jeux de données exploités par les algorithmes. Ces mesures constituent les fondations indispensables, tant sur le plan technique qu'éthique, pour garantir un déploiement solide et responsable des outils intelligents.

- **Prévoir des outils IA internes, sécurisés et conformes**

Compte tenu de la sensibilité des données industrielles manipulées par l'ENGTP, il est vivement recommandé de privilégier des solutions d'intelligence artificielle « on-premises » ou hébergées sur des serveurs nationaux hautement sécurisés. Ces solutions devront impérativement s'interfacer avec les outils déjà en place (tels que les SIEM, pare-feu et bases de données), fonctionner de manière autonome sans exposition aux réseaux publics, et offrir des interfaces permettant une interprétation humaine claire, favorisant ainsi l'explicabilité des décisions et la supervision des actions automatisées.

- **Accompagner les équipes par la formation et la sensibilisation**

L'introduction de l'intelligence artificielle dans un environnement de travail implique un véritable changement culturel. Pour accompagner cette transition, il est essentiel de former les RSSI, les administrateurs de bases de données (DBA) et les chefs de projet aux concepts fondamentaux de l'IA, d'organiser des ateliers pratiques autour des outils disponibles, et de mettre en place une communication claire et continue sur la complémentarité entre les rôles de l'IA et ceux de l'humain dans les processus critiques. Cette démarche favorisera l'appropriation progressive des technologies tout en renforçant la confiance des équipes.

- **Évaluer régulièrement l'impact et ajuster les choix technologiques**

Enfin, toute initiative d'intégration de l'intelligence artificielle doit faire l'objet d'une évaluation continue dans le temps. Cela passe par la réalisation d'audits réguliers afin de mesurer la performance des modèles déployés, par la conduite d'enquêtes internes visant à évaluer le niveau d'appropriation des outils par les utilisateurs, ainsi que par des ajustements progressifs du périmètre d'application, en tenant compte à la fois des retours d'expérience terrain et des évolutions du cadre réglementaire national. Cette approche itérative garantit une amélioration constante et un déploiement maîtrisé de l'IA.

Limites de la recherche

Cependant, plusieurs limites ont été relevées au cours de l'étude. D'un point de vue organisationnel, l'adoption de l'IA est freinée par un manque de ressources humaines qualifiées et par l'absence d'un cadre juridique spécifique en Algérie encadrant l'usage de ces technologies, notamment dans les entreprises publiques. De plus, la sensibilité des données traitées dans le secteur pétrolier impose des précautions supplémentaires, notamment en matière d'hébergement local et de protection des informations stratégiques.

Sur le plan méthodologique, la principale difficulté rencontrée a été l'accès limité à certaines informations internes, pour des raisons de confidentialité. De même, le faible nombre d'intervenants disponibles a réduit l'échantillon d'entretiens, limitant la généralisation des résultats.

Perspectives

Malgré ces limites, cette recherche ouvre plusieurs pistes intéressantes pour des travaux futurs. Il serait pertinent de mener des études comparatives avec d'autres entreprises publiques ou privées du secteur, afin d'évaluer les niveaux de maturité numérique et les stratégies d'intégration de l'IA dans la cybersécurité. Par ailleurs, la mise en place d'un cadre réglementaire national sur l'usage de l'IA, ainsi que le développement de solutions locales et sécurisées, apparaissent comme une condition essentielle pour favoriser une adoption progressive et maîtrisée de ces outils. Enfin, le renforcement des compétences des équipes par la formation continue représente un levier crucial pour réussir cette transition vers une gestion des risques plus intelligente, proactive et résiliente.

BIBLIOGRAPHIE

27005, N. I. (2018, 07). Technologies de l'information —Techniques de sécurité — Gestion des risques liés à la sécurité de l'information. *Troisième édition NORME INTERNATIONALEISO/IEC 27005*, p. 3.

31000, I. S. (2018, 02). Risk management — Guidelines. *NTERNATIONAL STANDARD ISO 31000*, p. 10.

Achir, W. &. (2024). L'intelligence artificielle au service de la gestion des risques. *Revue des Sciences Commerciales*, 118–132.

