MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANANGEMENT ENSM.
PÔLE UNIVERSITAIRE DE KOLÉA

MEMOIRE DE FIN D'ETUDES

MASTER PROFESSIONNEL EN MANAGEMENT STRATÉGIQUE ET SYSTÈME D'INFORMATION

ÉLABORATION D'UNE POLITIQUE DE SÉCURITÉ DES SYSTEMES D'INFORMATION

CAS : NAFTAL

Elaboré par : Mahmoudi Rawiya

Encadré par : Dr Boucheloukh Mohamed Faouzi

Année 2018/2019

Résumé

Le système d'information est considéré comme le cœur d'une entreprise et il est plus stratégique que jamais. Le protéger et assurer sa disponibilité sont devenus un nécessité. Il doit être exempt de tout type de menace qui peut toucher à sa confidentialité, intégrité ou disponibilité. Plusieurs solutions et normes de sécurité sont définies afin de maintenir un certain niveau de sécurité dans l'entreprise. Une analyse des risques est nécessaire pour faciliter l'application de ces normes.

Parmi les solutions existantes, nous proposons la Politique de Sécurité des Systèmes d'Information qui sert à orienter l'ensemble d'acteurs d'entreprise à maintenir la sécurité de leur système d'information.

Mots clés : Sécurité, système d'information, confidentialité, disponibilité, intégrité, EBIOS, PSSI, ISO 27001, besoins de sécurité, objectifs de sécurité, règles de sécurité, menaces, causes, risques, enjeux.

Abstract

The information system is considered the heart of a business and is more strategic than ever. Protecting it and ensuring its availability have become a necessity. It must be free from any kind of threat that may affect its confidentiality, integrity or availability. Several security solutions and standards are defined to maintain a certain level of security in the company. A risk analysis is necessary to facilitate the application of these standards.

Among the existing solutions, we propose the Security Policy for Information Systems, which serves to guide the whole of actors of company to maintain the security of their information system.

Keywords : Security, information system, confidentiality, availability, integrity, EBIOS, PSSI, ISO 27001, security needs, security objectives, security rules, threats, causes, risks, issues.

ملخص:

يعتبر نظام المعلومات قلب الشركات في الوقت الحالي وهو أكثر استراتيجية من أي وقت مضى. حمايته وضمان توافره أصبحت من الضروريات. يجب أن يكون خال من أي نوع من التهديد قد يؤثر على سريته أو سلامته أو توفره. تم تحديد العديد من الحلول والمعايير الأمنية للحفاظ على مستوى معين من الأمن في الشركة. من أجل تسهيل تطبيق هذه المعايير ينصح بالقيام بتحليل المخاطر مسبقا كأمر ضروري.

من بين الحلول القائمة، نقترح سياسة الأمن لنظم المعلومات التي تعمل على توجيه جميع الجهات الفاعلة في الشركة للحفاظ على أمن نظام المعلومات الخاص بهم.

الكلمات الرئيسية:

الأمن، نظام المعلومات، السرية، التوفر، النزاهة، EBIOS، PSSI، ISO 27001، الاحتياجات الأمنية، الأهداف الأمنية، قواعد الأمن، التهديدات، الأسباب، المخاطر، القضايا.

Remerciement

En tout premier lieu, je remercie le bon Dieu, tout puissant, de m'avoir donné la force et la patience d'achever ce travail.

Je tiens à remercier Mr Kamel OUALI, mon tuteur au niveau de NAFTAL pour m'avoir fait confiance et me donner la chance de faire ce travail. Mes remerciements vont également à Mr Faouzi Mohammed BOUCHELOUKH, mon encadreur qui m'a suivi et encouragé tout au long de mon travail malgré ses nombreuses préoccupations.

Je tiens également à remercier toute personne qui a contribué au succès de mon stage et à la rédaction de ce mémoire.

Table des matières

Table des figures

Liste d'abréviations

SI : Système d'Information

SSI : Sécurité des Systèmes d'Information

PSSI : Politique de Sécurité des Systèmes d'Information

ANSSI : Agence Nationale de Sécurité des Systèmes d'Information

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ISO : Organisation Internationale de Normalisation

SMSI : Système de Management de la Sécurité des Informations

:

Introduction

Actuellement, pour une entreprise, l'information représente un bien stratégique sujet à convoitise. Toute atteinte illégale à cette information peut générer des conséquences parfois majeures sur le plan financier, juridique, de réputation ou concurrentiel. Ce qui contribue le plus dans une atteinte pareille, est bien la technologie de l'information et de la communication. Malgré que cette dernière facilite le traitement de l'information, la diffusion et l'accessibilité à l'information, elle peut causer les actes malveillants ainsi que les attaques dangereuses. Donc qui dit sécurité de l'information, dit aussi sécurité des systèmes d'information.

De nos jours, Les systèmes d'informations représentent une partie stratégique dans l'entreprise et les administrations. Donc le SI tirant les conséquences de la stratégie, ce que exige leur protection.

La notion du risque lié aux systèmes d'information devient une source d'inquiétude et un enjeu quotidien très important à prendre en compte, ceci en partant de la phase de conception d'un système d'information jusqu'à son implémentation et le suivi de son fonctionnement.

En effet, ces dernières années, les travaux sur la sécurité informatique et plus globalement des systèmes d'information sont de plus en plus nombreux et déjà utilisés de manière effective, mais malheureusement les techniques d'attaques ne cessent pas de se développer. Les entreprises se trouvent obligées de dépenser pour protéger leur système et assurer leur survie, comme il est dit : "la sécurité a un coût", "Exact ! mais la non-sécurité a également un coût".

Dans ce contexte, ce mémoire propose une solution de sécurité pour les entreprises, plus précisément l'entreprise NAFTAL qui est une société algérienne de distribution et de commercialisation des produits pétroliers. Le travail dans ce projet consiste à protéger l'entreprise de toute forme de menace en sécurisant son système d'information. Cette sécurité peut être effectuée par plusieurs moyens tel que la politique de sécurité des systèmes d'information. Le choix de cette solution a été fait suite à une étude bibliographique effectuée dans ce domaine et aussi par une proposition de l'organisme d'accueil qui a privilégié cette solution à cause de ses besoins actuels.

Notre solution est un document appelé "Politique de Sécurité des Systèmes d'Information" contenant des lignes directrices et des orientations qui vont guider l'ensemble des différents acteurs de l'entreprise à faire leur travail d'une manière

sécurisée sans laisser des lacunes.

Ce document est organisé comme suit :

Une "problématique" décrivant le problème de notre recherche et Une description de "l'Organisme d'accueil". Un premier chapitre intitulé "Revue de littérature et cadre conceptuel" introduit des notions de bases et des définitions concernant la sécurité et le système d'information. Le deuxième chapitre "Cadre méthodologique" présente nos choix méthodologiques pour mener à bien le travail. Le dernier chapitre "Mise en place de la PSSI et Résultat" est consacré à la description de la réalisation de la solution et le résultat obtenue. Nous terminons ce document par une conclusion générale évoquant des perspectives pour le développement de ce travail.

Problématique

Cette section est basée sur les références suivantes : [5, 6, 7, 8]

Dans une entreprise, l'information qui est générée et transmise représente un patrimoine essentiel qui doit être préservé. Pour assurer leur survie et croissance, l'entreprise doit investir non seulement dans son capital physique mais également dans le capital informationnel. Surtout que de très nombreux flux d'information y transitent. Et comme l'entreprise est un système complexe, un problème d'arrangement de ces flux peut causer rapidement des problèmes de fonctionnement qui peuvent aggraver la situation en cas ou l'information est volée, perdue ou altérée.

Les entreprises sont censées collecter, mémoriser, traiter et diffuser l'information à un temps record en utilisant des procédures et des moyens afin que les informations circulent dans l'entreprise pour qu'elle soit valorisable et actionnable. Et c'est ce qui représente un système d'information.

A cette époque, le système d'information est devenu primordial. Il fait désormais partie intégrante du fonctionnement des entreprises, que se soit manuel ou informatisé, grâce à son rôle important : une aide pour la prise de décision, un outil de contrôle de l'évolution d'organisation et un outil de coordination des différentes activités de l'entreprise.

L'enjeu principal pour l'entreprise est de garder le bon fonctionnement de son système d'information et garantir certains critères de sécurité pour l'ensemble des informations comme suit :

- garantir la disponibilité de l'outil de travail pour l'ensemble des personnels de la structure ;
- garantir la confidentialité des informations, qu'elles soient professionnelles ou personnelles ;
- garantir l'intégrité des informations et des personnes ;
- assurer la protection des données sensibles de la structure (données scientifiques et techniques, données de gestion administrative, données individuelles) ;
- assurer la protection juridique (risques administratifs, risques pénaux, perte d'image de marque).

Donc protéger son système d'information revient à assurer au moins les critères de sécurité ci-dessus.

L'environnement lié aux technologies de l'information et de la communication est la cible de nombreuses menaces. L'usage de la nouvelle technologie, l'accès distants aux données internes de l'entreprise, connexion sans fil à Internet ... etc. facilitent la dématérialisation et la circulation rapide de l'information mais génèrent également de nouveaux risques. Ce qui renforce la vulnérabilité des systèmes d'information.

Selon Hub One[1], en Europe 57% des entreprises ont déjà connu un incident en matière de cyber-sécurité, 68% est le pourcentage d'augmentation d'attaques informatiques dans les entreprises en 2016 par rapport à 2015 et seulement 469 jours est nécessaire pour détecter une infection du SI dans l'entreprise. Quelles qu'en soient les causes, ces pertes engendrent des coûts directs (remplacement des équipements, chômage technique des salariés) et indirects (perte d'image) ainsi que des conséquences parfois irréversibles pour l'entreprise.

Sécuriser son système d'information ne se résume pas qu'à prendre de nouvelles mesures techniques, c'est aussi protéger l'information stratégique de l'entreprise (plans, fichiers client, etc.). Détruire, voler, altérer ou accéder à des données sensibles dans le but de modifier ou de nuire au bon fonctionnement aura certainement des conséquences parfois irréversibles pour l'entreprise

Par ailleurs, la sécurité des systèmes d'information représente également un avantage concurrentiel car elle offre la garantie aux clients et partenaires que les informations confidentielles, confiées à votre entreprise (cahiers des charges, plans), sont protégées.

Donc, Compte tenu de la complexité et de l'hétérogénéité du SI « Système d'information » dans une entreprise, il s'avère nécessaire de le protéger, en utilisant des méthodes pour recenser et savoir exactement : qu'est ce qu'il faut sécuriser ? par rapport à quoi ? dans quel contexte ? et comment ?

L'hypothèse de ce mémoire est donc, une approche formelle concrétisée par une PSSI « Politique de Sécurité du Système d'Information » permettant à un organisme d'avoir une approche méthodique et systématique pour garantir une sécurité homogène de son SI.

1. Le groupe Hub One est un opérateur de technologies digitales qui accompagne les entreprises et organisations publiques et privées, en France et à l'international, dans leur transformation numérique

Organisme d'accueil

Présentation :

Naftal est une société par actions (SPA) fondée en 1982 et filiale à 100% du groupe Sonatrach [2], Avec un effectif de 31285 agents (2015), un capital social de 40 000 000 000 DA et un chiffre d'affaire de 380 000 000 000 DA (2016).

Vocation principale :

La distribution et la commercialisation des produits pétroliers et dérivés sur le marché national.

Métier :

1. La commercialisation, le transport, le stockage et la distribution des produits pétroliers ;
2. Le marketing, la négociation et la relation client ;
3. La maintenance et la réhabilitation des infrastructures et équipements de production ;
4. Le management de projet.

Missions :

1. L'enfutage des GPL [3]
2. La formulation des bitumes
3. La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux
4. Le transport des produits pétroliers.

2. Société nationale pour la recherche, la production, le transport, la transformation, et la commercialisation des hydrocarbures

3. Gaz de Pétrole Liquéfié

Infrastructures :

1. 47 Dépôts carburants terre
2. 42 Centres et mini-centres GPL
3. 09 Centres vrac GPL
4. 47 Dépôts relais
5. 30 Centre et dépôts aviation
6. 06 Centres marine
7. 15 Centres bitumes
8. 24 Centres lubrifiants et pneumatiques
9. Un réseau de transport pipelines d'une longueur de (2 720 km)
10. Un parc roulant de 3 300 unités
11. Un réseau de stations-service de 674, dont 338 stations-service en gestion directe
12. Naftal dispose de deux centres de formation d'entreprise qui accompagnent les plans annuels et pluriannuels de formation.

Valeurs propres :

Communication, compétence, qualité de service, confiance.

Stratégie :

A travers son plan de développement, Naftal vise un double objectif :

1. poursuivre sa mission de distribution des produits pétroliers.
2. Améliorer sa qualité de service

Les principales actions menées par Naftal portent sur :

1. La modernisation et la réhabilitation de ses infrastructures de stockage.
2. La mise en conformité de ses installations avec les normes de protection de l'environnement et de sécurité industrielle.
3. La modernisation et l'extension de son réseau de stations-service.
4. Le renouvellement de ses moyens de transport par route et de son matériel de manutention.
5. L'augmentation de ses capacités de transport par pipe.
6. La promotion de ses produits propres : GPL et essence sans plomb.

Moyens principaux du SI :

Le SI de NAFTAL est formé de plusieurs moyens humains, de communication et de sécurité supportés par des outils informatiques, dont les principaux moyens sont :

- Data-center : un cloud privé avec des serveurs et un hyperviseur pour des solution de sauvegarde.
- Équipement de sécurité : Serveur antivirus, Firewall, IPS [4], WSA [5].
- Réseaux informatiques : matériels (Routeurs, Switch, Armoires et panneaux de brassage, Modems, Liaison fibre optique), réseaux (WLAN, WAN, LAN, Antenne 3G de l'opérateur hébergé et dédiée à NAFTAL).
- Logiciels : application métier (calcul paie, finance et comptabilité, gestion des stocks, gestion du transport, gestion de la commercialisation, gestion RH, gestion inventaire), messagerie électronique, site web, liaisons FTP..., lignes spécialisées RMS([6]), ADSL(Asymmetric Digital Subscriber Line), 3G, 4G.
- Liaison : VPN (IPsec [7]), Client VPN, MSAN [8], FTTx [9]
- Autres services comme : la téléphonie IP, solution de visio conférence, vidéo surveillance.

Organigramme de NAFTAL :

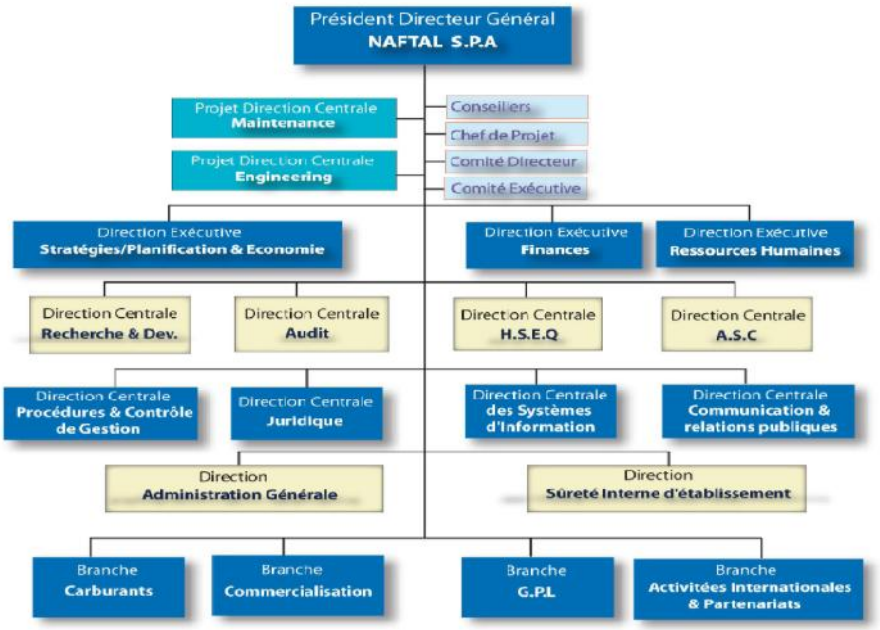

FIGURE 0.1: Organigramme de NAFTAL

4. Intrusion prevention system
5. Web Security Appliance
6. Réseau Multiservices
7. Internet Protocol Security
8. MultiService Access Node
9. Fiber To The ..

Chapitre 1

Revue de littérature et cadre conceptuel

1.1 Préliminaires

Cette section est basée sur les références suivantes : [1, 4]

Dans cette section on donne quelques notions et définitions liées à l'information, système d'information et à la sécurité de l'information.

Définition 1 ***Information*** *(information)*
Tout renseignement ou tout élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Exemple : *Un message, une liste de noms, une requête de certification, liste de révocation...etc.*

Définition 2 ***Système d'information*** *(information system)*
Ensemble des moyens humains et matériels ayant pour finalité de collecter, traiter, stocker, acheminer, présenter ou détruire l'information.

Définition 3 ***Sécurité de l'information*** *(information security)*
Satisfaction des besoins de sécurité des biens essentiels[1] *c-à-d la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ; en outre, d'autres propriétés peuvent être rajoutées.*

Définition 4 ***Besoins de sécurité*** *(sensitivity)*
Définition précise et non ambiguë du niveau d'exigences opérationnelles relatives à un bien essentiel pour un critère de sécurité donné.

Exemple : *Disponibilité, confidentialité, intégrité...etc.*

1. Information ou processus jugé comme important pour l'organisme.

Définition 5 ***Critère de sécurité*** *(security criteria)*
Caractéristique d'un bien essentiel permettant d'apprécier ses différents besoins de sécurité.

