الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique

Ecole Nationale Supérieure de Management
Koléa

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

MÉMOIRE DE FIN D'ÉTUDES

En vue de l'obtention d'un master professionnel en
« Management stratégique et système d'information »

Essai de mise en place d'une stratégie proactive de sécurité des systèmes d'information
Cas : La direction centrale digitalisation et système d'information de SONATRACH

Élaboré par :
MOUDJED Fatma

Encadré par :
DR. ABID Nabila
DR. DERRAR Hacene

Année Universitaire 2023/2024

REMERSIEMENT

Au terme de ce travail de recherche, il est essentiel pour moi de prendre un moment pour exprimer ma profonde gratitude envers toutes les personnes qui ont contribué à sa réalisation. De la guidance académique à l'appui émotionnel, chaque acteur a joué un rôle crucial dans ce mémoire.

Je tiens à exprimer ma profonde gratitude envers mes parents, ***Ismaël*** *et* ***Nora****, ainsi que mon frère* ***Billel*** *et mes sœurs* ***Sarah****,* ***Hadjer*** *et* ***Chaima****, pour leur soutien indéfectible et leurs encouragements constants tout au long de mes études. Leur confiance inébranlable et leur amour inconditionnel ont été des piliers sur lesquels je me suis appuyé dans les moments de doute et de difficulté.*

Je souhaite également remercier les personnes suivantes pour leur contribution précieuse à cette recherche :

Mes encadrants à l'École Nationale Supérieure de Management, Dr. ***ABID Nabila*** *et Dr****. DERRAR Hacene****, pour leur précieux éclairage et leur ouverture sur une diversité de domaines d'étude. Leurs conseils avisés ont été d'une grande valeur pour la construction de mon travail.*

Madame ***LEHANINE****, chef du département Management De La Sécurité Des Systèmes D'information, à* ***SONATRACH*** *pour son soutien et ses conseils avisés tout au long de cette recherche. Sa contribution a été essentielle pour orienter mes réflexions dans ce domaine spécifique.*

HAICHEUR Khadidja et BOUDISSA Abdel Moumen*, mes encadrants au sein du département Management de la Sécurité des Systèmes d'Information pour leur soutien constant, leur expertise et leurs conseils précieux dans le cadre de ce projet. Leur expérience pratique et leur disponibilité ont été des atouts essentiels pour la réussite de cette recherche.*

Je tiens également à remercier chaleureusement ***Aymen CHELLAL*** *pour son aide précieuse et pour toutes les informations qu'il m'a fournies. Ses conseils ont été d'une grande valeur ajoutée à travail.*

MOUDJED FATMA

RÉSUMÉ

Assurer la sécurité des systèmes d'information représente un élément essentiel pour les entreprises et leurs parties prenantes, nécessitant une organisation efficace, une surveillance rigoureuse et une gestion appropriée. Dans cette optique, l'élaboration d'une stratégie proactive de sécurité des systèmes d'information s'avère indispensable.

Notre objectif principal consiste à analyser le rôle d'une stratégie proactive dans le renforcement de la sécurité des systèmes d'information de SONATRACH, tout en adoptant une approche basée sur le cycle PDCA (Plan-Do-Check-Act).

Pour atteindre cet objectif, nous avons opté pour une approche qualitative, mettant en œuvre des entretiens semi-directifs avec les responsables de la Direction de la Sécurité des Systèmes d'information (DSSI).

Les résultats montrent que SONATRACH nécessite une planification stratégique formelle en matière de sécurité des systèmes d'information, car celle-ci est actuellement insuffisante voire inexistante.

Mot clés : sécurité, systèmes d'information, stratégie proactive, PDCA.

ABSTRACT

Ensuring the security of information systems is essential for companies and their stakeholders, requiring effective organization, rigorous monitoring, and proper management. In this context, the development of a proactive information systems security strategy is indispensable.

Our primary objective is to analyze the role of a proactive strategy in strengthening the security of SONATRACH's information systems, while adopting an approach based on the PDCA (Plan-Do-Check-Act) cycle.

To achieve this objective, we have chosen a qualitative approach, implementing semi-structured interviews with the managers of the Information Systems Security Department (DSSI).

The results show that SONATRACH requires a formal strategic plan for information systems security, as the current planning is insufficient or even non-existent.

Key words: information systems, security, proactive strategy, PDCA.

ملخص

ضمان أمان نظم المعلومات يمثل عنصرًا أساسيًا للشركات وأصحاب المصلحة، مما يتطلب تنظيمًا فعالًا، مراقبة صارمة وإدارة مناسبة .في هذا السياق، يعتبر وضع استراتيجية استباقية لأمن نظم المعلومات أمرًا لا غنى عنه.

هدفنا الرئيسي هو تحليل دور استراتيجية استباقية في تعزيز أمان نظم المعلومات في شركة سوناطراك، مع اتباع نهج يعتمد على دورة PDCA (خطط -نفذ-تحقق-تصرف).

لتحقيق هذا الهدف، اخترنا نهجًا نوعيًا، ينفذ من خلال مقابلات شبه موجهة مع مسؤولي إدارة أمن نظم المعلومات (DSSI).

تظهر النتائج أن سوناطراك تحتاج إلى تخطيط استراتيجي رسمي في مجال أمن نظم المعلومات، حيث أن الوضع الحالي غير كافٍ أو حتى غير موجود.

الكلمات الرئيسية :أمن، نظم المعلومات، استراتيجية استباقية، PDCA

Table des matières

REMERSIEMENT ..... **II**

RÉSUMÉ ..... **III**

Table des matières ..... **V**

Liste des tableaux ..... **VIII**

Liste des figures ..... **IX**

Liste des abréviations ..... **X**

INTRODUCTION **1**

1.1. Contexte et intérêt du thème ***2***

1.2. L'objectif de la recherche ***4***

1.3. Problématique ***4***

1.4. Méthode ***4***

1.5. Pertinence de la recherche ***4***

1.6. Structure de notre étude ***5***

CHAPITRE I : CADRE THÉORIQUE **7**

Introduction **8**

Section01 : Revue de la littérature **8**

1.1. Sécurité de l'information ***8***

1.2. Stratégie de cybersécurité ***11***

1.3. Stratégie de sécurité des systèmes d'information ***14***

1.4. Management de la sécurité des systèmes d'information selon la norme ISO/IEC27001 ..... ***16***

Section02 : Cadre conceptuel **18**

2.1. Sécurité des systèmes d'information (SSI) ***18***

2.2. Enjeux de la Sécurité des systèmes d'information 21

2.3. Le management de la Sécurité des Systèmes d'Information..... 22

2.4. Politique de sécurité des systèmes d'information (PSSI) 23

2.4.1. Définition de la politique de sécurité des systèmes d'information 23

2.4.2. Objectif et Finalité de la politique de sécurité des systèmes d'information 24

2.4.3. Concepts clés de l'élaboration d'une politique de sécurité des systèmes d'information 25

2.4.4. Impacts de la politique de sécurité des systèmes d'information sur le management dans l'entreprise 27

2.5. Normes, référentiels et méthodes pour une meilleure sécurité de l'actif informationnel 30

2.6. Concepts Clés de la sécurité des systèmes d'information..... 33

2.7. Les stratégies de sécurité contre les menaces et les vulnérabilités 35

Conclusion 38

CHAPITRE II : CADRE MÉTHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL 40

Introduction..... 41

Section 01 : Cadre méthodologique..... 41

1.1. Paradigme et démarche de recherche..... 41

1.2. Approche méthodologique..... 41

1.3. Méthodes de collecte de données dans la recherche qualitative..... 41

1.4. Sélection des interviewés 45

1.5. Déroulement de notre étude empirique..... 46

Section 02 : Présentation de l'organisme d'accueil 48

2.1. SONATRACH : une contribution essentielle à l'économie nationale..... 48

2.2. Bref rappel historique..... 48

2.3. La mission et les objectifs de SONATRACH 50

2.4. L'organigramme de la macrostructure de SONATRACH 51

Conclusion 53

CHAPITRE III : RESULTAT ET DISCUSSION 55

Introduction 56

Section 01 : Etat des lieux et proposition d'une méthode d'élaboration d'une stratégie proactive de la sécurité des systèmes d'information 56

1.1. Politique de sécurité des systèmes d'information 56

1.2. Analyse des risques 58

1.3. Organisation de la direction de sécurité des systèmes d'information 59

1.4. Culture et sensibilisation à la sécurité des systèmes d'information 60

1.5. Stratégie et gestion des vulnérabilités 61

1.6. Proposition d'une méthode établie pour élaborer une Stratégie Proactive de sécurité des systèmes d'information 62

1.7. Élaboration de de la stratégie proactive de sécurité des systèmes d'information . 65

Section 02 : Discussion, analyse critique et suggestions 70

2.1. Discussion 70

2.2. Analyse critique 70

2.3. Suggestions 72

Conclusion 75

CONCLUSION GÉNÉRALE 76

BIBLIOGRAPHIE 80

ANNEXES 85

Liste des tableaux

Tableau 1 : Méthodes proposées et suggestions selon les articles 12
Tableau 2 : L'architecture des entretiens 45
Tableau 3 : L'organisation de nos pratiques au sein de la DSSI de SH**.** 46
Tableau 4 : Des renseignements concernant les personnes interrogées 47

Liste des figures

Figure 1: Critères de sécurité 21
Figure 2 : De la politique d'entreprise a la politique de sécurité 25
Figure 3 : Les phases de l'élaboration d'une PSSI 27
Figure 4 : Les 37 processus de COBIT5 32
Figure 5 : Dates marquantes de l'historique de SONATRACH 49
Figure 6 : Organigramme de la macrostructure de SONATRACH 51
Figure 7 : Organigramme de la DC DSI 52
Figure 8 : Triangulation des méthodes de collectes de données qualitative 45
Figure 9 : Modèle de cycle PDCA et cycle de vie de la stratégie de sécurité SI de l'entreprise 64
Figure 10 : étapes d'élaboration d'une Stratégie SSI 65
Figure 11 : proposition d'un organigramme de la DSSI détaché de la DC DSI 74

Liste des abréviations

APO : Aligner, planifier, et organiser

ASSI : Agence de sécurité des systèmes d'information

BAI : Bâtir, acquérir et implémenter

Cobit : Control objectives for information and related technology

CSSI : Culture de sécurité SI

DC DSI : Direction centrale digitalisation et systèmes d'information

EDS : Evaluer, diriger et surveiller

ISACA : Information Systems Audit and Control Association

ISO : International Organization for Standardization

LSS : livrer, servir et soutenir

MEHARI : Méthode harmonisée d'analyse des risques

MSSI : Management de la sécurité des systèmes d'information

NCSS : Stratégie nationale de cybersécurité

PDCA : Plan, Do, Check, Act

RNSI : Référentiel national de la sécurité de l'information

SEM : surveiller, évaluer et mesurer

SH : SONATRACH

SI : Systèmes d'information

SOA : Statement of applicability

SSI : Sécurité des systèmes d'information

TI : Technologies de l'information

INTRODUCTION

1.1. Contexte et intérêt du thème

Avec la multiplication des cyberattaques de grande envergure et des incidents de sécurité, les organisations ont intensifié leurs efforts pour protéger leurs systèmes d'information. Cela se traduit par l'adoption de mesures de sécurité plus robustes, telles que le chiffrement des données, l'authentification multifactorielle, et la surveillance continue des réseaux. À l'ère numérique où les entreprises et les organisations dépendent de plus en plus des technologies de l'information, la sécurité des systèmes d'information revêt une importance cruciale. Les cybermenaces étant devenues omniprésentes, il est indispensable de mettre en place des stratégies proactives pour protéger les données et les systèmes d'information contre les menaces.

La sécurité des systèmes d'information pose des défis complexes, impliquant la compréhension des menaces potentielles, la conception de mesures de sécurité appropriées, ainsi que la mise en œuvre de politiques et de procédures adéquates. Cela rend le sujet riche en possibilités d'exploration et de recherche. Une stratégie proactive de sécurité peut avoir un impact significatif sur la résilience et la viabilité d'une organisation, comme l'affirme (Klaa, 2022).

Une étude approfondie de ce sujet peut fournir des insights précieux pour les entreprises et les décideurs, les aidant à prendre des décisions informées pour protéger leurs systèmes d'information. La nature des cybermenaces évolue constamment, nécessitant une adaptation continue des stratégies de sécurité. Cela crée un domaine de recherche dynamique où de nouvelles approches et technologies sont explorées pour faire face aux menaces émergentes.

Le thème de la stratégie proactive de sécurité des systèmes d'information, bien qu'il ne soit pas nouveau, demeure très pertinent. Il évolue avec les avancées technologiques et les nouvelles menaces. Abordé depuis de nombreuses années par des chercheurs, praticiens et experts, il reste un sujet en constante évolution en raison de la nature changeante des cybermenaces et des environnements technologiques.

Bien que de nombreux aspects de la sécurité des systèmes d'information aient été explorés, des lacunes et des défis persistent. Par exemple, l'essor de l'Internet des objets (IoT), de l'intelligence artificielle (IA) et la prolifération des appareils mobiles posent de nouveaux défis en matière de sécurité, nécessitant une attention particulière. Les travaux de recherche peuvent se concentrer sur divers aspects tels que la gestion des risques, les politiques de sécurité, la conformité réglementaire, la sensibilisation à la sécurité et la gestion des

incidents de sécurité. De plus, des recherches novatrices sont nécessaires pour développer de nouvelles stratégies et technologies permettant de faire face aux menaces émergentes et aux vulnérabilités.

L'Algérie accorde une attention particulière à la mise en place d'une stratégie nationale de sécurité des systèmes d'information, reconnaissant les défis croissants posés par les menaces cybernétiques. Cette initiative vise à relever plusieurs défis majeurs, tels que la transition vers un statut de producteur d'outils de défense cybernétique, la garantie de la flexibilité des systèmes sensibles et le contrôle des technologies avancées. Ces aspects nécessitent une étude approfondie et leur intégration dans la stratégie proactive de sécurité des systèmes d'information.

Les menaces croissantes en matière de sécurité des systèmes d'information, notamment les attaques soutenues par des États visant à perturber, influencer l'opinion publique ou diffuser de fausses informations, ont conduit l'Algérie à accorder une grande importance à la sécurisation de ses systèmes d'information. L'espionnage et la perturbation des infrastructures essentielles sont également des préoccupations majeures, tout comme la menace croissante due à l'augmentation de l'utilisation du numérique. Pour faire face à ces défis, des mesures sont prises, incluant la création d'une stratégie nationale de sécurité des systèmes d'information.

En effet, la sécurité des systèmes d'information est considérée comme un élément essentiel de la souveraineté numérique. Il est impératif de coordonner les efforts pour garantir cette souveraineté.

Après de nombreuses recherches et une réflexion approfondie, nous avons choisi le thème de "la stratégie proactive de sécurité des systèmes d'information" au sein du département Management de La Sécurité des Systèmes d'Information (MSSI) de la Direction Centrale Digitalisation et Systèmes d'Information (DC-DSI) de SONATRACH (SH). Cette décision découle de la reconnaissance de l'importance cruciale de la sécurité des systèmes d'information dans le contexte actuel marqué par une augmentation des cybermenaces.

Ce sujet revêt également un intérêt particulier pour l'État algérien, qui accorde une attention croissante à la protection des infrastructures numériques du pays.

1.2. L’objectif de la recherche

Notre objectif est de présenter une approche pour développer une stratégie proactive de sécurité des systèmes d'information, en nous appuyant sur le modèle PDCA. Ce modèle, également connu sous le nom de cycle d'amélioration continue, offre un cadre méthodologique efficace pour concevoir, mettre en œuvre, surveiller et ajuster les initiatives de sécurité. En intégrant le modèle PDCA dans le processus de développement de la stratégie de sécurité, nous visons à proposer une démarche systématique et itérative pour renforcer leur posture de sécurité et répondre aux défis menaces émergentes.

1.3. Problématique

Nous visons à répondre à la question suivante :

“Quelle stratégie proactive l’entreprise peut-elle déployer pour renforcer la sécurité des systèmes d'information ?”

Notre problématique nous pousse à élaborer des sous-questions afin de répondre de manière complète à notre question centrale. Les sous-questions comprennent :

1. Quels sont les objectifs stratégiques généraux de SONATRACH en matière de sécurité SI et comment ces objectifs sont-ils alignés sur la mission et les valeurs de l'entreprise ?
2. Comment SONATRACH évalue-t-elle actuellement les menaces et vulnérabilités potentielles affectant ses SI ?
3. Quels sont les processus décisionnels actuels concernant la sécurité SI chez SONATRACH, et qui sont les principaux acteurs impliqués dans ces processus ?

1.4. Méthode

Pour atteindre l'objectif de notre étude, nous avons choisi une approche méthodologique qualitative descriptive. Nous avons réalisé des entretiens semi-directifs à la Direction Sécurité des Systèmes d’Information (DSSI) de SONATRACH, afin de proposer une méthode pour l’élaboration d’une stratégie proactive visant à renforcer la sécurité des systèmes d’information.

1.5. Pertinence de la recherche

Ce projet nous offre une opportunité précieuse pour approfondir notre compréhension des stratégies proactives de sécurité des systèmes d'information et des meilleures pratiques pour renforcer cette sécurité.

En effet, les développements récents dans le domaine de la technologie de l'information ont accentué la nécessité de mettre en place des mesures de sécurité avancées.

Après avoir mené plusieurs recherches, nous avons constaté l'importance croissante de ces stratégies. De plus, certains enseignants de l'école ont souligné la pertinence de ce thème, ce qui a renforcé notre motivation à l'étudier. Ainsi, en réponse à la demande du chef du département MSSI, nous avons choisi ce sujet, en accord avec les nouvelles orientations stratégiques de la DSSI de SONATRACH.

- **Pertinence théorique :** D'un point de vue théorique, il apparaît que très peu de recherches et d'études ont été menées sur les stratégies proactives de renforcement de la sécurité des systèmes d'information, en particulier au niveau national. Notre étude vise à combler cette lacune en enrichissant la littérature existante sur les approches proactives de sécurité des systèmes d'information.

  D'une part, notre domaine de recherche s'appuie sur une revue de littérature approfondie. D'autre part, les résultats de cette étude pourraient ouvrir de nouveaux horizons pour des recherches futures, car il s'agit d'un domaine encore peu exploré dans notre contexte national.
- **Pertinence managériale :** D'un point de vue managérial, notre étude apportera une aide précieuse aux responsables de la DSSI et aux parties prenantes internes.

  Elle leur fournira des bases solides pour concevoir et mettre en œuvre des stratégies proactives visant à renforcer la sécurité de leurs systèmes d'information.

  En utilisant la méthode proposée et en suivant les bonnes pratiques identifiées, les responsables pourront améliorer la résilience et la sécurité de leurs systèmes d'information.

1.6. Structure de notre étude

Notre étude suit une structure définie, articulée comme suit :

Nous commençons par une introduction qui met en évidence l'intérêt et l'objectif de notre thème, ainsi que la problématique et la méthodologie utilisée dans cette étude.

Ensuite, nous présentons trois chapitres que nous décrivons ci-dessous :

- **Premier chapitre :** Ce chapitre est consacré à la revue de la littérature et au cadre conceptuel. Nous y définissons les concepts clés liés à notre sujet, tels que la sécurité de l'information, la stratégie de cybersécurité, la stratégie de sécurité des systèmes

d'information, la sécurité des systèmes d'information, la politique de sécurité des systèmes d'information et le management de la sécurité des systèmes d'information.

- **Deuxième chapitre :** L'objectif de ce chapitre est de décrire notre méthodologie de recherche ainsi que le contexte organisationnel dans lequel nous avons mené notre étude.
- **Troisième chapitre :** Ce chapitre présente les résultats obtenus sur le terrain, les suggestions, suivis d'une discussion approfondie de ces résultats.

Enfin, nous concluons notre étude en résumant les principaux résultats obtenus, en soulignant leurs implications théoriques et managériales, les perspectives, ainsi qu'en identifiant les limites de cette étude.

CHAPITRE I : CADRE THÉORIQUE

Introduction

Dans ce premier chapitre, nous abordons la partie théorique de notre recherche qui vise à instaurer une stratégie proactive de sécurité des systèmes d'information pour renforcer leur protection et faire face aux vulnérabilités au sein de la DC DCI-DSSI de SONATRACH.

La première section est consacrée à une revue de littérature au cours de laquelle nous avons examiné des articles traitant l'une des variables essentielles de notre étude, à savoir la sécurité de l'information, la stratégie de sécurité des systèmes d'information, la stratégie de cybersécurité et le management de la sécurité des systèmes d'information. Dans la deuxième section, nous nous concentrons sur le cadre conceptuel, où nous présentons les concepts clés de notre sujet pour faciliter la compréhension.

Section01 : Revue de la littérature

La sécurité des systèmes d'information (SSI) représente un enjeu crucial pour les organisations, confrontées à un environnement technologique en constante transformation. La mise en place d'une stratégie de sécurité de l'information (SSI) devient ainsi impérative pour garantir la protection des infrastructures informatiques et la confidentialité des données. Les recherches récentes insistent sur l'importance primordiale du management de la SSI, regroupant un ensemble de pratiques visant à prévenir les cybermenaces et à assurer la résilience des systèmes.

1.1. Sécurité de l'information

La cybersécurité et la conception de systèmes de sécurité de l'information dans les organisations ont été des enjeux cruciaux à l'heure actuelle.

L'évolution des structures organisationnelles a été nécessaire pour répondre efficacement aux défis de l'environnement de sécurité moderne, impliquant une adaptation constante aux nouvelles menaces et la mise en place de mesures proactives pour prévenir la criminalité en ligne.

Il a été essentiel de reconnaître les défis liés à l'expertise dans le domaine de la cybercriminalité. Les acteurs judiciaires ont dû être formés pour utiliser correctement les preuves électroniques et faire face aux complexités des affaires liées à la sécurité de l'information.

Le management de la sécurité de l'information a été un pilier fondamental de toute organisation, impliquant l'identification des informations sensibles, l'élaboration de politiques de sécurité et la mise en place de mesures de protection adéquates pour garantir la confidentialité et l'intégrité des données.

Pour relever ces défis, des propositions concrètes ont émergé. L'éducation continue et la recherche ont été essentielles pour former des professionnels capables d'anticiper les menaces et de les contrer efficacement.

La collaboration entre les acteurs, la sensibilisation du public et l'adoption d'une politique de sécurité intégrée ont été des éléments clés dans la lutte contre la cybercriminalité.

La sécurité de l'information et la cybersécurité ont exigé une approche holistique, combinant des mesures techniques, organisationnelles et humaines.

En favorisant l'éducation, la collaboration et l'adoption de politiques adaptées, les organisations ont pu renforcer leur résilience face aux menaces numériques croissantes. (Grzegorz & Klaudia , 2023).