Al Kurdi, B. A. (2024). *Studies in Big Data.* Cham: Springer.

Amina, t. (2020/2021). *Cours4_Analyse-de-risque.pdf*. Récupéré sur elearning.univ-eloued.dz: https://elearning.univ-eloued.dz/pluginfile.php/14772/mod_resource/content/1/Cours4_Analyse-de-risque.pdf

ANSSI. (2017, 09). Guide d'hygiène informatique. *Renforcer la sécurité de son système d'information en 42 mesures.*, p. 12.

ANSSI. (2018). Cartographie du système d'information 5étapes. *guide Cartographie du système d'information 5 étapes*, p. 9.

ASSOCIATIONS, F. O. (2003). CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES. *AIRMIC, ALARM, IRM:, translation copyright FERMA*, p. 3.

ASSOCIATIONS, F. O. (2003). CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES. *AIRMIC, ALARM, IRM: 2002, translation copyright FERMA*, pp. 5-7.

ASSOCIATIONS, F. O. (2003). CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES. *AIRMIC, ALARM, IRM: 2002, translation copyright FERMA:* , p. 4.

Badman, S. (2024, mai 12). *Qu'est-ce que la gestion des risques liés à l'IA ?* Récupéré sur IBM Think Blog: https://www.ibm.com/fr-fr/think/insights/ai-risk-management

Camacho, R. F. (2024). AI-driven Risk Management in Cybersecurity: A Simulation-Based Framework. *arXiv*.

Châtelain, Y., & Roche, L. (2000). cyber gagnant, Maxima. p. 31.

CLUB DE LA SECURITE DE L'INFORMATION FRANçAIS. (2010, 01). MEHARI 2010. *Principes fondamentaux et spécification*, p. 15.

clusif. (s.d.). *Les fondamentaux de Méhari*. Récupéré sur clusif.fr: https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/

Emblemsvåg Jan, e. E. (2006). Qualitative risk analysis: some problems and remedies. *Management Decision, vol. 44, no 3*, pp. p. 395-408.

Etiévant, H. (2006, 08 18). *Normes de sécurité : les méthodes d'analyse des risques*. Récupéré sur cyberzoide.developpez.com: https://cyberzoide.developpez.com/securite/methodes-analyse-risques/#LIII-E

Fakrane, H. &. (2020). Comparaison des méthodes d'analyse des risques pour les systèmes d'information. *Revue Africaine de la Recherche en Informatique et Mathématiques Appliquées (ARIMA)*, 37–62.

Fatna, B. (2023). ISO 27001 :2018 AS A GOOD STRATEGIC TOOL TO IT RISK MANAGEMENT . *Journal of Economic Growth and Entrepreneurship JEGE* , p. 53.

Filali, N. (2022). Revue des Sciences Commerciales. *La norme ISO/IEC 27001 : un levier stratégique pour la sécurité de l'information*, 182–193.

FRANÇAIS, C. D. (2010, 01). MEHARI 2010. *Principes fondamentaux et spécification fonctionnelles*, p. 17.

FRANÇAIS, C. D. (2011, 04). MEHARI 2010. *guide de la demarche d'analyse et de traitement des risque*, p. 5.

Hub france. (2024, 07). Opérationnaliser la gestion des risques des systèmes d'Intelligence Artificielle. *GT banque et auditabilité*.

Intervalle, M. (2024, 12 15). *intervalle-technologies.com/blog/gestion-du-risque-informatique/*. Récupéré sur www.ntervalle-technologies.com: ntervalle-technologies.com

Josée, S.-P. (2004). La gestion du risque comment améliorer le financement des PME et faciliter leur développement. *Canada: Presse de l'Université du Québec*, p. 288.

Kunle-Lawanson, O. (2022). *The role of AI in information security risk management.* Récupéré sur www.researchgate.net: https://www.researchgate.net/publication/385708512_The_role_of_AI_in_information_security_risk_management?enrichId=rgreq-7e2ed2694f357527adc10d137c586d37-XXX&enrichSource=Y292ZXJQYWdlOzM4NTcwODUxMjtBUzoxMTQzMTI4MTI4OTc4MTQ4MEAxNzMxMzk5OTQ4MzUy&el=1_x_3&_e

Kunle-Lawanson, O. (2022, 12). The role of AI in information security risk management. *Article in World Journal of Advanced Engineering Technology and Sciences* ·, p. 314.