Exemple : *Disponibilité, Intégrité, Confédentialité, Traçabilité...etc.*

Définition 6 ***Disponibilité*** *(availability)*
Propriété d'accessibilité au moment voulu des biens essentiels par les personnes autorisées (propriété d'une information ou d'un traitement d'être, à la demande, utilisable par une personne ou un système).

Définition 7 ***Intégrité*** *(integrity)*
Propriété d'exactitude et de complétude des biens essentiels (Propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée).

Définition 8 ***Confidentialité*** *(confidentiality)*
Propriété des biens essentiels de n'être accessibles qu'aux personnes autorisés (caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés)

Définition 9 ***Traçabilité*** *(traceability)*
la capacité de preuve, ou auditabilité ou imputabilité, propriété relative à la traçabilité des actions réalisées et à la conservation des preuves de ces actions.

Définition 10 ***Gestion des risques*** *(risk management)*
Processus itératif de pilotage, visant à maintenir les risques à un niveau acceptable pour l'organisme. La gestion des risques inclut typiquement l'appréciation, le traitement, la validation du traitement et la communication relative aux risques.

Définition 11 ***appréciation du risque*** *(risk assessment) vspace0.02cm*
Sous-processus de la gestion des risques visant à identifier, analyser et à évaluer les risques.

Définition 12 ***Analyse du risque*** *(risk analysis)*
utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Définition 13 ***Évaluation du risque*** *(evaluation of risk)*
processus de comparaison du risque estimé avec des critères de risque donnés pour en déterminer l'importance.

Définition 14 ***Traitement du risque*** *(risk treatment)*
Sous-processus de la gestion des risques permettant de choisir et de mettre en œuvre des mesures de sécurité visant à modifier les risques de sécurité de l'information (processus destiné à modifier un risque).

Définition 15 ***Objectif de sécurité*** *(security objective)*
Expression de la décision de traiter un risque selon des modalités prescrites. On distingue notamment la réduction, le transfert, le refus et la prise de risque.

Définition 16 ***Mesure de sécurité*** *(control)*
Moyen de traiter un risque de sécurité de l'information. La nature et le niveau de détail de la description d'une mesure de sécurité peuvent être très variables.

Définition 17 ***Menace*** *(threat)*
Moyen type utilisé par une source de menace.

Exemple : *Vol de supports ou de documents, piégeage du logiciel, atteinte à la disponibilité du personnel.*

Définition 18 ***Vulnérabilité*** *(vulnerability)*
Caractéristique d'un bien support[2] *qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information. (propriétés intrinsèques de quelque chose entraînant une sensibilité à une source de risque pouvant induire une conséquence).*

Exemple : *Crédulité du personnel, facilité de pénétrer sur un site, possibilité de créer ou modifier des commandes systèmes...etc.*

Définition 19 ***Risque*** *(risk)*
Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système.

Définition 20 ***Impact*** *(Impact)*
Conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement.

2. Bien sur lequel reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. On appréciera ses vulnérabilités mais pas ses besoins de sécurité.

1.2 Sécurité des systèmes d'information

Cette section est basée sur les références suivantes :[9, 10, 11, 12, 13, 14, 15]

L'information est une donnée qui constitue une signification pour une personne au moment où cette dernière va en prendre connaissance. Elle peut apporter à celui qui l'a détient un avantage substantiel, ce qui veut dire que cette information est valeureuse. Donc quelque soient les domaines, la maitrise de l'information peut s'avérer un atout décisif et compétitif de performance en bien gérant et préservant cette information.

Pour gérer l'information, on a absolument besoin d'un système d'information, surtout avec l'avènement des technologies de l'information et de la communication. Donc sécuriser l'information revient à sécuriser notre système d'information.

Pendant très longtemps, la sécurité des SI[3] a été considérée comme un second plan pour les entreprises. Mais à cause d'une multitude d'incidents et de plus grave sinistres qui provoquent de lourdes pertes, les organismes[4] ont pris conscience de la nécessité de la sécurité des SI et la considère dorénavant comme une discipline de première importance, car même s'ils ne vont pas engendrer des gains, ils vont certainement éviter des pertes.

Le concept de sécurité des systèmes d'information recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources d'un SI de toute malveillance, panne, mauvaise utilisation ou catastrophe naturelle qui rendent le SI partiellement ou totalement inutilisable conformément aux différentes critères de sécurité (Disponibilité, Intégrité, Confidentialité, Traçabilité...).

1.2.1 Enjeux

Un organisme peut faire face à plusieurs vulnérabilités qui menacent son SI. La perte, la manipulation ou le vol d'informations peuvent considérablement affaiblir l'entreprise. Pour faire face à ces risques, il est nécessaire de choisir les critères de sécurité à prendre en compte afin de garantir sa SSI[5] et surmonter les enjeux correspondants, et donc assurer les DICT[6] qui sont :

Disponibilité : Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés, càd ; Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

3. Système d'Information
4. le mot organisme est employé pour désigner globalement les entreprises, les organisations, administrations, collectivités territoriales...
5. Sécurité des Systèmes d'Information
6. Disponibilité, Intégrité, Confidentialité, Traçabilité

- **Pour une fonction** : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large.
- **Pour une information** : garantie de la disponibilité prévue pour l'accès aux données (délais et horaires).

Intégrité : Propriété d'exactitude et de complétude des éléments essentiels. càd, Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

- **Pour une fonction** : Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements automatisés ou non par rapport aux spécifications ; absence de résultats incorrects ou incomplets de la fonction.
- **Pour une information** : garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation ou d'usages non autorisés ; non-altération de l'information.

Confidentialité : Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés, càd, Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

- **Pour une fonction** : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel.
- **Pour une information** : protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel.

Traçabilité : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

- **Pour une fonction** : les parties impliquées dans une activité ne puissent déclarer à tort avoir été étrangères à tout ou partie de l'activité.
- **Pour une information** : conserve les traces de l'état et des mouvements de l'information.

Il peut être pertinent d'en ajouter d'autres tels que l'authentification. Lorsqu'un utilisateur veut accéder à un système d'information, il doit dans un premier temps effectuer une procédure d'identification et d'authentification.

Authentification : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange. est une phase qui permet à l'utilisateur d'apporter la preuve

de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.

1.2.2 Menaces et risques

Les systèmes d'information présentent des fragilités liées à diverses menaces dont les sources peuvent être environnementales (météo, incendie, etc.), intrinsèques (conception, technologies, etc.) mais aussi humaines (externes, internes, délibérées, par erreur ou par négligence) qui peuvent provoquer des risques tels que :

- Perte et destruction des données.
- Modification de données (Altération).
- Interception de données (Vol et espionnage).
- Indisponibilité du système.
- Dégradation de l'image de marque.
- Détournement d'activité via les technologies de l'information et de la communication.
- Sanctions juridiques pour défaut de protection de données de tiers ou utilisation prohibée (même involontaire) des technologies, par les membres d'une entreprise.

Ces risques peuvent engendrer des conséquences graves, perte financières, perte de contrat, des litiges ou même la fermeture de l'entreprise.

1.2.3 Les causes

Les sources des risques pour les systèmes d'information sont diverses et variées. Elles ont le plus souvent des causes d'origine humaines, extérieures ou techniques :

Causes humaines

- **La maladresse :** C'est lorsque quelqu'un peut exécuter un traitement non souhaité, effacer involontairement des données ou des programmes.
- **L'inconscience :** De nombreux utilisateurs méconnaissent les risques, et introduisent souvent des programmes malveillants sans le savoir, ou effectuent des manipulations inconsidérées.

- **La malveillance :** Une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes.

Causes extérieures

- **Un sinistre :** Vol, incendie, dégât des eaux, séisme...etc.
- **Une malveillance :** Une mauvaise manipulation entraînant une perte de matériel et/ou de données.
- **Problèmes électriques :** Panne total ou absence partielle du courant.

Causes techniques

- **Surchauffe :** C'est lorsque les processeurs produisent de la chaleur.
- **L"usure :** La détérioration résultant d'un usage prolongé.
- **Incidents liés au logiciel :** des failles permettant de prendre le contrôle total ou partiel d'un ordinateur.
- **Un programme malveillant :** un logiciel destiné à nuire au système.

Mais comment surmonter ces enjeux là ? comment faire face à ces risques et se protéger contre les menaces et ses causes ? Ces problématiques peuvent être résolues par ce qu'on appelle le Management de la sécurité des systèmes d'information.

1.2.4 Management de la sécurité des systèmes d'information

Le management de la sécurité des systèmes d'information a pour but de prévenir les informations qui différencient l'entreprise, à la fois en ligne et en personne. Un système de management de sécurité des systèmes d'information doit inclure des politiques et des processus qui protègent une organisation contre l'utilisation abusive des données par les employés ou par les tiers. Pour être efficaces, ces politiques doivent être appuyées et supervisées par la direction. Cette dernière doit également changer la culture de l'organisation pour refléter la valeur qu'elle accorde à la sécurité de l'information. Ce n'est pas une tâche facile, mais elle est essentielle à la mise en œuvre efficace d'un Système de sécurité.

Les entreprises se caractérisent par : le style de direction, la culture managériale... La gestion de la sécurité est spécifique à la structure organisationnelle de l'entreprise et dépend de sa stratégie. Mais il est important de souligner que pour mieux réussir cette gestion de sécurité, il faut s'organiser d'abord. L'entreprise doit impliquer la Direction Générale et solliciter la participation des différents niveaux hiérarchiques, notamment le département des systèmes d'information. Car L'efficacité de la sécurité d'un système d'information ne repose pas uniquement

sur les outils de sécurité mais également sur une stratégie, une organisation et des procédures cohérentes.. Cela nécessite une structure de gestion adéquate dont la mission est de gérer, mettre en place, valider, contrôler et faire comprendre à l'ensemble des acteurs de l'entreprise l'importance de la sécurité. Elle détermine également le comportement, les privilèges, les responsabilités de chacun.

La mission de sécurité dans un organisme s'adresse plus particulièrement aux responsables de la sécurité des systèmes d'information (RSSI), mais que fait un RSSI ?

Responsable de la Sécurité des Systèmes d'Information (RSSI)

La fonction de RSSI commence à se pérenniser au sein des grandes organisations. La plupart des grandes entreprises ont mis en place une fonction de responsable de la sécurité, ce qui témoigne de l'importance du sujet et de la maturité croissante de la fonction.

Le RSSI est chargé de concevoir et animer la démarche sécurité et confidentialité des systèmes d'information (matériels, données et logiciels), en veillant à ce que les niveaux de sécurité et de confidentialité soient conformes à la réglementation externe et aux standards internes.

Sa mission première est de définir la politique de sécurité du SI et de veiller à son application. Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble. Il est l'interface reconnu des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.

1.2.5 Document de sécurité des systèmes d'information

Plusieurs documents peuvent être identifier en cours de la gestion de la sécurité, parmis lesquels on cite :

- **Politique de sécurité des systèmes d'information (PSSI) :** C'est le document de plus haut niveau fixant notamment les objectifs de sécurité détaillés de l'entreprise et les règles de sécurité à mettre en place pour les atteindre. Validé par la direction générale, ce document permet d'organiser et de légitimer la mise en place de l'organisation relative à la SSI [7] et des recommandations plus spécifiques qui découlent de la politique de sécurité.

7. Sécurité des Systèmes d'Information

- **Spécifications de sécurité :** Dans un certain nombre de domaines, il est en effet utile de décliner les règles de haut niveau adoptées dans la PSSI pour les adapter à un contexte particulier.
  Exemple : D'un point de vue plus technique, la PSSI peut également se trouver déclinée dans les principaux domaines du système d'information pour détailler les règles de protection : du réseau, des systèmes d'exploitation, d'un SGBD [8], des serveurs HTTP [9], etc.

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

- **Charte de sécurité des SI :** C'est le document qui définit les droits et les obligations de chaque acteur dans un système d'information donné. Cette charte a pour but d'établir un code de déontologie pour régir l'utilisation des ressources informatiques mises a la disposition des utilisateurs.

- **Guides de configuration ou de recette sécurité :** Pour une mise en place efficace, ces règles de protection doivent pouvoir être précisément décrites dans le cas de certains systèmes d'exploitation, certains équipements réseaux ou certains logiciels. C'est alors le rôle des documents opérationnels. Ceux-ci peuvent prendre la forme de guides de configuration ou de cahiers de recette SSI. La principale distinction entre les deux documents tient avant tout à leur mode de mise en œuvre : le guide de configuration, dans une logique de coopération avec la SSI peut s'agir d'aider les administrateurs à mettre en place les mesures de sécurité décidées dans l'entreprise, dans une logique de validation et de contrôle. Par contre le deuxième document peut s'agir d'une procédure de recette (tests) permettant d'autoriser formellement l'ouverture d'un service ou d'un système agréé du point de vue de sa sécurité.

- **Analyse des risques :** En complément des documents de mise en place, la PSSI peut être accompagnée par un document d'analyse des risques qui permet de mieux comprendre la réalité des principaux biens, des menaces identifiées et des risques recensés dans l'entreprise.

- **Synthèse/Suivi :** Du point de vue du suivi de la sécurité, il est également important de prévoir l'existence de documents permettant de suivre la mise en place des règles de sécurité, de consolider les alertes de sécurité identifiées et enfin d'offrir une vue synthétique de la configuration effective des règles de sécurité.

- **Tableau de bord :** on peut envisager de rassembler un certain nombre d'indicateurs de sécurité au sein d'un tableau de bord de la sécurité. L'objectif de ce tableau est d'offrir à la direction un état de la situation générale de la SSI, dans l'objectif de présenter les effets de la mise en place de la politique

8. Système de Gestion de Base de Données
9. HTTP signifie HyperText Transfer Protocol . c'est un protocole de communication entre client et serveur développé pour le web.

de sécurité de l'entreprise ou éventuellement pour susciter cette mise en place.

Dans notre travail, on ne s'intéresse qu'à la politique de sécurité qui sera détaillée dans la section suivante.

1.3 Politique de sécurité du système d'information

Cette section est basée sur les références suivantes :[16, 17, 3, 12, 2]

On abordera dans cette section une étude bibliographique en présentant la politique de sécurité des systèmes d'information et les différentes méthodes d'analyse de risque aidant à la réalisation de cette politique.

1.3.1 Qu'est ce qu'une PSSI ?

Définition 21 *Une Politique de Sécurité de Système d'Information est un ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme.*

Pourquoi un organisme a besoin d'une PSSI ? Compte tenu du niveau des risques liés à la pression continue de la menace, une défaillance de la sécurité du système d'information pourrait entraîner des conséquences irréversibles sur la réalisation des objectifs stratégiques de l'organisme ou vis à vis du respect de ses obligations ou engagements. C'est pourquoi la PSSI doit être prise en compte et validée au niveau de responsabilité le plus élevé comme un instrument de gestion des risques SSI.

La PSSI traduit la reconnaissance formelle de l'importance accordée par la direction générale de l'organisme à la sécurité de son ou ses systèmes d'information. Elle définit la politique de sécurité d'une entité spécifique qui peut être un système technologique, une fonction automatisée ou une application mais aussi un organisme entier comme une entreprise. Une entreprise repose sur son personnel, sa culture, ses informations et ses processus de gestion (traitement, stockage ou/et transfert) des informations. Ce sont ces processus d'entreprise qui font toute la différence entre deux "organisations" au but similaire, dans le même secteur économique. Chaque processus repose sur l'organisation, les procédures et la technologie. Se limiter aux aspects technologiques est donc insuffisant car il est nécessaire de considérer également les aspects non techniques. La PSSI s'inscrit dans le système de management de l'organisme, donc de la sécurité des informations et processus, puis enfin de la SSI. Elle constitue en effet le premier document à formaliser dans l'étape de planification et sera suivie des étapes de mise en œuvre, de vérification et d'amélioration du système de management de la SSI. La PSSI constitue un cadre

de référence et de cohérence pour :

- l'intégration de la sécurité lors de la conception d'un système d'information ;
- l'ensemble des activités et des acteurs de l'organisme par rapport auxquels toute évolution du système d'information devra être justifiée ;
- Aider les personnes chargées d'élaborer et de mettre en œuvre des mesures, des consignes et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information.

Contenu d'une PSSI La PSSI dans sa globalité doit aborder les points suivants :

1. **Les éléments stratégiques :**
   - **Périmètre de la PSSI :** le champ d'application de la PSSI, par exemple en termes de domaines d'activités ou de systèmes d'information.
   - **Enjeux et orientations stratégiques :** C'est les enjeux liés au périmètre de la PSSI.
   - **Aspects légaux et réglementaires :** C'est le référentiel légal et réglementaire lié au périmètre de la PSSI.
   - **Échelle de besoins :** Une échelle de besoins comportant une pondération et des valeurs de référence selon les critères de sécurité choisis.
   - **Besoins de sécurité :** C'est les besoins de sécurité des domaines d'activité de l'organisme (ou des éléments essentiels), selon l'échelle de besoins établi.
   - **Les menaces :** C'est l'ensemble des origines de menaces retenues et non retenues pour le périmètre de l'étude.
2. **Objectifs et Règles de sécurité :** C'est l'ensemble des objectifs et des règles de sécurité classées par thème.