Dans cette article (Dwi Puji Lestari, Andika Luthfi Citra Tama, Siti Karlina, Achmad Sultan, & Tarwoto, 2024) ont mis en évidence l'importance de la sécurité des systèmes d'information et des facteurs qui l'ont influencée.

Ils ont abordé les aspects tels que la sécurité de l'information, les menaces et attaques cybernétiques, la sécurité physique et la technologie de l'information.

En se focalisant sur ces facteurs, les auteurs ont souligné l'importance de protéger les données sensibles dans l'ère numérique actuelle.

En analysant comment chaque facteur a impacté la sécurité des systèmes d'information, ils ont visé à mieux comprendre ces influences pour créer des politiques de sécurité efficaces.

L'étude de la littérature a exploré l'influence de la sécurité de l'information sur la sécurité des systèmes d'information, l'impact des menaces et attaques cybernétiques, le rôle de la sécurité physique et la pertinence de la technologie de l'information pour renforcer les mesures de sécurité.

En abordant ces facteurs de manière exhaustive, les organisations ont pu optimiser leurs efforts en matière de sécurité pour lutter contre les menaces de sécurité en constante évolution, protéger leurs précieuses informations et assurer la continuité opérationnelle face aux potentielles cyberattaques.

(Zhenkun & Yiyu, 2024), quant à eux, ont examiné la sécurité de l'information pour la transformation numérique de l'industrie de l'exposition et a identifié quatre problèmes principaux rencontrés pendant ce processus : une infrastructure imparfaite, un risque de concordance des données et des informations, des risques dans les formes de gestion industrielle et une asymétrie de la sécurité des informations industrielles.

Ainsi, les chercheurs ont ensuite proposé quatre stratégies pour résoudre ces problèmes de sécurité de l'information : mise en place d'une infrastructure complète, normalisation du degré de concordance des données et des informations, innovation des formes industrielles et construction d'une plateforme de données massives.

De plus, ces stratégies ont visé à réduire les risques liés aux données d'information dans l'industrie de l'exposition, améliorer l'exactitude du traitement des informations industrielles et répondre aux besoins de développement globaux de l'industrie pendant la transformation numérique.

Les chercheurs ont également souligné la nécessité de faire correspondre avec précision les données et les informations, de développer une nouvelle dynamique pour le développement économique et de réguler les informations internes de l'industrie afin de renforcer la sécurité des données d'information. (Zhenkun & Yiyu, 2024)

Par ailleurs, (Fernando S. Meirelles. & Pigola, 2024), ont discuté du thème de la confiance en la technologie de la sécurité de l'information.

Ils ont mis l'accent sur l'importance de faire confiance à la technologie qui facilite la protection des informations sensibles.

Ensuite, ils ont exploré divers aspects de la confiance en la technologie de la sécurité de l'information, tels que la fiabilité des mesures de sécurité, le niveau de confiance dans la sauvegarde des données et l'impact de la confiance sur le comportement des utilisateurs vis-à-vis des protocoles de sécurité.

Ainsi, ils ont souligné l'importance d'établir une confiance dans la technologie pour assurer l'efficacité des mesures de sécurité et la protection des informations précieuses.

Leur recherche a également abordé les implications potentielles du manque de confiance en la technologie de la sécurité de l'information, y compris les risques et les vulnérabilités qui peuvent en découler.

En plus, ils ont visé à mettre en lumière le rôle crucial de la confiance dans le maintien des systèmes d'information sécurisés et l'importance de favoriser la confiance parmi les utilisateurs pour améliorer la posture de sécurité globale. (Fernando S. Meirelles. & Pigola, 2024).

Par ailleurs, (Shabunina , Tur , & Sarancha , 2023) se sont concentrés sur l'analyse du concept américain des menaces liée à la sécurité de l'information et sur la détermination des domaines prioritaires d'activité des États-Unis dans la création d'un cyberespace national sécurisé.

Ils ont utilisé des méthodes de cognition générale et spéciale, telles que l'approche systémique, l'analyse, la synthèse et la méthode logique, ainsi que des méthodes d'analyse de contenu, de surveillance comparative et analytique des ressources Internet des organismes gouvernementaux américains responsables de la sécurité de l'information.

Les menaces à la sécurité nationale des États-Unis sont principalement venues des États et des intermédiaires agissant dans leurs intérêts, dans un contexte de mondialisation des systèmes d'information.

Le concept américain a couvert trois niveaux clés de cybersécurité, à savoir l'État, les entreprises privées et les utilisateurs individuels.

Les priorités de défense pour les États-Unis ont inclus la protection des infrastructures critiques, des réseaux et systèmes d'information, le contrôle de la qualité de l'équipement informatique, la formation de mécanismes de communication inter niveaux efficaces et la sensibilisation à tous les niveaux.

Enfin, les auteurs ont souligné l'importance de la coopération internationale sur les questions de sécurité de l'information.

1.2. Stratégie de cybersécurité

(Azmi, Tibben, & Khin , 2016), ont examiné les motifs derrière le développement des stratégies de cybersécurité nationales, mettant en lumière l'importance de la collaboration internationale, de la protection des infrastructures critiques, de l'intégration de la cybersécurité dans les stratégies nationales de défense et de sécurité, ainsi que des programmes de sensibilisation et de formation en cybersécurité. (Azmi, Tibben, & Khin , 2016)

Dans cette optique, (Cruquenaire, 2022), a souligné l'importance de renforcer la cybersécurité dans le contexte des stratégies européennes, proposant des initiatives telles que le renforcement de l'Agence européenne pour la cybersécurité (ENISA) et la mise en place de schémas européens de certification de cybersécurité. (Cruquenaire, 2022)

(KLAIC, 2015), a proposé une méthode pour le développement des stratégies de cybersécurité nationales, mettant l'accent sur l'harmonisation avec les exigences nationales et internationales, l'évaluation des spécificités sectorielles, l'identification des prérequis organisationnels, l'évaluation de l'environnement des menaces, et l'établissement d'un processus de coordination et de gestion complet. (KLAIC, 2015)

(Chander, 2019), a mis en évidence l'importance cruciale des systèmes d'information dans la société numérique et proposé des stratégies pour protéger ces systèmes contre les

cybermenaces, notamment en renforçant la coordination entre l'académie, l'industrie et le gouvernement, et en proposant des initiatives telles que la création d'un organe central pour coordonner les efforts des différentes agences impliquées dans la cybersécurité. (Chander, 2019)

(Olaru & Maftei, 2021), dans leur étude, ont examiné l'implémentation de management de la sécurité des systèmes d'information et d'une stratégie de cybersécurité en utilisant la méthodologie SCRUM.

Ils ont souligné l'importance de cette approche proactive et adaptable pour renforcer la résilience face aux menaces numériques. (Olaru & Maftei, 2021).

(Judijanto, Rahardian, Muthmainah, & Moh , 2023), ont analysé les stratégies de détection des menaces, les stratégies de prévention et la gestion des risques cybernétiques pour la sécurité des réseaux informatiques gouvernementaux en Indonésie, soulignant l'importance d'une approche proactive et de l'adoption de cadres tels que le NIST Cybersecurity Framework et l'ISO 27001. (Judijanto, Rahardian, Muthmainah, & Moh , 2023)

Enfin, (Senol & Karacuha, 2020), ont offert un cadre systématique pour l'élaboration d'une stratégie nationale de cybersécurité (NCSS), soulignant l'importance du modèle PDCA pour une amélioration continue de la cybersécurité et proposant un organigramme en 8 étapes pour créer et mettre en œuvre ces stratégies. (Senol & Karacuha, 2020)

Ces auteurs ont donc proposé des approches variées mais complémentaires pour élaborer des stratégies de cybersécurité, mettant en avant l'importance de la coordination, de l'évaluation des menaces, de la formation et de la sensibilisation, ainsi que de la mise en œuvre de mesures technologiques et procédurales pour renforcer la sécurité des systèmes d'information.

Tableau 1 : Méthodes proposées et suggestions selon les articles

Article	Méthodes proposées et suggestions
(Azmi & Tibben, 2016) "Motives behind Cyber Security Strategy Development A Literature Review of National Cyber Security Strategy"	• Collaboration internationale, • La protection des infrastructures critiques, • L'intégration de la cybersécurité dans les stratégies nationales de défense et de sécurité, • Des programmes de sensibilisation et de formation en cybersécurité.

(Cruquenaire, 2022) “La cybersécurité, un enjeu à la croisée des stratégies européennes”	• Définir un cadre pour la mise en place de schémas nationaux de certification de cybersécurité des produits et services.
(Klaic, 2016) “A Method for the Development of Cyber Security Strategies”	• La méthode proposée pour élaborer une stratégie de cybersécurité repose sur plusieurs étapes clés : 1. Identification de la portée de la stratégie 2. Sélection des éléments de base de la stratégie 3. Définition des domaines et des interrelations en matière de cybersécurité 4. Corrélation entre la stratégie et le plan d'action de mise en œuvre
(Chander, 2019) “A Case for National Cyber Security Strategy”	• La nécessité d'une coordination entre l'académie, l'industrie et le gouvernement pour développer des technologies de cybersécurité indigènes. • La création d'un organe central pour coordonner les efforts des différentes agences impliquées dans la cybersécurité
(Olaru & Maftei, 2021) “Information Security Management System and Cyber Security Strategy Implementation in the Context of SCRUM”	• La méthode SCRUM • Les suggestions de l'article portent sur l'implémentation d'un système de gestion de la sécurité de l'information (ISMS) et d'une stratégie de cybersécurité en utilisant la méthodologie SCRUM
(Judijanto et al., 2023) “Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia”	• Approche proactive en matière de gestion des risques cybernétiques, en utilisant des cadres tels que le NIST Cybersecurity Framework et l'ISO 27001 pour identifier, évaluer et atténuer les risques de manière proactive. • La mise en place de mesures procédurales telles que des audits de sécurité réguliers, des évaluations de vulnérabilité et une gestion efficace des correctifs pour

	renforcer la sécurité des systèmes d'information gouvernementaux. • L'importance de promouvoir une culture organisationnelle consciente de la cybersécurité et la sécurité SI • L'adoption de cadres de confiance zéro
(Senol & Karacuha, 2020a) "Creating and Implementing an Effective and Deterrent National Cyber Security Strategy"	• Proposition d'un organigramme en 8 étapes pour l'élaboration de la stratégie nationale de cybersécurité (NCSS). • L'utilisation du modèle PDCA (Plan, Do, Check, Act) pour l'amélioration continue de la stratégie de cybersécurité.

Source : élaboré par nous même à partir de la revue de littérature

1.3. Stratégie de sécurité des systèmes d'information

(Klaa, 2022), a mis en lumière les défis de la cybercriminalité et des cyberattaques perpétrées par des États à travers le cyberespace, soulignant également l'importance des stratégies et des outils de cyberdéfense pour garantir la sécurité des systèmes d'information nationaux. Son étude a souligné la complexité croissante des attaques cybernétiques et leur potentiel pour menacer la souveraineté nationale, nécessitant ainsi une stratégie proactive en matière de sécurité des systèmes d'information. (Klaa, 2022)

En réponse à cela, (Guelaa-Drous, 2022), a analysé spécifiquement l'importance de la sécurité des systèmes d'information et de la cybercriminalité en Algérie. Son étude s'est concentrée sur les défis uniques rencontrés par le pays en matière de sécurité SI et a proposé des stratégies sécuritaires et techniques pour contrer la cybercriminalité tout en protégeant la souveraineté nationale. (Guelaa-Drous, 2022)

(Boukers, 2022), a identifié les vecteurs des cyberattaques et a exposé les défis de la sécurité des systèmes d'information, mettant l'accent sur l'organisation de formations de sensibilisation pour renforcer la sécurité au niveau organisationnel et national. Son analyse approfondie des différents types de menaces cybernétiques a offert des perspectives précieuses pour comprendre les failles potentielles dans les systèmes d'information. (Boukers, 2022)

Tout en reconnaissant les menaces croissantes en matière de sécurité des systèmes d'information, (Chaib, 2022), a souligné également la nécessité de protéger ces systèmes et

a mis en évidence l'importance de développer une stratégie nationale de sécurité des systèmes d'information pour relever les défis. Son étude a mis en avant la nécessité d'une coopération internationale pour renforcer la sécurité numérique dans un monde de plus en plus interconnecté. (Chaib, 2022)

(Denden, 2020), a analysé la stratégie de sécurité de l'État algérien face à la cybercriminalité, en proposant des mesures législatives, procédurales et de coopération internationale pour renforcer la sécurité numérique du pays. Son étude approfondie des politiques et des pratiques de sécurité informatique en Algérie a offert des recommandations concrètes pour renforcer la posture de sécurité du pays. (Denden, 2020)

Enfin, (Boughrara, 2018), s'est concentré sur l'analyse de la stratégie de sécurité des systèmes d'information en Algérie et a identifié les défis spécifiques auxquels le pays était confronté. Son étude a mis en évidence les lacunes dans la stratégie de sécurité existante et a proposé des recommandations pour renforcer la résilience du pays face aux menaces numériques, en mettant particulièrement l'accent sur les aspects juridiques et réglementaires. (Boughrara, 2018)

Ces études ont souligné l'importance cruciale de la sécurité des systèmes d'information pour protéger les intérêts nationaux dans un environnement numérique en constante évolution. Elles ont mis en lumière les risques posés par la cybercriminalité et les cyberattaques, émanant aussi bien d'acteurs étatiques que non étatiques, et ont souligné la nécessité de développer des stratégies nationales robustes pour y faire face.

Le renforcement des capacités de défense des systèmes d'information, notamment par le biais de la formation et de la sensibilisation des professionnels de la sécurité, a été identifié comme une priorité.

De plus, les recherches ont mis en avant l'importance de la collaboration internationale pour contrer les menaces numériques et ont souligné la nécessité d'une adaptation continue aux évolutions des technologies et des menaces.

Il a également été recommandé d'améliorer les cadres juridiques et réglementaires pour mieux protéger les infrastructures critiques et de mettre en place des mécanismes de gouvernance efficaces pour assurer une protection adéquate dans le cyberespace.

Malgré cette convergence, les approches méthodologiques varient d'un article à l'autre, certains privilégiant des analyses statistiques tandis que d'autres adoptent des études analytiques ou des discussions conceptuelles. Bien que tous reconnaissent l'importance de la coopération internationale, le niveau de détail sur la manière de la mettre en œuvre diffère. Cependant, des lacunes sont également identifiées dans les recherches.

Premièrement, certains articles pourraient manquer de profondeur dans l'analyse des lacunes juridiques et réglementaires spécifiques en matière de sécurité des systèmes d'information en Algérie.

Deuxièmement, il est souligné un besoin potentiel de recherche plus approfondie sur les menaces spécifiques aux systèmes d'information affectant l'Algérie et sur les réponses adaptées à ces menaces.

Enfin, la coordination entre les acteurs nationaux et internationaux pour renforcer la sécurité des systèmes d'information aurait pu être davantage explorée dans certains articles.

1.4. Management de la sécurité des systèmes d'information selon la norme ISO/IEC27001

Dans le domaine de la sécurité des systèmes d'information, la norme ISO/IEC 27001 a occupé une place prépondérante, comme l'a souligné (Filali, 2020). Son analyse a mis en avant l'impact crucial de cette norme sur l'élévation de la crédibilité des systèmes de gestion de la sécurité des systèmes d'information (SMSI) au sein des organisations. L'étude a mis en lumière l'importance stratégique de l'ISO/IEC 27001 en tant que référence internationale pour établir des pratiques de sécurité solides et fiables. (Filali, 2020)

(Alexei, 2022), s'est penché quant à lui sur l'adoption de l'ISO 27001 dans les organisations publiques de Moldavie. Cette recherche a mis en exergue la nécessité d'aligner les contrôles nationaux avec les normes internationales pour garantir la protection des données et accroître la confiance des partenaires étrangers. (Alexei, 2022)

Dans une étude pratique, (Fotis Kitsios , Elpiniki Chatzidimitriou , & Maria Kamariotou, 2023), ont décrit la stratégie adoptée par une entreprise du secteur des technologies de l'information pour se conformer à la norme ISO 27001. Leur analyse a mis en évidence l'importance de la planification stratégique et de l'engagement de la direction pour renforcer la sécurité des systèmes d'information. (Fotis Kitsios , Elpiniki Chatzidimitriou , & Maria Kamariotou, 2023)

(Sahraoui , Bensedira, & Bouheroud, 2020), exploré quant à eux l'évolution de la diffusion de l'ISO 27001 dans les organisations commerciales, soulignant les défis et les opportunités rencontrés lors de sa mise en œuvre. Cette étude a mis en évidence l'impact de l'ISO 27001 sur les activités commerciales, notamment en termes de compétitivité sur le marché mondial et de confiance des clients. (Sahraoui , Bensedira, & Bouheroud, 2020)

(Ramos Mamami, Cahuaya Ancco, René Llanqui, & Argollo, 2023), ont analysé l'impact de la norme ISO 27001 sur la politique informatique et la gestion de la sécurité des systèmes d'information. Leur étude a souligné l'importance de la conformité à cette norme pour

garantir un niveau satisfaisant de protection des données. (Ramos Mamami, Cahuaya Ancco, René Llanqui, & Argollo, 2023)

Enfin, (Junaid, 2013), a mis en lumière l'importance vitale de l'ISO 27001 dans les systèmes de gestion de la sécurité des systèmes d'information, soulignant son rôle essentiel pour garantir la confidentialité, l'intégrité et la disponibilité des informations. (Junaid, 2013)

L'importance de la norme ISO/IEC 27001 dans le domaine de la sécurité des systèmes d'information est indiscutable.

Cette norme a offert un cadre solide pour établir, mettre en œuvre, maintenir et améliorer un système de management de la sécurité de l'information (MSSI). En adoptant les principes de l'ISO/IEC 27001, les organisations ont pu renforcer la protection de leurs données sensibles, accroître la confiance de leurs partenaires et clients, et se conformer aux exigences réglementaires en matière de sécurité de l'information.

Cependant, la mise en œuvre de l'ISO/IEC 27001 a pu présenter des défis. Les recommandations issues des études sur ce sujet ont été précieuses pour guider les organisations dans leur démarche. Ces recommandations incluent souvent l'importance de l'engagement de la direction, la sensibilisation des employés, la documentation des processus, et la surveillance continue des pratiques de sécurité.

Les méthodologies utilisées pour évaluer et mettre en œuvre l'ISO/IEC 27001 ont varié d'une étude à l'autre. Certaines ont privilégié les approches quantitatives, telles que les analyses statistiques, tandis que d'autres ont adopté des méthodes qualitatives, comme les études de cas ou les entretiens. Le choix de la méthodologie a souvent dépendu des objectifs de recherche et de la nature spécifique de l'organisation étudiée.

Malgré les nombreux avantages de l'ISO/IEC 27001, des lacunes ont également pu être identifiées dans la littérature.

Ces lacunes peuvent concerner la profondeur de l'analyse des risques spécifiques à l'organisation, les défis rencontrés lors de la mise en œuvre de la norme, ou encore les stratégies de gouvernance et de conformité. Identifier ces lacunes a permis d'orienter les futures recherches et de proposer des solutions adaptées aux besoins des organisations.

Section02 : Cadre conceptuel

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent.

Elle n'est plus confinée uniquement au rôle de l'informaticien. La stratégie de sécurité est le premier élément du management de la sécurité des systèmes d'information (MSSI) au sein d'une organisation.

Elle garantit une approche globale, homogène et hiérarchisée de la sécurité du SI. L'idée dans cette partie est de nous interroger sur les enjeux de la sécurité du SI au sein d'une entreprise ainsi que le rôle primordial de la vision stratégique dans la SSI.

2.1. Sécurité des systèmes d'information (SSI)

- **Les systèmes d'information : Clarification conceptuelle**

(R. REIX & F. ROWE, 2002), affirment qu'« un système d'information est un système d'acteurs sociaux qui mémorise et transforme des représentations via des technologies de l'information et des modes opératoires ».

Dans cette définition, le système d'information aide l'acteur à former des représentations et qu'en fait le système ne peut le faire sans l'acteur, le système interface-acteur est le véritable générateur de l'information.

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

(Jacques SORNET, Hengoat OONA, & Nathalie LE GALLO , 2016) : Le système d'information peut se définir par son objectif, qui est d'assurer la saisie, la conservation, le traitement et la circulation des informations, de façon que chacun, dans l'organisation, puisse disposer au bon moment des données dont il a besoin pour remplir sa tâche.

Pour eux, le système d'information répond aux besoins courants, aide aux prises de décision et à la préparation de l'avenir (veille informationnelle, gestion des connaissances).

Parmi les diverses définitions, nous retenons que le SI se définit comme un ensemble complexe de relations structurées impliquant des individus (le personnel), des machines (les ordinateurs), des logiciels et des procédures.

Son objectif principal est de faciliter les opérations de l'entreprise et de fournir des informations pertinentes pour éclairer la prise de décisions.

Après avoir fait un bref rappel sur les systèmes d'information (SI), il est maintenant impératif de discuter de la sécurité des SI. La sécurisation de ces systèmes, en constante évolution, représente un enjeu majeur pour toute organisation moderne.

- **Définition de la sécurité des systèmes d'information**

La sécurité d'un SI est l'ensemble des moyens techniques ou non, de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des équipements et/ou des données traitées ou transmises et des services connexes offerts ou rendus accessibles par le système.

L'on déduit de cette définition qu'il s'agit d'un ensemble de facteurs, qui assurent pour le système d'information, une assurance de Disponibilité, d'Intégrité et de Confidentialité.

Pour (ORTALO, 1988), assurer la sécurité d'un système consiste à garantir le maintien d'un certain nombre de propriétés de sécurité définissant les caractéristiques de confidentialité, d'intégrité et de disponibilité qui doivent être maintenues dans le système.

Ceci implique d'empêcher la réalisation d'opérations illégitimes contribuant à mettre à défaut ces propriétés, mais aussi de garantir la possibilité de réaliser des opérations légitimes dans le système.

D'après (ISO 27002, 2005), la sécurité de l'information est l'état de protection face aux risques identifiés et résultant de l'ensemble des mesures de sécurité prises par une entreprises pour préserver : la confidentialité, l'intégrité et la disponibilité de l'information que détient l'entreprise quel que soit le support (papiers, électronique etc…).

Il ressort de cette définition que la sécurité de l'information est l'ensemble des mesures prises pour faire face aux risques auxquels le système est confronté.

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

En considérant l'ensemble de ces définitions, nous pouvons compléter en affirmant que la SSI englobe un ensemble de mesures (techniques, procédurales, juridiques et humaines) mises en place pour assurer la Disponibilité, l'Intégrité et la Confidentialité du SI.