Kunle-Lawanson, T. (2022). The role of AI in information security risk management. *World Journal of Advanced Engineering Technology and Sciences*, 45–54.

Louisot, J.-P. (2022). management des risues 100 Questions pour comprendre et agir. *afnor edition*, pp. 255-256.

nations, l. c. (2016). Guide d'introduction à la gestion des risques au sein d'une Première Nation . p. 4.

Odeh, M. H. (2023). The Role of Artificial Intelligence in Predictive Risk Assessment and Business Continuity. *Risks*, 19.

Pastre, D. (1999/2000). Université Paris 5 - Maîtrise de mathématiques - Maîtrise MASS - MST ISASH 1999/2000 Dominique Pastre Maîtrise de mathématiques - Maîtrise

MASS Module INTELLIGENCE ARTIFICIELLE. *Université Paris 5 - Maîtrise de mathématiques - Maîtrise MASS - MST ISASH 1999/2000 Dominique Pastre Université Paris 5 - Module INTELLIGENCE ARTIFICIELLE DEFINITION - GENERALITES - HISTORIQUE – DOMAINES*, pp. 8-10.

Reix, R. (1995). système d'information et management des organisations,. *système d'information et management des organisations, Vuibert, France*, p. 123.

Rivière, G. (2017). informatisation du système d'information,. *informatisation du système d'information, ESTIA, France.* , p. 23.

Soravito, G. (2023). Artificial Intelligence and Project Management. *Journal of Innovation Management*, 78–91.

T, A. (2010). Misconceptions of Risk. *John Wiley & Sons Chichester, UK*, p. 252 p.

Turcotte, M. N. (2010). American Institute for Chartered Property Casualty Underwriters, Télé-Université Staff Université du Québec et Université du Québec. Télé-université. *Universite du Quebec Teleuniversite.* , pp. 59-60.

ZAGRÉ, T. (2016, juin 7). GESTION DES RISQUES ET AMÉLIORATION DE LA QUALITÉ DÉCISONNELLE POUR UNE MEILLEURE CLÔTURE DES PROJETS MINIERS. *THÈSE PRÉSENTÉE À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE UNIVERSITÉ DU QUÉBEC* , pp. 15-16.

ANNEXES

Annexe 1 : matrice d'analyse thématique - partie A –

	A : la stratégie actuelle de gestion des risques des SI	B : les normes ou référentiels sont appliqué	C : les fréquence les processus de gestion des risques	D : les méthodes ou outils utiliser	E : les types de risques SI
1 : Entretien 01	nous avons structuré la gestion des risques SI autour d'une identification systématique des actifs critiques et d'une analyse permanente de leur exposition aux menaces, qu'elles soient internes (erreurs humaines, procédures défaillantes) ou externes (cyberattaques, pannes matérielles) Nous concentrons d'abord nos	Au sein de l'ENGTP, la gestion des risques des systèmes d'information est principalement inspirée par les principes de la norme ISO 31000:2018, sans pour autant prétendre à une conformité stricte ou formelle à cette dernière. Notre démarche reste néanmoins	Chez ENGTP, nous procédons à une révision formelle de notre gestion des risques SI chaque année, dans le cadre de notre programme global d'audits internes et d'amélioration continue de la sécurité nous réévaluons l'évolution de nos actifs critiques, les incidents survenus, les	L'identification et l'évaluation des risques liés aux systèmes d'information reposent sur une approche structurée combinant outils internes et référentiels externes nous utilisons un outil open source d'évaluation des risques adapté aux standards communs (normes ISO/IEC 27005 et ISO/IEC 31000)	Les risques que nous rencontrons le plus fréquemment concernent principalement la compromission des mots de passe des utilisateurs. Ce type de risque représente plus de 90 % des incidents identifiés Il s'agit de cas où les utilisateurs adoptent des pratiques faibles en matière de création et de gestion de