Qualité d'une PSSI Quant à la qualité, une PSSI de bonne qualité doit répondre aux caractéristiques suivantes :

- Les objectifs et les règles énoncées doivent être réalistes.
- La PSSI doit être applicable, avec des moyens nécessairement limités (notamment du point de vue humain).
- La politique doit correspondre à une vision à long terme. Ce type de document ne peut pas être révisé tous les ans. Il doit donc être suffisamment

générique pour rester en application quelques années.

- La clarté et la concision sont nécessaires à certains moments pour énoncer des règles claires.

- La PSSI (et notamment ses règles) doit être basée sur des rôles ou des profils d'utilisateurs : les systèmes changent, la notion même d'utilisateur (au sens informatique) peut changer pour des raisons techniques, il faut s'appuyer des notions un peu plus abstraites pour définir les règles de sécurité impliquant les droits des utilisateurs.

- La PSSI doit permettre une définition claire des domaines de responsabilité et d'autorité, notamment sur les systèmes techniques. L'objectif est alors de pouvoir trancher efficacement entre des points de vue contradictoires.

- La PSSI doit être à jour, elle doit être revue périodiquement ou quand les évolutions de l'entreprise le nécessitent.

Finalité d'une PSSI Les finalités d'une politique sécurité s'articulent autour de quatre axes suivants :

1. sensibiliser aux risques pesant sur les systèmes d'information et aux moyens disponibles pour s'en prémunir et ce, avec l'appui de la direction générale de Naftal.

2. créer une structure chargée d'élaborer, de mettre en œuvre des règles consignes et procédures cohérentes pour assurer la sécurité des systèmes informatiques et la doter de moyens humains et matériel nécessaires..

3. promouvoir la collaboration entre les différents unités et directions de l'établissement pour l'élaboration et la mise en œuvre des règles, consignes et procédures définies, susciter la confiance dans le système d'information de l'établissement.

4. faciliter la mise au point et l'usage du système d'information pour tous les utilisateurs autorisés de l'établissement.

Des audits sont nécessaires suite à la mise en place initiale d'une politique de sécurité, puis régulièrement pour s'assurer que les mesures de sécurité sont mises à niveau et que les usages restent conformes aux procédures. Ainsi que La PSSI est un document évolutif qui doit être régulièrement révisé afin de prendre en compte les évolutions du contexte (modifications des processus, du système d'information, des personnels, de l'organisation) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux).

1.3.2 Analyse de Risques

L'élaboration d'une PSSI s'appuie sur le référentiel de l'organisme et sur une analyse des risques SSI. Organiser cette sécurité n'est pas une chose facile, c'est pourquoi il existe des méthodes reconnues d'analyse de risques pour aider les responsables à mettre en place une bonne politique de sécurité et à procéder aux audits permettant d'en vérifier l'efficacité.

Qu'est ce que l'Analyse de Risques ?

L'analyse des risques consiste en une identification systématique et permanente et en une analyse de la présence de dangers et de facteurs de risque dans des processus de travail et des situations de travail concrètes sur le lieu de travail dans une entreprise, un chantier ou une institution.

L'analyse des risques se compose de trois phases :

1. l'identification des dangers ;
2. la définition et la détermination des risques ;
3. l'évaluation des risques.

Parmi plusieurs méthodes, on abordera ici quelque unes plus populaires et non abandonnées employées en Europe et en Amérique du Nord.

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) :

EBIOS permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoin de l'entreprise (ou d'une administration). Elle a été créée par l'ANSSI [10] (auparavant la DCSSI [11]), du Ministère de la Défense (France). Elle est destinée avant tout aux administrations françaises et aux entreprises.

Cette méthode décline les normes internationales [ISO 27005] et [ISO 31000], tout en satisfaisant les exigences de gestion des risques de l'[ISO 27001]. Elle peut s'appliquer au secteur public et au secteur privé, à des petites structures (petites et moyennes entreprises, collectivités territoriales...) et à des grandes structures (ministère, organisation internationale, entreprise multinationale...), à des systèmes en cours d'élaboration et à des systèmes existants.

La méthode EBIOS se compose de 5 guides (Introduction, Méthodologie, Principes, Références ssi) et d'un logiciel permettant de simplifier l'application de la méthodologie explicitée dans ces guides. L'ANSSI possède un centre de formation où sont organisés des stages à destination des organismes publics français. Un club d'utilisateurs EBIOS a été créé en 2003 et constitue une communauté experts permettant le partage des expériences. Une base de connaissances à laquelle se

10. Agence Nationale de Sécurité des Systèmes d'Information
11. Direction Centrale de la Sécurité des Systèmes d'Information

connecte le logiciel EBIOS permet d'avoir à accès à la description d'un ensemble de vulnérabilités spécifiques, de contraintes de sécurité, de méthodes d'attaques.

La méthode EBIOS est découpée en 5 étapes (modules) :

1. Étude du contexte
2. Étude des événements redoutés
3. Étude des scénarios de menaces
4. Étude des risques
5. Étude des mesures de sécurité

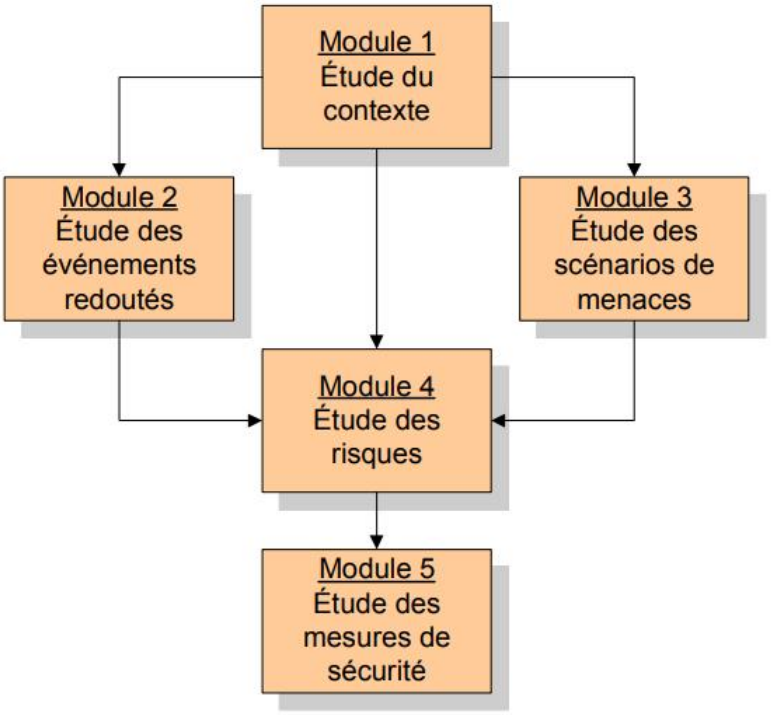

FIGURE 1.1: Les cinq modules de la méthode EBIOS[1]

Cette méthode sera détaillée dans le prochain chapitre.

MEHARI (MEthode Harmonisée d'Analyse de RIsques) :

C'est une méthode développée par le CLUSIF [12] depuis 1995, elle est dérivée des méthodes Melisa et Marion. Existant en langue française et en anglais, elle est utilisée par de nombreuses entreprises publiques ainsi que par le secteur privé. Elle respecte les lignes directrices tracées par la norme ISO/IEC 27005 et permet une intégration dans une démarche complète qui permet d'être utilisée aussi dans le cadre d'un Système de Management de la Sécurité de l'Information (ISO/IEC

12. Club de la sécurité de l'information français

27001 :2013) grâce à sa capacité à impliquer et sensibiliser la Direction de l'entité comme les responsables opérationnels.

La méthode MEHARI peut être réalisée selon plusieurs démarches, basées sur le même modèle de risque, intégrant l'évaluation des enjeux business, des menaces et des vulnérabilités attachées aux actifs dans des situations de risque.

La démarche générale de Mehari consiste en l'analyse des enjeux de sécurité : quels sont les scénarios redoutés ?, et en la classification préalable des entités du SI en fonction de trois critères de sécurité de base (confidentialité, intégrité, disponibilité). Ces enjeux expriment les dysfonctionnements ayant un impact direct sur l'activité de l'entreprise. Puis, des audits identifient les vulnérabilités du SI. Et enfin, l'analyse des risques proprement dite est réalisée.

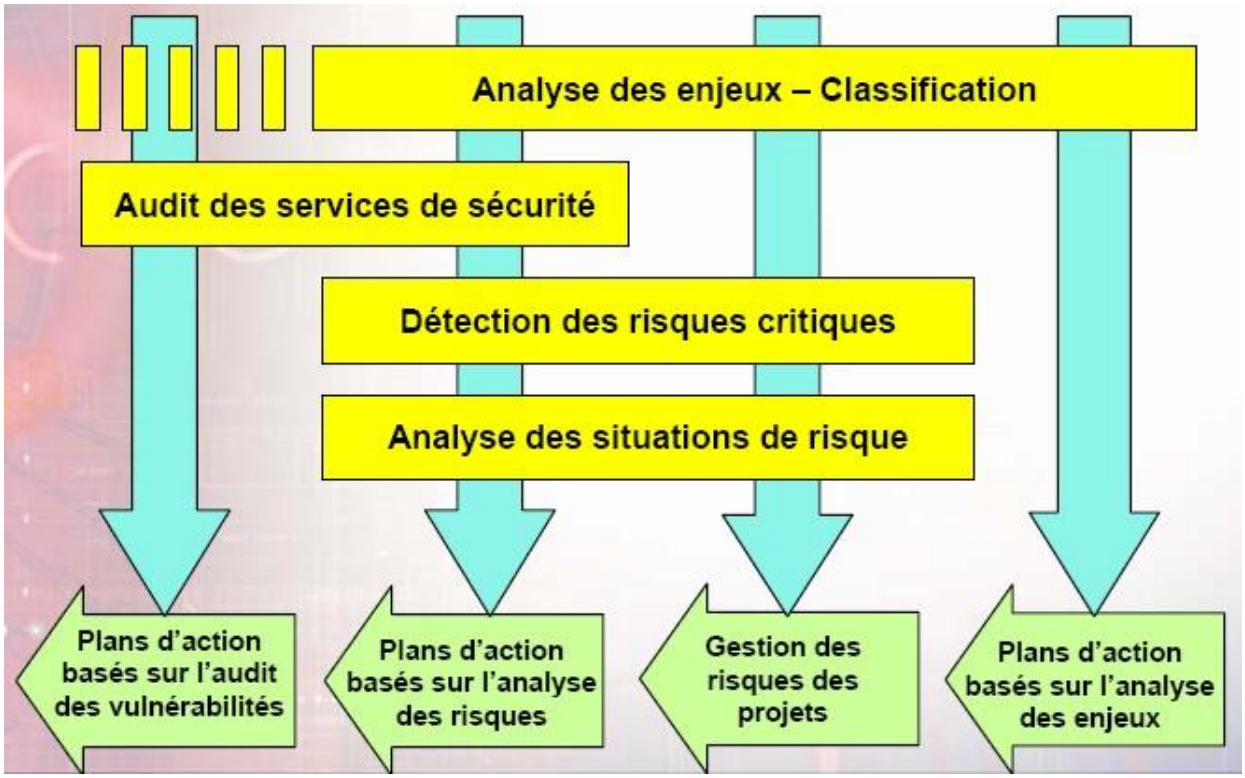

FIGURE 1.2: Schéma général de la méthode Mehari[2]

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) :

La méthode OCTAVE provient de l'université américaine Carnegie Mellon University. Celle-ci est réputée pour ses travaux en matière de sécurité informatique. OCTAVE fut créé en 1999 et une deuxième version parut en 2001. De plus, une version allégée nommée OCTAVE-S fut présentée en 2003.

Elle est utilisée dans les grandes entreprises (plus de 300 employés) et fournit les lignes directrices pour la conduite de la sécurité intérieure. Par contre OCTAVE-S a été développée pour les petites entreprises (moins de 100 employés) et suppose que les personnes chargées de l'évaluation des risques, les exigences de sécurité, les menaces et les pratiques de sécurité de l'organisation sont connues, et ils ne nécessitent pas de mener des entrevues, des sondages et des ateliers.

OCTAVE se spécialise dans l'évaluation des vulnérabilités et des menaces sur les actifs opérationnels importants d'une entreprise. L'un des objectifs principaux des créateurs était de mettre au point une méthode pouvant être pilotée à l'interne dans l'entreprise.

OCTAVE fournit un Framework d'évaluation des risques, composé de quatre phases :

1. Définir les paramètres : Établir les critères d'évaluation.
2. Définir les profils d'actifs : Établir les profils des actifs informationnels et identifier les intervenants.
3. Identifier les menaces : Identifier les domaines de préoccupation et les scénarios de menaces.
4. Identifier et atténuer les risques : Identifier les risques, analyser les risques, et choisir une approche face aux risques.

CRAMM (CCTA Risk Analysis and Management Method) :

Cramm est une méthode d'analyse de risque, conforme aux normes BS7799 et ISO 17799. C'est une méthode exhaustive assez lourde, réservée aux grandes entreprises puisqu'elle recourt à près de 3 000 points de contrôle. Elle possède deux variantes : Cramm Express et Cramm Expert.

Des logiciels sont fournis avec la méthode à des fins de simulation, de reporting et de suivi des mesures de sécurité.

La méthode Cramm est composée de 3 phases :

1. Identification de l'existant
2. Évaluation des menaces et des vulnérabilités
3. Choix des remèdes

FIGURE 1.3: Démarche générale de la méthode Cramm[2]

De nombreuses méthodes d'analyse des risques existent, certaines simples d'utilisation, avec parfois des outils logiciels simplifiant l'utilisation. D'autres méthodes sont réservées à des grands comptes du fait de leur complexité et des ressources humaines impliquées. le choix de la méthode se fait selon la méthode qui s'applique le mieux à l'entreprise.

Conclusion Le chapitre actuel présente quelques notions de base qu'il faut savoir pour pouvoir élaborer une PSSI, le chapitre suivant présente les différents méthodes et outils du processus de réalisation.

Chapitre 2

Cadre méthodologique

Dans ce chapitre on va préciser les différents choix pris, la démarche adoptée afin d'élaborer la PSSI et les techniques de recueil d'informations choisies.

2.1 Le choix du thème de recherche

La sécurité au sein des organismes présente des avantages et correspond à une obligation juridique et sociale. Les entreprises apprécient bien le faite qu'être sécurisé contribue à réduire toute malveillance ou accident pouvant toucher à leur système.

Donc la sécurité est un sujet vraiment important, mais malheureusement il est assez négligé par la plupart des entreprises algériennes. Le choix de ce sujet est fait par une conscience de l'utilité de la sécurité pour une entreprise, précisément la sécurité des systèmes d'information vue que le SI englobe toutes les entités touchant à l'information qui est le trésor d'une entreprise.

NAFTAL se considère comme un géant dans son domaine en Algérie, et comme son département de sécurité au niveau de la direction générale est très récent, cette entreprise a besoin d'élaborer la PSSI qui sera le premier référentiel de sécurité de l'entreprise. Ceci constitue un thème important pour répondre à un besoin parmi les besoins actuels de NAFTAL.

D'un autre part, il ya la volonté d'approfondir mes connaissances sur la sécurité au sein des entreprises grâce à l'actualité du thème et son rôle primordial dans la vie des organismes.

2.2 Objectif de la recherche

Le but de notre recherche consiste à mettre en place une PSSI, à travers notre étude nous avons fixé les objectifs suivants :

- Connaitre réellement les besoins de sécurité de NAFTAL.
- Réfléchir aux solutions convenables, pour améliorer ou maintenir un certain niveau de sécurité.
- Connaitre les méthodes à suivre pour pouvoir élaborer la PSSI.
- Doter Naftal de son document de référence en matière de SSI de l'organisme.

2.3 Choix du terrain de recherche

Après plusieurs recherches, le choix du terrain est tombé sur l'entreprise NAFTAL pour plusieurs raisons : tout d'abord son désir actuel est rapide de l'élaboration d'une PSSI vu qu'elle vient de créer son département de sécurité, et être dans une cellule spécialisée dans la sécurité est mieux qu'être perdu entre les différents services. Ainsi que le SI de NAFTAL est très intéressant en termes de variété, ce qui rend la recherche large et le travail plus utile.

2.4 Méthode de recherche

Dans notre travail, on a adopté la méthode de recherche qualitative, qui vise à comprendre le phénomène d'étude et d'établir le sens des propos recueillis, ou de comportements observés, et de décrire les différents aspects liés à notre thème, où on a compris le phénomène d'étude par un processus personnel par aller au contact des acteurs, faire de l'observation participante, collecter les données au fur et à mesure du travail. On a cherché les avis des acteurs participant au SI de NAFTAL et essayé de les comprendre dans un contexte sécuritaire.

Notre méthode de recherche se caractérise par une visée compréhensive, qui se donne pour objectif de comprendre l'action dans une situation.

2.5 Outils de collecte de données

Dans le but de pouvoir rassembler les informations relatives à notre thème de recherche et réaliser le travail, on a eu recours aux techniques de recherche suivantes :

1. La documentation :

La recherche documentaire est une méthode de collecte de données qu'on utilise dès qu'on a à rédiger un mémoire ou une thèse. Durant notre travail, on a consulté plusieurs documents de différentes sources.

- Des documents internes se trouvant dans la bibliothèque (Documentation) de NAFTAL qui contient les différentes données existantes et les informations

relatives à l'entreprise.

- Des documents externes concernant la méthodologie d'élaboration d'une PSSI (livres, articles, papiers, rapports, thèses) et surtout les guides d'application des différentes méthodes.

- Et enfin le guide méthodologique promu par l'ENSM pour la rédaction du mémoire écrit.