Ainsi, la sécurité d'un SI peut être vue comme sa non-vulnérabilité aux menaces auxquelles il est soumis, c'est-à-dire l'impossibilité que des attaques induisent des conséquences graves sur l'état du SI ou sur son fonctionnement.

Pour ce faire, trois principaux critères ont été définis qui sont aussi, depuis plus de vingt ans les piliers de la sécurité de l'information (MCLEOD & SCHELL , 2007): il s'agit de la confidentialité, l'intégrité et la disponibilité. Ces critères connus sous l'acronyme anglais de CIA pour Confidentiality Integrity Availability (en français DIC pour Disponibilité Intégrité et Confidentialité) sont d'ailleurs formellement définis par la norme ISO/IEC 13335-1.

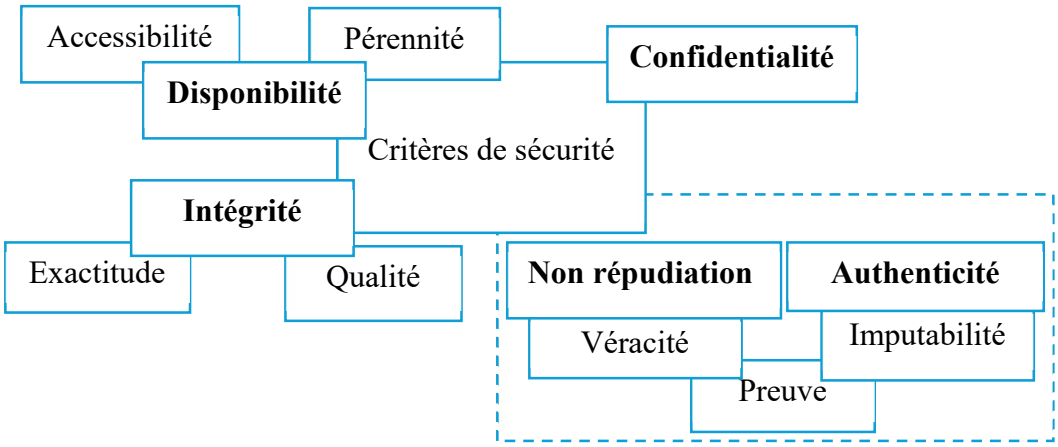
Nous définissons ces critères de base comme suit :

- ✓ **Confidentialité (confidentiality)** : l'information ne doit être divulguée à toute personne, entité ou processus non autorisé. En d'autres termes, la confidentialité garantit qu'une donnée n'est accessible qu'aux seuls utilisateurs autorisés ;
- ✓ **Intégrité (integrity) :** le caractère correct et complet des actifs doit être préservé. En d'autres termes, l'intégrité garantit qu'une donnée n'a subi aucune altération ou destruction, volontaire ou accidentelle, depuis sa création et conserve un format permettant son utilisation. L'intégrité des données comprend généralement quatre aspects l'intégralité, la précision, l'exactitude, l'authenticité et la validité.
- ✓ **Disponibilité (availability) :** l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. En d'autres termes, la disponibilité garantit qu'une ressource du SI est accessible aux utilisateurs autorisés au moment voulu.

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

- ✓ **Authentification (authentification) :** elle consiste à vérifier l'identité d'une entité (utilisateur ou machine) afin d'autoriser son accès à une ressource (système, réseau, application) ;
- ✓ **Non-répudiation (non repudiation)** : elle assure qu'un échange électronique ne peut être remis en cause par l'une des parties, notamment par l'utilisation du certificat numérique ;
- ✓ **Imputabilité (accountability) :** conjuguant authentification et non-répudiation, elle permet de faire porter la responsabilité d'une action à un utilisateur. Ce critère prend une place grandissante avec l'expansion du commerce électronique, notamment avec la signature électronique ;
- ✓ **Traçabilité (traceability) :** elle garantit que les accès et tentatives d'accès aux ressources du SI sont tracés, que ces traces sont conservées et exploitables.

Figure 1: Critères de sécurité



Source : élaboré par nous-même d'après (Ghernaouti, 2016)

Après avoir examiné la sécurité des systèmes d'information (SSI), il est maintenant approprié de nous interroger sur les raisons pour lesquelles il est essentiel de sécuriser son SI.

2.2. Enjeux de la sécurité des systèmes d'information

Intrusions, vols d'informations, déni de service, attaque virale, chantage au cryptage de données… la liste des cybermenaces semble s'allonger sans fin ces dernières années.

Ainsi, pour une entreprise connectée à internet, le problème n'est pas de savoir si on va se faire attaquer mais quand cela va arriver.

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

- **Enjeux stratégiques et organisationnels**

On dit le plus souvent que l 'information c'est le pouvoir. On ne peut décider sans avoir l'information à temps.

Pour une entreprise, les dirigeants doivent s'appuyer sur un certain nombre d'indicateurs issus du système d'information pour les analyser (la finesse et la pertinence de ces indicateurs est primordiale), examiner les solutions possibles aux problèmes identifiés, choisir en envisageant les conséquences de chaque solution, et enfin décider d'une solution.

Pour se faire, le SI doit répondre aux critères de sécurité évoqués plus haut. Pour une meilleure gouvernance des risques, il est essentiel que la sécurité du SI s'aligne sur la stratégie générale de l'entreprise, au même titre que le marketing, la finance ou encore la recherche & le développement.

Outre cela, ce qui a toujours permis aux entreprises les plus compétitives de nos jours d'atteindre leurs objectifs et ainsi de l'emporter sur leurs rivales (avantage concurrentiel) est bien leur SI qui devient dès lors un outil précieux, irremplaçable, en un mot vital.

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

2.3. Le management de la sécurité des systèmes d'information

Le management de la sécurité s'intègre généralement dans un cadre de gouvernance de la sécurité, dirigé par l'entité responsable de la sécurité. Cette situation nécessite une approche pluridisciplinaire de cette entité, comprenant notamment :

- La formalisation et le suivi de la mise en œuvre de la Politique de Sécurité.
- Les interactions avec les acteurs métiers, l'évaluation de leurs risques et le soutien sécuritaire pour leurs projets informatiques.
- La gestion du Plan de Continuité d'Activité (PCA).
- Les initiatives de sensibilisation et de communication.
- La supervision stratégique et budgétaire des plans d'actions sécuritaires.
- La conformité aux exigences légales.

La mise en place d'une organisation de gestion de la sécurité permet de structurer une démarche méthodologique visant à maintenir un niveau de sécurité souvent laissé jusque-là à un stade préliminaire.

Le management de la sécurité s'articule autour de quatre missions principales :

- **Études et standards de sécurité :** Cette mission vise principalement à rédiger la politique de sécurité ou le Plan de Continuité d'Activité (PCA), puis à les intégrer dans les processus opérationnels. Elle transforme ainsi les concepts et les directives en actions concrètes sur le système d'information, couvrant à la fois les impératifs de prévention et de défense.
- **Contrôle de la sécurité :** Cette étape regroupe toutes les actions permettant d'évaluer le niveau de sécurité de tout ou partie du système d'information : identification exhaustive des menaces, évaluation de l'efficacité des mesures de protection, suivi des procédures correctrices pour se conformer aux normes. Elle vise à maîtriser les risques.
- **Administration de la sécurité :** Cette fonction englobe les actions visant à mettre en œuvre, surveiller et appliquer les règles de sécurité aux systèmes d'information. Elle couvre les aspects techniques des objectifs de prévention, de défense et de détection. Les actions de configuration maintiennent les composants du système à un niveau optimal

de sécurité, tandis que la supervision permet de détecter les événements anormaux et d'initier les actions correctives.

- **Pilotage de la sécurité :** Cette mission englobe tous les objectifs de sécurité et joue un rôle central dans le dispositif de gestion de la sécurité. Elle assure la coordination et l'homogénéité des actions de sécurité au quotidien, de manière proactive et réactive (veille de sécurité, solutions réactives). Elle permet de surveiller le niveau de sécurité interne et externe, de fournir des rapports et des tableaux de bord, et de répondre efficacement aux nouvelles menaces en cas de crise.

Ces diverses fonctions s'appliquent à toutes les composantes du Système d'Information (SI), et chacune d'entre elles joue un rôle essentiel dans la gestion de sa sécurité. Cependant, nous examinerons de manière approfondie la première fonction, qui consiste à définir une politique de sécurité.

2.4. Politique de sécurité des systèmes d'information (PSSI)

2.4.1. Définition de la politique de sécurité des systèmes d'information

(ANSSI, 2004), définissait la politique de sécurité d'un système d'information (qu'on abrègera par la suite par l'acronyme PSSI, comme étant « l'ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du système d'information de l'organisme » (ANSSI, 2004). Cette définition synthétique de la Politique de Sécurité des Systèmes d'Information (PSSI) met en lumière son caractère organisationnel et stratégique plutôt que purement technique.

Elle ne se réduit pas à une simple liste de mesures techniques, mais englobe les aspects organisationnels et stratégiques essentiels.

Bien qu'elle intègre des solutions techniques pour résoudre les défis spécifiques rencontrés par l'entreprise ou l'organisation, la PSSI inclut également un ensemble d'obligations, de principes, de règles et de procédures visant à assurer une sécurité optimale des systèmes d'information.

(Jacques, Hengoat OONA, & Nathalie, DCG 8, Systèmes d'information de gestion - Manuel et applications,, 2016): Une politique de sécurité exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Une politique de sécurité concrétise une stratégie sécuritaire et est un outil indispensable à la gouvernance de la sécurité. Elle spécifie les moyens (ressources, procédures, outils, etc.) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité.

La politique de sécurité fait le lien entre la stratégie de sécurité de l'entreprise et la réalisation opérationnelle de la sécurité. L'on déduit qu'une politique de sécurité est une vision stratégique de la maitrise des risques.

L'ANSSI rappelle bien dans ses documentations que la PSSI est un document de stratégie pour l'entreprise. En effet, il s'agit pour elle de définir les orientations stratégiques concernant la sécurité de son système d'information qui, on l'a vu, est désormais prépondérant aujourd'hui dans ses activités.

L'ANSSI précise d'ailleurs un point très important concernant la mise en place d'une telle réflexion.

Selon ces définitions, il apparaît clairement qu'une politique de sécurité constitue le premier pilier de la sécurisation du Système d'Information (SI). C'est pourquoi il est crucial que la direction s'approprie et s'implique dans l'élaboration de ce manuel.

Le document de PSSI d'une entreprise prévoit donc une organisation de la sécurité du système d'information, ou seulement d'une de ses parties.

Effectivement, cela souligne le fait que le support de l'information dans l'entreprise ne se limite pas à un simple rôle de support. Il n'est pas aussi évident qu'il n'y paraît.

À première vue, on pourrait penser que le système d'information est subordonné à l'organisation de l'entreprise et doit la refléter, notamment en ce qui concerne la segmentation des parties du système d'information selon les différents métiers ou directions de l'entreprise. Cependant, lorsque le système d'information influence l'organisation de l'entreprise, cette idée préconçue est remise en question. En réalité, lorsqu'il s'agit de sécuriser notre système d'information, il devient évident que l'organisation initialement envisagée de l'entreprise est susceptible d'être modifiée.

Cette remise en question de l'organisation initialement envisagée de l'entreprise nous pousse à nous interroger sur le rôle et la raison d'être d'une PSSI dans un tel contexte évolutif.

2.4.2. Objectif et finalité de la politique de sécurité des systèmes d'information

Dans le paragraphe précédent, nous avons examiné la Politique de Sécurité des Systèmes d'Information (PSSI) et commencé à envisager ses répercussions.

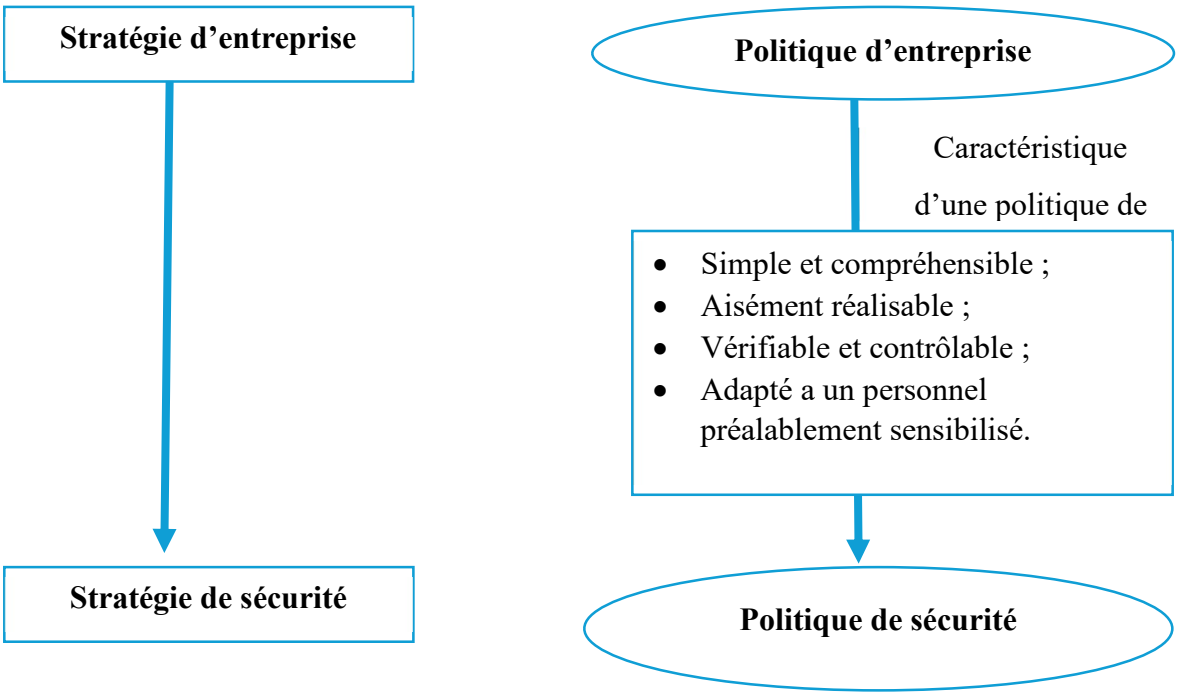
Il est également crucial de se pencher sur sa justification. Pourquoi les entreprises sont-elles encouragées à élaborer un tel document ? Ce document doit évidemment exercer un impact significatif et des conséquences techniques afin d'atteindre l'objectif de sécurisation du système d'information. L'objectif fondamental de la PSSI, qu'elle soit globale ou partielle, est d'assurer la meilleure protection possible des informations qu'elle contient.

Ces données sont vitales pour l'entreprise, et aucune faille ne peut être tolérée, car une intrusion dans le système entraînerait des répercussions potentiellement désastreuses. Les menaces peuvent inclure l'espionnage, l'intelligence économique, le vol de données pour la revente, ou encore la mise en péril de l'existence même de l'entreprise.

Il est cependant important de se rappeler, lors de la rédaction de ce document stratégique qu'est la PSSI, que le risque zéro n'existe pas.

La sécurité d'un système d'information ne sera jamais parfaite, indépendamment de la manière dont la conception et la mise en œuvre de la politique de sécurité ont été réalisées.

Figure 2 : De la politique d'entreprise a la politique de sécurité



Source : élaboré par nous même à partir des définitions

2.4.3. Concepts clés de l'élaboration d'une politique de sécurité des systèmes d'information

Après avoir clarifié le rôle de la politique de sécurité du système d'information en entreprise, examinons maintenant son processus d'élaboration.

Pour une meilleure compréhension de cette démarche, nous allons détailler les concepts clés de la conception de ce document, en mettant l'accent uniquement sur les aspects de la science de gestion plutôt que sur les aspects techniques.

- **Dimensions essentielles pour la politique de sécurité des systèmes d'information**

Tout d'abord, il convient de rappeler les quatre dimensions fondamentales sur lesquelles repose une Politique de Sécurité des Systèmes d'Information (PSSI).

En premier lieu, il y a la dimension juridique. En effet, une PSSI doit nécessairement s'inscrire dans le cadre juridique du pays où elle sera mise en œuvre.

Par exemple, en Algérie, la promulgation de la Loi 18-07 du 10 juin 2018 (Journal officiel n°34 du 10 juin 2018) illustre cette dimension.

De plus, l'installation de l'Autorité Nationale de Protection des Données à Caractère Personnel le 11 août 2022 renforce cette dimension en passant de la consécration de ce droit à sa garantie par cette Autorité.

De même, le Règlement Général sur la Protection des Données (RGPD) entré en vigueur le 25 mai 2018 en Europe met en évidence l'importance de la dimension juridique.

Les entreprises doivent désormais respecter de nouvelles règles concernant la collecte et l'utilisation des données des utilisateurs, ce qui s'applique également aux systèmes d'information.

Ainsi, l'utilisation d'outils pour garantir la sécurité ou surveiller la qualité des systèmes d'information doit se conformer à des lois spécifiques.

Ensuite, une dimension organisationnelle est également cruciale, car la PSSI affectera inévitablement l'organisation de l'entreprise. Cette composante sera abordée plus en détail ultérieurement. Une autre dimension essentielle est la dimension économique.

Les impacts organisationnels de la PSSI peuvent influencer les performances économiques de l'entreprise, soit en augmentant les coûts, soit en prévenant les cyberattaques, apportant ainsi des avantages économiques significatifs. Affecter des ressources humaines à l'élaboration de la PSSI peut réduire les ressources disponibles pour d'autres activités opérationnelles, potentiellement engendrant des pertes.

Cependant, la Direction doit réaliser un arbitrage adéquat pour gérer efficacement ce projet.

Enfin, les dimensions technique et humaine sont également cruciales. La dimension technique intervient rapidement lorsque des concepts et des règles de sécurité sont proposés. Il est essentiel que la politique reste réaliste et évite des actions techniquement irréalisables ou nécessitant un budget exorbitant.

Le facteur humain est déterminant, car il faudra non seulement former les employés et autres intervenants à la politique de sécurité, mais aussi s'assurer qu'ils respectent les règles définies par la PSSI. Pour ce faire, il est nécessaire que les utilisateurs comprennent bien les objectifs et les implications de la politique, et qu'ils perçoivent l'intérêt des règles afin de les respecter. Les utilisateurs ont tendance à adhérer aux règles qui leur ont été expliquées de manière claire et concrète.

Il est donc crucial de donner à la PSSI une signification tangible et compréhensible pour les salariés de l'entreprise.

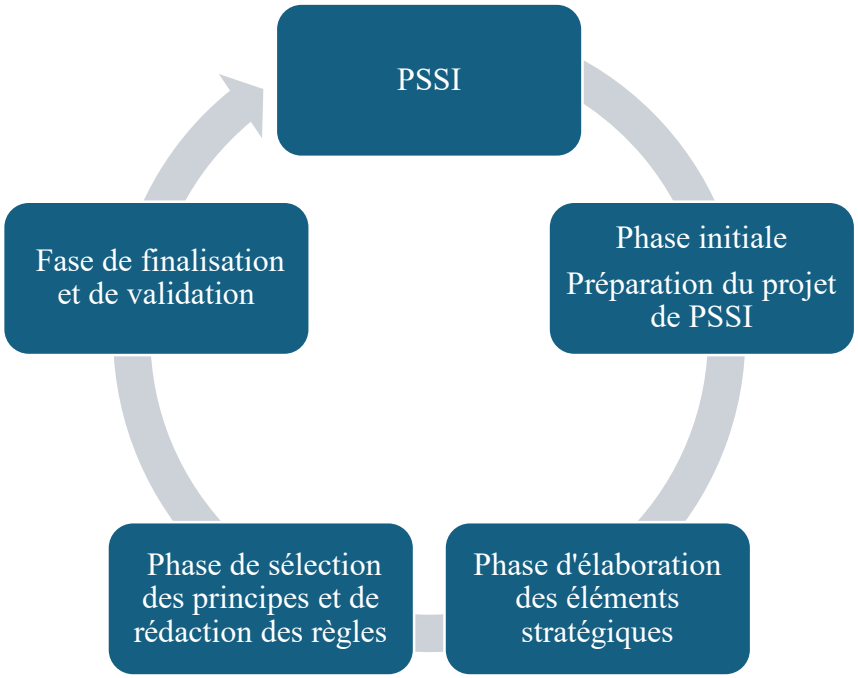
- **Phases de l'élaboration d'une politique de sécurité des systèmes d'information**

L'élaboration de la Politique de Sécurité des Systèmes d'Information (PSSI) se déroule en quatre phases distinctes et interdépendantes.

Chaque phase doit être complètement achevée et validée avant de passer à la suivante, car les éléments utilisés dans chaque phase reposent sur les étapes précédentes. Ainsi, concevoir une PSSI peut être comparé à un exercice en tiroirs, où le succès pour répondre à une question dépend de la réponse correcte à la question précédente.

Cependant, il n'y a pas de bonnes ou mauvaises façons d'aborder chaque étape, et le processus peut être comparé à l'élaboration d'un planning avec des jalons à valider avant de passer à l'étape suivante.

Figure 3 : Les phases de l'élaboration d'une PSSI



Source : Élaboré par nous-même d'après (ANSSI, 2004)

2.4.4. Impacts de la politique de sécurité des systèmes d'information sur le management dans l'entreprise

La PSSI est un document essentiel qui établit des règles visant à mettre en œuvre une stratégie spécifique de sécurité des données, comme mentionné précédemment.

Ces règles guident non seulement les actions techniques à mettre en place au niveau du système d'information lui-même ou du périmètre surveillé par la PSSI, mais elles englobent

également un ensemble de règles plus "comportementales" applicables à chaque utilisateur du système d'information.

Nous allons donc d'abord voir quels sont les impacts concrets en termes de management des collaborateurs, puis l'apport que le management peut constituer pour la sécurité du système d'information.

- **Politique de sécurité des systèmes d'information et management des collaborateurs**

La PSSI a un impact direct sur le management des collaborateurs, en particulier dans les départements SI, qui sont particulièrement sensibles à ce niveau. En effet, les collaborateurs sont tout aussi cruciaux que la technologie elle-même pour garantir la sécurité du système d'information.

L'argument principal en faveur de cette idée est que même si une entreprise dispose des meilleurs équipements techniques et des règles de contrôle d'accès les plus strictes sur ses pares-feux et autres dispositifs, une erreur humaine peut compromettre la sécurité du système d'information, malgré toutes les mesures techniques mises en place.

- **Nécessité du management pour assurer la sécurité des systèmes d'information**

On s'attachera ici à la démonstration de la nécessité du management pour garantir une sécurité suffisante du système d'information.

En effet, et il faut insister sur ce point, on aura pu tout mettre en œuvre pour avoir le meilleur système de protection pour sécuriser le système d'information (on entend par là la sécurisation aussi bien technologique que physique), le facteur humain restera tout de même le maillon faible de la boucle.