	efforts sur les éléments les plus sensibles de notre SI : bases de données stratégiques, applications métiers essentielles et infrastructures réseau garantissant la connectivité entre le siège et nos directions régionales Pour établir notre cartographie initiale des risques, nous avons ciblé deux grandes catégories : les risques techniques et les risques organisationnel, nous appliquons des	adaptée aux réalités industrielles de l'ENGTP, caractérisées par la diversité des sites, la complexité des infrastructures, et la nécessité de maintenir une flexibilité opérationnelle	nouveaux projets Ce cycle annuel nous permet d'actualiser notre cartographie des risques, de redéfinir nos priorités et d'ajuster nos mesures de sécurité Par ailleurs, nous restons vigilants et pouvons déclencher des mises à jour ponctuelles dès l'identification d'un incident critique, la réalisation d'un audit externe ou tout changement	Cet outil offre la flexibilité nécessaire pour répondre aux spécificités de notre environnement industriel, tout en respectant une méthodologie rigoureuse d'identification, d'analyse et d'évaluation des risques Cette méthodologie d'évaluation de personalisation est consolidée parl'utilisation d'outils de collecte structurée, tels que : Des questionnaires thématiques permettant	mots de passe Cette vulnérabilité expose nos systèmes à des risques d'accès non autorisé, de fuite d'informations sensibles, et de perturbation des opérations critiques, nous faisons face à des pannes matérielles (hardware), notamment sur les serveurs anciens, les équipements réseau vieillissants, et certains postes de travail déployés dans les zones industrielles isolées Les erreurs de

	mesures éprouvées telles que l'installation d'antivirus certifiés avec mises à jour régulièrest des échanges sensibles et la mise en place de contrôles d'accès renforcés notre approche reste majoritaire réactive, axée sur la détection et la correction post-incident, Questionnaire interne structuré		majeur du SI Cette combinaison d'un processus structuré et de mises à jour réactives est essentielle pour garantir l'efficacité de notre dispositif de sécurité dans un environnement industriel dynamique, renforcer la maturité de notre cybersécurité et à soutenir les objectifs d'entreprise.	d'obtenir une vision exhaustive des points faibles nous réalisons également des campagnes d'audit interne, associées à des sessions d'auto-évaluation de la conformité aux exigences de notre politique de sécurité informatique Capables d'améliorer la précision de l'identification des risques et d'optimiser la réactivité de notre dispositif de sécurité	manipulation des utilisateurs constituent également un risque récurrent des erreurs telles que la mauvaise manipulation de fichiers sensibles, la désactivation accidentelle de paramètres de sécurité, ou la suppression involontaire de données critiques ,

2 : Entretien 02	En tant que Responsable des Projets des Systèmes d'Information à l'ENGTP, ma démarche de gestion des risques est étroitement liée à la conduite des projets de déploiement des infrastructures SI, qu'il s'agisse de solutions logicielles, de systèmes réseau ou d'environnements applicatifs destinés à soutenir les opérations industrielles de l'entreprise Ma stratégie repose principalement	À mon niveau, je n'applique pas de norme précise pour encadrer la gestion des risques SI Même si cette méthode n'est pas formalisée selon un standard, elle est efficace pour assurer un suivi adapté à nos besoins immédiats	J'actualise le registre des risques en moyenne tous les six mois. Cette périodicité, non imposée formellement, correspond naturellement aux jalons clés du projet ou à l'apparition d'événements susceptibles de modifier son périmètre Je procède notamment à une mise à jour du tableau des risques Après la phase de déploiement Mon	Ma méthode de gestion des risques reste avant tout pratique, simple et adaptée au rythme des projets que je pilote J'utilise principalement un fichier Excel structuré, que j'ai développé moi-même au fil des années l'efficacité, la rapidité de mise à jour et la simplicité d'Excel répondent à mes contraintes quotidiennes	Les risques que je rencontre le plus fréquemment sont liés à la chaîne logistique et à la coordination des phases critiques de déploiement L'un des risques majeurs que nous subissons régulièrement concerne les retards dans la livraison du matériel informatique, des licences logicielles ou des solutions tierces nécessaires à l'implémentation. Ces délais impactent directement notre capacité