2. L'observation :

Tout travail scientifique se fait par une observation de la réalité, qui permet d'accéder directement aux faits, de la recherche du sujet jusqu'à la fin de travail.

Dans notre travail, on a opté pour l'observation non-participante, où on était des observateurs externes qui ne font pas partie des membres des groupes observés. toutes les remarques étaient faites à distance durant les visites effectuées. Le temps passé durant le stage nous a permis de comprendre la communauté de l'entreprise et observer les composants de son système d'information. Durant cette période, on a procédé à des entretiens libres, informels, sur toutes sortes de questions. C'était une bonne méthode pour apprendre quelque chose des véritables processus décisionnels, par opposition aux procédures formelles.

3. Les entretiens :

L'entretien est une situation de communication orale, l'un est l'enquêteur et l'autre l'enquêté. Durant notre travail, l'entretien était le moyen le plus efficace et rapide, surtout que les enquêtés étaient des personnes du Département Sécurité & Conformité et de la Direction Centrale des Systèmes d'information.

les entretiens effectués étaient des entretiens semi-directifs individuels et en groupe en vue d'orienter l'enquête dans le sens et l'objectif de l'entretien et avoir le maximum des informations plus détaillées relatives au sujet.

Les questions posées étaient assez précisément formulées, et des nouvelles questions sont posées dans chaque étape de travail. par exemple les premiers entretiens étaient sur le sujet en général, on parlais du système d'information de NAFTAL et de leur besoins de sécurité.

Les questions étaient plus ou moins nombreuses, pas toutes préparées à l'avance avec un guide souple et une possibilité de discuter de thèmes non planifiés.

2.6 Méthodologie et normes utilisées

Dans cette section, on va parler de la méthode suivie pour élaborer notre PSSI. Les références de cette sections sont les suivantes[3, 18, 19, 4] :

2.6.1 Méthodologie d'élaboration d'une PSSI

L'élaboration d'une PSSI requiert une approche globale, considérant non seulement les domaines techniques tels que la sécurité logique, la sécurité des matériels informatiques et la sécurité des réseaux, mais aussi les domaines non techniques tels que la sécurité physique, la sécurité liée aux aspects humains et la sécurité organisationnelle.

Le guide d'élaboration de PSSI qu'on a suit se présente sous forme de plusieurs documents par la DCSSI, actuellement l'ANSSI.

L'ANSSI :

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale. L'ANSSI remplace la Direction centrale de la sécurité des systèmes d'information (DCSSI), créée par décret en juillet 2001. L'agence assure la mission d'autorité nationale en matière de sécurité des systèmes d'information. L'ANSSI, service à compétence nationale, assure la sécurité des systèmes d'information gouvernementaux et est aussi chargée d'une mission de conseil et de soutien aux administrations et aux entreprises, avec une mission renforcée au profit des opérateurs d'importance vitale (OIV).[20]

Présentation générale de la démarche :

La démarche, qui est menée sous la forme d'un "projet PSSI", se base sur le référentiel de l'organisme (schéma directeur, meilleures pratiques, directives internes...) et une analyse des risques SSI préalable fournit en effet les éléments permettant d'effectuer et de justifier les choix, de légitimer l'action et de garantir la cohérence avec le contexte particulier de l'organisme.

Cette démarche est décomposée en quatre phases successives, comme présente la figure suivante :

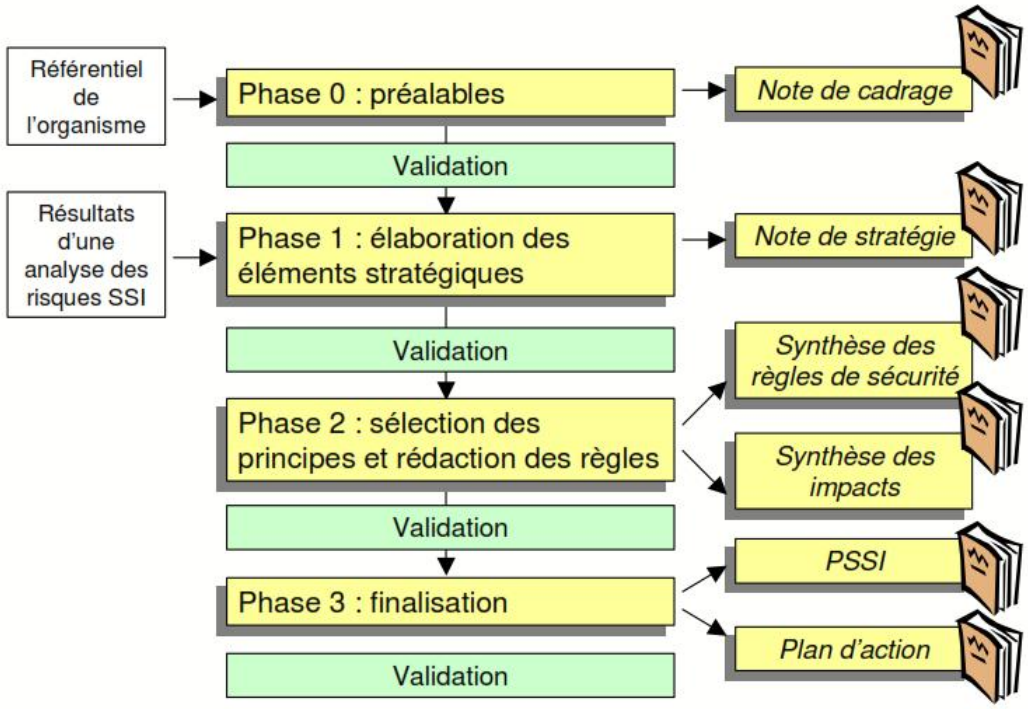

FIGURE 2.1: Démarche générale d'élaboration de PSSI selon l'ANSSI[3]

Phase 0 : Préalables La phase 0 est un préalable à la démarche d'élaboration. Elle consiste à organiser le projet PSSI (chef de projet, comité de pilotage, calendrier, disponibilité d'un budget et d'objectifs de sécurité...) et à constituer le référentiel (du système d'information, de la SSI, des aspects déontologique et contractuels). Une note de cadrage formalise les informations nécessaires pour cette phase.

Phase 1 : Élaboration des éléments stratégiques La phase 1 permet de recueillir l'ensemble des éléments stratégiques nécessaires à la rédaction d'une note de stratégie de sécurité qui servira de base à l'élaboration de la PSSI et à toute autre étude de sécurité. Ces éléments stratégiques forment le périmètre que doit couvrir la PSSI. Ils sont constitués des enjeux et des orientations stratégiques en matière de SSI, de la prise en compte des aspects légaux et réglementaires, de l'élaboration d'une échelle de besoins, de l'expression des besoins de sécurité généraux, de l'identification des éléments menaçants et de leurs méthodes d'attaque.

Donc les éléments stratégiques seront :

1. Le périmètre
2. Les enjeux et les orientations stratégiques
3. Les lois et les règlements applicables

4. Une échelle de besoins de sécurité
5. Les besoins de sécurité
6. Les origines des menaces

C'est dans cette phase où intervient la partie d'analyse des risques qui est la partie la plus importante. L'analyse des risques a pour effet de déterminer plus facilement les éléments stratégiques, de déterminer les critères de sélection des principes de sécurité à développer et de guider l'élaboration des règles de sécurité.

Phase 2 : Sélection des principes et rédaction des règles La phase 2 consiste à choisir les principes de sécurité à prendre en compte dans le référentiel du guide et à les décliner en règles de sécurité sur la base des éléments stratégiques. Des synthèses des règles de sécurité (adressée au comité de pilotage) et des impacts organisationnels et financiers (adressés à la Direction générale) doivent être rédigées.

C'est l'expression des besoins de sécurité qui contribue au choix des principes de sécurité qui peuvent être parmi les neuf principes suivants :

1. Sensibilisation
2. Responsabilité
3. Réaction
4. Éthique
5. Démocratie
6. Évaluation des risques
7. Conception et mise en œuvre de la sécurité
8. Gestion de la sécurité
9. Réévaluation

Phase 3 : Finalisation L'objectif de cette phase est de produire le document validé exprimant la Politique de Sécurité des Systèmes d'Information de l'organisme. Ce document devra être validé et signé par la hiérarchie. Puis assurer l'application de la PSSI au système d'information de l'organisme.

2.6.2 Méthode d'analyse des risques

Comme mentionné précédemment, l'élaboration d'une PSSI se base principalement sur une analyse des risque. Pour la réalisation de cette dernière, on a choisi de travaillé avec la méthode EBIOS. Ce choix a été fait selon plusieurs critères :

1. EBIOS est faite à l'ANSSI par un club qui s'appelle club EBIOS, et se considère comme un outil complémentaire aux guides de PSSI.

2. La démarche méthodologique proposée par EBIOS apporte une vision globale et cohérente de la sécurité des systèmes d'information.

3. Promue par l'ANSSI et reconnue par les administrations françaises, EBIOS est aussi une référence dans le secteur privé et à l'étranger.

4. Plusieurs sociétés de conseil ont adopté la démarche EBIOS dans leur rôle d'assistance aux maîtrises d'ouvrage.

5. La qualité de la documentation : des guides simples et bien détaillés, ce qui rend la méthode facile à comprendre et à appliquer.

6. Un seul et même outil permet de réaliser différentes démarches sécuritaires : l'élaboration d'un schéma directeur SSI, pour réaliser les premières étapes d'une politique SSI et d'un tableau de bord SSI, pour contribuer à la rédaction d'un Profil de Protection (PP), pour rédiger une FEROS ou encore pour tout autre cahier des charges SSI.

7. la compatibilité avec des normes internationale ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001.

8. Une méthode populaire et très connue.

Présentation de la méthode EBIOS :

EBIOS est une méthode qui permet d'analyser des risques, de les évaluer et de les traiter dans le cadre d'une amélioration continue, selon une démarche itérative de cinq modules. La spécificité d'EBIOS réside dans sa souplesse d'utilisation. Il s'agit d'une véritable boîte à outils, dont les activités à réaliser, leur niveau de détail et leur séquencement seront adaptés à l'usage désiré.

Les cinq modules d'EBIOS :

1. Étude du contexte
2. Étude des événements redoutés
3. Étude des scénarios de menaces
4. Étude des risques
5. Étude des mesures de sécurité

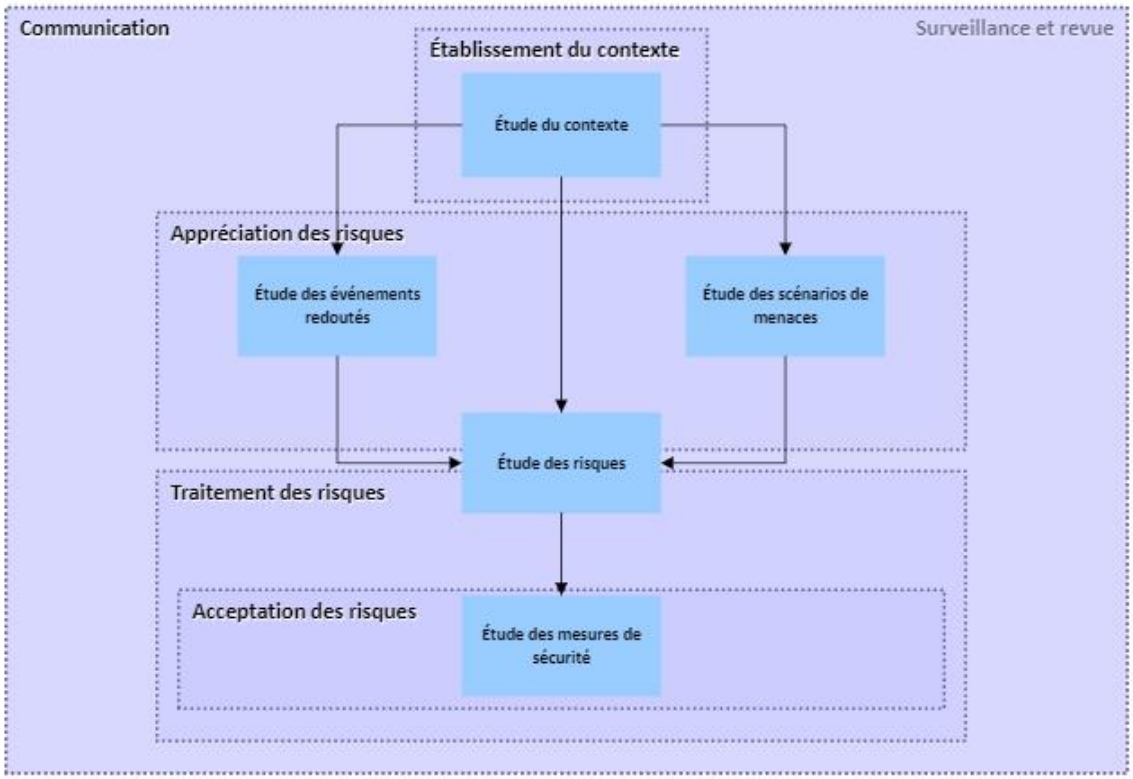

FIGURE 2.2: Démarche générale d'élaboration de PSSI selon l'ANSSI

Module 1 : Étude du contexte Ce module a pour objectif de collecter les éléments nécessaires à la gestion des risques, afin qu'elle puisse être mise en œuvre dans de bonnes conditions, qu'elle soit adaptée à la réalité du contexte d'étude et que ses résultats soient pertinents et utilisables par les parties prenantes. Il permet notamment de formaliser le cadre de gestion des risques dans lequel l'étude va être menée. Il permet également d'identifier, de délimiter et de décrire le périmètre de l'étude.

Le module comprend les activités suivantes :

1. **Définir le cadre de la gestion des risques :** circonscrire le périmètre d'étude et de définir le cadre dans lequel la gestion des risques va être réalisée.

2. **Préparer les métriques :** fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques. Elle peut être commune à plusieurs études.

3. **Identifier les biens :** identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.

Module 2 : Étude des événements redoutés Ce module a pour objectif d'identifier de manière systématique les scénarios génériques que l'on souhaite éviter concernant le périmètre de l'étude : les événements redoutés. Les réflexions sont menées à un niveau davantage fonctionnel que technique (sur des biens essentiels et non sur des biens supports).

À l'issue de ce module, les événements redoutés sont identifiés, explicités et positionnés les uns par rapport aux autres, en termes de gravité et de vraisemblance par les deux activités suivantes :

1. **Analyser tous les événements redoutés :** identifier et à estimer les événements redoutés pour chaque critère de sécurité et chaque bien essentiel identifié.

2. **Évaluer chaque événement redouté :** juger de l'importance des événements redoutés en les hiérarchisant selon les critères de gestion des risques retenus.

Module 3 : Étude des scénarios de menaces Ce module a pour objectif d'identifier de manière systématique les modes opératoires génériques qui peuvent porter atteinte à la sécurité des informations du périmètre de l'étude : les scénarios de menaces. Les réflexions sont menées à un niveau davantage technique que fonctionnel (sur des biens supports et non plus des biens essentiels).

À l'issue de ce module, les scénarios de menaces sont identifiés, explicités et positionnés les uns par rapport aux autres en termes de vraisemblance par les deux activités suivantes :

1. **Analyser tous les scénarios de menaces :** identifier les scénarios de menaces pour chaque critère de sécurité et chaque bien support identifié et à les estimer en termes de vraisemblance.

2. **Évaluer chaque scénario de menace :** juger de l'importance des scénarios de menaces en les hiérarchisant selon les critères de gestion des risques retenus.

Module 4 : Étude des risques Ce module a pour objectif de mettre en évidence de manière systématique les risques pesant sur le périmètre de l'étude, puis de choisir la manière de les traiter en tenant compte des spécificités du contexte. Les réflexions sont menées à un niveau davantage fonctionnel que technique.

En corrélant les événements redoutés avec les scénarios de menaces susceptibles de les engendrer, ce module permet d'identifier les seuls scénarios réellement pertinents vis-à-vis du périmètre de l'étude. Il permet en outre de les qualifier explicitement en vue de les hiérarchiser et de choisir les options de traitement adéquates. À l'issue de ce module, les risques sont appréciés et évalués, et les choix

de traitement effectués par les deux activités suivantes :

1. **Apprécier les risques :** mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.

2. **Identifier les objectifs de sécurité :** choisir la manière dont chaque risque devra être traité au regard de son évaluation.

Module 5 : Étude des mesures de sécurité Ce module a pour objectif de déterminer les moyens, de traiter les risques et de suivre leur mise en œuvre, en cohérence avec le contexte de l'étude. Les réflexions sont préférentiellement menées de manière conjointe entre les niveaux fonctionnels et techniques.

Il permet de trouver un consensus sur les mesures de sécurité destinées à traiter les risques, conformément aux objectifs précédemment identifiés, d'en démontrer la bonne couverture. Le module comprend les activités suivantes :

1. **Formaliser les mesures de sécurité à mettre en œuvre :** déterminer les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés.

2. **Mettre en œuvre les mesures de sécurité :** élaborer et de suivre la réalisation du plan de traitement des risques par les mesures de sécurité afin de pouvoir prononce l'homologation de sécurité.

C'est dans ce module où on fait appel aux normes qui contient des orientations ou des mesures à appliquer. Dans notre travail, on a choisi de faire recours à l'ISO 27001 car :

- L'entreprise NAFTAL a exigé l'utilisation de la norme ISO 27001.

- La norme ISO 27001 est la seule norme auditable internationalement qui définisse les exigences pour un système de gestion de la sécurité de l'information.

Donc tout objectif et mesure dans la PSSI est pris de l'ISO 27001.

