**MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE**

**ÉCOLE NATIONALE SUPÉRIEURE DE MANAGEMENT**

**ENSM. Pôle Universitaire de KOLÉA**

**MÉMOIRE DE FIN D'ÉTUDE**

**Master Académique en Management stratégique et système d'information**

# Mise en place d'une démarche de gestion des risques informatiques au sein de la direction Technologies de l'Information en utilisant la méthode EBIOS RM

## Cas : SONATRACH L'Activité Commercialisation

**Élaboré par :**

GHERABLI IMENE

**Encadré par :**

Pr. SAHEL SIDI MOHAMMED.

Mme CHERKIT Fatima Zahra

**MEMBRES DE JURYS :**

Mr ZERROUTI Président
Mme CHADER: Examinateur
Mme CHERKIT: Encadreur

**Année 2020/2021**

## RÉSUMÉ

L'objectif principal de cette recherche est de s'assurer que la méthode EBIOS RM est utilisée dans le service informatique de la direction Technologies de l'Information pour la gestion des risques informatiques, plus précisément l'application de la méthode des licences. Mettre en œuvre la gestion de la prévision des risques informatiques au sein du département informatique.

Des méthodes qualitatives sont utilisées pour répondre aux questions de recherche.

Les résultats ont montré qu'il y avait des lacunes dans l'ensemble du processus, ce qui on a permis de faire des suggestions pour l'améliorer la gestion du système informatique.



**Mots clés : Système d'Information - Système d'Information - Risque Informatique - Gestion des Risques - EBOIS RM - Plan de Reprise d'Activité.**



## ABSTRACT

The main objective of this research is to ensure that the EBIOS RM method is used in the IT department of the Information Technologies department for IT risk management, more specifically the application of the licensing method. Implement IT risk forecasting management within the IT department.

Qualitative methods are used to answer the research questions.

The results showed that there were shortcomings in the whole process, which made it possible to make suggestions for improving it in order to ensure the quality of the management information system.



**Keywords : Information System - IT System - IT Risk - Risk Management – EBOIS RM - business recovery plan.**



## ملخص

في قسم تكنولوجيا المعلومات بقسم تكنولوجي EBIOS RM الهدف الرئيسي من هذا البحث هو التأكد من استخدام طريقة المعلومات لإدارة مخاطر تكنولوجيا المعلومات، وبشكل أكثر تحديدًا تطبيق طريقة الترخيص. تنفيذ إدارة التنبؤ بمخاطر تكنولوجيا المعلومات داخل قسم تكنولوجيا المعلومات.

تستخدم الأساليب النوعية للإجابة على أسئلة البحث.

بتقديم اقتراحات لتحسينها من أجل ضمان جودة نظام أظهرت النتائج وجود ثغرات في العملية برمتها، مما سمح المعلومات الإدارية.



**- الكلمات الرئيسية: نظام المعلومات - نظام تكنولوجيا المعلومات - مخاطر تكنولوجيا المعلومات - إدارة المخاطر خطة استعادة الأعمال -EBOIS RM.**

## REMERCIEMENTS

Je tiens à remercier mes encadreurs à l'École nationale supérieure de management (ENSM) à KOLÉA Mme CHERKIT FATIMA ZAHRA et Pr. SAHEL SIDI MOHAMMED, lors de leur accompagnement durant mon travail de recherche, qui étaient tout le temps présent et à l'écoute pour me conseiller et me diriger.

Je remercie également mon tuteur à Sonatrach L'Activité Commercialisation Mr HADDADI SMAINE qui m'encourageait durant ma période de stage en me donnant toute l'information nécessaire.

Merci à tous les cadres dirigeants de la Sonatrach COM que j'avais le plaisir de les rencontrer pour leur temps précieux.

Je tiens en particulier à remercier ma maman et mon papa pour leur inconditionnel soutien durant mes études, ma sœur et mon frère, et tous mes amis pour les encouragements qu'ils n'ont jamais cessé de me donner.

## TABLE DES MATIÈRES

## LISTE DES TABLEAUX

## LISTE DES FIGURES

## LISTE DES ABRÉVIATIONS

**ANSSI :** Agence nationale de la sécurité des systèmes d'information

**DCSSI** : Direction centrale de la sécurité des systèmes d'information.

**DG :** La Direction Générale.

**DTI :** la Direction Technologies de l'Information.

**EBIOS RM** : Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager.

**IEC/CEI :** International Electrotechnique Commission / Commission Électronique Internationale.

**ISO :** Organisation internationale de normalisation.

**NTIC** : Nouvelles technologies de l'information et de la communication.

**PRA :** Plan de reprise d'activité.

**RSSI :** responsable de la sécurité des systèmes d'informations

**SH-COM :** SONATRACH L'Activité Commercialisation

**SI :** Système d'Information.

**SSI :** Sécurité Système d'Information.

# INTRODUCTION

De nos jours, l'informatique est devenue une science couvrant tous les domaines du travail et de la vie. En raison de l'avancée de l'informatique, il est logique que nous puissions avoir une autre vision de la gestion dans tous les domaines des activités humaines (gestion du personnel, partage de l'information, sécurité de l'information, etc.).