	sur l'expérience acquise dans le suivi et la mise en œuvre de projets similaires. Cela me permet d'anticiper les risques susceptibles de compromettre la qualité, les délais ou la disponibilité des ressources durant les différentes phases du projet Ces risques peuvent être techniques (retards dans la livraison des équipements, incompatibilités logicielles, instabilité des systèmes), organisationnel		approche consiste à identifier les risques en fonction des réalités opérationnelles, sans m'imposer de cadre normatif		à respecter le calendrier initial du projet et peuvent entraîner des effets en cascade Un autre type de risque, plus humain, concerne la résistance au changement des utilisateurs Ces risques, sont parfois difficiles à anticiper dans leur intensité. Ils exigent donc une vigilance continue, une planification réaliste et une coordination étroite entre les différents acteurs du projet,

	s (absence de coordination interservices, manque de				notamment les fournisseurs, la DSI, les équipes métiers et les utilisateurs finaux.

Annexe 2 matrice d'analyse thématique - partie B -

	A : l'utilisation une autre méthode	B : utilisation des méthodes comme MEHARI, EBIOS ou OCTAVE
1 : Entretien 01	En revanche, nous avons développé une méthode interne, épurée et personnalisée, qui s'appuie sur les grands principes universels de la gestion des risques, tout en restant adaptée aux spécificités de notre organisation industrielle Cette approche se structure en quatre grandes étapes séquentielles : Identification - évaluation – traitement -réévaluation Cette méthode, bien qu'épurée, permet de garder un pilotage pragmatique et efficace des risques SI sans alourdir les procédures internes. Elle est également suffisamment flexible pour être enrichie au fil du temps. Elle nous permet surtout de concilier la rigueur nécessaire à la protection de nos actifs critiques avec la réalité opérationnelle de l'ENGTP, où la priorité est de maintenir la disponibilité, la sécurité et l'efficacité de nos systèmes d'information au service de l'activité industrielle	nous n'avons pas formellement utilisé les méthodes standards pour la gestion des risques des systèmes d'information Personnellement, en tant que Responsable de la Sécurité des Systèmes d'Information, je connais bien la méthode EBIOS, notamment ses étapes d'identification des événements redoutés, d'analyse des scénarios de menace et de définition des objectifs de sécurité Toutefois, l'application intégrale de cette méthode m'a semblé relativement lourde à mettre en œuvre dans notre contexte, principalement en raison de la charge de travail importante Quant aux méthodes MEHARI et OCTAVE, elles n'ont pas été retenues non plus pour les mêmes raisons : la complexité de leur mise en œuvre, la nécessité de mobiliser durablement plusieurs acteurs métiers et les contraintes de ressources ne sont pas compatibles avec la dynamique actuelle de l'entreprise

2 : Entretien 02	Plutôt que d'appliquer une méthode spécifique ou formalisée, je construis ma gestion des risques au cas par cas, en fonction des particularités de chaque projet Je m'appuie sur l'analyse des contraintes opérationnelles, des délais et des ressources disponibles pour identifier les risques, les évaluer et définir les actions nécessaires Cette approche souple et pragmatique me permet de réagir rapidement face aux imprévus, sans être limité par un cadre méthodologique rigide	Mon objectif est d'être réactif et pratique, sans m'enfermer dans une méthode formelle qui pourrait alourdir la gestion opérationnelle
3 : entretien 03	La méthode est celle du RSSI	La méthode est celle du RSSI