2.6.3 Norme ISO 27 001

La norme internationale ISO/IEC 27001, Publiée en octobre 2005 et révisée en 2013, par l'Organisation Internationale pour la Standardisation (ISO), son titre est "Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences", expose les exigences relatives aux systèmes de management de la sécurité des informations (SMSI) [1], et est la norme la plus célèbre de la famille ISO/IEC 27000. Elle a été élaborée pour fournir un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SMSI.

Spécificités de la norme 27001 :

1. ISO 27001 est harmonisée avec d'autres référentiels de systèmes de management tels qu'ISO 9001 et ISO 14001.
2. ISO 27001 met l'accent sur le processus d'amélioration continue de votre système de management de la sécurité des données.
3. La norme clarifie les exigences en matière de documentation et d'enregistrements.
4. Elle comprend un processus d'évaluation et de management des risques basé sur le modèle PDCA (Plan, Do, Check, Act).

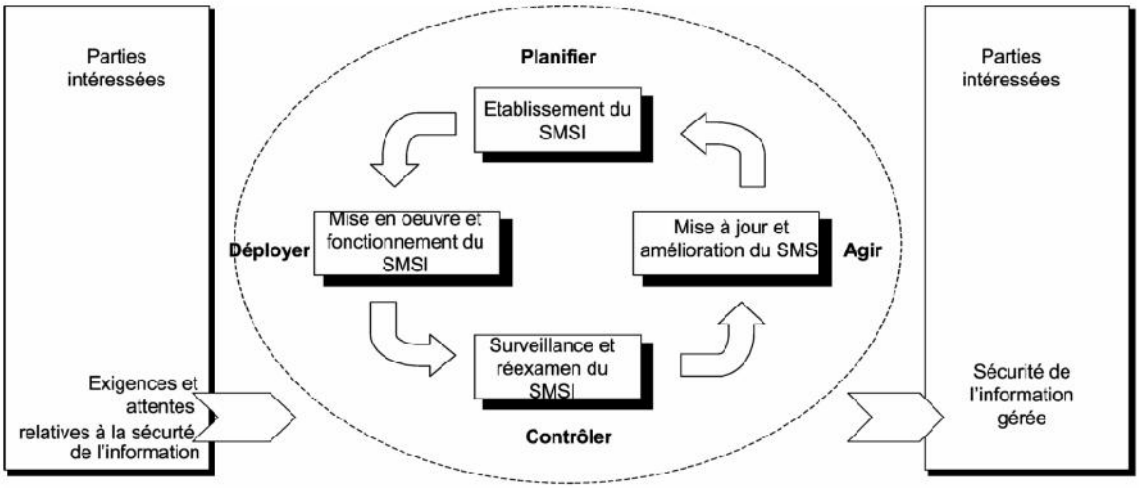

FIGURE 2.3: Modèle PDCA appliqué aux processus SMSI [4]

1. partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information

Domaine d'application : L'ISO 27001 couvre tous les types d'organismes (par exemple entreprises commerciales, organismes publics, organismes à but non lucratif). Elle spécifie les exigences relatives à la mise en œuvre des mesures de sécurité adaptées aux besoins de chaque organisme ou à leurs parties constitutives. Les exigences fixées dans cette norme internationale sont génériques et prévues pour s'appliquer à tout organisme, quels que soient son type, sa taille et sa nature.

La structure de la norme :

1. **Phase d'établissement (Plan) :** Etablir la politique, les objectifs, les processus et les procédures du SMSI relatives à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux de l'organisme.

2. **Phase d'implémentation (Do) :** Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI.

3. **Phase de maintien (Check) :** Evaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique et rendre compte des résultats à la direction pour réexamen.

4. **Phase d'amélioration (Act) :** Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne du SMSI et de la revue de direction, ou d'autres informations pertinentes, pour une amélioration continue dudit système.

Conclusion : Le chapitre actuel présente le cadre méthodologique adopté pour notre mémoire, le détail du processus de réalisation et le résultat obtenu seront dans le chapitre suivant.

Chapitre 3

Mise en place de la PSSI et Résultat

Ce chapitre présente la description de la solution proposée à notre problématique dont le but est de sécuriser tout le système d'information de NAFTAL. Ce chapitre comprend les étapes faites pour la réalisation de la PSSI et quelques exemples du résultat.

3.1 Phase 1 : Préalables

La première phase est une phase préliminaire qui doit permettre la présentation du projet au niveau des responsables et de faire valider ainsi ses objectifs et les moyens qu'il convient d'y consacrer. Et comme mon promoteur (tuteur au sein de l'entreprise) est le responsable de sécurité, toutes les étapes ont été discuté et validé avec lui.

L'objectif de cette phase est de définir les objectifs et moyens à mettre en œuvre pour l'élaboration de la PSSI et constituer le référentiel documentaire.

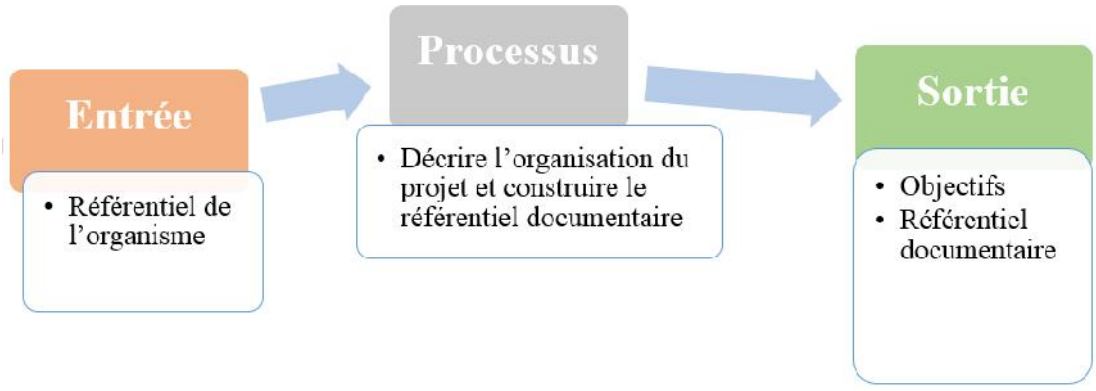

FIGURE 3.1: Phase 1 : Préalables

Donc dans cette phase, on a discuté le projet dans sa globalité, définit les objectifs qu'on veut atteindre à la fin du travail, et surtout organisé les tâches par définir un plan de travail à suivre durant la période du stage. Puis on a identifié le référentiel documentaire de l'organisme (SI, SSI, aspects déontologiques et contractuels) qui servira de base à la suite de la démarche.

Le référentiel documentaire est important car il reflète la particularité de l'organisme, et la réalisation d'une politique de sécurité doit se construire de façon adaptée au contexte particulier de chaque organisme. La base documentaire peut regrouper par exemple tout ce qui est dans cette liste ou plus :

1. Le référentiel du ou des systèmes d'information.

2. Le référentiel de sécurité interne :
   - Schéma directeur informatique et SSI ;
   - Analyses de risques ;
   - Résultats d'audits de sécurité...etc.

3. Obligations contractuelles des prestataires ou partenaires.

4. Obligations contractuelles auxquelles l'organisme s'est engagé vis à vis de ses clients ou partenaires spécifiques :
   - Contrat de coopération ou de partenariat avec d'autres organismes ;
   - Contrat de prestation de service à d'autres organismes ;
   - Conditions de garantie applicables aux produits ou services proposés ;
   - Conventions bilatérales (comme par exemple des conventions de preuve)...etc.

5. Grands principes d'éthique :
   - au plan national, la protection de la vie privée ;
   - les clauses particulières dans les contrats régissant les relations de l'organisme avec ses partenaires et/ou clients ;
   - les codes éthiques des métiers des technologies de l'information dont une liste des références est proposée en annexe...etc.

6. aspects légaux et réglementaires :
   - Les textes législatifs majeurs, qui sont décrits en annexe, dont la loi informatique et liberté, la loi sur la protection des droits d'auteur, la loi relative à la fraude informatique, la loi sur le secret des communications, les lois sur la cryptologie ;
   - Les textes et recommandations énoncées au plan national et international dont une liste de références se trouve en annexe ;
   - Le règlement intérieur, qui peut également contenir des exigences concernant le système d'information ;

- La préservation des intérêts vitaux de l'État sur le plan de la protection des informations sensibles relevant ou non du secret de défense ;
- Le droit d'auteur ;
- La propriété intellectuelle et du copyright ;
- L'utilisation de moyens cryptographiques ;
- La protection des consommateurs ;
- Obligations réglementaires spécifiques à l'organisme concerné...etc.

3.2 Phase 2 : Élaboration des éléments stratégiques

Après avoir construit le référentiel documentaire, on va l'utiliser pour élaborer les éléments stratégique à l'aide d'une analyse de risques en utilisant la méthode EBIOS précédemment définit.

Donc l'objectif de cette phase est de déterminer les axes stratégiques et les premières grandes orientations à partir desquelles sera déclinée la PSSI. Pour cela, on va obligatoirement identifier et prendre en compte le périmètre d'étude, le contexte, les enjeux et orientations stratégiques, le référentiel réglementaire, l'échelle de besoins, les besoins de sécurité des biens à protéger et les origines des menaces.

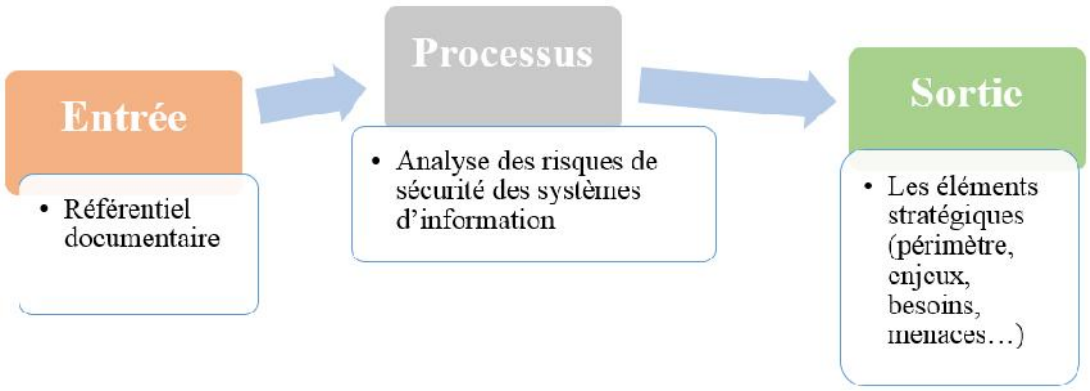

FIGURE 3.2: Phase 2 : élaboration des éléments stratégiques

Les étapes de cette phase étaient comme suit et les éléments stratégiques étaient extraites au fur et à mesure de l'analyse :

3.2.1 Description du contexte général

La première étape était la description du contexte, cette description a commencé par une présentation de l'organisme dont le but de faciliter l'intégration de la gestion des risques dans la culture, la structure et les processus de l'organisme en mettant en évidence les éléments qu'il conviendra de considérer dans la réflexion de sécurité de l'information.

La présentation contient les informations suivantes :
- La description générale de l'organisme ;
- Les aptitudes en termes de ressources (capital, personnels, technologies...etc) ;
- Les missions (ce que l'organisme doit faire) ;
- Les valeurs (ce que l'organisme fait bien) ;
- Les métiers (ce que l'organisme sait faire) et la culture ;
- L'organisation, et les principaux processus métiers, rôles et responsabilités ;
- Les politiques, les objectifs et les stratégies mises en place pour les atteindre.

Autres éléments peuvent être ajoutés comme :
- Les systèmes d'information, flux d'information et processus de prise de décision ;
- Les normes, principes directeurs et modèles adoptés par l'organisme ;
- Les relations avec les parties prenantes internes ;
- La forme et l'étendue des relations contractuelles ;
- Des éléments de conjoncture internes ;
- Des éléments de contexte socioculturel.

3.2.2 Délimitation du périmètre de l'étude et ses enjeux

Dans cette deuxième partie, on a circonscrit le périmètre d'étude au sein du contexte général qu'on a décrit précédemment, c-à-d la partie concernée par l'étude. On a commencé par une étude globale de l'organisme mais on s'intéresse maintenant à son système d'information, dont on précise le sous-ensemble constituant le système-cible de l'étude et ses enjeux.

Le périmètre qu'on a défini correspond à l'ensemble du système d'information de l'entreprise. Il comprend l'ensemble des moyens humains, techniques et organisationnels permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et tiers de l'entreprise, quelle que soit la forme sous laquelle elles sont exploitées (électroniques, imprimées, manuscrites, vocales, images, ...etc). Donc notre PSSI va être appliquée aux actifs matériels, immatériels et aux ressources humaines.

Ce périmètre inclut :

En terme de ressources humaine :

- l'ensemble des personnels autorisés à accéder, utiliser ou traiter au niveau fonctionnel ou technique, des informations ou des biens du système d'information de NAFTAL.
- les tiers définis comme étant toute personne morale ou physique, dès lors qu'ils utilisent les systèmes d'information de NAFTAL ou que leurs propres systèmes sont reliés aux réseau informatique de NAFTAL.

En terme d'actifs immatériels :

- l'ensemble du patrimoine informationnel associé à NAFTAL :
  — les connaissances issues de ses activités de recherche et développement
  — l'ensemble des bases de données liées à l'administration, la gestion, la recherche et aux ressources humaines.
  — les données associées à la gestion de sécurité des personnes et des biens (contrôle d'accès, hygiène et sécurité).
- les composants logiciels du système d'information.

En terme d'actifs matériels :

tous les composants matériel des systèmes d'information :

- Les postes de travail (PC, portables, stations de travail...)
- les réseaux de communication.
- les serveurs hébergeant les données et les applications
- Bâtiments et locaux hébergeant les ressources humaines, les archives et les moyens informatiques.

Enjeux : Ce périmètre du système peut être en face aux plusieurs vulnérabilités qui le menacent. La perte, la manipulation ou le vol d'informations...etc. Pour faire face à ces risques, il est nécessaire de surmonter les enjeux correspondants, et donc assurer les DICT (Disponibilité, Intégrité, Confidentialité et la Traçabilité) en plus de ces 4, Il peut être pertinent d'en ajouter d'autres tels que l'authentification.

3.2.3 Identification des biens essentiels et biens supports

Pour être plus précis, on a déterminé les entités cibles qui composent notre périmètre. Ces entités présentent les biens essentiels et les biens supports. On a commencé par les **biens essentiels** qui représentent toute fonction ou information jugée comme importante pour l'organisme. C'est le patrimoine informationnel, ou les "biens immatériels", que l'on souhaite protéger, c'est-à-dire ceux pour lesquels le non respect de la disponibilité, de l'intégrité, de la confidentialité, voire d'autres critères de sécurité, mettrait en cause la responsabilité du dépositaire, ou causerait

un préjudice à eux-mêmes ou à des tiers.

Ci-après une liste de quelques services parmi les services de NAFTAL qui se considèrent comme importants et qui doivent être inclut dans la PSSI :

- Service de messagerie sur Exchange,
- Portail + Site web,
- Service de paiement électronique,
- Service de gestion de Stock de carburants,
- Service de gestion des ressources humaines,
- Service de gestion et de distribution des BAG,
- Service de réplication des données critiques vers un site de secours,
- Service de sauvegarde et d'archivage et de reprises de données,_
- Service de vidéoconférence interne,
- Service de gestion et de partage électronique des fichiers et de gestion de contenu sur SharePoint,
- Service de monitoring et de surveillance du réseau WAN et des équipements LAN.

Cette liste est non-exhaustive, d'autres services peuvent y être ajoutés.

Quant aux **biens supports**, C'est les Biens sur lesquels reposent des biens essentiels. On distingue notamment les systèmes informatiques, les organisations et les locaux. Donc ça concerne des composants du système d'information, qu'il s'agisse de biens techniques ou non techniques, supports aux biens essentiels précédemment identifiés. On note que ces biens supports possèdent des vulnérabilités que des sources de menaces pourront exploiter, portant ainsi atteinte aux biens essentiels.

ça se peut être un matériel, logiciel, réseau, site, personnel ou même une organisation. parmi ces biens on peut citer :

- Internet et Intranet,
- Réseau local (Ethernet),
- Locaux de l'entreprise,

- Réseau WIFI,
- Site web de NAFTAL (www.naftal.dz),
- Progiciels, logiciels et application métier (ex : SharePoint),
- Matériel fixe (ex : Ordinateur Bureautique, Serveurs),
- Périphérique de traitement (ex : imprimante),
- Outils de communication (ex : ligne téléphonique),
- Systèmes d'exploitations (ex : Unix, Windows),
- Utilisateurs,
- Clients, Fournisseurs, Partenaires.