La PSSI peut s'appuyer sur des éléments très bien conçus tels que la gestion des mots de passe, la configuration des équipements et des règles qui, pour être déjouées, doivent être contournées de façon extrêmement difficile (cela réduisant par conséquent la surface d'attaque et donc la probabilité d'une compromission de la sécurité du système d'information).

En revanche, si l'humain, qui rappelons Le, est au cœur de ce système, défaille (ce qui n'est malheureusement pas impossible), alors la construction s'écroule, comme pourrait le faire un château de cartes auquel on retirerait la moindre carte le composant.

Le collaborateur définit ses mots de passe qui sont, la plupart du temps, régis par une politique définie dans la PSSI.

Ce collaborateur, par peur d'oublier un mot de passe possiblement long ou fréquemment modifié, peut par exemple l'écrire sur un post-it ou bien l'inscrire dans un cahier ou un classeur Excel.

En revanche, un tiers peut très bien récupérer ce post-it, lire cette page de cahier ou bien entrer en possession de ce fichier Excel.

Il sera alors en possession d'un secret qui lui permettra de réaliser des opérations malintentionnées sur le réseau de l'entreprise. Pourtant, le collaborateur n'a pas enfreint la politique des mots de passe.

Le management devra être attentif à tous ces comportements qui mettent en danger la sécurité du système d'information malgré le fait que les consignes établies par la PSSI sont respectées. Ils sont aussi les personnes privilégiées pour faire remonter des observations du terrain qui peuvent grandement améliorer la PSSI.

Dans cet exemple, le manager ayant été témoin de ce genre de pratiques pourrait les faire remonter à l'équipe projet et ainsi conduire à la mise en place de l'utilisation obligatoire d'un gestionnaire de mots de passe sécurisé (à condition bien sûr de ne pas tomber dans le même travers en notant le mot de passe maître de ce gestionnaire sur une feuille volante ou un post-it).

Un autre élément qui mérite d'être ici souligné est l'importance du management dans la détection des éléments sensibles ou fragiles de leur équipe. En effet, un collaborateur fragile, par exemple en début de risque psychosociaux peut conduire à une faille dans la sécurité du système d'information.

Un autre exemple de collaborateur que l'on peut qualifier de sensible serait un collaborateur important au sein de l'organisation et qui est régulièrement démarché par des concurrents.

Ces collaborateurs peuvent, aussi bien pour l'une ou pour l'autre de ces catégories, représenter un risque pour l'atteinte des objectifs de sécurisation du système d'information. En effet, le premier peut, du fait de sa fragilité, conduire à divulguer à des tiers des informations sensibles qu'il devrait normalement garder pour lui, ou bien être beaucoup plus distrait et donc moins vigilant car préoccupé ou stressé et là encore divulguer des informations sensibles comme des identifiants ou autres.

Pour le second exemple abordé plus avant, les collaborateurs souvent démarchés par les concurrents peuvent se révéler être des sources de renseignements en faisant fuiter volontairement des informations contre une gratification avantageuse, ou en sabotant.

Le management est donc en première ligne pour détecter rapidement ces éléments pouvant venir compromettre la sécurité des systèmes d'information.

En effet, celui-ci est au plus proche du terrain car il peut suivre les collaborateurs et agir rapidement par des entretiens ou une attention plus grande portée à ces cibles faciles pour attaquants et/ou concurrents.

2.5. Normes, référentiels et méthodes pour une meilleure sécurité de l'actif informationnel

Il existe plusieurs normes, référentiels des méthodes qui permettent aux organisations de disposer d'un ensemble de procédures et de règles afin d'assurer une meilleure sécurité de leur actif informationnel. Ils constituent donc, des guides méthodologiques, des moyens pour un management efficace de la sécurité. Ils servent également d'arsenal pour les professionnels de la sécurité des SI.

- **ISO/IEC 27001**

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

- ✓ Définir une politique de la sécurité des informations ;
- ✓ Gérer les risques identifiés ;
- ✓ Choisir et mettre en œuvre les contrôles ;
- ✓ Préparer un SOA (Statement Of Applicability).

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

- **ISO/IEC 27002**

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

- ✓ Chapitre 1 : Politique de sécurité ;
- ✓ Chapitre 2 : Organisation de la sécurité de l'information ;
- ✓ Chapitre 3 : Gestion des biens ; Chapitre 4 : Sécurité liée aux ressources humaines ;
- ✓ Chapitre 5 : Sécurité physique et environnementale ;
- ✓ Chapitre 6 : Gestion des communications et de l'exploitation ;

- ✓ Chapitre 7 : Contrôle d'accès ;
- ✓ Chapitre 8 : Acquisition, développement et maintenance des systèmes d'information ;
- ✓ Chapitre 9 : Gestion des incidents liés à la sécurité de l'information ;
- ✓ Chapitre 10 : Gestion de la continuité d'activité
- ✓ Chapitre 11 : Conformité légale et réglementaire.

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

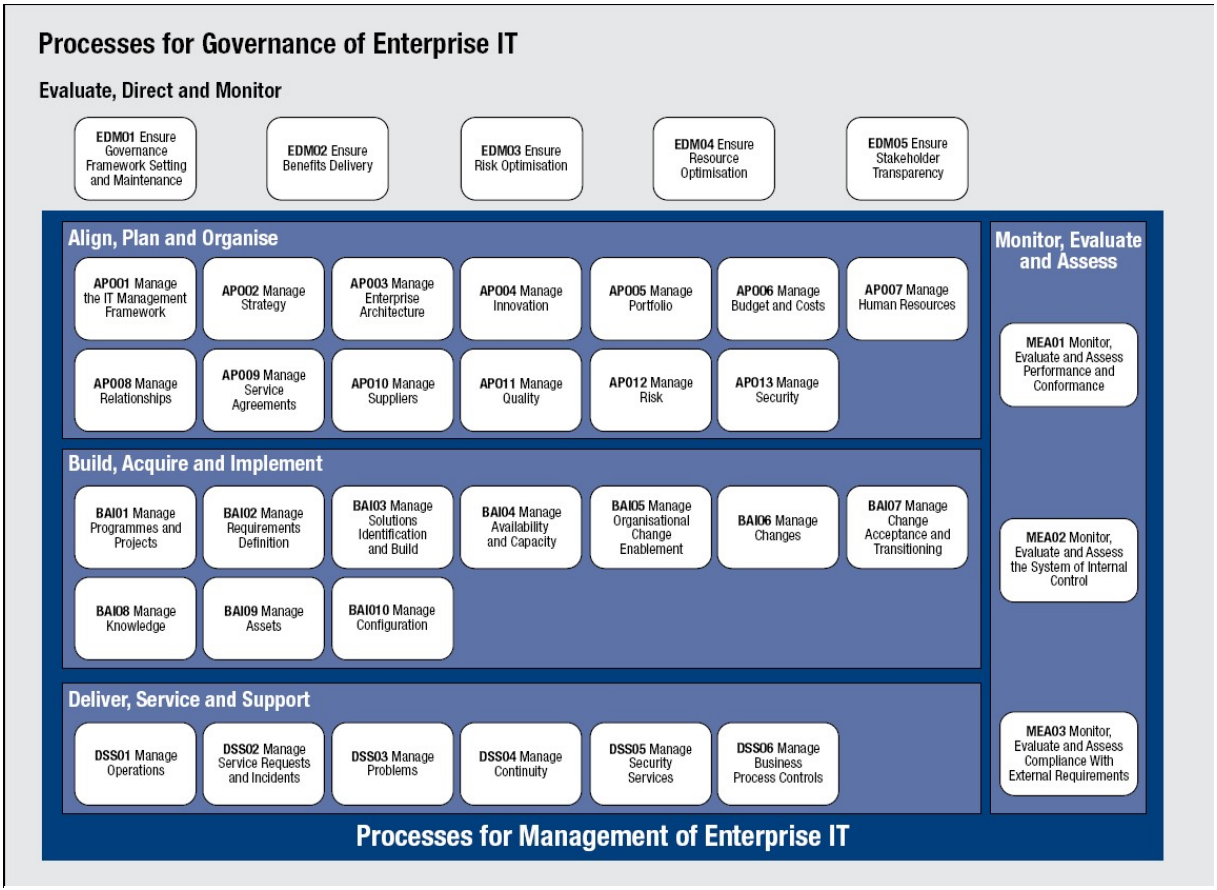
- ✓ La définition du périmètre à protéger (liste des biens sensibles) ;
- ✓ L'identification de la nature des menaces ;
- ✓ L'évaluation de leur impact sur le système d'information ;
- ✓ La détection de mesures de protection à mettre en place pour réduire les impacts.

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

- **Cobit**

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

Figure 4 : Les 37 processus de COBIT5



Source : (BLOGSPOT, 2014)

- **Référentiel National de Sécurité de l'Information (RNSI)**

Le Référentiel National de Sécurité de l'Information (RNSI 2020) vise à fournir un cadre et une série de prérequis pour élaborer et mettre en œuvre la politique de sécurité des systèmes d'information au sein des organismes publics et de leurs entités affiliées.

Les recommandations incluses dans ce document offrent une approche de sécurisation de l'information centrée sur la gestion des risques, en mettant l'accent sur la confidentialité, l'intégrité et la disponibilité des données. Les objectifs du référentiel, perceptibles à travers ses divers domaines, sont les suivants :

- ✓ Renforcer le niveau de sécurité des systèmes d'information et la protection des données des organismes en mettant en place des contrôles de sécurité appropriés ;
- ✓ Adopter une approche basée sur l'évaluation des risques lors de la mise en œuvre des contrôles de sécurité ;
- ✓ Définir les rôles et les responsabilités appropriés en matière de protection des données.

- **MEHARI**

MEHARI (Méthode Harmonisée d'Analyse de Risques) est issue de la fusion de deux méthodes que sont MELISA (Méthode d'évaluation de la vulnérabilité résiduelle des SI) et MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) ((MENTHONNEX, 1995). Elle est la propriété de CLUSIF. Cette méthode apporte des conseils, fait référence à un cadre méthodologique cohérent et fournit un ensemble d'outils et de bases de connaissance sur des domaines spécifiques tels que l'analyses des enjeux, l'étude des vulnérabilités, les scénarii de risques, le pilotage de la sécurité de l'information (Clusif, 2010)

2.6. Concepts clés de la sécurité des systèmes d'information

Il est essentiel de prendre en compte certains concepts fondamentaux pour bien comprendre la sécurité des systèmes d'information, tels que :

- **Risque**

La norme ISO définit le risque dans les termes suivants : « L'effet de l'incertitude sur l'atteinte des objectifs » (ISO/CEI GUIDE 73, 2009). Les risques sont généralement caractérisés par des événements et des conséquences potentielles ou une combinaison de ceux-ci. Elle peut être quantifiée en considérant trois éléments : La menace, la vulnérabilité et l'impact.

En général, le risque en termes de sécurité est caractérisé par l'équation suivante :

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

- **Menace**

C'est la cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation (ISO/CEI 27002, 2022) elle peut avoir plusieurs sources. Les menaces exploitent les vulnérabilités pour déclencher des attaques qui entraînent des risques.

- **Vulnérabilité**

C'est une faiblesse des procédures de sécurité techniques et physiques ou encore d'une absence de protection qui peuvent être exploités par une menace". (CAIRN.INFO, 2019).

- **Impact**

C’est la conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement (EBIOS, 2010).

- **Cybermenace**

(ANSSI, 2023), une cybermenace représente un risque d'attaque visant les systèmes informatiques des infrastructures d'une entreprise, d'un État ou d'une organisation, qu'elle soit privée ou publique, ainsi que de leurs systèmes d'information. Ces menaces peuvent cibler des équipements isolés ou en réseau, connectés ou non, tels que des ordinateurs, des serveurs, des imprimantes, des smartphones, des tablettes ou d'autres appareils. L'objectif d'une cybermenace est de compromettre la sécurité d'un système d'information en altérant sa disponibilité, son intégrité ou sa confidentialité, ainsi que celle des informations qu'il contient. La plupart des attaques informatiques débutent par la prise de contrôle d'un système informatique.

- **Cybersécurité**

“C’est ensemble de technologies et de bonnes pratiques visant à protéger les appareils, les données et les logiciels contre les attaques cybernétiques”. (Boukers, 2022).

- **La gestion des risques**

La gestion des risques se caractérise par un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux spécificités de chaque entreprise, permettant aux dirigeants de maintenir les risques à un niveau acceptable. Cette gestion vise principalement quatre objectifs :

1. Créer et protéger la valeur et les actifs de l'organisation ;
2. Garantir des processus décisionnels et organisationnels propices à l'atteinte des objectifs;
3. Assurer la cohérence des actions et des valeurs organisationnelles ;
4. Mobiliser et organiser les collaborateurs autour d'une vision partagée des risques clés et les sensibiliser aux risques inhérents.

Cependant, l'efficacité de ce dispositif repose sur une politique de gestion des risques clairement définie, qui oriente cette activité et précise les responsabilités des principaux acteurs.

- **Le responsable de la sécurité des systèmes d'information (RSSI)**

Le RSSI est chargé de prévenir les risques dès leur phase de développement, de proposer des plans d'action de réduction et de contrôle des risques, de suivre la mise en place des actions décidées, de rendre compte à la 9 Direction Générale et de communiquer sur la sécurité du SI avec le ou les Directeurs en charge des SI (AMRAE-CLUSIF, 2006).

Cependant, l'efficacité de tout dispositif nécessite une politique de gestion des risques clairement définie, car c'est cette politique qui guide cette activité et définit les responsabilités des principaux acteurs.

- **Culture sécurité des systèmes d'information**

"La culture sécurité des systèmes d'information est l'ensemble des manifestations visibles et invisibles partagées par les membres d'une organisation. Ces manifestations incluent les hypothèses, les croyances, les valeurs, les artefacts et les pratiques formelles et informelles qui influencent les actions et les comportements des utilisateurs concernant la protection du système d'information de l'organisation". (Olfa, 2021).

La culture sécurité des systèmes d'information englobe les attitudes, croyances, valeurs, artefacts et pratiques qui influent sur la protection des données au sein d'une organisation. Elle se manifeste à travers des éléments visibles comme les politiques de sécurité et des éléments invisibles tels que les valeurs partagées. Cette culture influence directement les actions des individus en matière de sécurité.

Une culture sécurité solide renforce la stratégie de sécurité en favorisant la conformité et la résilience, tandis qu'une culture faible peut compromettre les efforts de sécurité. Ainsi, la compréhension et la gestion de la culture sécurité sont essentielles pour garantir le succès de la stratégie de sécurité des systèmes d'information.

2.7. Les stratégies de sécurité contre les menaces et les vulnérabilités

Une stratégie de sécurité est un plan global et structuré destiné à protéger les actifs informationnels et les infrastructures d'une organisation contre diverses menaces et vulnérabilités.

Elle comprend un ensemble de principes, de politiques, de procédures, et de mesures techniques et organisationnelles, mises en place pour prévenir, détecter, et répondre aux incidents de sécurité.

- **Stratégie nationale de cybersécurité (NCSS)**

L'histoire du terme “cyberspace” remonte à plusieurs décennies. Le terme "cyber" est apparu il y a sept décennies (OTTIS & LORENTS, 2010).

(Wiener, 1948), a inventé le terme “cybernétique” pour décrire “les interactions entre les humains (ou les animaux) avec une machine qui peut fournir un environnement alternatif”.

Le terme “cyberspace” a été utilisé pour la première fois au début des années 1980, décrivant “une représentation graphique des données abstraites provenant des banques de chaque ordinateur dans le système humain” (Gibson, 1984) Depuis lors, le terme est entré dans l'usage courant, notamment dans l'étude des systèmes d'information (OTTIS & LORENTS, 2010).

Souvent, les définitions de la cybersécurité et de la sécurité de l'information sont utilisées de manière interchangeable, ce qui peut être le cas dans certains pays (Lujif, Besseling, Spoelstra, & De Graaf , 2013).

Cependant, (Solms & Niekerk, 2013) tentent de clarifier les différences entre les deux. La sécurité de l'information concerne la protection de l'information en tant qu'actif, sous forme physique ou non physique ; tandis que la cybersécurité concerne la protection à la fois des actifs informationnels et non informationnels via l'infrastructure des TIC (Solms & Niekerk, 2013).

D'un point de vue des systèmes d'information, cette distinction apparaît comme trompeuse lorsqu'on considère le travail des professionnels des systèmes d'information.

C'est parce que les actifs informationnels que (Solms & Niekerk, 2013) cherchent à distinguer de l'infrastructure font en réalité partie intégrante de cette infrastructure.

De la même manière, les systèmes d'information peuvent être essentiels au fonctionnement d'une entreprise bancaire, tout comme ils sont fondamentaux pour garantir le bon fonctionnement d'un barrage ou d'une centrale électrique, comme le démontre amplement le ver informatique Stuxnet qui a été utilisé pour perturber le programme nucléaire iranien (Shakarian,, Shakarian , & Ruef, 2013)

Gardant à l'esprit que la distinction que (Solms & Niekerk, 2013) font à une certaine véracité, nous définissons la Stratégie nationale de cybersécurité (NCSS) comme "un plan ou une méthode prudente de protection à la fois des actifs informationnels et non informationnels via l'infrastructure des TIC pour atteindre des objectifs nationaux particuliers généralement sur une longue période. (Lujif, Besseling, Spoelstra, & De Graaf , 2013); (Solms & Niekerk, 2013).

En utilisant cette définition, il est compréhensible que la NCSS cherche à répondre aux objectifs d'une nation qui ont des implications pour son gouvernement, ses entreprises et sa société civile.

La transition de la stratégie nationale de cybersécurité vers une stratégie de cybersécurité au sein d'une organisation témoigne de la reconnaissance croissante de la nécessité de protéger les actifs informationnels et non informationnels à travers les infrastructures des technologies de l'information et de la communication (TIC).

Cela implique un engagement à élaborer des plans détaillés pour anticiper, détecter et répondre aux menaces numériques, tout en assurant la continuité des opérations essentielles.

- **Stratégie de sécurité des systèmes d'information**

Il est important de noter qu'il n'existe pas de définition précise et universelle de la stratégie de sécurité des systèmes d'information.

Cependant, en combinant les perspectives de différents chercheurs et praticiens, nous pouvons déduire que cette stratégie englobe un ensemble d'actions et de mesures visant à garantir la sécurité, la résilience et la protection des systèmes d'information au sein d'une organisation.

La stratégie de sécurité des systèmes d'information peut être définie donc comme un plan d'action exhaustif élaboré pour garantir la sécurité, la résilience et la protection des systèmes d'information au sein d'une organisation.

Cette stratégie englobe à la fois des aspects tactiques immédiats et des considérations à long terme pour assurer la SSI.

Elle repose sur une approche descendante, en établissant des objectifs spécifiques et des protocoles détaillés pour contrer les menaces actuelles, tout en adoptant une vision prospective pour anticiper et prévenir les défis futurs.

La stratégie de sécurité des systèmes d'information vise à établir une ligne de défense robuste, à renforcer la posture de sécurité de l'organisation et à garantir la continuité des opérations dans un environnement cybernétique en constante évolution.

- **Stratégie de cybersécurité**

La cybersécurité est un enjeu primordial dans le monde moderne, nécessitant des stratégies efficaces pour protéger les organisations.

Une stratégie de cybersécurité est définie comme un plan d'action visant à maximiser la sécurité et la résilience d'une organisation, en établissant des objectifs et des protocoles pour garantir la sécurité des systèmes d'information.

De plus, cette stratégie comprend un plan global détaillant les mesures à prendre pour sécuriser les actifs sur une période de trois à cinq ans.

Ainsi, en combinant ces approches, une stratégie de cybersécurité intègre à la fois des protocoles spécifiques et une vision à long terme pour la protection des SI.

- **Étendue d'une stratégie de cybersécurité**

Selon (Klaic, 2015), une stratégie de cybersécurité constitue l'un des piliers fondamentaux pour édifier la dimension virtuelle de la société, conjointement avec d'autres stratégies connexes axées sur des questions telles que la société numérique, l'économie numérique, l'accès et la connectivité, entre autres, (European Comission, 2015).

La plupart des stratégies nationales de cybersécurité, en particulier celles élaborées après 2010, émanent d'une perspective considérant le cyberespace comme une dimension virtuelle de la société, (European Comission, 2015).

Cette vision implique le développement de capacités spécifiques et la coordination de tous les secteurs de la société pour garantir la protection des valeurs fondamentales telles que la liberté, l'équité, la transparence et l'application efficace de la règle de droit au sein de la dimension virtuelle de notre société contemporaine.

Une stratégie de cybersécurité doit détailler les moyens d'atteindre la vision choisie dans la partie de son champ d'action relative aux questions de sécurité dans la dimension virtuelle de la société. Une analyse approfondie a été menée, débouchant sur les lignes directrices suivantes pour définir l'étendue d'une stratégie de cybersécurité. Cinq domaines clés ont été identifiés à cet égard :

- Identification des secteurs/sous-secteurs de la société,
- Évaluation des spécificités sectorielles,
- Identification des conditions préalables organisationnelles,
- Évaluation de l'environnement de menace, et
- Mise en place d'un processus global de coordination et de gestion.

Conclusion

Dans ce chapitre, notre travail s'est articulé en deux sections distinctes. La première partie a été dédiée à une revue de la littérature, examinant les recherches antérieures sur la sécurité de l'information, la stratégie de sécurité des systèmes d'information, la cybersécurité et le management de la sécurité des systèmes d'information.

L'objectif principal était de comprendre en profondeur les concepts clés de ces domaines. Cependant, nous avons noté un manque significatif de recherches spécifiquement axées sur la stratégie de sécurité des systèmes d'information, soulignant ainsi un besoin potentiel de recherches supplémentaires dans ce domaine.

La deuxième section, divisée en deux sous-sections, a abordé le cadre conceptuel, nous permettant de présenter les différents concepts qui seront explorés dans notre pratique. Pour le prochain chapitre, notre attention se portera sur la méthodologie de recherche adoptée pour cette étude, ainsi que sur la présentation détaillée de l'entreprise accueillante.

CHAPITRE II : CADRE MÉTHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

Introduction

Nous allons explorer dans ce chapitre la méthodologie de recherche adoptée pour cette étude, ainsi que le contexte organisationnel de l'organisme d'accueil.

Une explication détaillée de la méthodologie, des outils et des techniques de recherche utilisés pour collecter des données pertinentes sera fournie afin de résoudre le problème de recherche.

De plus, nous fournirons un aperçu de la structure organisationnelle, y compris l'organigramme et les missions de la direction, au sein de laquelle notre stage s'est déroulé, afin de faciliter la réalisation des objectifs de l'étude.