Annexe 3 matrice d'analyse thématique - partie c -

	A : les obstacles à l'adoption de l'IA dans votre entreprise	B : une expérience de l'utilisation de l'intelligence artificielle	C : l'IA peut contribuer à améliorer la détection et la prévention des risques SI	D : les conditions
1 : Entretien 01	Pour l'instant, chez ENGTP, nous n'avons pas rencontré de freins internes significatifs à l'adoption de l'IA pour la sécurité des SI. Au contraire, l'enthousiasme est réel et croissant le principal point de vigilance est juridique et réglementaire. La législation algérienne interdit strictement l'externalisation des données sensibles Par conséquent,	Oui, chez ENGTP, nous explorons déjà l'intégration de l'IA générative dans notre processus de traitement des risques SI J'utilise ce type d'IA comme outil d'aide à la décision technique pour définir des mesures d'atténuation adaptées à nos équipements et logiciels Elle m'a fourni un ensemble de recommandations concrètes, telles	Oui, je suis convaincue que l'intelligence artificielle peut apporter une réelle valeur ajoutée dans la détection et la prévention des risques liés aux systèmes d'information, en particulier dans un environnement industriel complexe comme celui d'ENGTP L'IA a l'avantage de pouvoir analyser des volumes massifs de données, ce qui dépasse largement les capacités humaines en	Je pense que pour réussir l'intégration de l'IA dans la gestion des risques SI à l'ENGTP, il est crucial d'impliquer activement le top management La direction générale doit d'abord voir des résultats concrets : montrer comment l'IA peut, par exemple, anticiper des risques complexes qu'une analyse manuelle ne détecterait pas, accélérer la prise de décision lors

	nous ne pouvons pas recourir à des services d'IA hébergés hors du territoire ou sur des cloud non maîtrisés localement pour ces catégories de données nous privilégions des traitements réalisés en interne ou sur des plateformes locales, et nous anonymisons systématiquement les données non classifiées	que : Désactiver les services système non essentiels Mettre en place des stratégies d'accès plus strictes Renforcer la journalisation d'audit Configurer des règles avancées dans le Pare-feu Windows Activer la surveillance des comptes à privilèges Appliquer des politiques de sécurité réseau renforcées Cette démarche nous permet de gagner un temps précieux, d'améliorer la qualité de nos mesures de sécurité et de standardiser	temps réel. Dans le domaine de la cybersécurité, cela permet par exemple : De traiter des millions de logs système pour repérer des anomalies, D'identifier des comportements inhabituels ou des signaux faibles indicateurs d'intrusion, Et d'anticiper des menaces potentielles bien avant qu'elles n'affectent les opérations Utilisée de manière structurée et critique, elle peut renforcer efficacement les dispositifs de sécurité et améliorer la réactivité de	d'incidents, ou encore assurer la continuité des opérations industrielles critiques Au final, c'est l'adhésion et le soutien du top management, fondés sur des indicateurs clairs et des gains mesurables, qui permettront d'accélérer l'adoption de l'IA dans nos processus de gestion des risques informatiques

		progressivement nos pratiques selon des référentiels à jour nous utilisons l'IA comme un outil d'assistance, et non comme une solution de remplacement à l'expertise humaine Les décisions finales restent prises par les équipes techniques.	l'entreprise face aux risques	

2 : Entretien 02	À mon niveau, je ne perçois pas d'obstacles particuliers à l'adoption de l'intelligence artificielle au sein de l'ENGTP l'environnement économique et politique actuel encourage activement l'intégration de ces nouvelles technologies, en particulier dans les secteurs industriels et stratégiques Le gouvernement algérien lui-même incite les entreprises nationales à tirer parti de l'IA pour améliorer leur productivité, renforcer leur sécurité, et moderniser leurs	Oui, j'utilise l'intelligence artificielle, notamment les outils d'IA générative accessibles en ligne, dans le cadre de la gestion des projets IT deux éléments sont particulièrement critiques pour moi : Le degré de compatibilité technique avec l'environnement existant, Et l'adéquation de la solution aux exigences du cahier des charges je m'appuie sur l'IA pour gagner du temps dans l'analyse préliminaire, en posant des questions	je suis convaincu que l'intelligence artificielle a un véritable rôle à jouer dans l'amélioration de la détection et de la prévention des risques liés aux systèmes d'information L'arrivée de l'IA, notamment des modèles génératifs, a profondément changé ma manière de travailler je peux obtenir en quelques secondes des réponses contextualisées, précises et parfois même structurées sous forme de recommandations elle est déjà un levier de	Pour ma part, l'idéal serait d'intégrer l'intelligence artificielle directement dans les outils que nous utilisons au quotidien, notamment ceux dédiés à la gestion de projets IT Ce que j'attends, c'est l'acquisition d'un outil de gestion de projet moderne qui intègre l'IA de manière native, c'est-à-dire intelligemment intégrée dans l'interface et les fonctionnalités, pas simplement ajoutée comme un module annexe