3.2.4 Expression des besoins de sécurité

Définition des critères de sécurité :

On a choisi d'évaluer notre SI sur la base d'un certain nombre de critères de sécurité. On distingue généralement les quatre principaux critères de sécurité suivants :

- **La disponibilité** qui consiste à garantir l'accès à un service ou à une ressource.
- **L'intégrité** qui consiste à s'assurer que les données n'ont pas été altérées.
- **La confidentialité** qui consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs concernés.
- **La traçabilité** qui consiste à garantir qu'aucun des correspondants ne pourra nier la transaction.

l'élaboration d'une échelle de besoins

Pour l'échelle de besoins qui est une échelle de mesure utile à l'expression des besoins de sécurité pour les domaines d'activités identifiés dans la PSSI ou les fonctions et informations identifiées dans les études de sécurité dans le périmètre de la PSSI, on a choisi de la faire comme le fait la majorité des études établies :

Échelle de besoin	Disponibilité	Intégrité	Confidentialité	Traçabilité
Niveau 1	Le bien peut être indisponible sans limite	Absence de besoin d'intégrité sans conséquences (Ex : aucune vérification)	Absence de besoin de confidentialité, bien qui peut être connu de tout public (Ex : données publiques)	Le bien ne requiert pas d'auditabilité. Aucun besoin de génération de traces.
Niveau 2	Le bien peut être indisponible pendant une durée importante mais limitée	Le bien accepte une perte importante d'intégrité (Ex : vérification des données, sans validation)	Le bien ne peut être accessible qu'à des groupes de personnes, identifiés et validés par une personne morale.	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori.
Niveau 3	Le bien peut être indisponible pendant une courte durée (Ex : arrêt du réseau, de la messagerie, données vitales non disponibles)	Le bien n'accepte qu'une faible perte d'intégrité (Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.)	Le bien ne doit être accessible qu'à des groupes de personnes, identifiés, qualifiés et validés par une personne morale pour un objectif ou une finalité donné.	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori et être imputables à leurs auteurs.
Niveau 4	Le bien ne doit pas être indisponible (Ex : système de sécurité)	L'intégrité totale du bien est nécessaire (Ex : données avec au moins deux niveaux de validation et de contrôle différents)	Le bien ne doit être accessible qu'à des personnes habilitées et nominativement identifiées(Ex : données secret défense.)	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori et être imputables à leurs auteurs de la façon la plus irréfutable possible.

TABLE 3.2: Echelles de besoins de sécurité

3.2.5 Étude des menaces et vulnérabilité

Dans cette étape, on a déterminé les sources de menaces et les vulnérabilités pertinentes vis-à-vis du contexte particulier du périmètre de l'étude. On a réfléchi aux origines des risques en répondant à : qui ou quoi pourrait porter atteinte aux

besoins de sécurité exprimés et engendrer les impacts identifiés ? et à travers quelles vulnérabilités ?

Les menaces étaient variées entre des menaces passives [1] et d'autres actives [2]. Y avait des menaces dues aux accidents : incendies, inondations, pannes d'équipements, catastrophes naturelles...etc. et des menaces dues aux malveillances : vols d'équipements, copies illicites, sabotage matériel, attaques logiques, intrusion et écoute, actes de vengeance...etc.

Toutes ces menaces peuvent se réaliser à cause des vulnérabilités existantes au sein du SI, ces vulnérabilités sont regroupées en plusieurs familles : humaines, techniques et physiques. On peut nommer par exemple :

- **Humaines :** Une maladresse, malveillance, inconscience...etc.
- **techniques :** Surchauffe, usure, incidents liés au logiciel, Programme malveillant...etc.
- **physiques :** Non-redondance(données, logiciels..), manque de contrôle d'accès aux éléments physiques(bâtiments, salles informatiques...), mauvaise gestion des ressources, sinistres...etc.

3.3 Phase 3 : Sélection des principes et rédaction des règles

Dans cette troisième phase, on avait à déterminer les mesures de sécurité, pour cela on a commencé par faire une étude des risque afin de déterminer nos objectifs de sécurité qui se déclinent après à des règles de sécurité.

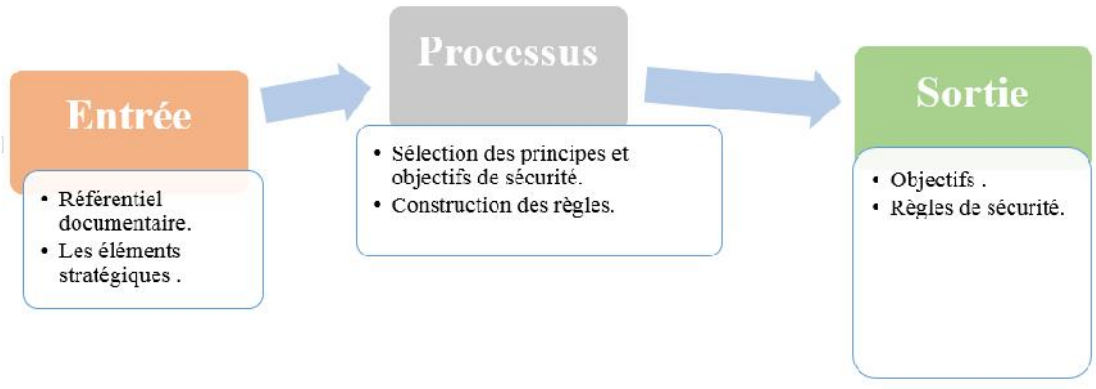

FIGURE 3.3: Phase 3 : sélection des principes et rédaction des règles

1. Menaces qui consistent à écouter ou copier des informations de manière illicite
2. Menaces qui consistent à altérer des informations ou le bon fonctionnement d'un service

3.3.1 Étude des risques

L'étude des risque a été réalisée par les deux activités suivantes :

1. Appréciation des risques

Cette activité a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude. pour cela on a :

— Déterminé **les événements redoutés :** c'est les événements indésirables qui peuvent remplacer un événement ordinaire ou normal. la réflexion à ces événements est menée à un niveau davantage fonctionnel que technique, qui veut dire que ces événements touchent aux biens essentiels précédemment déterminés.

— Déterminé**les scénarios de menaces :** qui concernent les biens supports, c'est les scénarios qui peuvent engendrer les événements redoutés et provoquer un risque.

Après avoir terminé les deux activités précédentes, on les a combiné (événements redoutés et scénarios de menaces) pour avoir notre liste de risques potentiels qui seront ensuite triés selon leur gravité. Il y a des petits risques tolérables, des risques moyens qui peuvent être graves et des risques catastrophiques. Ces risques vont être traités de différentes manières : soit les accepter, les rejeter, les transférer ou les réduire par la mise en place des mesures de sécurité. Les risques qu'on va traiter sont seulement les risques qu'on peut les réduire avec des mesures de sécurité.

2. Identification des principes et objectifs de sécurité

Cette activité est complémentaire de la partie précédente pour la détermination des règles. Une fois les risques sont déterminés, on peut facilement savoir les principes qu'il conviendra de développer et instancier en règles de sécurité lors de la tâche suivante et les objectifs qu'on veut atteindre en termes de sécurité. ces principes sont décrits à travers les lignes directrices suivantes :

- Sensibilisation
- Responsabilité
- Réaction
- Éthique
- Démocratie
- Évaluation des risques
- Conception et mise en œuvre de la sécurité
- Gestion de la sécurité
- Réévaluation

Tandis que les objectifs qu'on a déterminé étaient liés aux titres suivants :

- Politique de sécurité de l'information,
- Organisation interne,
- Tiers,
- Responsabilités relatives aux actifs,
- Classification des informations,
- Sécurité liée aux ressources humaines,
- Sécurité physique et environnementale,
- Gestion de l'exploitation et des télécommunications,
- Contrôle d'accès,
- Acquisition, développement et maintenance des systèmes d'information,
- Gestion des incidents liés à la sécurité de l'information,
- Gestion de la continuité de l'activité,
- 15 Conformité.

3.3.2 Détermination des exigences de sécurité

La mise en place des règles de sécurité était la dernière tâche à faire. Les règles ont été déterminées selon les objectifs et les principes précédents par les décliner en un ou plusieurs règles adaptées à notre contexte du périmètre de la PSSI.

Pour déterminer ces règles, on a basé sur la norme de sécurité ISO 27001 contenant les exigences de sécurité. Ci-après des exemples de quelques mesures parmi les mesures retenues :

- **Organisation interne :**
  - La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.
  - Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement...etc.

- **Tiers :**
  - Les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers doivent être identifiés, et des mesures appropriées doivent être mises en œuvre avant d'accorder des accès.
  - Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux actifs de l'organisme...etc.

- **Gestion des actifs :**

  — Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré.
  — La propriété de chaque information et des moyens de traitement de l'information doit être attribuée à une partie définie de l'organisme...etc.

- **Sécurité liée aux ressources humaines :**

  — La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.
  — Les responsabilités relatives aux fins ou aux modifications de contrats doivent être clairement définies et attribuées...etc.

- **Sécurité physique et environnementale :**

  — Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).
  — Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé...etc.

- **Gestion de l'exploitation et des télécommunications :**

  — Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.
  — Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme...etc.

- **Contrôle d'accès :**

  — Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.
  — L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel...etc.

Cette liste n'est pas exhaustive. Plusieurs autres mesures ont été ajoutées au niveau de la PSSI.

3.4 Phase 4 : Finalisation

L'objectif de cette phase est de produire le document validé exprimant la Politique de Sécurité des Systèmes d'Information de l'organisme. Ce document devra être validé et signé par la hiérarchie. Dans notre cas le document est validée seulement par le tuteur de stage qui est le responsable du département de sécurité. Après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires...) dans un but de communication et sensibilisation.

FIGURE 3.4: Phase 4 : finalisation

Résultat : le résultat final était un document de 35 pages contenant les parties suivantes :

1. Préambule
2. Contexte

I **Éléments stratégiques :**

1 Périmètre
2 Enjeux
3 Échelle de besoins
4 Besoins de sécurité
5 Origines des menaces

II **Objectifs et Règles de sécurité**

Pour assurer la mise en œuvre de cette politique au système d'information de l'organisme, on doit la compléter par un **plan d'action** qui est destiné à vivre et à être tenu à jour. Ce plan comprendra deux principaux volets :

- Des actions de type méthodologique, organisationnelle ou procédurale, applicable à l'ensemble de l'organisme participant au périmètre de l'étude ;

- des actions de type technique, concernant les éléments fédérateurs du système d'information.

On peut accompagner ces actions par des recommandations concernant les outils et méthodes de mise en œuvre.

Dans ce plan d'action, on doit surtout traiter : les points d'accès, d'identification, d'authentification et de l'autorisation, tout en respectant les aspects de la sécurité des informations qui permettent d'assurer une protection adéquate : la responsabilité, la prise de conscience et l'administration.

Conclusion : On a présenté dans ce chapitre le processus suivi pour la réalisation de la PSSI, et quelques exemples du résultat obtenu.

Conclusion

Le projet décrit dans ce document porte sur le problème de la sécurité des systèmes d'information des entreprises. Bien qu'il existe diverses solutions, elles restent non encore satisfaisantes et globales, ça reste un problème important à étudier et attend des solutions meilleures. Surtout que toute innovation technologique ouvre dans le même temps de nouvelles brèches dans lesquelles s'engouffrent les réseaux criminels.

En partant du constat qu'il n'existe pas de documents d'orientation globales ou spécifiques de sécurité des systèmes d'information clairement définies dans l'entreprise NAFTAL, on s'est permis à penser à mettre en place un document globale qui va construire une référence principale qui reflète la vision stratégique de NAFTAL en matière de sécurité des systèmes d'information. Un document qui va définir les objectifs de sécurité à atteindre, les principales dispositions à mettre en œuvre ainsi que les moyens à accorder pour y parvenir, et contient entre autres les enjeux de sécurité de l'entreprise, ses besoins de sécurité, ainsi que les vulnérabilités et les menaces pouvant impacter l'entreprise.

La solution proposée était donc l'élaboration d'une *"Politique de Sécurité des Systèmes d'Information"*. Une politique qui décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme. Pour y faire, on s'est inspiré de l'ensemble des guides de l'ANSSI [3].

Le travail réalisé consiste à effectuer les traitements suivants : On a commencé par un recueil de diverses informations sur l'entreprise pour connaitre son état actuel pour constituer un "référentiel documentaire". Ensuite, on a spécifié les éléments stratégiques (Contexte, Périmètre, Enjeux, Référentiel réglementaire, Besoins de sécurité, Origines des menaces)qui sont les premières grandes orientations à partir desquelles sera déclinée la PSSI. L'étape actuelle est basée essentiellement sur une analyse des risques, cette dernière est faite à l'aide de la méthode EBIOS promue aussi par l'ANSSI. L'étape suivante est la détermination des exigences de sécurité, ceci à l'aide de la norme internationale de sécurité ISO 27001. Enfin, un document final validé est produit exprimant la PSSI.

3. Agence Nationale de la Sécurité des Systèmes d'Information

Perspectives :

En perspective de ce travail nous envisageons de réaliser les phases suivantes :

— Décliner la PSSI en plusieurs plans d'action afin de la traduire en actions claires, spécifiques et applicables et faire en sorte que la mise en œuvre de la PSSI s'accompagne de consultations, d'une coordination et coopération entre les différents acteurs du système d'information.

— Actualiser chaque année ou chaque deux années la PSSI en fonction des événements majeurs affectant la mission ou la vie de l'organisme, ou une fois au moins tous les cinq ans, pour vérifier l'adéquation des règles par rapport à l'évolution du système d'information de l'organisme et de la technologie en sécurité des SI.

— Étendre le champ d'application de la PSSI, c'est-à-dire, décliner la PSSI globale en actions spécifiques qui seront plus détaillées et plus fines.

Bibliographie

[1] Bureau assistance et conseil (BAC) Agence nationale de la sécurité des systèmes d'information (ANSSI). *Expression des Besoins et Identification des Objectifs de Sécurité EBIOS, MÉTHODE DE GESTION DES RISQUES*, 25 janvier 2010.

[2] Normes de sécurité : les méthodes d'analyse des risques. https ://cyberzoide.developpez.com/securite/methodes-analyse-risques/, 19 août 2006.

[3] Bureau conseil de la DCSSI. *Guide pour l'élaboration d'une politique de sécurité de système d'information, SECTION 2 : METHODOLOGIE.* 51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP, 3 mars 2004.

[4] ISO. *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Exigences, NORME INTERNATIONALE ISO/CEI 27001*, 2005.

[5] LASBORDES Pierre. *La sécurité des systèmes d'information : un enjeu majeur pour la France.* La Documentation française, janvier 2006.

[6] Espace Numérique Entreprises. *Sécurité des Systèmes d'Information, Guide pratique à l'usage des dirigeants.* Villa Créatis - 2, rue des Mûriers CP 601 - 69258 LYON CEDEX 09, janvier 2010.

[7] GIP RENATER. Pourquoi la securite ? https ://services.renater.fr/ssi/securite/pourquoi, 2008.

[8] Anne Facq Françoise Gazelle Gabrielle Feltin Olivier Servas, Nicole Dausque. Pourquoi et comment adapter une politique de sécurité pour les entités du cnrs. 13, 2006.

[9] Bruno DOUCENDE. *Sécurité des Systèmes d'Information.* Technopole du chateau Gombert 'les baronnies', Bat A Rue Paul Langevin 13 013 -Marseille, 2009.

[10] Robert Longeon Jean-Luc Archimbaud. *Guide de la sécurité des systèmes d'information à l'usage des directeurs (de laboratoires de recherche)*, 1099.

[11] Pr Antoine Bouët. Synthèse sur la sécurité du système d'information (si). https ://openclassrooms.com/fr/courses/2256686-synthese-sur-la-securite-du-systeme-dinformation-si, 30/09/2014.

[12] Rabah Aoudjehane. Securite du systeme d'information dans une entreprise. https ://www.linkedin.com/pulse/s11 décembre 2016.

[13] Un groupe de réflexion du Cigref (Club informatique des grandes entreprises françaises). *Sécurité des systèmes d'information, Quelle politique globale de gestion des risques ?* Septembre 2002.

[14] REGIONS JOB. Responsable sécurité des systèmes d'information (rssi). https ://www.regionsjob.com/observatoire-metiers/fiche/responsable-securite-des-systemes-dinformation-rssi.

[15] Sécurité des systèmes informatiques/sécurité informatique/le domaine ssi. https ://fr.wikibooks.org/wiki/S28 juillet 2016.

[16] Sécurité des systèmes informatiques/sécurité informatique/le domaine ssi/documents ssi. https ://fr.wikibooks.org/wiki/S28 juillet 2016.

[17] Bureau conseil de la DCSSI. *Guide pour l'élaboration d'une politique de sécurité de système d'information, SECTION 1 : INTRODUCTION.* 51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP, 3 mars 2004.

[18] Bureau conseil de la DCSSI. *Élaboration de politiques de sécurité des systèmes d'information : MÉMENTO.* 51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP, 3 mars 2004.

[19] Bureau assistance et conseil (BAC) Agence nationale de la sécurité des systèmes d'information (ANSSI). *Expression des Besoins et Identification des Objectifs de Sécurité EBIOS, MÉMENTO*, 4 février 2004.

[20] Centre Français de Recherche sur le Renseignement. *AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI).*

ANNEXE : POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION NAFTAL

POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION NAFTAL

Date	Version	Évolution du document
20/03/2019	V 1.0	Publication de la première version de la Politique de sécurité des systèmes d'information de NAFTAL.

Préambule

Le document présent est un document interne représentant une politique de sécurité des systèmes d'information, reflétant la vision stratégique de la direction de l'organisme NAFTAL en matière de sécurité des systèmes d'information.

La PSSI [4] est un ensemble des éléments stratégiques, des directives, procédure, code de conduite, règles organisationnelles et techniques visant en général à protéger le système d'information de l'organisme.

Elle s'inscrit dans le système de management de l'organisme, donc de la sécurité des informations et processus, puis enfin de la SSI [5]. Elle constitue en effet le premier document à formaliser dans l'étape de planification et sera suivie des étapes de mise en œuvre, de vérification et d'amélioration du système de management de la SSI. Elle contribue à :

1. assurer la continuité des activités de l'entreprise.
2. prévenir la fuite d'informations sensibles.
3. Adopter les bons réflexes au quotidien concernant les principes de sécurité de l'entreprise, dans le but de réduire les incidents de sécurité et les couts associés.
4. renforcer la confiance des clients dans les entreprises et dans les téléprocédures.