Cependant, lorsque le processus d'une entreprise devient un objectif, l'entreprise sera confrontée à des menaces, et ces menaces deviendront des risques. Cependant, il n'est pas facile de comprendre clairement les interférences entre les menaces et les processus métier clés. Par conséquent, pour aller de l'avant, toute organisation doit entreprendre des actions visant à comprendre son environnement et à comprendre ses propres opérations. Ce n'est que dans ce cas qu'il disposera de paramètres lui permettant de contrôler sa récupération.

En effet, la mise en place du PRA (Activity Recovery Plan) permet aux organisations de s'assurer qu'en cas de sinistre, le système d'information de l'entreprise peut redémarrer rapidement ses activités tout en limitant les pertes de données. A cet égard, certains éléments de bonnes pratiques sont indispensables, à commencer par le test de routine de cette PRA.

Surtout, il est actuellement possible de mettre en œuvre un PRA quelle que soit la structure et la taille de l'entreprise. Raison pour laquelle, nous initions la présente étude dont la thématique porte sur **«** Mise en place d'une démarche de gestion des risques informatiques au sein de la Direction Technologies de l'Information en utilisant la méthode EBIOS RM » dans le but d'élucider les questions autour de la reprise d'activité au sein Entreprise.

**Problématique :**

Quelle est le processus pour une meilleure gestion des risques informatiques au sein de la Direction Technologies de l'information

Cette interrogation principale nous conduit à ces sous questionnements :

- Comment peut-on appliqué la méthode - EBIOS RM dans la gestion des risques au sien de la DTI ?
- Comment sont-ils traités ? Quels outils ou logiciels sont utilisés pour leur traitement ?
- Qui a la responsabilité de ce type de risque dans l'entreprise ?

**L'hypothèse :**

« Une hypothèse est une proposition qui anticipe une relation entre deux termes qui, selon le cas, peuvent être des concepts ou des phénomènes. Une hypothèse est donc une proposition provisoire, une présomption, qui demande à être vérifiée » selon Raymond Quivy ET Lac Van (1995 : p135).

Afin de répondre à la question principale de la problématique, on a choisi de poser l'hypothèse suivante :

Un plan de reprise informatique peut être une approche efficace afin d'assurer une meilleure gestion des risques informatiques au sein de la Direction Technologies de l'information.

# CHAPITRE 1 : REVUE DE LITTÉRATURE ET CADRE CONCEPTUEL DE LA RECHERCHE

**Section n°01 : Revue de littérature**

Cette partie de travail consistera à passer en revue les principales recherches qui ont été effectuées sur la méthode EBIOS dans le domaine de l'analyse des risques.

La méthode EBIOS a été développée par la Direction centrale de la sécurité des systèmes d'information (DCSSI) et maintenue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en 1995 et mise à jour régulièrement, Elle a connu une évolution en 2010 puis a été renommée en EBIOS Risk Manager, bénéficiant de ses 15 années d'expérience dans le domaine de la gestion des risques. Il permet d'évaluer et de traiter les risques liés à la sécurité des systèmes d'information (SSI). Il peut également communiquer au sein de l'organisation et de ses partenaires pour constituer un outil complet de gestion des risques SSI.

La nouvelle méthode EBIOS, plus simple et plus claire, offre la possibilité d'élaborer et de suivre des plans d'action liés à la sécurité des systèmes d'information.

Modulaire et conforme aux normes internationales ISO/IEC 31000, ISO/IEC 27005, ISO/IEC 27001, la méthode EBIOS reste la boîte à outils de base pour toute réflexion sur la sécurité de l'information :

- Etablir son référentiel SSI ;
- Gestion des risques de l'organisation ;
- Mettre en place un système de gestion de la sécurité de l'information ;
- Élaborer des réglementations, des stratégies, des politiques, des plans d'action ou des tableaux de bord SSI.

Choisissez quatre types de systèmes comme sources ou cibles de danger : individus isolés (acteurs), population (réseau d'acteurs), écosystèmes (environnement) et équipements/entreprises (systèmes éco-sociaux).