	infrastructures	techniques ciblées la réponse générée par l'IA m'a permis de comprendre qu'il existait un risque potentiel de compatibilité avec les équipements Huawei	productivité et de sécurisation évident dans le contexte des projets informatiques	
3 : entretien 03	Le seul obstacle que je vois c'est la nature sensible des données	Connaissant la popularité de notre SGBD, je sais que l'IA génère des réponses de très bonne qualité dans ce contexte Récemment, j'ai été obligé de me conformer à la loi 18-07 algérienne qui vise à protéger les données personnelles	J'aurais aimé que je puisse interroger l'IA directement à partir d'un programme ou application Cette IA, doit avoir accès à mes bases de données pour que les réponses soient précises	L'adoption d'une IA « On Premises » spécialisée intégrée au SIEM de l'entreprise

		Question à l'IA : pour Microsoft SQL Server, quelles sont les configurations qui m'éviteront le risque de non-conformité avec la loi 18-07 algérienne ? La réponse est très riche et pertinente ! ça m'a permis d'ajuster pas mal de paramètres dont je n'avais même pas connaissance		

Annexe 4 matrice d'analyse thématique - partie D -

	A : l'avenir de la gestion des risques SI
1 : Entretien 01	Dans un contexte de digitalisation accélérée, l'avenir de la gestion des risques des systèmes d'information reposera sur une combinaison intelligente entre l'expertise humaine et les technologies d'intelligence artificielle L'IA représente un formidable levier d'assistance pour renforcer la détection des anomalies, anticiper les risques émergents, prioriser les réponses aux incidents, et automatiser certaines tâches complexes de surveillance et d'analyse de données À l'ENGTP, dans une perspective de modernisation progressive de nos dispositifs de sécurité, il est évident que l'intégration de ces technologies sera un levier important pour renforcer notre résilience numérique je vois l'avenir de la gestion des risques SI comme un modèle hybride, où les technologies d'intelligence artificielle viendront enrichir les capacités humaines, sans jamais les remplacer
2 : Entretien 02	je vois déjà les effets positifs de l'intelligence artificielle dans mon métier, notamment en matière de prise de décision, d'analyse rapide de données techniques et d'identification de risques projet évoluera vers une nouvelle génération de gestion de projet, pilotée non plus uniquement par des humains, mais par ce que j'appelle des « Intelligent Project Managers » la combinaison IA + expertise humaine sera la clé pour atteindre un niveau de gestion des risques plus intelligent, plus agile et plus réactif
3 : entretien 03	Je trouve des difficultés à cerner les limites de l'IA. J'espère qu'un jour on puisse arriver à une IA qui puisse faire la conception d'une architecture sécurisée pour l'entreprise, d'écrire des politiques et procédures détaillées et de gérer les risques mieux qu'une équipe de spécialistes

Annexe 5 : Fiche d'évaluation du risque brut

NOM DE L'ÉVALUATEUR :	K.AKKOUCHE
DATE DE L'ÉVALUATION :	31 December 2024
ÉLÉMENT ÉVALUÉ :	Serveur Base de données
ORGANISATION :	ENGTP

CRITICITÉ DU PROJET	CAPACITÉ D'INTERVENTION EN CAS DE CRISE	SEUIL DE RISQUE
Calculated	Calculated	Calculated

ID #	MENACE	VULNERABILITY	RISQUE INHÉRENT			RISQUE ACCEPTABLE?
			VRAISEMBLANCE	IMPACT	COTE DE RISQUE	
1	Panne Serveur Physique Hote	Conditions de fonctionnement, Panne composant electronique, Climat...	3	5	15	Yes
6	Attaque sur Vulnérabilité connue SQL Server/Windows	Patch non appliqués, produit obsolète	2	5	10	Yes
9	Compromission mot de passe (Interne)	Aucune politique Soft/Hard pour les mots de passes SQL Server / Applications	3	2	6	Yes
10	Crash suite à une mise à jour automatique incompatible	Mises à jour déployées sans tests préalables.	1	4	4	Yes