Ce document est défini à l'aide de la méthode EBIOS [6] qui permet d'apprécier et de traiter les risques, elle est conforme aux normes suivantes : ISO 27001, 27005 et 31000. Cette méthode est composée de 5 modules :

1. Etude du contexte
2. Etude des évènements redoutés
3. Etude des scénarios de menaces
4. Etude des risques
5. Etude des mesures de sécurité

La PSSI est un instrument de sensibilisation et de communication qui s'adresse à l'ensemble des utilisateurs internes du SI de l'organisme (Direction, intervenants IT, personnels administratifs, techniques et commerciaux, ouvriers ...etc.) ainsi qu'à toute personne ou organisme extérieur (partenaire, prestataire, sous-traitants,

4. Politique de Sécurité des Systèmes d'Information
5. Sécurité des Systèmes d'Information
6. Expression des Besoins et Identification des Objectifs de Sécurité

fournisseurs, clients. . . etc.) susceptible de se connecter, d'utiliser ou d'intervenir sur le SI de l'établissement.

Contexte

Présentation :

Naftal est une société par actions (SPA) fondée en 1982 et filiale à 100% du groupe Sonatrach [7], Avec un effectif de 31285 agents (2015), un capital social de 40 000 000 000 DA et un chiffre d'affaire de 380 000 000 000 DA (2016).

Vocation principale :

La distribution et la commercialisation des produits pétroliers et dérivés sur le marché national.

Métier :

1. La commercialisation, le transport, le stockage et la distribution des produits pétroliers ;
2. Le marketing, la négociation et la relation client ;
3. La maintenance et la réhabilitation des infrastructures et équipements de production ;
4. Le management de projet.

Missions :

1. L'enfutage des GPL [8]
2. La formulation des bitumes
3. La distribution, le stockage et la commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux
4. Le transport des produits pétroliers.

7. Société nationale pour la recherche, la production, le transport, la transformation, et la commercialisation des hydrocarbures

8. Gaz de Pétrole Liquéfié

Infrastructures :

1. 47 Dépôts carburants terre
2. 42 Centres et mini-centres GPL
3. 09 Centres vrac GPL
4. 47 Dépôts relais
5. 30 Centre et dépôts aviation
6. 06 Centres marine
7. 15 Centres bitumes
8. 24 Centres lubrifiants et pneumatiques
9. Un réseau de transport pipelines d'une longueur de (2 720 km)
10. Un parc roulant de 3 300 unités
11. Un réseau de stations-service de 674, dont 338 stations-service en gestion directe
12. Naftal dispose de deux centres de formation d'entreprise qui accompagnent les plans annuels et pluriannuels de formation.

Valeurs propres :

Communication, compétence, qualité de service, confiance.

Stratégie :

A travers son plan de développement, Naftal vise un double objectif :

1. poursuivre sa mission de distribution des produits pétroliers.
2. Améliorer sa qualité de service

Les principales actions menées par Naftal portent sur :

1. La modernisation et la réhabilitation de ses infrastructures de stockage.
2. La mise en conformité de ses installations avec les normes de protection de l'environnement et de sécurité industrielle.
3. La modernisation et l'extension de son réseau de stations-service.
4. Le renouvellement de ses moyens de transport par route et de son matériel de manutention.
5. L'augmentation de ses capacités de transport par pipe.
6. La promotion de ses produits propres : GPL et essence sans plomb.

Moyens principaux du SI :

Le SI de NAFTAL est formé de plusieurs moyens humains, de communication et de sécurité supportés par des outils informatiques, dont les principaux moyens sont :

- Data-center : un cloud privé avec des serveurs et un hyperviseur pour des solution de sauvegarde.
- Équipement de sécurité : Serveur antivirus, Firewall, IPS [9], WSA [10].
- Réseaux informatiques : matériels (Routeurs, Switch, Armoires et panneaux de brassage, Modems, Liaison fibre optique), réseaux (WLAN, WAN, LAN, Antenne 3G de l'opérateur hébergé et dédiée à NAFTAL).
- Logiciels : application métier (calcul paie, finance et comptabilité, gestion des stocks, gestion du transport, gestion de la commercialisation, gestion RH, gestion inventaire), messagerie électronique, site web, liaisons FTP..., lignes spécialisées RMS([11]), ADSL(Asymmetric Digital Subscriber Line), 3G, 4G.
- Liaison : VPN (IPsec [12]), Client VPN, MSAN [13], FTTx [14]
- Autres services comme : la téléphonie IP, solution de visio conférence, vidéo surveillance.

Organigramme de NAFTAL :

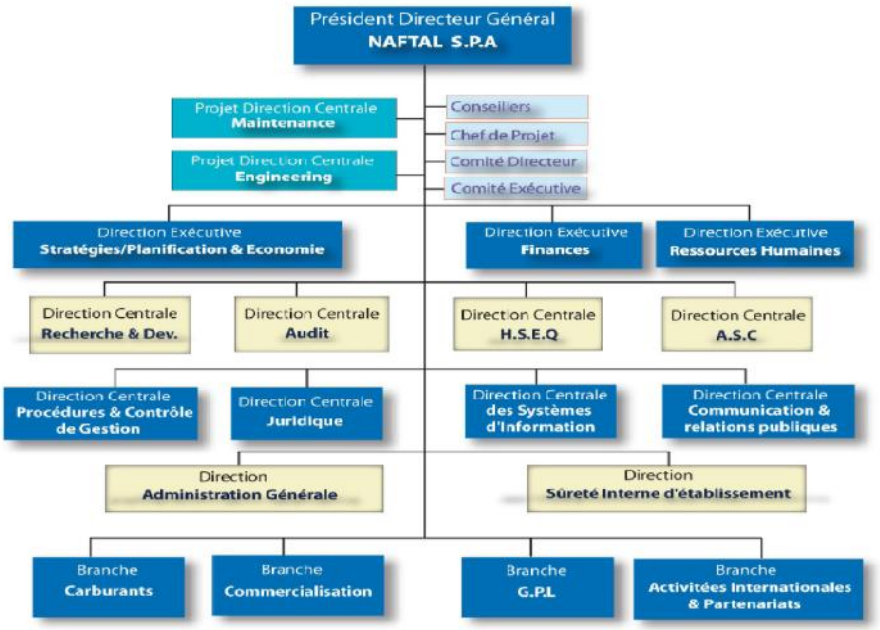

FIGURE 3.5: Organigramme de NAFTAL

9. Intrusion prevention system
10. Web Security Appliance
11. Réseau Multiservices
12. Internet Protocol Security
13. MultiService Access Node
14. Fiber To The ..

Première partie

Eléments stratégiques

Périmètre

La politique de sécurité des systèmes d'information de l'entreprise NAFTAL s'applique à l'ensemble de son système d'information. Elle comprend l'ensemble des moyens humains, techniques et organisationnels permettant, en support à l'activité, de créer, de conserver, d'échanger et de partager des informations entre les acteurs internes et tiers de l'entreprise, quelle que soit la forme sous laquelle elles sont exploitées (électroniques, imprimées, manuscrites, vocales, images, ...etc). Donc elle s'applique aux actifs matériels, immatériels et aux ressources humaines. ça inclut :

En terme de ressources humaine :

- l'ensemble des personnels autorisés à accéder, utiliser ou traiter au niveau fonctionnel ou technique, des informations ou des biens du système d'information de NAFTAL.
- les tiers définis comme étant toute personne morale ou physique, dès lors qu'ils utilisent les systèmes d'information de NAFTAL ou que leurs propres systèmes sont reliés aux réseau informatique de NAFTAL.

En terme d'actifs immatériels :

- l'ensemble du patrimoine informationnel associé à NAFTAL :
  - les connaissances issues de ses activités de recherche et développement
  - l'ensemble des bases de données liées à l'administration, la gestion, la recherche et aux ressources humaines.
  - les données associées à la gestion de sécurité des personnes et des biens (contrôle d'accès, hygiène et sécurité).

- les composants logiciels du système d'information.

En terme d'actifs matériels :

tous les composants matériel des systèmes d'information :

- les réseaux de communication.
- les serveurs hébergeant les données et les applications
- Bâtiments et locaux hébergeant les ressources humaines, les archives et les moyens informatiques.

Enjeux

NAFTAL peut être en face aux plusieurs vulnérabilités qui menacent son SI. La perte, la manipulation ou le vol d'informations peuvent considérablement affaiblir l'entreprise. Pour faire face à ces risques, il est nécessaire de choisir les critères de sécurité à prendre en compte afin de garantir sa SSI et surmonter les enjeux correspondants, et donc assurer les DICT [15] :

Disponibilité : Propriété d'accessibilité au moment voulu des éléments essentiels [16] par les utilisateurs autorisés, càd ; Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

- **Pour une fonction** : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large.
- **Pour une information** : garantie de la disponibilité prévue pour l'accès aux données (délais et horaires).

Intégrité : Propriété d'exactitude et de complétude des éléments essentiels. càd, Les données doivent être celles que l'on s'attend à ce qu'elles soient, et ne doivent pas être altérées de façon fortuite ou volontaire.

- **Pour une fonction** : Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements automatisés ou non par rapport aux spécifications ; absence de résultats incorrects ou incomplets de la fonction.
- **Pour une information** : garantie d'exactitude et d'exhaustivité des données vis-àvis d'erreurs de manipulation ou d'usages non autorisés ; non-altération de l'information.

Confidentialité : Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés, càd, Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

- **Pour une fonction** : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère

15. Disponibilité, Intégrité, Confidentialité, Traçabilité

16. les éléments essentiels sont les fonctions et les informations constituant la valeur ajouté du système d'information pour l'organisme

confidentiel.

- **Pour une information** : protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel.

Traçabilité : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

- **Pour une fonction** : les parties impliquées dans une activité ne puissent déclarer à tort avoir été étrangères à tout ou partie de l'activité.
- **Pour une information** : conserve les traces de l'état et des mouvements de l'information.

il peut être pertinent d'en ajouter d'autres tels que l'authentification. Lorsque un utilisateur veut accéder à un système d'information, il doit dans un premier temps effectuer une procédure d'identification et d'authentification.

Authentification : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange. est une phase qui permet à l'utilisateur d'apporter la preuve de son identité. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question : "Êtes-vous réellement cette personne ?". L'utilisateur utilise un authentifiant ou "code secret" que lui seul connait.

Échelle de besoins :

Échelle de besoin	**Disponibilité**	**Intégrité**	**Confidentialité**	**Traçabilité**
Niveau 1	Le bien peut être indisponible sans limite	Absence de besoin d'intégrité sans conséquences (Ex : aucune vérification)	Absence de besoin de confidentialité, bien qui peut être connu de tout public (Ex : données publiques)	Le bien ne requiert pas d'auditabilité. Aucun besoin de génération de traces.
Niveau 2	Le bien peut être indisponible pendant une durée importante mais limitée	Le bien accepte une perte importante d'intégrité (Ex : vérification des données, sans validation)	Le bien ne peut être accessible qu'à des groupes de personnes, identifiés et validés par une personne morale.	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori.
Niveau 3	Le bien peut être indisponible pendant une courte durée (Ex : arrêt du réseau, de la messagerie, données vitales non disponibles)	Le bien n'accepte qu'une faible perte d'intégrité (Ex : données qui sont validées et contrôlées par des moyens techniques ou humains.)	Le bien ne doit être accessible qu'à des groupes de personnes, identifiés, qualifiés et validés par une personne morale pour un objectif ou une finalité donné.	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori et être imputables à leurs auteurs.
Niveau 4	Le bien ne doit pas être indisponible (Ex : système de sécurité)	L'intégrité totale du bien est nécessaire (Ex : données avec au moins deux niveaux de validation et de contrôle différents)	Le bien ne doit être accessible qu'à des personnes habilitées et nominativement identifiées(Ex : données secret défense.)	Les actions sur ce bien doivent pouvoir faire l'objet d'analyse a posteriori et être imputables à leurs auteurs de la façon la plus irréfutable possible.

TABLE 3.4: Echelles de besoins de sécurité

Besoins de sécurité

3.5 Protection des outils de travail

les postes informatiques, les réseaux, les applications et les données, constituent « le Système d'Information » du NAFTAL. Cet ensemble est indispensable à la fois pour les activités nécessaires, mais aussi pour la gestion des entités. La disponibilité et l'intégrité de cet outil doivent donc impérativement être placées à l'abri de menaces internes ou externes.

3.6 Protection des données

Il s'agit souvent de « données sensibles » telles que :

- **Les données scientifiques :** liées à des contrats industriels, à un savoir-faire interne, expérimentales, liées à des coopérations nationales ou internationales, scientifiques, techniques, économiques, liées à la valorisation de la recherche, liées au centre de documentation, téléphoniques et de visioconférences.

- **Les données de gestion :** authentification, gestion comptable et financière, gestion des ressources humaines, documents contractuels.

- **Les données nominatives :** liées à la vie privée des personnes, liées à l'enseignement.

- **Les données stratégiques :** informations d'ordre politique ou stratégique ou touchant des questions de défense, informations sécurité...

3.7 Protection juridique

la mise en œuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cybersurveillance...). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée.

Origines des menaces

3.8 Causes humaines

- **La maladresse :** C'est lorsque quelqu'un peut exécuter un traitement non souhaité, effacer involontairement des données ou des programmes.

- **L'inconscience :** De nombreux utilisateurs méconnaissent les risques, et introduisent souvent des programmes malveillants sans le savoir, ou effectuent des manipulations inconsidérées.

- **La malveillance :** Une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes.

3.9 Causes extérieures

- **Un sinistre :** Vol, incendie, dégât des eaux, séisme...etc.

- **Une malveillance :** Une mauvaise manipulation entraînant une perte de matériel et/ou de données.

- **Problèmes électriques :** Panne total ou absence partielle du courant.

3.10 Causes techniques

- **Surchauffe :** C'est lorsque les processeurs produisent de la chaleur.

- **L"usure :** La détérioration résultant d'un usage prolongé.

- **Incidents liés au logiciel :** des failles permettant de prendre le contrôle total ou partiel d'un ordinateur.

- **Un programme malveillant :** un logiciel destiné à nuire au système.

Virus	Programme se dupliquant sur d'autres ordinateurs
worm (vers)	Exploite les ressources d'un ordinateur afin d'assurer sa reproduction
wabbit	Programme qui se réplique par lui-même (mais qui n'est ni un virus, ni un ver)
cheval de Troie (trojan horse)	Programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur
backdoor	Ouvreur d'un accès frauduleux sur un système informatique, à distance .
spyware (logiciel espion)	Collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers.
keylogger	Programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier.

TABLE 3.5: Attaques par programmes malveillants

Spam	Un email non sollicité. Ils encombrent le réseau, et font perdre du temps.
Phishing (hameçonnage)	Un email se faisant passer pour un organisme officiel et demandant de fournir des informations confidentielles.
Hoax (canular)	Un email incitant à retransmettre le message à ses contacts sous divers prétextes. Ils encombrent le réseau, et font perdre du temps. Dans certains cas, ils incitent à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

TABLE 3.6: Attaques par messagerie

Sniffing	Technique permettant de récupérer toutes les informations transitant sur un réseau. Utilisée pour récupérer les mots de passe, et pour identifier les machines qui communiquent sur le réseau.
Spoofing	Technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Utilisée pour récupérer des informations sensibles.
Denial of service (déni de service)	Technique visant à générer des arrêts de service, et ainsi d'empêcher le bon fonctionnement d'un système.

TABLE 3.7: Attaques sur le réseau

Deuxième partie

Objectifs et Règles de sécurité

Objectifs de sécurité et mesures

3.11 Politique de sécurité

Objectif	**Politique de sécurité de l'information** : Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.
Mesure	• **Document de politique de sécurité de l'information :** Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés. • **Réexamen de la politique de sécurité de l'information :** Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être réexaminée à intervalles fixés préalablement ou en cas de changements majeurs.

3.12 Organisation de la sécurité de l'information

Objectif 1	**Organisation interne** : Gérer la sécurité de l'information au sein de l'organisme.
Mesure	• **Implication de la direction vis-à-vis de la sécurité de l'information :** La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

	• **Coordination de la sécurité de l'information :** Les activités relatives à la sécurité de l'information doivent être coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme. • **Attribution des responsabilités en matière de sécurité de l'information :** Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement. • **Système d'autorisation concernant les moyens de traitement de l'information :** n système de gestion des autorisations doit être défini et mis en œuvre pour chaque nouveau moyen de traitement de l'information. • **Engagements de confidentialité :** Les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme, doivent être identifiées et réexaminées régulièrement. • **Relations avec les autorités :** Des relations appropriées doivent être mises en place avec les autorités compétentes. • **Relations avec des groupes de spécialistes :** Des contacts appropriés doivent être entretenus avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles. • **Réexamen indépendant de la sécurité de l'information :** Des réexamens réguliers et indépendants de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectués ; de tels réexamens sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité.

Objectif 2	**Tiers** : Assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à l'organisme et consultés, traités, communiqués ou gérés par des tiers.
Mesure	• **Identification des risques provenant des tiers :** Les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers doivent être identifiés, et des mesures appropriées doivent être mises en œuvre avant d'accorder des accès.

	• **La sécurité et les clients :** Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux actifs de l'organisme. • **La sécurité dans les accords conclus avec des tiers :** Les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, doivent couvrir l'ensemble des exigences applicables en matière de sécurité.