Section 01 : Cadre méthodologique

Cette section donne un aperçu complet de toutes les méthodes, pratiques et outils mis en œuvre dans notre étude.

1.1. Paradigme et démarche de recherche

L'approche globale de cette recherche est fondée sur une démarche inductive, adoptant particulièrement un paradigme constructiviste, qui repose sur l'idée que notre image de la réalité, ou les notions structurant cette image, sont le produit de l'esprit humain en interaction avec cette réalité, et non le reflet exact de la réalité elle-même, selon (BESNIER, 2005, p. 44)

A la suite de cette orientation conceptuelle, entrons désormais dans la dimension pratique en détaillant l'approche méthodologique que nous avons privilégiée pour atteindre nos objectifs de la recherche.

1.2. Approche méthodologique

Notre objectif de recherche consiste à proposer une méthode établie pour élaborer une Stratégie Proactive de Sécurité SI, au sein de la DSSI de SH.

Pour ce faire, nous adopterons une méthodologie qualitative, impliquant la réalisation d'entretiens, d'observations sur le terrain ainsi que la collecte et l'analyse de documents.

Dans la prochaine partie, nous examinerons de près notre méthodologie de collecte de données.

1.3. Méthodes de collecte de données dans la recherche qualitative

D'après (Madjed, 2016), il existe quatre techniques fondamentales pour la collecte de données dans la recherche qualitative : l'entretien individuel, l'entretien de groupe, l'observation et l'analyse documentaire.

Après avoir mené des recherches approfondies et examiné diverses publications concernant la méthodologie de recherche, ainsi qu'échangé à ce sujet avec plusieurs professeurs, nous avons conclu que l'approche qualitative est la plus pertinente pour atteindre nos objectifs et recueillir les informations nécessaires pour répondre à notre problématique.
Cette démarche implique la réalisation d'entretiens avec les responsables de la DC DSI, des observations sur le terrain, ainsi qu'une recherche documentaire approfondie.
Par suite de l'identification des différentes techniques de collecte de données en recherche qualitative, nous examinerons maintenant de manière spécifique la recherche documentaire ainsi que l'observation et l'entretien.

- **La recherche documentaire**

Pour étayer notre étude, nous avons d'abord exploré différentes sources d'informations, telles que les données internes de la DSSI, les sites web institutionnels et les informations disponibles publiquement, et se conformément à la démarche inductive.
Ensuite, nous avons approfondi notre analyse en étudiant les théories contemporaines relatives à la sécurité SI et aux stratégies de sécurité associées.
Notre démarche de recherche a été enrichie par la consultation de diverses ressources, comprenant des ouvrages spécialisés, des thèses accessibles à la bibliothèque de l'École Nationale Supérieure de Management (ENSM), ainsi que des articles académiques disponibles en ligne.
Après avoir étudié ces différentes sources d'informations telles que les données internes de la DSSI et les informations publiques, nous avons décidé d'adopter une approche d'observation directe sur le terrain pour compléter notre recherche.

- **L'observation**

Dans la méthodologie d'observation, le niveau d'implication du chercheur dans les activités des participants varie en fonction du type et de la nature de la recherche. Cette implication peut aller de la participation active à une observation plus distante où le chercheur adopte un rôle de spectateur pendant la collecte d'informations.
Après avoir examiné la technique d'observation, nous aborderons maintenant la phase des entretiens autrement dit entrevues.

1. Observation participante ou le chercheur s'intègre directement dans le groupe ou la communauté qu'il étudie. Il participe aux activités quotidiennes des membres du groupe tout en collectant des données. Cette méthode permet au chercheur d'obtenir

une perspective interne et de mieux comprendre les significations et les dynamiques internes du groupe.

2. L'observation non participante, aussi appelée observation indirecte, ou le chercheur observe le groupe ou la communauté sans y participer directement. Le chercheur reste en retrait et observe les interactions et les comportements sans s'impliquer activement.

Au sein de SONATRACH, nous avons observé que la PSSI ne remplit pas efficacement son rôle stratégique. Cette insuffisance expose l'entreprise à divers risques et menaces qui pourraient entraîner des conséquences graves.

Cette observation a été réalisée à travers l'observation participante, où nous nous sommes immergés dans les activités quotidiennes de l'entreprise pour mieux comprendre les dynamiques internes et les pratiques en place.

Cependant, il a été constaté que la PSSI de SONATRACH est inadéquate et ne parvient pas à répondre efficacement aux besoins de sécurité de l'entreprise.

Cette insuffisance peut résulter de plusieurs facteurs, tels qu'un manque de mise à jour des politiques, des procédures inefficaces ou une formation insuffisante des employés.

De plus, nous avons observé que SONATRACH présente plusieurs vulnérabilités. Par exemple, le manque de suivi régulier des accès des utilisateurs aux systèmes critiques peut permettre à des employés ou des ex-employés d'accéder à des informations sensibles de manière non autorisée.

- **L’entretien**

L'entretien, une méthode largement employée dans la recherche sociale, offre une plateforme pour explorer des sujets sensibles, des expériences individuelles et les perspectives des individus au sein de la société.

En permettant d'explorer en profondeur les pensées, les sentiments et les points de vue des participants, elle contribue à la compréhension des dynamiques sociales.

En forgeant une relation de confiance entre le chercheur et le participant, elle favorise la fiabilité et la précision des données recueillies.

Il existe deux approches principales d'entretien : l'entretien directif et l'entretien semi-directif.

1. L'entretien directif implique une série de questions préétablies, posées de manière uniforme à tous les participants. Le chercheur adopte une neutralité et une objectivité, favorisant des réponses précises et rationnelles.

2. À l'inverse, l'entretien semi-directif est moins structuré, laissant place à des questions ouvertes et approfondies. Le chercheur assume un rôle plus interactif, permettant une exploration plus libre des pensées et des comportements des participants, sans être limité par des hypothèses préconçues.

Nous avons opté pour notre recherche pour l'entretien semi-directif, nous avons préparé un guide d'entretien, adressé aux responsables de la DSSI, le nombre des interviewés était de 5, et la durée moyenne des entretiens était de 30 à 45 minutes, afin de leur permettre d'exprimer leur idée, et d'approfondir chaque question également.

Le guide d'entretien (ANNEXE A) a été structuré en deux principales sections, nous allons présenter et expliquer chaque partie ci-dessous :

Le guide a été initié par une brève introduction dans laquelle nous avons fourni nos informations personnelles (nom, prénom, spécialité) ainsi que le thème de notre étude. Ensuite, l'objectif principal de la recherche a été exposé, suivi d'une assurance aux interviewés quant à l'anonymat de leurs réponses.

Il a également été précisé que les informations recueillies seraient utilisées uniquement à des fins de recherche.

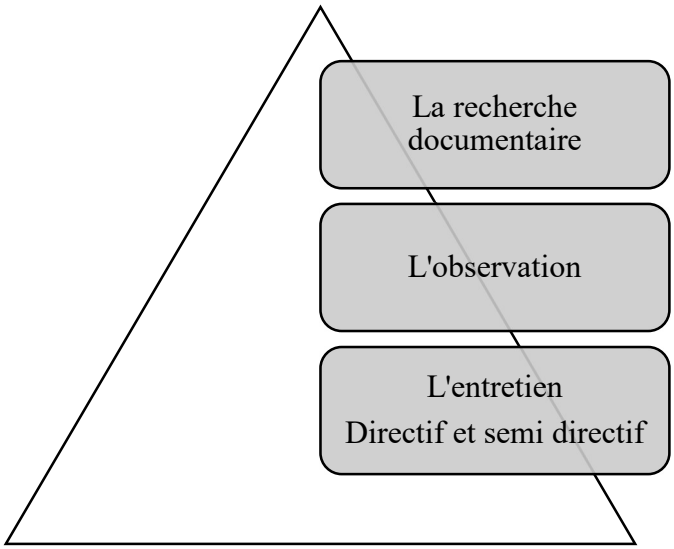
Enfin, des remerciements ont été exprimés aux responsables pour le temps qu'ils nous ont accordé afin de répondre à nos questions.

La seconde partie du guide était dédiée aux questions, qui étaient organisées en différentes rubriques, à savoir :

- Informations sur les interviewés
- Organisation et Responsabilités de la fonction de sécurité des systèmes d'information
- Stratégie et Gestion des Vulnérabilités
- Culture et Sensibilisation à la Sécurité des SI

La triangulation des données, telle que recommandée par les auteurs émanant du courant qualitatif, nous avons permis d'avoir des éléments de réponse à notre problématique.

Figure 5 : Triangulation des méthodes de collectes de données qualitative



Source : élaboré par nous-même d'après (Madjed, 2016)

1.4. Sélection des interviewés

Pour la sélection de nos interviewés, nous avons choisi nos interlocuteurs en fonction de leur grade au sein de la DSSI, ainsi que de leur ancienneté et de leur intérêt pour le sujet.
Ainsi, tous les responsables de la DSSI ont été inclus dans notre échantillon.
Les entretiens ont été réalisés en face à face et enregistrés par téléphone, avec l'accord préalable des interviewés.

Tableau 2 : L'architecture des entretiens

Méthode	Entretiens semi-directifs réalisés face à face
Objet d'analyse	Évaluation des Pratiques et Stratégies Actuelles de Sécurité des Systèmes d'Information
Nombre de cas retenus	5
Public cible	Employés de la DSSI
Nombre d'entretien	5
Date d'entretien	22-26/05/2024
Durée moyenne par entretien	30-45 minutes
Matériaux empiriques	Enregistrement total des entretiens par téléphone portable et google docs
Interviewés	Chef département MSSI Chef département SOSI

	2 ingénieurs en MSSI 1 ingénieurs en SOSI

Source : Élaboré par nous-même

1.5. Déroulement de notre étude empirique

Le tableau ci-dessous présente en détail notre travail :

Tableau 3 : L'organisation de nos pratiques au sein de la DSSI de SH**.**

Phase	Étape	Description
Phase 01	Étape 01 : Observation du terrain	Nous avons mené une observation sur le terrain pour cerner les exigences en sécurité
Phase 02	Étape 01+ 02 : Évaluation et analyse	Nous avons élaboré un guide d'entretiens semi-directifs, puis réalisé un état des lieux à travers des entretiens avec les responsables,
Phase 03	Étape 01 : Proposition d'une méthode d'élaboration d'une stratégie Proactive de Sécurité SI chez SH	Nous avons proposé une méthode structurée pour mettre en place une stratégie proactive de sécurité SI.

Source : élaboré par nous même

Dans cette optique, nous avons également entrepris une analyse approfondie du terrain ainsi qu'une étude documentaire pour cerner précisément les besoins en matière de sécurité de la DSSI.

Nous avons également élaboré un guide d'entretien destiné aux responsables de la DSSI. Les résultats des entretiens ont été présentés et évalués de manière intégrale. L'objectif était d'évaluer les pratiques des responsables ainsi que leur degré de compréhension et de familiarité avec la stratégie de sécurité SI.,

Concernant les personnes interrogées, une diversité a été recherchée, incluant à la fois des femmes et des hommes. Les informations générales sur les personnes interrogées sont résumées dans le tableau ci-dessous :

Tableau 4 : Des renseignements concernant les personnes interrogées

Id interviewés	**Genre**	**Tranche d'âge**	**Poste de travail**	**Durée de l'entretien**	**La date de l'entretien**
A1	Femme	46-55 ans	Chef département MSSI	40 minutes	26/05/2024
A2	Homme	46-55 ans	Chef département SOSI	35 minutes	26/05/2024
A3	Femme	26-35 ans	Ingénieur en sécurité SI	45 minutes	22/05/2024
A4	Homme	26-35 ans	Ingénieur en sécurité SI	40 minutes	22/05/2024
A5	Homme	36-45 ans	Ingénieur en sécurité SI	30 minutes	22/05/2024

Source : élaboré par nous même

Pour analyser les résultats des entretiens, une approche qualitative rigoureuse a été employée, en prenant en considération les réponses fournies par les cinq interviewés désignés respectivement comme A1, A2, A3, A4, et A5.

Chaque réponse a été examinée minutieusement afin d'identifier les thèmes récurrents, ainsi que les discordances et les contradictions éventuelles entre les différents participants. Après une catégorisation par thème, une analyse verticale et horizontale a été réalisée.

Par exemple, lors de l'exploration de l'organisation de la fonction de sécurité des systèmes d'information, les réponses des interviewés ont été comparées afin de mettre en lumière les similitudes et les disparités dans la description de cette organisation.

De même, pour les questions relatives à la stratégie et à la gestion des vulnérabilités, une analyse des réponses a été réalisée pour déceler les convergences et les divergences dans les approches et les pratiques des répondants.

Cette méthodologie qualitative nous a permis d'appréhender les différentes perspectives et pratiques en matière de sécurité SI au sein de SH.

Section 02 : Présentation de l’organisme d’accueil

Notre stage s'est déroulé au sein du département MSSI de la DC DSI de SONATRACH, la Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures. SONATRACH, également connue sous le nom de SH, est la principale entreprise nationale pétrolière et gazière, jouant un rôle prépondérant dans le secteur énergétique du pays. Cette entreprise occupe une place stratégique dans l'économie algérienne en raison de son influence significative sur la production et la distribution des ressources énergétiques.

Parlant désormais de sa contribution essentielle à l’économie nationale.

2.1. SONATRACH : une contribution essentielle à l'économie nationale

Depuis plus de 50 ans, SONATRACH joue un rôle essentiel dans l'économie algérienne en exploitant efficacement les ressources en hydrocarbures du pays.

En tant que l'un des principaux producteurs de pétrole en Afrique, la société a établi des partenariats solides avec des compagnies étrangères pour exploiter les gisements clés du Sahara algérien. Elle dispose également d'un vaste réseau de pipelines s'étendant sur près de 22 000 km, ainsi que de plusieurs ports pétroliers pour faciliter le transport des hydrocarbures à travers le pays.

Outre sa contribution significative à l'industrie pétrolière, SONATRACH participe activement à l'économie nationale en générant des emplois pour les citoyens locaux et en stimulant la croissance économique.

Cependant, la forte dépendance de l'Algérie aux exportations de pétrole et de gaz expose le pays à des risques économiques à long terme.

Pour atténuer cette vulnérabilité, SONATRACH a entrepris des réformes visant à diversifier ses activités et à encourager les investissements dans d'autres secteurs clés de l'économie nationale, tels que l'agriculture et le tourisme.

Remontons brièvement dans le passé pour retracer l'histoire de SONATRACH.

2.2. Bref rappel historique

Depuis les premières années de son existence, d'importants changements ont été réalisés au sein de SONATRACH et dans le secteur des hydrocarbures, comme indiqué dans la figure ci-dessous :

Figure 6 : Dates marquantes de l'histoire de SONATRACH

1963-1967	Création de la société a été officialisée par le décret numéro 63/491, la désignant comme la Société Nationale pour la Recherche, la Production,
1973	La nationalisation des hydrocarbures a placé la SH dans une nouvelle dynamique, marquée par une planification de plus en plus rigoureuse.
1980-1985	Entre 1963 et 1981, la SH est passée d'une entreprise de 33 personnes à une organisation comptant plus de 103 300 employés. Pendant cette période, elle a étendu son domaine d'activité pour englober toute la chaîne
1986-1990	La loi 86/14 du 19 août 1986 a redéfini les cadres juridiques régissant les activités de prospection, d'exploration, de recherche et de transport
1991-1999	La loi 91/01, adoptée en décembre 1991, a apporté des amendements significatifs permettant aux sociétés étrangères, notamment dans le secteur gazier, de récupérer leurs investissements et de bénéficier d'une rémunération équitable pour leurs efforts. Cette évolution a entraîné l'établissement de liens avec plus de 130 compagnies pétrolières, y compris les majors, et la signature de 26 contrats de recherche et de
2014	À la suite de la nomination d'un nouveau PDG, ce dernier a dressé un constat alarmant de la situation actuelle de l'entreprise SH. Parmi les problèmes identifiés, on trouve un organigramme inadapté, l'absence d'une stratégie à long terme et un nombre excessif de filiales. Pour remédier à cette situation, une réorganisation intelligente du groupe est
2018	SH annonce l'acquisition de la raffinerie italienne d'Augusta, ainsi que de trois terminaux pétroliers en Italie. De plus, un accord est signé avec la compagnie pétrolière française Total en vue de la construction d'une

Source : Élaboré par nous-même (Inspiré du site officiel de SH)

2.3. La mission et les objectifs de SONATRACH

1. La mission

Au cours des dernières années, la mission de SONATRACH s'est articulée autour de plusieurs domaines clés, comprenant notamment :

- ✓ Prospection, recherche, exploitation et développement des ressources en hydrocarbures en Algérie, afin de garantir un approvisionnement énergétique durable pour le pays.
- ✓ Transformation, raffinage et commercialisation des hydrocarbures et de leurs dérivés, ainsi que diversification des marchés et des produits à l'exportation.
- ✓ Gestion des réseaux de transport, de stockage et de chargement des hydrocarbures, avec garantie de la sécurité et de la protection des installations pétrolières.
- ✓ Développement et mise en œuvre de programmes de formation continue pour les employés et les cadres, visant à renforcer les compétences et les capacités de l'entreprise.
- ✓ Promotion du développement économique et social de l'Algérie, en contribuant à la création d'emplois, à la formation des jeunes et au développement des infrastructures.

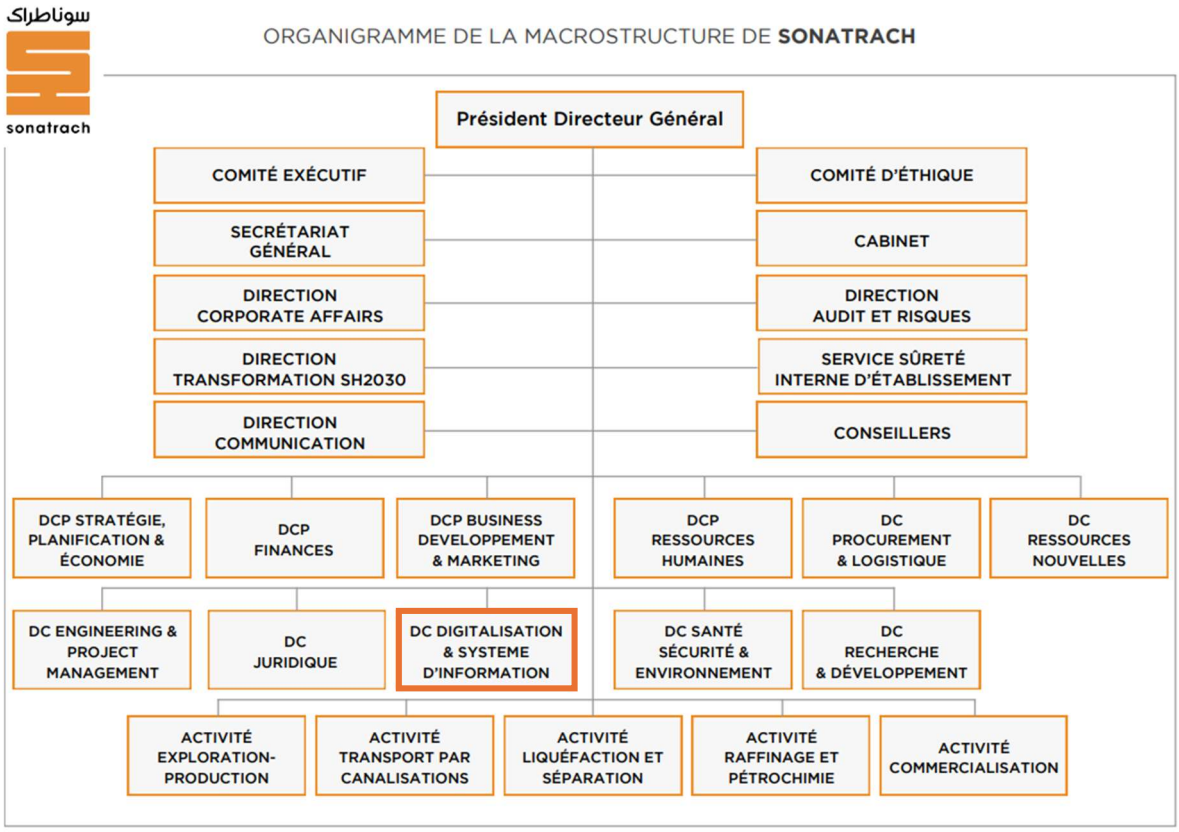
2. Les objectifs

Les objectifs organiques de SONATRACH sont les suivants :

- ➢ Renforcer le rôle de la Direction Générale dans la conception de la stratégie, l'orientation, la coordination, le pilotage et la gestion.
- ➢ Concentrer les structures opérationnelles pour une synergie accrue, tout en garantissant une meilleure efficacité.
- ➢ Favoriser la décentralisation tout en maintenant une maîtrise des pouvoirs et des responsabilités claires, dans le cadre de procédures bien établies et renforçant le contrôle.
- ➢ Assurer la réactivité, la transparence et la fluidité de l'information nécessaire à la conduite et au pilotage des activités, afin d'assurer l'efficacité globale de l'entreprise.