Annexe 6 : Mesures d'atténuation prévues à horizon fin 2024

STRATÉGIE DE GESTION DES RISQUES	MESURES D'ATTÉNUATION (Mis En Place à fin 2024)
Gérer	Serveurs équivalents, Sauvegardes complètes, Serveur virtualisé, Tolérance à l'arret de quelques heures sans grand impact, DataCenter Aux Normes.
Accepter	Version Windows supporté , WSUS, Licences support SQL Server
Gérer	Politique des mots de passes rédigée / Appliquée partiellement
Gérer	Possibilité de rollback, tolérance assez élevée à l'arret des services le temps de la remédiation.

Annexe 7 : Évaluation du risque résiduel et acceptabilité

RISQUE RÉSIDUEL			RISQUE ACCEPTABLE	NOTES
VRAISEMB LANCE	IMPACT	CO TE DE RISQUE		
2	5	10	Yes	Gérer les sauvegardes/Restaurations avec Solution Entreprise Acquise pour accélerer la remise en marche.
2	5	10	Yes	Mise à niveau obligatoire des systèmes & Infrastructure SQL Server avant fin 2025
2	2	4	Yes	Implémenter (Hard Coder) la complexité des mots de passes. Vérifier, changer et diffuser de nouveaux mots de passes (tous les DBA's)
1	3	3	Yes	Vu la lourdeur d'une solution de test (environnement séparé), la stratégie actuelle présente un seuil acceptable en matière de disponibilité. (la mise à jour est plus critique que le risque d'arret).

Annexe 8 page d'accueil de leurs Site Web

ENGTP	**Guide d'entretien**	المدرسة الوطنية العليا للمناجمنت Ecole Nationale Supérieure de Management

Bonjour, nous sommes étudiantes en Master 2 Management Stratégique et Systèmes d'Information. Dans le cadre de notre mémoire de fin d'études, nous réalisons une étude sure « L'intégration de l'intelligence artificielle dans la gestion des risques des systèmes d'information : Cas de l'entreprise ENGTP »

Cet entretien a pour but d'analyser l'apport potentiel de l'IA dans l'optimisation de la gestion des risques SI et d'examiner les conditions organisationnelles qui facilitent son adoption. De mieux comprendre les pratiques actuelles dans votre entreprise ainsi que votre point de vue sur l'apport potentiel de l'IA dans ce domaine.

Vos réponses resteront confidentielles et seront utilisées uniquement à des fins académiques.

Questions de l'entretien :

- Combien d'années d'expérience avez-vous dans ce domaine ?

Partie A : Gestion des risques SI

- Comment décririez-vous la stratégie actuelle de gestion des risques des systèmes d'information dans votre entreprise ?
- Quels types de risques SI rencontrez-vous le plus fréquemment ?
- Quelles méthodes ou outils utilisez-vous pour identifier et évaluer ces risques ?
- À quelle fréquence les processus de gestion des risques sont-ils mis à jour ?
- Quelles normes ou référentiels sont appliqués pour encadrer la gestion des risques SI dans votre organisation ?

Partie B : Outils & Méthodes de gestion des risques

- Avez-vous déjà utilisé des méthodes comme MEHARI, EBIOS ou OCTAVE ? Pourquoi ?
- Si vous utilisez une autre méthode laquelle ?
- Quels sont selon vous les avantages et limites de ces méthodes ?

Partie C : L'Intelligence Artificielle dans la gestion des risques

- Avez-vous une idée ou une expérience de l'utilisation de l'intelligence artificielle dans votre entreprise, notamment dans le domaine de la sécurité ou de la gestion des risques ? pouvez vous me donner un exemple
- Pensez-vous que l'IA peut contribuer à améliorer la détection et la prévention des risques SI ? Comment ?
- Quels sont, selon vous, les obstacles à l'adoption de l'IA dans votre entreprise ?
- Quelles conditions faciliteraient l'intégration de l'IA dans la gestion des risques SI?

Partie D : Vision stratégique

- Comment percevez-vous l'avenir de la gestion des risques SI dans un contexte de digitalisation croissante ?