3.13 Gestion des actifs

Objectif 1	**Responsabilités relatives aux actifs** : Mettre en place et maintenir une protection appropriée des actifs de l'organisme.
Mesure	• **Inventaire des actifs :** Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré. • **Propriété des actifs :** La propriété de chaque information et des moyens de traitement de l'information doit être attribuée à une partie définie de l'organisme. • **Utilisation correcte des actifs :** Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.

Objectif 2	**Classification des informations :** : Garantir un niveau de protection approprié aux informations.
Mesure	• **Lignes directrices pour la classification :** Les informations doivent être classées en termes de valeur, d'exigences légales, de sensibilité et de criticité. • **Marquage et manipulation de l'information :** Un ensemble approprié de procédures pour le marquage et la manipulation de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisme.

3.14 Sécurité liée aux ressources humaines

Objectif 1	**Avant le recrutement :** Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées et réduire le risque de vol, de fraude ou de mauvais usage des équipements.
Mesure	• **Rôles et responsabilités :** Les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers doivent être définis et documentés conformément à la politique de sécurité de l'information de l'organisme. • **Sélection :** Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, les vérifications des informations concernant tous les candidats doivent être réalisées conformément aux lois, aux règlements et à l'étique et doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés. • **Conditions d'embauche :** Dans le cadre de leurs obligations contractuelles, les salariés, contractants et utilisateurs tiers doivent se mettre d'accord sur les modalités du contrat d'embauche les liant et le signer. Ce contrat doit définir leurs responsabilités et celles de l'organisme quant à la sécurité de l'information.

Objectif 2	**Pendant la durée du contrat :** Veiller à ce que tous les salariés, contractants et utilisateurs tiers soient conscients des menaces pesant sur la sécurité de l'information, de leurs responsabilités financières ou autres, et disposent des éléments requis pour prendre en charge la politique de sécurité de l'organisme dans le cadre de leur activité normale et réduire le risque d'erreur humaine.

Mesure	• **Responsabilités de la direction :** La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme. • **Sensibilisation, qualification et formations en matière de sécurité de l'information :** L'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers doivent suivre une formation adaptée sur la sensibilisation et doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions. • **Processus disciplinaire :** Un processus disciplinaire formel doit être élaboré pour les salariés ayant enfreint les règles de sécurité.

Objectif 3	**Fin ou modification du contrat :** Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.
Mesure	• **Responsabilités en fin de contrat :** Les responsabilités relatives aux fins ou aux modifications de contrats doivent être clairement définies et attribuées. • **Restitution des actifs :** Tous les salariés, contractants et utilisateurs tiers doivent restituer la totalité des actifs de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord. • **Retrait des droits d'accès :** Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.

3.15 Sécurité physique et environnementale

Objectif 1	**Zones sécurisées :** Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.

Mesure	• **Périmètre de sécurité physique :** Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil). • **Contrôles physiques des accès :** Les zones sécurisées doivent être protégées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité est admis. • **Sécurisation des bureaux, des salles et des équipements :** Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements. • **Protection contre les menaces extérieures et environnementales :** Des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme, doivent être conçues et appliquées. • **Travail dans les zones sécurisés :** Des mesures de protection physique et des directives pour le travail en zone sécurisée doivent être conçues et appliquées.
	• **Zones d'accès public, de livraison et de chargement :** Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés. Les points d'accès doivent également, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

Objectif 2	**Sécurité du matériel :** Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisme.

Mesure	• **Choix de l'emplacement et protection du matériel :** Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé. • **Services généraux :** Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux. • **Sécurité du câblage :** Les câbles électriques ou de télécommunications transportant des données doivent être protégés contre toute interception d'information ou dommage. • **Maintenance du matériel :** Le matériel doit être entretenu correctement pour garantir sa disponibilité permanente et son intégrité. • **Sécurité du matériel hors des locaux :** La sécurité doit être appliquée au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site. • **Mise au rebut ou recyclage sécurisé(e) du matériel :** out le matériel contenant des supports de stockage doit être vérifié pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut. • **Sortie d'un actif :** Un matériel, des informations ou des logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.

3.16 Gestion de l'exploitation et des télécommunications

Objectif 1	**Procédures et responsabilités liées à l'exploitation :** Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.
Mesure	• **Procédures d'exploitation documentées :** Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés. • **Management des modifications :** Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés. • **Séparation des tâches :** Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme. • **Séparation des équipements de développement, d'essai et d'exploitation :** Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.

Objectif 2	**Gestion de la prestation de service conclus avec un tiers :** Mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service conclus avec un tiers.

Mesure	• **Prestation de service :** Il doit être assuré que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers. • **Surveillance et examen des services tiers :** Les services, rapports et enregistrements fournis par les tiers doivent être régulièrement contrôlés et réexaminés, et des audits doivent être régulièrement réalisés. • **Gestion des modifications dans les services tiers :** Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.

Objectif 3	**Planification et acceptation du système :** Réduire le plus possible le risque de pannes du système.
Mesure	• **Dimensionnement :** L'utilisation des ressources doit être surveillée et ajustée au plus près, et des projections doivent être faites sur les dimensionnements futurs pour assurer les performances requises par le système. • **Acceptation du système :** Les critères d'acceptation doivent être fixés pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.

Objectif 4	**Protection contre les codes malveillant et mobile :** Protéger l'intégrité des logiciels et de l'information.
Mesure	• **Mesures contre les codes malveillants :** Des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre. • **Mesures contre le code mobile :** Lorsque l'utilisation de code mobile est autorisée, la configuration doit garantir que le code mobile fonctionne selon une politique de sécurité clairement définie et tout code mobile non autorisé doit être bloqué.

Objectif 5	**Sauvegarde :** Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.
Mesure	• **Sauvegarde des informations :** Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

Objectif 6	**Gestion de la sécurité des réseaux :** Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle elles s'appuient.
Mesure	• **Mesures sur les réseaux :** Les réseaux doivent être gérés et contrôlés de manière adéquate pour qu'ils soient protégés des menaces et pour maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit. • **Sécurité des services réseau :** Pour tous les services réseau, les fonctions réseau, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.

Objectif 7	**Manipulation des supports :** Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) d'actifs et l'interruption des activités de l'organisme.
Mesure	• **Gestion des supports amovibles :** Des procédures doivent être mises en place pour la gestion des supports amovibles. • **Mise au rebut des supports :** Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles. • **Procédures de manipulation des informations :** Des procédures de manipulation et de stockage des informations doivent être établies pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage. • **Sécurité de la documentation système :** La documentation système doit être protégée contre les accès non autorisés.

Objectif 8	**Échange des informations :** Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.
Mesure	• **Politiques et procédures d'échange des informations :** Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tous types d'équipements de télécommunication. • **Accords d'échange :** Des accords doivent être conclus pour l'échange d'informations et de logiciels entre l'organisme et la partie externe. • **Supports physiques en transit :** Les supports contenant des informations doivent être protégés contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme. • **Messagerie électronique :** Les informations liées à la messagerie électronique doivent être protégées de manière adéquate. • **Systèmes d'information d'entreprise :** Des politiques et procédures doivent être élaborées et mises en œuvre pour protéger l'information liée à l'interconnexion de systèmes d'informations d'entreprise.

Objectif 9	**Services de commerce électronique :** Assurer la sécurité des services de commerce électronique, ainsi que leur utilisation sécurisée.
Mesure	• **Commerce électronique :** Les informations liées au commerce électronique transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées. • **Transactions en ligne :** Les informations liées aux transactions en ligne doivent être protégées pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission. • **Informations à disposition du public :** L'intégrité des informations mises à disposition sur un système accessible au public doit être protégée pour empêcher toute modification non autorisée.

Objectif 10	**Surveillance :** Détecter les traitements non autorisés de l'information.
Mesure	• **Journaux d'audit :** Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès. • **Surveillance de l'exploitation du système :** Des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information doivent être établies et les résultats des activités de surveillance doivent être réexaminés périodiquement. • **Protection des informations journalisées :** Les équipements de journalisation et les informations journalisées doivent être protégés contre le sabotage et les accès non autorisés. • **Journal administrateur et journal d'opérations :** Les activités de l'administrateur système et de l'opérateur système doivent être journalisées. • **Rapports d'anomalies :** Les éventuels défauts doivent être journalisés et analysés et les mesures appropriées doivent être prises. • **Synchronisation des horloges :** Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps précise et préalablement définie.

3.17 Contrôle d'accès

Objectif 1	**Exigences métier relatives au contrôle d'accès :** Maîtriser l'accès à l'information.
Mesure	• **Politique de contrôle d'accès :** Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.

Objectif 2	**Gestion des accès des utilisateurs :**
Mesure	• **Enregistrement des utilisateurs :** Une procédure formelle d'inscription et désincription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie. • **Gestion des privilèges :** L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées. • **Gestion du mot de passe utilisateur :** L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel. • **Réexamen des droits d'accès utilisateurs :** La direction doit réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.

Objectif 3	**Responsabilités de l'utilisateurs :** Empêcher l'accès d'utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information.
Mesure	• **Utilisation du mot de passe :** Il doit être demandé aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe. • **Matériel utilisateur laissé sans surveillance :** Les utilisateurs doivent s'assurer que tout matériel laissé sans surveillance est doté d'une protection appropriée. • **Politique du bureau propre et de l'écran vide :** Une politique du bureau propre doit être adoptée pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide doit également être adoptée pour les moyens de traitement de l'information.

Objectif 4	**Contrôle d'accès réseau :** Empêcher les accès non autorisés aux services disponibles sur le réseau.

Mesure	• **Politique relative à l'utilisation des services en réseau :** Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation. • **Authentification de l'utilisateur pour les connexions externes :** Des méthodes d'authentification appropriées doivent être utilisées pour contrôler l'accès des utilisateurs distants.
	• **Identification des matériels en réseaux :** L'identification automatique de matériels doit être considérée comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques. • **Protection des ports de diagnostic et de configuration à distance :** L'accès physique et logique aux ports de diagnostic et de configuration à distance doit être contrôlé. • **Cloisonnement des réseaux :** Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés sur le réseau. • **Mesure relative à la connexion réseau :** Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, la capacité de connexion réseau des utilisateurs doit être restreinte, conformément à la politique de contrôle d'accès et aux exigences relatives aux applications métier. • **Contrôle du routage réseau :** Des mesures du routage des réseaux doivent être mises en œuvre afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications métier.

Objectif 5	**Contrôle d'accès au système d'exploitation :** Empêcher les accès non autorisés aux systèmes d'exploitation.

Mesure	• **Ouverture de sessions sécurisées :** L'accès aux systèmes d'exploitation doit être soumis à une procédure sécurisée d'ouverture de session. • **Identification et authentification de l'utilisateur :** Un identifiant unique et exclusif doit être attribué à chaque utilisateur et une technique d'authentification doit être choisie, permettant de vérifier l'identité déclarée par l'utilisateur. • **Système de gestion de mots de passe :** Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité. • **Emploi des utilitaires système :** L'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application doit être limité et contrôlé étroitement. • **Déconnexion automatique des sessions inactives :** Les sessions inactives doivent être déconnectées après une période d'inactivité définie. • **Limitation du temps de connexion :** Les temps de connexion doivent être restreints afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.

Objectif 6	**Contrôle d'accès aux applications et à l'information :** Empêcher les accès non autorisés aux informations stockées dans les applications.
Mesure	• **Restriction d'accès à l'information :** Pour les utilisateurs et le personnel chargé de l'assistance technique, l'accès aux informations et aux fonctions applicatives doit être restreint conformément à la politique de contrôle d'accès. • **Isolement des systèmes sensibles :** Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé).

Objectif 7	**Informatique mobile et télétravail :** Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail.
Mesure	• **Informatique et communications mobiles :** Une procédure formelle et des mesures de sécurité appropriées doivent être mises en place pour assurer une protection contre le risque lié à l'utilisation d'appareils informatiques et de communication mobiles. • **Télétravail :** Une politique, des procédures et des programmes opérationnels spécifiques au télétravail doivent être élaborés et mis en œuvre.

3.18 Acquisition, développement et maintenance des systèmes d'information

Objectif 1	**Exigences de sécurité applicables aux systèmes d'information :** Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information.
Mesure	• **Analyse et spécification des exigences de sécurité :** Les exigences métier relatives aux nouveaux systèmes d'information ou les améliorations apportées aux systèmes d'information existants doivent spécifier les exigences de sécurité.

Objectif 2	**Bon fonctionnement des applications :** Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.
Mesure	• **Validation des données en entrée :** Les données entrées dans les applications doivent être validées afin de vérifier si elles sont correctes et appropriées. • **Mesure relative au traitement interne :** Des contrôles de validation doivent être inclus dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés. • **Intégrité des messages :** Les exigences permettant d'assurer l'authentification et la protection de l'intégrité des messages dans les applications doivent être identifiées, et des mesures appropriées doivent être identifiées et mises en œuvre. • **Validation des données en sortie :** Les données de sortie d'une application doivent être validées pour assurer que le traitement des informations stockées est correct et adapté aux circonstances.

Objectif 3	**Mesures cryptographiques :** Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.
Mesure	• **Politique d'utilisation des mesures cryptographiques :** Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre. • **Gestion des clés :** Une procédure de gestion des clés doit favoriser l'utilisation par l'organisme de techniques cryptographiques.

Objectif 4	**Sécurité des fichiers système :** Garantir la sécurité des fichiers système.

Mesure	• **Mesure relatives aux logiciels en exploitation :** Des procédures doivent être mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation. • **Protection des données système d'essai :** Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées. • **Contrôle d'accès au code source du programme :** L'accès au code source du programme doit être restreint.

Objectif 5	**Sécurité en matière de développement et d'assistance technique :** Garantir la sécurité du logiciel et des informations d'application.
Mesure	• **Procédures de contrôle des modifications :** La mise en œuvre des modifications doit être contrôlée par le biais de procédures formelles. • **Réexamen technique des applications après modification du système d'exploitation :** Lorsque des modifications sont apportées aux systèmes d'exploitation, les applications critiques métier doivent être réexaminées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité. • **Restrictions relatives à la modification des progiciels :** La modification des progiciels ne doit pas être encouragée, et doit être limitée aux changements nécessaires. Un contrôle strict doit également être exercé sur ces modifications. • **Fuite d'informations :** Toute possibilité de fuite d'informations doit être empêchée. • **Externalisation du développement logiciel :** Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme.

Objectif 6	**Gestion des vulnérabilités techniques :** Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.
Mesure	• **Mesure relative aux vulnérabilités techniques :** Toute information concernant toute vulnérabilité technique des systèmes d'information en exploitation doit être obtenue à temps, l'exposition de l'organisme aux dites vulnérabilités doit être évaluée et les actions appropriées doivent être entreprises pour traiter le risque associé.

3.19 Gestion des incidents liés à la sécurité de l'information

Objectif 1	**Remontée des événements et des failles liés à la sécurité de l'information :** Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permet la mise en œuvre d'une action corrective, dans les meilleurs délais.
Mesure	• **Remontée des événements liés à la sécurité de l'information :** Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées. • **Remontée des failles de sécurité :** Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Objectif 2	**Gestion des incidents liés à la sécurité de l'information et des améliorations :** Garantir la mise en place d'une approche cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.
Mesure	• **Responsabilités et procédures :** Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information. • **Exploitation des incidents liés à la sécurité de l'information déjà survenus :** Des mécanismes doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés. • **Collecte de preuves :** Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).

3.20 Gestion de la continuité de l'activité

Objectif 1	**Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information :** Empêcher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les défaillances majeures des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.
Mesure	• **Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité :** Un processus de continuité de l'activité dans l'ensemble de l'organisme doit être élaboré et géré, qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme. • **Continuité de l'activité et appréciation du risque :** Les événements pouvant être à l'origine d'interruptions des processus métier doivent être identifiés, tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information. • **Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information :** Des plans doivent être élaborés et mis en œuvre pour maintenir ou restaurer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux. • **Cadre de la planification de la continuité de l'activité :** Un cadre unique pour les plans de continuité de l'activité doit être géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance. • **Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité :** Les plans de continuité de l'activité doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.

3.21 Conformité

Objectif 1	**Conformité aux exigences légales :** Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité.

Mesure	• **Identification de la législation en vigueur :** Pour chaque système d'information et pour l'organisme, toutes les exigences légales, réglementaires et contractuelles en vigueur doivent être définies, documentées et mises à jour, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences. • **Droits de propriété intellectuelle (DPI) :** Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires. • **Protection des enregistrements de l'organisme :** Les enregistrements importants doivent être protégés contre la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier. • **Protection des données et confidentialité des informations relatives à la vie privée :** La protection et la confidentialité des données doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant. • **Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information :** Les utilisateurs doivent être dissuadés de toute utilisation de moyens de traitement de l'information à des fins illégales. • **Réglementation relative aux mesures cryptographiques :** Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.

Objectif 2	**Conformité avec les politiques et normes de sécurité et conformité technique :** S'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme.
Mesure	• **Conformité avec les politiques et les normes de sécurité :** Les responsables doivent s'assurer de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité. • **Vérification de la conformité technique :** La conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité doit être vérifiée régulièrement.

Objectif 3	**Prises en compte de l'audit du système d'information :** Optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système d'information.
Mesure	• **Contrôles de l'audit du système d'information :** Les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation doivent être planifiées de manière précise et doivent être le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier. • **Protection des outils d'audit du système d'information :** L'accès aux outils d'audit du système d'information doit être protégé afin d'empêcher tous mauvais usage ou compromission éventuels.