2.4. L'organigramme de la macrostructure de SONATRACH

Figure 7 : Organigramme de la macrostructure de SONATRACH



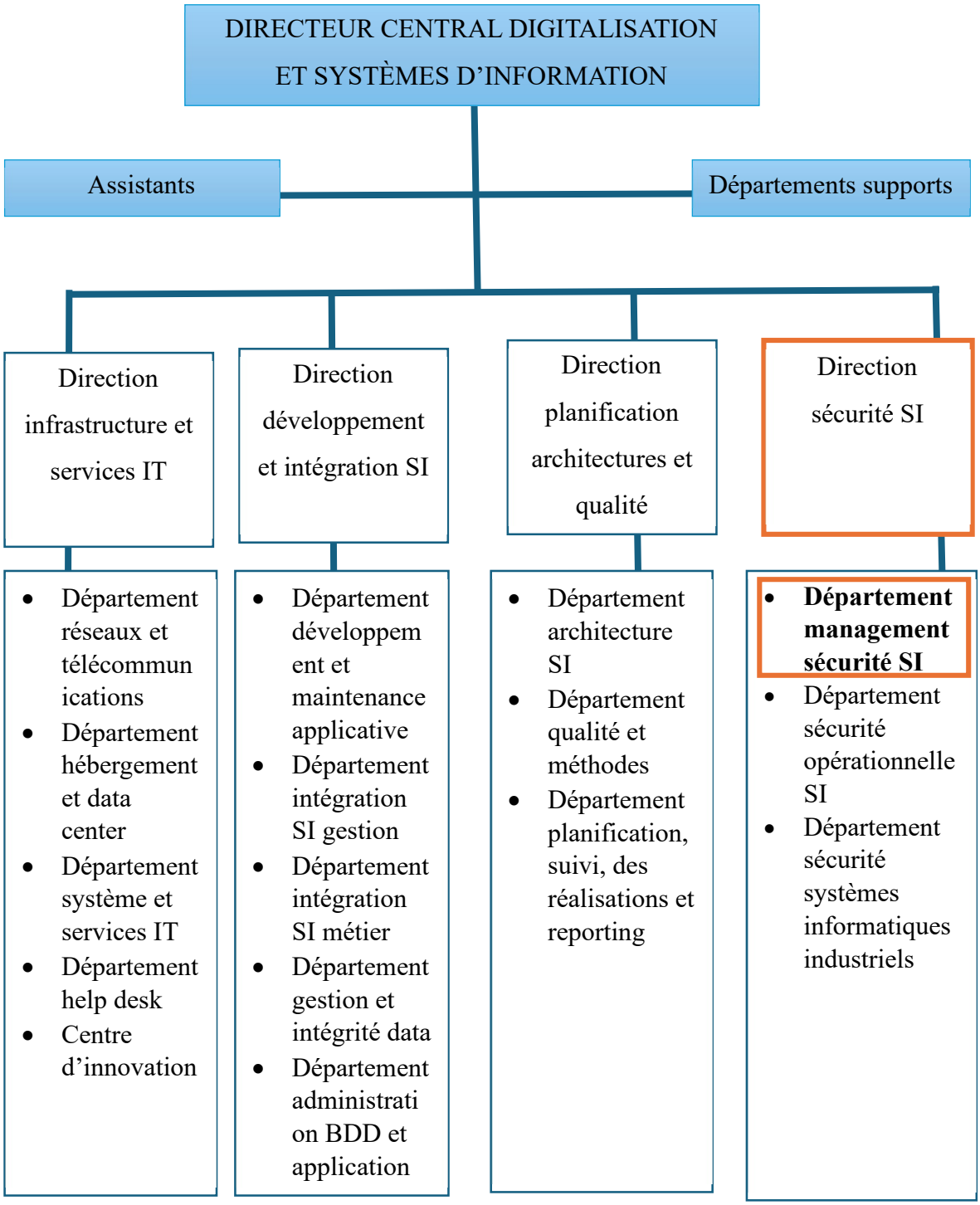
Source : Site officiel de SONATRACH

- **La direction centrale digitalisation et systèmes d'information (DC DSI)**

Le 17 juin 2020, le top management a décidé de réorganiser la Direction Centrale Informatique et Système d'Information, qui sera désormais connue sous le nom de Direction Centrale Digitalisation et Système d'Information (DC DSI). Cette décision établit la structure et les missions de la DC DSI.

La DC DSI est organisée comme suit :

Figure 8 : Organigramme de la DC DSI



Source : élaboré par nous-même e d'après un document interne **(A-1020 (R1))**

Dans le cadre de notre étude, nous nous intéressons à la Direction Sécurité Systèmes d'Information, dont les missions principales sont les suivantes :

- Élaboration et mise en œuvre de la stratégie SSI ;
- Gouvernance de la sécurité des systèmes d'information ;
- Gestion des risques et menaces ;

- Déploiement et supervision des solutions de sécurité ;
- Sensibilisation et liaison avec les instances nationales.

Notre stage s'est déroulé au sein de cette direction, plus précisément au niveau du Département Management Sécurité Systèmes d'Information, dont les missions principales sont les suivantes :

- Élaborer et maintenir la politique de sécurité SI ;
- Contribuer à l'étude et à la mise en place de solutions de sécurité SI ;
- Gérer les risques et menaces de sécurité SI ;
- Sensibiliser aux risques de sécurité SI ;
- Assurer la veille, la réponse et la supervision de la sécurité SI.

Cependant, la DSSI devrait idéalement être indépendante de la DC DSI. En effet, les décisions relatives à la sécurité SI doivent être prises directement par la DSSI pour garantir une réponse rapide et appropriée aux menaces et incidents de sécurité.

Actuellement, cette dépendance structurelle peut entraîner une influence excessive de la DC DSI sur la DSSI, ce qui peut compromettre l'efficacité et l'autonomie des décisions en matière de sécurité.

Une DSSI indépendante permettrait d'assurer une gestion plus robuste et impartiale des risques, ainsi qu'une meilleure adaptation des stratégies de sécurité aux besoins spécifiques de l'entreprise.

De plus, cela favoriserait une responsabilisation accrue au sein de la DSSI, permettant ainsi de renforcer la culture de la sécurité au sein de l'organisation. Cela pourrait également permettre une allocation plus efficace des ressources et une meilleure coordination des initiatives de sécurité à travers l'ensemble de l'entreprise.

Conclusion

Ce chapitre se divise en deux parties. La première se concentre sur la méthodologie de notre étude, où une approche qualitative a été utilisée en conjonction avec des outils spécifiques pour obtenir nos résultats.

La seconde partie traite de la présentation de l'organisme d'accueil. Nous avons d'abord souligné son importance dans l'économie nationale, puis fourni un bref rappel historique pour situer son évolution dans le temps.

Ensuite, nous avons examiné en détail la mission globale de SONATRACH ainsi que ses objectifs spécifiques pour mieux comprendre sa stratégie.

De plus, nous avons étudié l'organigramme détaillé de SONATRACH en mettant en lumière la Direction centrale de la digitalisation et des systèmes d'information (DC DSI). Cette présentation nous a permis de mieux appréhender le contexte organisationnel dans lequel notre étude s'inscrit.

CHAPITRE III : RESULTATS ET DISCUSSION

Introduction

Notre objectif à ce stade est de proposer une méthode de mise en œuvre d'une stratégie proactive pour renforcer la sécurité des systèmes d'information, en nous appuyant sur une revue approfondie de la littérature.

En effet, cette stratégie vise à identifier et à prévenir les vulnérabilités ainsi que les menaces potentielles avant qu'elles ne se manifestent, en utilisant des techniques avancées et des meilleures pratiques reconnues.

Ainsi, nous mettrons l'accent sur les résultats qualitatifs de notre étude. Plus précisément, l'application initiale de cette stratégie sera dirigée vers la DSSI, responsable de la sécurité des systèmes d'information au sein de SONATRACH. En mettant en œuvre cette stratégie, nous visons non seulement à renforcer la SSI contre les cyberattaques, mais aussi à améliorer la détection et la réponse aux incidents, et à assurer une gestion continue des risques liés à la sécurité SI.

Section 01 : Etat des lieux et proposition d'une méthode d'élaboration d'une stratégie proactive de la sécurité des systèmes d'information

Dans cette section, nous analysons la politique de sécurité des SI de la SONATRACH, par la suite, nous proposant une méthode visant à établir une stratégie de sécurité SI en suivant la démarche PDCA (Planifier, Faire, Vérifier, Agir).

1.1. Politique de sécurité des systèmes d'information

Au sein de SONATRACH, nous avons observé que la Politique de Sécurité des Systèmes d'Information (PSSI) ne remplit pas efficacement son rôle stratégique.

Cette insuffisance expose l'entreprise à divers risques et menaces qui pourraient entraîner des conséquences graves.

Cette observation a été réalisée à travers l'observation participante, où nous nous sommes immergés dans les activités quotidiennes de l'entreprise pour mieux comprendre les dynamiques internes et les pratiques en place.

SONATRACH, en tant que compagnie nationale algérienne d'hydrocarbures, joue un rôle crucial dans l'économie du pays par la production et l'exportation de pétrole et de gaz.

La protection de ses systèmes d'information est donc essentielle pour garantir la sécurité des données sensibles, des opérations critiques et des infrastructures.

La PSSI est censée assurer cette protection en définissant des règles et des pratiques pour prévenir les cybermenaces, les accès non autorisés et les pertes de données.

Selon les extraits des entretiens que nous avons réalisés, "la politique de sécurité du système d'information de SONATRACH est élaborée avec une attention particulière à la sécurité des systèmes d'information (SSI).

Chaque politique spécifique par domaine d'activité intègre des mesures de sécurité des SI qui sont alignées sur les meilleures pratiques et les normes de sécurité des systèmes d'information. Ces mesures comprennent la mise en place de contrôles d'accès, la surveillance continue des réseaux, le cryptage des données sensibles, ainsi que des procédures de gestion des incidents de sécurité.

En outre, la PSSI prévoit des missions d'audit régulières spécifiquement dédiées à l'évaluation de la sécurité des SI. Ces audits visent à vérifier la conformité des systèmes, des processus et des pratiques de sécurité avec les normes établies, ainsi qu'à identifier les éventuelles vulnérabilités et les risques pour les systèmes d'information.

En intégrant des mesures de sécurité des SI dans sa politique de sécurité globale, SONATRACH renforce la protection de ses données et de ses infrastructures informatiques contre les cybermenaces.

Cela permet à l'entreprise de garantir la disponibilité, l'intégrité et la confidentialité de ses informations critiques, tout en assurant la continuité de ses opérations dans un environnement numérique en constante évolution.

Cependant, il a été constaté que la PSSI de SONATRACH est inadéquate et ne parvient pas à répondre efficacement aux besoins de sécurité de l'entreprise.

Cette insuffisance peut résulter de plusieurs facteurs, tels qu'un manque de mise à jour des politiques, des procédures inefficaces ou une formation insuffisante des employés.

De plus, nous avons observé que SONATRACH présente plusieurs vulnérabilités. Par exemple, le manque de suivi régulier des accès des utilisateurs aux systèmes critiques peut permettre à des employés ou des ex-employés d'accéder à des informations sensibles de manière non autorisée.

En raison de ces faiblesses, SONATRACH est confrontée à plusieurs risques et menaces : les employés peuvent être victimes de phishing, permettant aux attaquants d'accéder aux systèmes internes.

De plus, des attaques par ransomware peuvent chiffrer les données critiques, exigeant une rançon pour leur restauration.

Des accès non autorisés aux informations sensibles peuvent compromettre la confidentialité des données. Des pratiques faibles de gestion des mots de passe peuvent également permettre des accès non autorisés.

Des attaques par déni de service peuvent perturber les opérations, causant des interruptions dans la production et la distribution.

De plus, une maintenance inadéquate ou une absence de redondance peut entraîner des pannes systèmes affectant les opérations critiques.

L'observation que la PSSI de SONATRACH ne remplit pas bien son rôle stratégique est cruciale car elle révèle des vulnérabilités significatives.

En renforçant la PSSI, SONATRACH pourra mieux protéger ses actifs, ses données et ses opérations contre les risques et menaces croissants, assurant ainsi une continuité et une sécurité optimales de ses activités.

1.2. Analyse des risques

Lors de notre stage chez Sonatrach, nous avons eu l'occasion de mener une observation approfondie sur les types de risques de sécurité auxquels les systèmes d'information de l'entreprise peuvent être confrontés. Cette analyse se base sur nos observations directes et les discussions que nous avons eues avec plusieurs responsables de la sécurité informatique.

Les systèmes d'information de Sonatrach sont particulièrement vulnérables aux cyberattaques, y compris les attaques par phishing, les logiciels malveillants et les attaques par déni de service (DDoS).

Cybercriminels cherchent constamment à infiltrer les systèmes pour voler des informations sensibles ou perturber les opérations. "Nous recevons fréquemment des alertes de tentatives d'intrusion et de phishing. Notre équipe de sécurité doit constamment être vigilante pour prévenir ces attaques," nous a confié un responsable de la sécurité des systèmes d’information.

Les menaces internes représentent également un risque significatif pour Sonatrach. Les employés, qu'ils soient mécontents ou simplement négligents, peuvent causer des dommages considérables, comme le vol de données, l'accès non autorisé à des informations sensibles, ou des erreurs humaines. Un directeur des ressources humaines a mentionné : "L'une de nos plus grandes préoccupations est de s'assurer que nos employés sont bien formés et conscients des politiques de sécurité. Un employé négligent peut involontairement causer des dommages significatifs.

Les pannes de matériel et les défaillances logicielles constituent un autre risque majeur. Une infrastructure défaillante peut entraîner des interruptions de service et des pertes de données critiques. À ce sujet, un ingénieur système senior a expliqué : "Nous devons nous assurer

que notre infrastructure est robuste et redondante pour minimiser les risques de pannes. Les tests réguliers de nos systèmes sont cruciaux.

Sonatrach doit se conformer à diverses réglementations locales et internationales. La non-conformité peut entraîner des sanctions juridiques et financières, ce qui rend la surveillance et l'application des normes réglementaires essentielles. "Nous devons constamment surveiller les mises à jour des réglementations pour nous assurer que nos systèmes sont conformes. Cela inclut des audits réguliers et des mises à jour de notre documentation de conformité," a souligné le responsable de la conformité.

Les risques physiques, tels que les catastrophes naturelles (incendies, inondations) ou les intrusions physiques, peuvent également affecter la sécurité des systèmes d'information de Sonatrach. Pour se prémunir contre ces risques, des mesures de sécurité physique strictes ont été mises en place. Le chef de la sécurité physique a indiqué : "Nous avons mis en place des mesures de sécurité physique rigoureuses, y compris des contrôles d'accès et des systèmes de surveillance, pour protéger nos installations contre les intrusions et les catastrophes naturelles.

L'analyse des risques de sécurité des systèmes d'information de Sonatrach a révélé plusieurs types de menaces potentielles, allant des cyberattaques aux risques internes, en passant par les défaillances techniques, la non-conformité réglementaire, et les risques physiques. Il est impératif pour Sonatrach de maintenir une vigilance constante et de mettre en œuvre des mesures de sécurité robustes pour protéger ses systèmes d'information. Les témoignages des responsables de la sécurité soulignent l'importance d'une approche proactive et intégrée de la gestion des risques.

1.3. Organisation de la direction de sécurité des systèmes d’information

Les résultats des entretiens soulignent une organisation structurée de la fonction de sécurité des systèmes d'information (SSI) au sein de SONATRACH. La Direction Centrale Digitalisation et Système d'Information (DC DSI) abrite la Direction de la Sécurité des Systèmes d'Information (DSSI), directement rattachée au Président Directeur Général.

Cette dernière est composée de trois départements spécialisés : le Management de la Sécurité SI (MSSI), la Sécurité Opérationnelle (SOSI) et la Sécurité des Systèmes Informatiques Industriels (SSII). De plus, chaque direction IT dispose d'un département SSI fonctionnellement lié à la DSSI.

Les principales responsabilités sont réparties entre ces parties prenantes : la DSSI est chargée de la gouvernance de la SSI et de la définition de la stratégie de sécurité de l'entreprise, tandis

que les départements MSSI, SOSI et SSII sont responsables de l'élaboration des politiques, de la gestion des incidents et des vulnérabilités, ainsi que de la sensibilisation à la sécurité. La coordination entre les différents départements est assurée par des réunions, des workshops, et des journées dédiées à la collaboration, facilitant ainsi le partage d'informations et de bonnes pratiques.

En ce qui concerne la communication des incidents de sécurité et des vulnérabilités identifiées, plusieurs canaux sont utilisés, notamment le courriel, le téléphone et un site intranet dédié à la sécurité.

Cependant, certains aspects, tels que la structure hiérarchique et les flux de décision concernant la gestion des vulnérabilités, restent moins clairs.

Enfin, les relations avec les fournisseurs externes ou les partenaires impliqués dans la sécurité des systèmes d'information sont gérées à travers des contrats de service ou d'acquisition de solutions.

Au cours des entretiens, plusieurs personnes ont partagé leurs perspectives sur la manière dont la sécurité des systèmes d'information est gérée chez SONATRACH.

Un responsable de la DSSI a déclaré : Notre objectif principal est de garantir que les systèmes d'information de SONATRACH sont protégés contre les cybermenaces et les risques. Nous travaillons en étroite collaboration avec les différents départements pour assurer une approche globale de la sécurité. Un membre du département MSSI a ajouté : Nous sommes constamment en train d'évaluer les menaces et les vulnérabilités, et de mettre en place des mesures préventives pour les atténuer. La sensibilisation à la sécurité est également une priorité pour nous.

En ce qui concerne les relations avec les fournisseurs externes, un responsable de la DSSI a expliqué : Nous sélectionnons soigneusement nos fournisseurs en fonction de leur capacité à garantir la sécurité de leurs produits ou services. Nous nous assurons également que les contrats établissent clairement les attentes en matière de sécurité.

Ces informations obtenues à travers les entretiens mettent en évidence l'importance accordée à la sécurité des SI chez SONATRACH, avec une répartition claire des responsabilités et des processus établis pour assurer la protection des systèmes d'information de l'entreprise.

1.4. Culture et sensibilisation à la sécurité des systèmes d’information

Les résultats des entretiens révèlent une diversité de pratiques en matière de sensibilisation à la SSI au sein de SH.

Certains participants ont souligné qu'une plateforme de sensibilisation à la sécurité des SSI est en cours de déploiement, illustrant ainsi une initiative proactive visant à renforcer la sensibilisation à la sécurité.

D'autres ont indiqué que des notices et des courriels de sensibilisation sont régulièrement envoyés aux utilisateurs SI via la messagerie professionnelle, permettant ainsi de diffuser des informations sur les bonnes pratiques de sécurité de manière directe et ciblée.

Il a également été noté qu'une règle dans la charte d'utilisation appropriée des SI oblige les utilisateurs à signaler tout incident, démontrant ainsi une volonté d'instaurer une culture de transparence et de responsabilité en matière de sécurité.

Cependant, certains ont relevé l'absence de récompenses ou de reconnaissance pour les pratiques sécuritaires, ce qui pourrait limiter l'engagement des employés envers la sécurité des SSI.

D'autres ont souligné que la résistance est gérée en impliquant la hiérarchie, mettant en évidence l'importance du leadership dans la promotion d'une culture de sécurité.

Enfin, la répétition des notices et des courriels de sensibilisation a été mentionnée comme une pratique régulière, soulignant ainsi l'importance de maintenir une sensibilisation continue à la sécurité.

Ces résultats mettent en lumière la diversité des approches en matière de sensibilisation à la sécurité des SSI, avec des initiatives positives mais aussi des aspects à améliorer pour renforcer la culture de sécurité au sein de l'organisation.

1.5. Stratégie et gestion des vulnérabilités

Les L'analyse de l'existant révèle des perspectives divergentes quant à l'existence d'une stratégie globale de sécurité des systèmes d'information (SSI) au sein de SONATRACH.

Certains répondants ont mentionné l'absence d'une stratégie formelle de sécurité des SI, mettant ainsi en lumière une lacune potentielle dans la gouvernance de la sécurité SI au sein de SONATRACH. Par exemple, un intervenant a déclaré : Nous manquons d'une vision claire et d'une stratégie définie en matière de sécurité des systèmes d'information. Cela rend difficile la prise de décision efficace dans ce domaine.

D'autres ont fait référence à la Politique de Sécurité des Systèmes d'Information (PSSI) de SONATRACH comme étant le document stratégique définissant les orientations et les principes de sécurité pour l'entreprise.

Cela suggère que la PSSI est perçue comme un cadre directeur pour le management de la sécurité des SI, impliquant une stratégie implicite dans son contenu. Un autre participant a

affirmé : La PSSI est notre feuille de route en matière de sécurité des systèmes d'information. Elle définit nos objectifs et nos mesures de sécurité essentielles.

En ce qui concerne les processus d'identification, d'évaluation et de priorisation des vulnérabilités, les réponses indiquent une certaine ambiguïté ou un manque de clarté, ce qui soulève des questions quant à la robustesse des pratiques de gestion des risques au sein de l'organisation. Un répondant a exprimé ses préoccupations : Nous manquons de processus clairs pour identifier et prioriser les vulnérabilités. Cela peut compromettre notre capacité à anticiper et à contrer les menaces potentielles.

La planification à long terme des actions de sécurité des SI semble également être une zone floue, avec des réponses indiquant une absence de processus ou de stratégie clairement définis pour guider les initiatives de sécurité à long terme. Un intervenant a déclaré : Nous avons besoin d'une vision à long terme en matière de sécurité des SI pour garantir une protection efficace de nos actifs informatiques et de nos données sensibles.

Les mécanismes de suivi et d'évaluation de l'efficacité des mesures de sécurité semblent être principalement axés sur des activités d'audit et de contrôle, ce qui reflète une approche réactive plutôt que proactive dans l'évaluation de la performance de la sécurité des SI. Un participant a souligné : Nous devons passer à une approche plus proactive dans l'évaluation de notre posture de sécurité, en mettant en place des mécanismes de suivi continus et des indicateurs de performance clairs.

Enfin, en ce qui concerne la conformité aux normes et réglementations en matière de sécurité des SI, les réponses indiquent que des directives claires sont établies pour se conformer aux exigences légales et réglementaires, avec des audits périodiques pour vérifier la conformité. Un répondant a déclaré : Nous accordons une grande importance à la conformité aux normes de sécurité des SI, ce qui nous permet de maintenir un niveau élevé de protection et de transparence dans nos opérations.

En résumé, ces résultats mettent en évidence des disparités dans la perception et la mise en œuvre de la stratégie proactive de sécurité des SI au sein de SONATRACH, soulignant la nécessité d'une clarification des processus et des orientations stratégiques pour renforcer la gouvernance et l'efficacité de la sécurité informatique dans l'organisation.

1.6. Proposition d'une méthode établie pour élaborer une stratégie proactive de sécurité des systèmes d’information

Après des échanges approfondis avec diverses parties prenantes de SONATRACH, nous avons constaté que l'organisation est confrontée à la nécessité pressante de développer une

stratégie proactive en matière de sécurité des systèmes d'information (SSI). Cette conclusion découle d'une prise de conscience collective de l'importance de disposer d'une vision à long terme pour garantir la protection et la résilience des SI de l'entreprise.

Une stratégie proactive de sécurité des SI permettrait à SONATRACH de prendre des mesures anticipées pour identifier, évaluer et atténuer les risques pesant sur ses SI.

Cela implique non seulement la mise en place de mesures de sécurité robustes, mais aussi une planification stratégique pour faire face aux menaces émergentes et aux évolutions technologiques à long terme.

En outre, une telle stratégie offrirait une orientation claire et cohérente à tous les acteurs impliqués dans la sécurité des SI, en définissant des objectifs à atteindre et des actions à entreprendre pour renforcer la posture de sécurité globale de l'organisation.

L'élaboration d'une stratégie proactive de sécurité des SI nécessiterait une collaboration étroite entre les différentes parties prenantes de SONATRACH, ainsi qu'une analyse approfondie des besoins, des risques et des opportunités spécifiques à l'entreprise.

Elle devrait également être alignée sur les objectifs et les valeurs stratégiques de l'organisation, tout en tenant compte des exigences réglementaires et des meilleures pratiques de l'industrie.

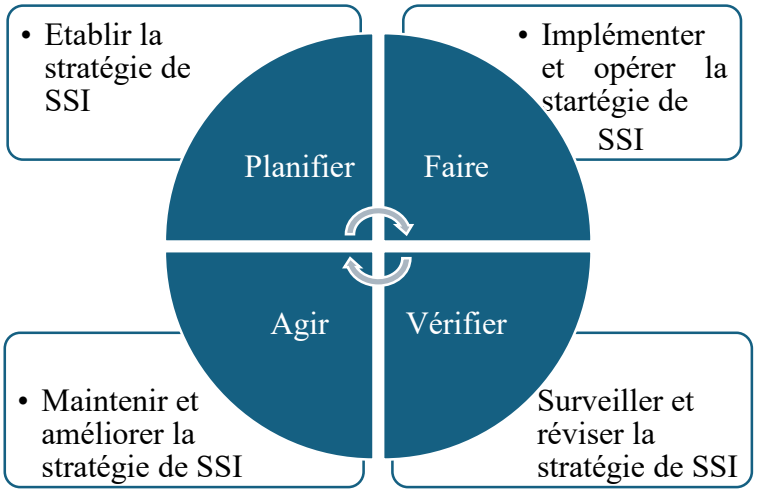
De plus, afin de se conformer aux exigences du Référentiel National de Sécurité des Systèmes d'Information (RNSI), qui requiert spécifiquement l'élaboration d'une stratégie proactive de sécurité, SONATRACH est confronté à une impérative nécessité d'action. Cette directive réglementaire souligne l'importance de mettre en place une approche stratégique anticipative pour faire face aux menaces évolutives et garantir la protection des systèmes d'information de l'entreprise.

Ainsi, l'élaboration d'une stratégie proactive de sécurité des SI devient non seulement une exigence organisationnelle, mais aussi une exigence légale, imposée par les normes et réglementations en vigueur. Cette démarche démontre l'engagement de SONATRACH à se conformer aux normes de sécurité établies, tout en renforçant sa posture de sécurité et sa résilience face aux cybermenaces.

C’est pour cela, que nous proposans une méthode visant à établir une stratégie de sécurité SI en suivant la démarche PDCA (Planifier, Faire, Vérifier, Agir).

Selon les directives de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA, 2012), l'approche PDCA est également utilisée pour élaborer, contrôler et améliorer en continu les stratégies, politiques et processus de cybersécurité.

Figure 9 : Modèle de cycle PDCA et cycle de vie de la stratégie de sécurité SI de l'entreprise



Source : élaboré par nous-même inspirer de (Moen, s.d.), (M. Tekerek, 2008)& (ENISA, 2012)

(ENISA, 2012), affirme que le management d'une stratégie de SSI se décompose en deux étapes principales :

- Développement et mise en œuvre de la stratégie
- Évaluation et maintenance de la stratégie

Par ailleurs, trois approches peuvent être adoptées pour élaborer une stratégie de SSI :

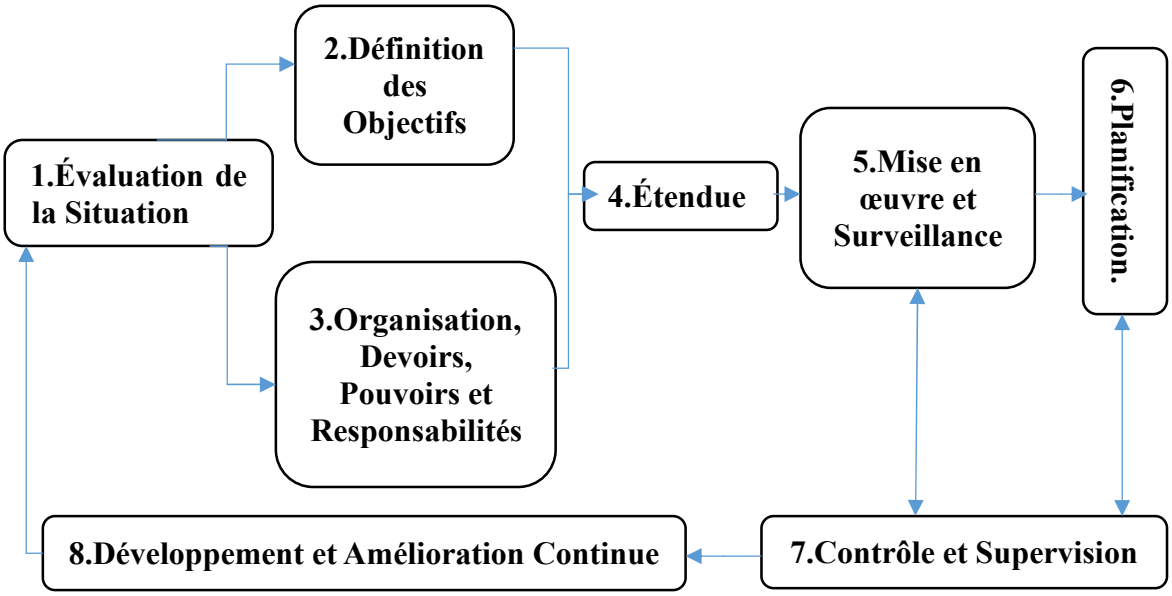
- **Approche linéaire** : la stratégie est développée, mise en œuvre, évaluée, puis finalement arrêtée ou remplacée.
- **Approche du cycle de vie** : les résultats de la phase d'évaluation sont utilisés pour maintenir et ajuster la stratégie elle-même.
- **Approche hybride** : plusieurs cycles d'amélioration continue à différents niveaux peuvent coexister.

La stratégie est développée et mise en œuvre lors des phases 1 et 2 (PD), puis elle est évaluée et maintenue lors des phases 3 et 4 (CA). Ces activités incluent à la fois des évaluations ponctuelles et des évaluations continues et périodiques (voir figure 08).

1.7. Élaboration de de la stratégie proactive de sécurité des systèmes d'information

En nous inspirant des travaux de (Senol & Karacuha, 2020b) voici les 8 étapes d'élaboration de la stratégie proactive de SSI que nous avons proposés à la direction MSSI :

Figure 10 : étapes d'élaboration d'une Stratégie SSI



Source : élaboré par nous-même d'après (Senol & Karacuha, 2020)

✓ **Première Étape : Évaluation de la Situation**

Dans cette phase initiale du processus d'élaboration de la stratégie de sécurité des systèmes d'information chez SONATRACH, nous entreprenons une évaluation approfondie du contexte opérationnel. Cette évaluation, similaire à l'estimation de la situation décrite, vise à déterminer la voie d'action la plus appropriée en examinant tous les paramètres liés au passé, au présent et au futur. Nous analysons les facteurs pertinents pour SONATRACH, en les comparant aux meilleures pratiques nationales et internationales en matière de sécurité SI. Ce processus inclut une étude des politiques, des réglementations en vigueur.

✓ **Deuxième étape : Définition des Objectifs**

Cette étape implique de définir clairement les objectifs de la stratégie de sécurité des systèmes d'information de SONATRACH. Ces objectifs devraient être alignés sur la vision et les valeurs de l'entreprise, tout en prenant en compte les défis spécifiques auxquels elle est confrontée dans son environnement opérationnel. Il est crucial de formuler des objectifs clairs, mesurables et réalisables, qui contribueront à renforcer la résilience et la sécurité SI

contre les menaces émergentes. De plus, ces objectifs devraient être évolutifs, afin de s'adapter aux besoins changeants de l'entreprise.

- ✓ **Troisième étape : Organisation, Devoirs, Pouvoirs et Responsabilités**

Cela implique de mettre en place une structure organisationnelle claire, d'assigner des rôles et des responsabilités précis à chaque entité concernée, de définir les pouvoirs et les autorités nécessaires, et d'établir des mécanismes de coordination et de communication efficaces. En bref, cette étape vise à assurer une gestion efficace de la sécurité SI de SH en garantissant une structure organisationnelle solide et des processus clairs pour tous les acteurs impliqués.

- ✓ **Quatrième étape : Étendue**

Dans cette partie de la stratégie de sécurité SI, tous les niveaux de SONATRACH, doivent être identifiés en spécifiant leurs devoirs et responsabilités de manière générale. La cybersécurité personnelle est principalement la responsabilité de chaque individu, mais SONATRACH a également le devoir de fournir une formation et une sensibilisation sur cette question. En ce qui concerne la sécurité SI de SONATRACH, chaque individu peut avoir des actions et des contributions à apporter. La sécurité des SI et des infrastructures critiques de SONATRACH devrait être une priorité en matière de sécurité SI. À cet égard, les devoirs et responsabilités doivent être déterminés, les principes de contrôle et d'audit ainsi que les sanctions doivent être identifiés, et des plans et réglementations doivent être élaborés à cet effet.

- ✓ **Cinquième étape : Mise en œuvre et Surveillance**

Dans cette phase de l'élaboration de la stratégie proactive de sécurité SI pour SONATRACH, les modalités d'action visant à atteindre les objectifs identifiés lors de l'évaluation des situations et des cibles sont examinées. Afin de mettre en œuvre les décisions prises par suite de ces évaluations, des plans nécessaires sont élaborés et exécutés en collaboration avec les départements de sécurité informatique concernés, ainsi que les institutions publiques et privées sous leur responsabilité et coordination.

Il est essentiel de définir clairement les responsabilités de chaque partie prenante impliquée dans la mise en œuvre de la stratégie. Les rôles doivent être assignés de manière précise à chaque département et individu concerné, ce qui permettra d'assurer une coordination efficace et d'éviter toute confusion. En identifiant les parties prenantes et leurs rôles respectifs, SONATRACH pourra garantir que chaque acteur connaît ses responsabilités et contribue activement à la sécurité des systèmes d'information.

La définition des objectifs et des finalités des actions planifiées est une étape cruciale. Il s'agit de clarifier les raisons et les bénéfices attendus pour chaque tâche et activité. En précisant les objectifs, SONATRACH pourra aligner ses efforts de sécurité sur des résultats concrets et mesurables, ce qui facilitera l'évaluation de l'efficacité des initiatives entreprises. Établir un calendrier détaillé des actions à entreprendre est également fondamental. Ce calendrier doit spécifier les délais et les échéances pour chaque étape du plan, permettant ainsi de suivre les progrès réalisés et d'ajuster les actions en fonction des besoins. Une planification rigoureuse garantit que les activités sont menées en temps opportun et de manière coordonnée.

La détermination des lieux où les actions devront être menées, qu'ils soient physiques ou virtuels, est une autre considération importante. Les infrastructures critiques doivent être prises en compte pour assurer leur sécurisation. En précisant les lieux d'intervention, SONATRACH pourra concentrer ses efforts sur les zones les plus vulnérables et prioritaires. Les méthodes et procédures à utiliser pour atteindre les objectifs doivent être clairement décrites. Cela inclut les outils et technologies à déployer pour assurer la sécurité des systèmes d'information. Une description détaillée des méthodes garantit que les actions sont menées de manière cohérente et efficace.

Enfin, une liste complète des actions spécifiques à réaliser doit être établie. Cela comprend la mise en place de systèmes de réponse aux incidents cybernétiques, la gestion de crise, la collecte de renseignements cybernétiques, et d'autres tâches essentielles. En détaillant ces actions, Sonatrach pourra s'assurer que toutes les mesures nécessaires sont prises pour protéger ses systèmes d'information.

- ✓ **Sixième étape : Évaluation et Réajustement**

L'étape d'évaluation et de réajustement revêt une importance capitale dans le processus d'élaboration de la stratégie proactive de sécurité SI de Sonatrach. Elle implique une analyse méthodique des résultats obtenus après la mise en œuvre des plans, afin d'identifier les écarts éventuels par rapport aux objectifs initiaux et de déterminer les ajustements nécessaires pour optimiser continuellement la stratégie.

Cette évaluation repose sur des critères objectifs et mesurables, incluant les indicateurs de performance définis dans les plans antérieurs. Elle intègre également les retours d'expérience des parties prenantes impliquées dans la mise en œuvre, permettant ainsi de saisir les défis rencontrés sur le terrain et de saisir les opportunités d'amélioration.

À partir de cette analyse, des ajustements sont opérés sur les plans et les stratégies existants. Ces ajustements peuvent comprendre la révision des objectifs, la mise à jour des mesures de sécurité, l'adaptation des procédures aux nouvelles menaces ou aux évolutions de l'environnement opérationnel, ainsi que la réaffectation des ressources si nécessaire.

L'évaluation et le réajustement constituent des processus continus et itératifs, intégrés à la gestion globale de la sécurité des systèmes d'information de Sonatrach. Cette approche garantit la capacité de l'organisation à demeurer agile et résiliente face aux défis changeants du paysage de la cybersécurité.

✓ **Septième étape : Contrôle et Supervision**

Cette phase implique une surveillance systématique, des audits et des rapports sur la mise en œuvre du plan stratégique.

Des activités de contrôle et d'inspection scientifiques doivent être entreprises en se basant sur des données statistiques avancées et des critères prédéfinis. Les résultats de la mise en œuvre du plan doivent être mesurés en les comparant aux objectifs fixés, et la cohérence et la pertinence de ces objectifs doivent être analysées.

Des plans d'actions de contrôle et d'audit internes et externes doivent être aussi élaborés, comprenant des normes et des tâches spécifiques à réaliser. Les activités d'audit doivent être menées de manière impartiale, et les résultats doivent être comparés aux audits précédents pour identifier les progrès réalisés et les domaines nécessitant des améliorations.

✓ **Huitième étape : Développement et Amélioration Continue**

Cette étape marque le point culminant de l'élaboration de la stratégie de sécurité des systèmes d'information de Sonatrach. Elle s'appuie sur les principes du développement continu et itératif, en tirant parti des enseignements des étapes précédentes et en s'engageant dans un processus d'amélioration continue.

Le développement de la stratégie SSI de Sonatrach repose sur une approche proactive, où les plans et les stratégies sont continuellement réévalués et adaptés en fonction des nouvelles informations et des résultats obtenus. Les rapports générés à partir des activités de contrôle et d'inspection fournissent une base solide pour cette réévaluation, en permettant une comparaison entre les résultats prévus et réels.

Cette étape implique une analyse approfondie des écarts entre les activités planifiées et leur mise en œuvre effective. Les erreurs, les lacunes et les points positifs identifiés lors de la mise en pratique sont examinés de manière exhaustive, et des actions correctives sont entreprises pour résoudre les problèmes et intégrer les leçons apprises dans les plans futurs.

Le développement de la stratégie SSI de Sonatrach nécessite la participation active de tous les niveaux de direction et des parties prenantes concernées. Une approche collaborative favorise la diffusion d'une culture de la sécurité et encourage l'innovation dans les pratiques de sécurité. En cultivant cette culture de l'amélioration continue, Sonatrach peut rester à la pointe de la sécurité des systèmes d'information et répondre efficacement aux défis en constante évolution.

Section 02 : Discussion, analyse critique et suggestions

2.1. Discussion

Dans le cadre de notre recherche, nous avons pu identifier plusieurs aspects clés concernant la sécurité des systèmes d'information (SSI) au sein de Sonatrach. En particulier, nous avons relevé un besoin urgent de mettre en place une stratégie proactive de sécurité des SI à long terme.

Cela nous a conduit à proposer une méthode éprouvée pour concevoir une stratégie proactive de sécurité SI en utilisant l'approche PDCA, laquelle est largement reconnue pour son efficacité dans l'élaboration, le contrôle et l'amélioration continue des stratégies de sécurité, comme préconisé par (ENISA, 2012).

Dans cette optique, nous avons opté pour les étapes définies par (Senol & Karacuha, 2020b) dans l'élaboration d'une stratégie proactive de sécurité SI au sein de Sonatrach, car ces dernières s'inspirent également des principes promus par (ENISA, 2012). En adoptant cette approche, nous avons cherché à assurer une démarche méthodique et rigoureuse dans l'élaboration de la stratégie de sécurité SI pour Sonatrach. Cette approche présente l'avantage d'intégrer un processus cyclique de planification, d'exécution, de vérification et d'ajustement, permettant ainsi une adaptation continue aux évolutions technologiques et aux menaces émergentes, et favorisant ainsi la résilience et la robustesse du dispositif de sécurité des SI de Sonatrach.

De manière générale, nous sommes conscients qu'une élaboration réussie d'une stratégie proactive de sécurité SI nécessite une planification préalable et des étapes d'implémentation soigneusement dirigées. Par conséquent nous avons proposé une méthode de son élaboration en tenant compte des renseignements tirés de nos investigations.

2.2. Analyse critique

Au cours de cette phase, nous entreprendrons une analyse des résultats obtenus afin d'identifier les lacunes et les insuffisances. Cette démarche nous permettra ensuite de formuler des propositions visant à remédier aux déficiences relevées.

a) Politique de sécurité des systèmes d'information

L'analyse des réponses des interviewés sur PSSI de Sonatrach révèle plusieurs lacunes significatives. Malgré l'énoncé de directives spécifiques, la PSSI néglige de prendre en compte l'aspect organisationnel et ne satisfait pas complètement à sa fonction de document stratégique, en omettant notamment de traiter des orientations à long terme en matière de

sécurité. De plus, un écart avec les normes officielles établies par l'État algérien est observé, soulignant un manque d'alignement réglementaire.

Bien que des missions d'audit régulier soient prévues, leur exécution effective est déficiente, révélant un décalage entre les dispositions prévues par la politique de sécurité et leur mise en œuvre concrète.

En l'absence d'une PSSI clairement établie comme document stratégique, la gestion des collaborateurs en matière de sécurité des systèmes d'information est compromise, pouvant entraîner un manque de sensibilisation aux responsabilités en matière de sécurité et une application inadéquate des bonnes pratiques.

b) Organisation de la direction de sécurité des systèmes d'information

Les lacunes identifiées dans l'organisation de la Direction de la Sécurité des Systèmes d'Information (DSSI) de Sonatrach comprennent des divergences de perception quant à la clarté des responsabilités attribuées à chaque département, ce qui soulève des préoccupations concernant la confusion potentielle dans la répartition des tâches.

De plus, le fait que la DSSI soit actuellement rattachée à la Direction Centrale des Systèmes d'Information (DC DSI) est considéré comme une configuration non optimale, susceptible d'entraîner des inefficacités dans la gestion et la coordination des activités de sécurité informatique.

En outre, malgré la tenue de réunions et l'utilisation de canaux de communication, des incertitudes persistent quant à l'uniformité et à l'efficacité des pratiques de coordination entre les départements.

Enfin, la diversité des canaux de communication utilisés pour signaler les incidents de sécurité indique un manque de standardisation dans les procédures de signalement, pouvant entraîner des retards dans la détection et la gestion de ces incidents.

c) Culture et sensibilisation à la sécurité des systèmes d'information

Les pratiques de sensibilisation, de signalement des incidents et de partage des bonnes pratiques en matière de sécurité SI au sein de SH présentent plusieurs lacunes.

Une diversité et une incohérence des programmes de sensibilisation et de formation en sécurité SI sont observées, suggérant un besoin d'harmonisation pour instaurer une culture de sécurité cohérente.

De plus, l'universalité du respect des obligations de signalement des incidents reste incertaine, indiquant un défi dans la promotion d'une culture de signalement. Ainsi, la variation des mécanismes de partage des bonnes pratiques révèle un besoin d'approche

structurée pour assurer leur efficacité et favoriser l'apprentissage continu en matière de sécurité SI chez SH.

d) Stratégie et gestion des vulnérabilités

Les lacunes identifiées dans les processus de gestion des vulnérabilités au sein de SH comprennent des incohérences dans l'application des bonnes pratiques et des normes de sécurité, révélant un manque de standardisation et de cohérence dans ces pratiques.

Cette situation soulève des interrogations quant à la fiabilité et à l'efficacité des processus utilisés pour évaluer et classer les vulnérabilités au sein de l'organisation.

De plus, concernant la planification à long terme de la sécurité des systèmes d'information, une absence de stratégie claire est notée, ce qui limite la capacité de Sonatrach à anticiper et à répondre de manière proactive aux menaces de sécurité émergentes.

Cette lacune souligne le besoin d'une approche plus stratégique et proactive dans la gestion des risques liés à la sécurité des systèmes d'information.

Des incohérences sont également observées dans la documentation et le suivi des actions de sécurité.

L'absence d'un plan d'action formel pour suivre les mesures de sécurité compromet la capacité de l'organisation à évaluer et à améliorer de manière continue sa posture de sécurité.

Cette lacune soulève des préoccupations quant à la gestion efficace des risques et à la capacité de Sonatrach à maintenir un niveau de sécurité optimal dans ses opérations informatiques.

2.3. Suggestions

En analysant les résultats obtenus et en les comparant aux théories et aux meilleures pratiques en matière de sécurité SI, il apparaît qu'il existe un écart significatif entre les pratiques actuelles de Sonatrach et les cadres théoriques établis.

Cette divergence indique des faiblesses et des lacunes dans les approches actuelles de gestion de la sécurité des systèmes d'information.

Par conséquent, nous avons élaboré plusieurs propositions visant à renforcer la SSI de Sonatrach.

Ces propositions sont conçues pour aligner les pratiques de l'entreprise avec les principes théoriques, améliorer la résilience contre les menaces de sécurité et garantir une gestion plus efficace des risques associés aux systèmes d'information.

a) Suggestions concernant la politique de sécurité des systèmes d'information

1. Pour remédier à cette situation, il est impératif d'établir une stratégie de SI claire et intégrée dans l'entreprise. Cette stratégie devrait être élaborée en collaboration avec toutes les parties prenantes concernées, en tenant compte des objectifs commerciaux et des exigences réglementaires. Elle devrait également être alignée sur les meilleures pratiques de l'industrie et sur les normes de sécurité internationales ;
2. Il est aussi impératif de mettre en place un processus d'audit régulier. Ces audits doivent être réalisés de manière systématique et impartiale, en mettant l'accent sur la conformité aux politiques de sécurité établies, ainsi que sur la détection et la correction des vulnérabilités potentielles.

b) Suggestions concernant l'organisation de la direction de la sécurité des systèmes d'information

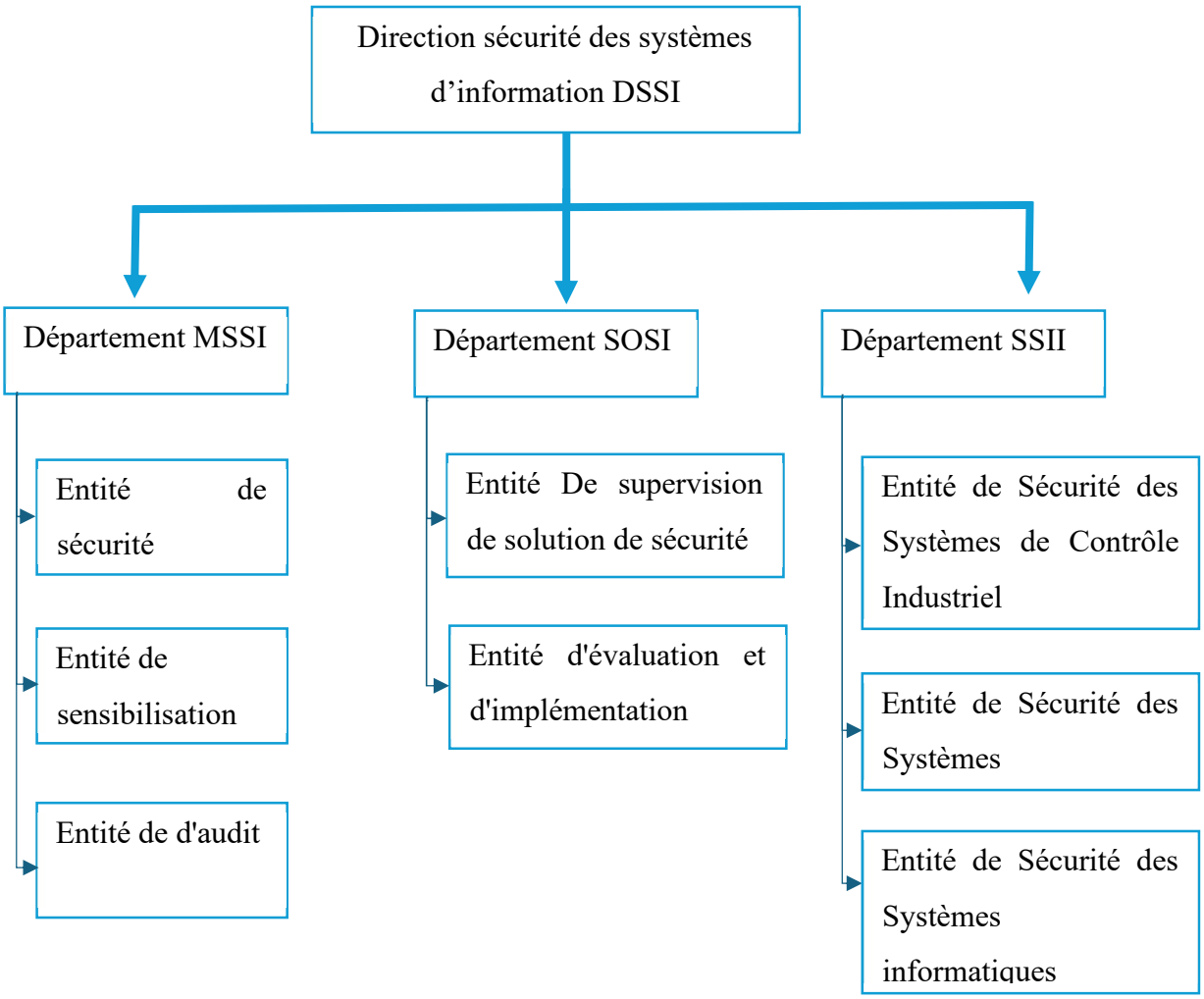
1. Clarifier les responsabilités et les processus de décision ;
2. Renforcer la coordination interdépartementale ;
3. Séparer la DSSI de la DC DSI. En effet, la sécurité SI constitue un domaine stratégique nécessitant une attention particulière et des compétences spécialisées.

   En séparant la DSSI de la DC DSI, Sonatrach peut créer une entité dédiée exclusivement à la sécurité SI, dotée des ressources et des pouvoirs nécessaires pour élaborer et mettre en œuvre des politiques de sécurité robustes, superviser la conformité aux normes et réglementations, et coordonner les initiatives de cybersécurité à travers l'ensemble de l'organisation.

   Cette séparation permet également de clarifier les responsabilités et les chaînes de commandement, favorisant ainsi une prise de décision plus rapide et plus efficace en cas d'incident ou de menace.

   En somme, en dissociant la direction SSI de la DC DSI, Sonatrach renforce sa posture en matière de cybersécurité et renforce sa capacité à faire face aux défis croissants en matière de sécurité SI.

Figure 11 : proposition d'un organigramme de la DSSI détaché de la DC DSI



Source : Proposé par nous même

c) Suggestions concernant la culture et la sensibilisation à la sécurité des systèmes d'information

1. Développer des programmes de sensibilisation et de formation uniformes pour les employés ;
2. Mettre en place des canaux de communication efficaces pour signaler les incidents et partager les bonnes pratiques ;
3. Intégrer la sécurité dans la culture organisationnelle à tous les niveaux ;
4. Réviser et mettre à jour la charte d'utilisation des systèmes d'information pour clarifier les attentes en matière de signalement des incidents ;
5. Organiser des forums de partage de connaissances pour encourager l'échange d'informations et de solutions entre les employés.

d) Propositions concernant la stratégie et gestion des vulnérabilités

1. Standardisation des processus de gestion des vulnérabilités tels que les KPI (indicateurs clés de performance) ;
2. Mise en Place d'un Plan d'Action pour la Documentation et le Suivi des Actions de Sécurité en utilisant les tableaux de bord ;
3. Amélioration de la Coordination et de la Communication Inter-départements ;

Conclusion

Dans ce chapitre, nous avons détaillé la partie pratique de notre étude en présentant les étapes de l'élaboration d'une stratégie de sécurité SI en utilisant l'approche PDCA, les entretiens semi-directifs et les étapes d'élaboration proposées par (Senol & Karacuha, 2020b). L'analyse de ces entretiens nous a permis d'identifier les lacunes et les divergences présentes au sein de la Direction de la Sécurité des Systèmes d'Information de Sonatrach. A la fin, nous avons formulé plusieurs propositions visant à renforcer la sécurité des SI chez Sonatrach, en alignant les pratiques de l'entreprise avec les principes théoriques et en améliorant la résilience contre les menaces de sécurité. Ces recommandations sont conçues pour assurer une gestion plus efficace des risques et pour instaurer une culture de sécurité plus robuste au sein de l'organisation.

CONCLUSION GÉNÉRALE

Notre travail de recherche avait pour objectif principal l'élaboration d'une stratégie proactive de sécurité des systèmes d'information au sein de Sonatrach en utilisant l'approche PDCA. Cette approche, largement reconnue pour son efficacité en matière d'amélioration continue, nous a semblé particulièrement adaptée pour structurer et améliorer les pratiques de sécurité SI. Pour répondre à notre problématique : Quelle stratégie proactive l'entreprise peut-elle déployer pour renforcer la sécurité des systèmes d'information ?

Nous avons mené une étude qualitative à travers des entretiens semi-directifs avec plusieurs responsables au sein de la Direction de la Sécurité des Systèmes d'Information de Sonatrach. Ces entretiens ont permis d'examiner les pratiques actuelles et d'identifier les lacunes et les divergences dans le management de la sécurité des SI. Les questions posées aux responsables ont couvert divers aspects, tels que les processus de gestion des vulnérabilités, la planification stratégique, la documentation des actions de sécurité et les programmes de sensibilisation et de formation.

L'analyse des entretiens nous a révélé plusieurs incohérences dans les processus de gestion des vulnérabilités, la planification stratégique à long terme, et la documentation des actions de sécurité. Les processus d'identification, d'évaluation et de priorisation des vulnérabilités présentent des incohérences, avec un manque de processus formel et standardisé.

En ce qui concerne la planification stratégique à long terme, il y a un manque de vision stratégique cohérente pour la sécurité des SI, mettant en lumière une lacune dans la capacité de Sonatrach à anticiper et répondre aux menaces de sécurité émergentes.

De plus, la documentation et le suivi des actions de sécurité montrent des incohérences dans l'utilisation des politiques et procédures, compromettant potentiellement la capacité de l'organisation à évaluer et à améliorer continuellement sa posture de sécurité.

Pour renforcer la sécurité des SI chez Sonatrach, nous avons proposé plusieurs mesures concrètes.

Il est essentiel de développer des programmes de formation et de sensibilisation uniformes et réguliers pour tous les employés, assurant ainsi une formation continue pour maintenir un haut niveau de sensibilisation aux enjeux de sécurité SI.

La mise en place de protocoles standardisés pour le signalement des incidents de sécurité est également cruciale pour garantir une réponse rapide et efficace.

En adoptant un processus formel et standardisé pour la gestion des vulnérabilités, incluant l'identification, l'évaluation et la priorisation, Sonatrach pourra mieux gérer les risques.

Par ailleurs, il est nécessaire de définir et de communiquer une stratégie de sécurité des SI à long terme, alignée avec les objectifs de l'entreprise, et de veiller à sa mise à jour régulière pour refléter les évolutions des menaces et des technologies.

- **Avantages**

Examiner le champ de la recherche scientifique.

Appliquer les acquis académiques de l'ENSM en passant de la théorie à la pratique.

Confronter les connaissances théoriques avec la réalité professionnelle au sein de l'organisation.

Profiter de l'expertise des cadres supérieurs et apprendre de leur expérience.

Développer des compétences en gestion et présentation des données.

- **Obstacles**

Contraintes temporelles liées à la durée limitée du stage.

La confidentialité des données liées à la SSI.

- **Limites**

Nous avons rencontré quelques difficultés au cours de notre recherche. La sécurité des systèmes d'information est un domaine complexe nécessitant des efforts continus pour son amélioration. La diversité des perceptions et des pratiques au sein de la DSSI a rendu difficile l'identification d'une approche unifiée.

De plus, l'absence d'un cadre de référence bien défini pour certaines pratiques a limité notre capacité à formuler des recommandations exhaustives. De plus les contraintes de temps et la disponibilité limitée des responsables ont restreint la profondeur de notre analyse et la collecte d'informations.

Pour conclure, ce mémoire met en lumière les défis et les opportunités pour renforcer la sécurité des SI chez SONATRACH. Les recommandations proposées visent à surmonter les incohérences actuelles, améliorer la résilience organisationnelle et garantir une protection optimale contre les menaces émergentes. En adoptant ces mesures, Sonatrach pourra établir une posture de sécurité robuste et durable, essentielle pour sa souveraineté numérique et son efficacité opérationnelle.

Ces efforts contribueront non seulement à sécuriser les systèmes d'information de l'organisation, mais aussi à instaurer une culture de sécurité proactive et réactive face aux évolutions des menaces. Il est impératif que SONATRACH continue à investir dans la formation de ses employés, l'adoption de normes de sécurité rigoureuses et l'amélioration continue de ses processus de gestion de la sécurité pour rester à la pointe de la cybersécurité.

- **Perspectives**

Notre étude pourra être utilisée dans diverses recherches futures, notamment pour évaluer l'efficacité des stratégies de sécurité dans différentes industries sensibles telles que l'énergie, les télécommunications et la finance.

Elle pourra servir de base pour des recherches sur l'application de l'intelligence artificielle et du machine learning dans la gestion des menaces, et optimiser les politiques de sécurité en fonction des évolutions technologiques. De plus, elle pourra informer des programmes éducatifs et des formations, ainsi que des études sur les plans de continuité des activités et la résilience organisationnelle.

BIBLIOGRAPHIE

Bibliographie

Articles

Alexei. (2022, 01 02). ENSURING INFORMATION SECURITY IN PUBLIC ORGANIZATIONS IN THE . Moldova: Journal of Social Sciences.

Azmi, R., Tibben, W., & Khin , T. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy.

Boughrara. (2018, 09). Cybernitic Security : The Agerian strategy of security and. Algérie : مجلة الدراسات االفريقية وحوض النيل – المركز الديمقراطي العربي .

Boukers. (2022, 06 22). La cybersécurité: Dangers, menaces et défis nécessitant des pratiques, des recommandations et des stratégies spécifiques. Algérie : مجلة االبحاث في الحماية االجتماعية.

Chaib. (2022, 04 07). Strategic mechanism of combating cyber crime under the new environment of digital communication. Algérie: Law and Political Science Journal.

Chander. (2019). A Case for National Cyber Security Strategy.

Cruquenaire. (2022). La cybersécurité, un enjeu à la croisée des stratégies européennes.

Denden. (2020, 11 19). The Security Strategy of the Algerian State. Algérie : مجلة صوت القانون.

Dwi Puji Lestari, Andika Luthfi Citra Tama, Siti Karlina, Achmad Sultan, & Tarwoto. (2024). Factors Affecting Information System Security: Information Security, Cyber Threats and Attacks, Physical Security, and Information Technology (Literature Review)2024.

Fernando S. Meirelles., F., & Pigola, A. (2024). Trust in information security technology.

Filali. (2020, 12 06). The role of ISO/IEC 27001 in raising the credibility of the ISMS in the organization. Algérie : مجلـة إضافات اقتصادية.

Fotis Kitsios , Elpiniki Chatzidimitriou , & Maria Kamariotou. (2023, 03 27). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability 2023, 15, 5828.

Ghernaouti, S. (2016). *Cybersécurité, Sécurité informatique et réseaux.* Dunod.

Gibson. (1984). *Neuromancer.*

Grzegorz , P., & Klaudia , S. (2023). CYBERSECURITY AND THE SCOPE OF DESIGNING INFORMATION SECURITY SYSTEMS IN THE ORGANIZATION.

Guelaa-Drous. (2022, 12 12). National Cyber Security: A reading of the most important Security and. Algérie: مجلـة الرواق للدراسات.

Judijanto, L., Rahardian, R., Muthmainah, H., & Moh , E. (2023). Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia. West Science Information System and Technology.

Junaid. (2013, 01). ISO 27001: Information Security Management Systems. Allemagne : Reaserch-gate .

Klaa, C. (2022, 04 27). Cyber security and the challenges of espionage and penetration of countries. Algérie: مجلـة الحقوق والعلوم الإنسانية.

Klaic. (2015). A Method for the Development of Cyber Security Strategies.

KLAIC, A. (2015). A Method for the Development of Cyber Security Strategies.

Lujif, H., Besseling, k., Spoelstra, M., & De Graaf , P. (2013). *Ten national cyber security strategies: A comparison," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics).*

Olaru, M., & Maftei, M. (2021). Information Security Management System and Cyber Security Strategy Implementation in the Context of SCRUM. Retrieved from Georg Sven Lampe

Ramos Mamami, Cahuaya Ancco, René Llanqui, & Argollo. (2023, 03 30). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. Espagne: Revista Innovación y Software.

Sahraoui , Bensedira, & Bouheroud. (2020, 04 26). Spread Application of Information Security Management System ISO27001 in Business Organizations: Evaluation Study for the Period y for the Period. Algérie: مجلة آفاق علمية.

Senol , M., & Karacuha, E. (2020, may). *Creating and Implementing an Effective and Deterrent National Cyber Security Strategy*. Retrieved from https://www.hindawi.com/journals/je/2020/5267564/

Sites web

ANSSI. (2004). Retrieved from https://cyber.gouv.fr/publications/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation

ANSSI. (2023). Retrieved from https://cyber.gouv.fr/le-panorama-de-la-cybermenace

BLOGSPOT. (2014). Retrieved from https://gouvsi.blogspot.com/2014/10/cobit-5-en-francais-un-progres.html

CAIRN.INFO. (2019). Retrieved from https://www.cairn.info/revue-les-cahiers-de-la-justice-2019-4-page-619.htm

Clusif. (2010). Retrieved from https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/

EBIOS. (2010). Retrieved from https://club-ebios.org/site/wp-content/uploads/presentations/ClubEBIOS-2010-03-23-GRALL.pdf

ENISA. (2012). Retrieved from https://www.bing.com/search?q=ENISA%2C+National+Cyber+Security+Strategies+Practical+Guide+on+Development+and+Execution%2C+ENISA+Publications%2C+Heraklion%2C+Greece%2C+2012.&cvid=dbd405af422e431782f22e4f49433a82&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzkxNGowajmo

European Comission. (2015). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. Retrieved from http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Hennie, v., & Sonja , B. (2004). *Analyse et gestion du risque bancaire : un cadre de référence pour l'évaluation de la gouvernance d'entreprise et du risque financier*. Retrieved from https://bibliotheque.univ-catholille.fr/Default/doc/SYRACUSE/335800/analyse-et-gestion-du-risque-bancaire-un-cadre-de-reference-pour-l-evaluation-de-la-gouvernance-d-en?_lg=fr-FR

ISO 27002. (2005). Retrieved from https://www.iso.org/fr/home.html

ISO/CEI 27002. (2022). Retrieved from https://www.iso.org/fr/standard/54533.html

ISO/CEI GUIDE 73. (2009). Retrieved from https://www.iso.org/obp/ui/#!iso:std:44651:fr

Jacques , S. (n.d.)

MCLEOD , & SCHELL . (2007). Retrieved from https://books.google.dz/books/about/Management_Information_Systems.html?id=wlhGAAAAYAAJ&redir_esc=y

Moen, R. (n.d.). *Foundation and History of the PDSA Cycle*. Retrieved from https://deming.org/uploads/paper/PDSA_History_Ron_Moen.pdf.

Ouvrages

AMRAE-CLUSIF. (2006). *RM et RSSI : Deux métiers qui s'unissent pour la gestion des risques liés au système d'information*.

BIDAN, M. (2013). *Le système d'information de gestion en question.*

Jacques SORNET, Hengoat OONA, & Nathalie LE GALLO . (2016). *DCG 8, Systèmes d'information de gestion - Manuel et applications.*

Jacques, S., Hengoat OONA, O., & Nathalie, L. (2016). *DCG 8, Systèmes d'information de gestion - Manuel et applications,.*

M. Tekerek. (2008). Information security management. Journal of Science and Engineering,.

Madjed, R. (2016). Scientific Research Methodology. بيروت: Friedrich Ebert.

Olfa. (2021). Conception et mise en oeuvre d'une culture sécurité des systèmes d'information : le cas des PME.

ORTALO, R. (1988). Évaluation quantitative de la sécurité des systèmes d'information. 193.

OTTIS, & LORENTS. (2010). "Cyberspace: Definition and Implication," in Proceeding of the 5th International Conference Information Warfare and Security. pp. 267-269.

R, R. (1998). Systèmes d'information et management des organisations, .

R. REIX, & F. ROWE. (2002). Faire la recherche en système d'information : de l'histoire au concept. 366.

Shabunina , V., Tur , O., & Sarancha , V. (2023). INFORMATION SECURITY MANAGEMENT: AMERICAN EXPERIENCE. pp. 90-98.

Shakarian,, p., Shakarian , J., & Ruef, A. (2013). "Attacking Iranian Nuclear Facilities: Stuxnet," in Introduction to Cyber-Warfare: A Multidisciplinary Approach, .

Solms, V., & Niekerk, V. (2013). *From information security to cyber security," Computers & security* .

Wiener, N. (1948). *Cybernetics: Control and Communication in the Animal and the Machin.*

Zhenkun , H., & Yiyu, C. (2024, May). Research on Information Security of Digital Transformation of Exhibition Industry. pp. 229-232.

ANNEXES

Annexe A

Guide d'entretien

ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT

ENSM-Koléa

Guide d'entretien : « *La Stratégie de Sécurité des Systèmes d'Information face aux Menaces Émergentes* »

Objet et intérêt de l'étude :

Madame/Monsieur,

Je suis MOUDJED Fatma, étudiante en Master 2 dans la spécialité de Management Stratégique et Système d'Information à l'École Nationale Supérieure de Management de Koléa. Dans le cadre de la préparation de mon projet de fin d'études, j'effectue une étude intitulée "La Stratégie de Sécurité des Systèmes d'Information face aux Menaces Émergentes - Cas d'étude de la DSSI de SONATRACH" en vue de l'obtention du diplôme de Master Professionnel.

Nous souhaiterions vous solliciter pour nous aider à enrichir notre étude en répondant à ce guide d'entretien. Celui-ci est destiné aux responsables de la DSSI de SONATRACH. L'objectif de cet entretien est de répondre à l'objectif de notre étude, a savoir la mise en place d'une stratégie proactive de sécurité des systèmes d'information

NOTE : Demander la permission de faire un enregistrement vocal de l'entretien, et s'assurer l'anonymat de l'interviewé.

Informations sur les interviewés

- Genre
- Tranche d'âge
- Poste de travail
- Nombre d'années d'expérience

Thème 1 : Organisation et Responsabilités de la fonction de sécurité des systèmes d'information

1. Pouvez-vous décrire comment est organisée la fonction de sécurité des systèmes d'information dans votre organisation ?
2. Quelles sont les responsabilités principales des différentes parties prenantes impliquées dans la sécurité des systèmes d'information ?
3. Comment s'assure-t-on de la coordination entre les différents départements ou équipes concernés par la sécurité des systèmes d'information ?
4. Quels canaux de communication sont utilisés pour signaler les incidents de sécurité ou les vulnérabilités identifiées ?
5. Quelle est la structure hiérarchique et les flux de décision concernant la gestion des vulnérabilités dans votre organisation ?
6. Comment gérez-vous les relations avec les fournisseurs externes ou les partenaires impliqués dans la sécurité des systèmes d'information ?

Thème 2 : Stratégie et Gestion des Vulnérabilités

1. Pouvez-vous décrire la stratégie globale de sécurité des systèmes d'information de votre organisation ?
2. Quels processus utilisez-vous pour identifier, évaluer et prioriser les vulnérabilités ?
3. Comment planifiez-vous les actions de sécurité des SI sur le long terme ?
4. Comment sont prises les décisions concernant la mise en œuvre des mesures de sécurité pour traiter les vulnérabilités identifiées ?
5. Comment documentez-vous et suivez-vous les actions prises pour remédier aux vulnérabilités ?
6. Quels mécanismes utilisez-vous pour évaluer l'efficacité des mesures de sécurité mises en place ?
7. Comment assurez-vous la conformité aux normes et réglementations en matière de sécurité des systèmes d'information ?

Thème 3 : Culture et Sensibilisation à la Sécurité des SI

1. Comment instaurez-vous une culture de la sécurité des systèmes d'information au sein de votre organisation ?
2. Quels programmes de sensibilisation ou de formation sont mis en place pour sensibiliser les employés aux enjeux de sécurité informatique ?
3. Comment les employés sont-ils impliqués dans la remontée des incidents de sécurité ou la détection des vulnérabilités ?
4. Quels sont les mécanismes de récompense ou de reconnaissance pour les pratiques sécuritaires au sein de votre organisation ?
5. Comment gérez-vous la résistance au changement lors de la mise en œuvre de nouvelles mesures de sécurité ?
6. Quels sont les mécanismes de partage des bonnes pratiques en matière de sécurité des systèmes d'information au sein de votre organisation ?

Remerciements

Je vous remercie d'avoir bien voulu nous accorder de votre temps pour cet entretien, bien évidemment nous vous ferons part des résultats de notre recherche. Au revoir !

NOTE : Demander le contact de l'interviewée :

- Adresse électronique professionnelle :
- Numéro de téléphone :
- LinkedIn :