Selon le Club EBIOS, la relation un à un entre chacun des quatre systèmes conduit à aborder les risques, les dangers, la santé et la sécurité, les conditions de travail et les risques majeurs, selon OLIVIER GRANDAMAS5 (2012). Cette approche présente plusieurs avantages : elle est pragmatique et actionnable, elle passe par des transactions, donne au groupe de travail l'opportunité de faire le point sur les systèmes informatiques utilisés, imagine d'où pourraient provenir les menaces, décrit les événements terribles, définit un plan par métiers, DSI, et SI Les mesures des risques identifiés par la direction de la sécurité partent des plus probables (données inaccessibles, sites Internet, messages, arrêt de production, fraude).

La synthèse sera soumise à la direction générale pour comprendre, arbitrer, déterminer les priorités et éventuellement dégager des ressources (humaines et financières) pour mettre en œuvre la stratégie proposée par Marie de Fréminville (2019).

A l'issue de ces modules, tous les scénarios doivent avoir été planifiés, identifiés, et les informations nécessaires pour guider la prévention des risques doivent avoir été collectées.

## Section n°02 : Cadre conceptuel de la recherche

### 1. Gestion des risque lies au système d'information

### A. Définition de Systèmes D'information :

Le système d'information (SI) est l'élément central d'une entreprise ou d'une organisation. Disposant d'un ensemble de moyens matériels, humains et logiciels, il permet aux différents intervenants de communiquer des informations et de communiquer.

Le SI permet de créer, collecter, stocker, traiter et modifier des informations sous différents formats.

L'objectif d'SI est de fournir des informations aux bonnes personnes dans le bon format au bon moment

Une organisation est constituée d'une série de systèmes. Il existe des systèmes d'exploitation, de contrôle et d'information, qui sont trois sous-systèmes en interaction :

- ✓ Le système opérant : c'est ce qui est à la base de toute organisation, c'est ce système qui permet la transformation de l'information dont l'objectif est de la restituer à la bonne personne. Il correspond aux différents services d'une entreprise.
- ✓ Le système de pilotage : C'est ce qui va contrôler et piloter le système opérant. Il se situe donc à la tête du système d'information fixant les objectifs et prenant les décisions.
- ✓ Le système d'information : C'est ce qui intervient entre les deux autres systèmes. Ce système s'occupe de collecter, stocker, transformer et diffuser des données et informations dans le système opérant et de pilotage.
- ✓ En résumé, un système d'information permet au système opérant de communiquer des informations qui ont été collectées et modifiées au système de pilotage qui est en charge de contrôler et prendre des décisions.

### B. Risques informatiques :

Avant de présenter un essai de panorama de risques informatiques, il est nécessaire de comprendre au préalable ce que l'on entend par risque.

#### a. Définition du risque :

Selon le Guide ISO 73, le risque est défini comme « l'impact de l'incertitude sur la réalisation des objectifs ». Cet effet correspond à un écart négatif ou positif par rapport à l'objectif initial (CLAUDE, 2012 : p39). Habituellement, un spread positif est une opportunité.

En revanche, pour IFACI (in Renard, 2010 : p155), le risque est défini comme « un ensemble d'événements pouvant avoir un impact négatif sur l'entité. Le contrôle interne et l'audit sont principalement chargés de s'assurer que plus."

Par conséquent, le risque informatique doit être considéré comme un risque découlant de l'utilisation, de la propriété, du fonctionnement, de l'impact et de l'adoption de l'informatique dans l'organisation.

Pour parler de risque, il faut combiner deux (02) éléments. En effet, d'une part, il doit y avoir une menace, et d'autre part, les gens doivent être sensibles à cette menace.

**RISQUE = MENACE * VULNÉRABILITÉ**

D'après la norme ISO/CEI 27002 : 2005, la menace est définie comme « la cause potentielle d'un incident indésirable pouvant entraîner des dommages au sein d'un système ou d'un organisme ». La vulnérabilité (encore faille ou brèche) quant à elle est définie comme « la faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace » (CLAUDE, 2012 : p41-42). En effet, le bien dont il est question ici est en fait un actif informationnel.

### b. Les types de risques informatiques :

Les risques informatiques peuvent être présentés selon diverses approches (fonctionnelle, par nature, synthétique, etc.). L'approche synthétique ayant l'avantage d'identifier les principaux risques informatiques est à considérer prioritairement dans l'entreprise (DARSA, 2013 : p218), c'est elle que nous adopterons pour la présentation des types de risques informatiques (Annexe I, page 83).

Les risques informatiques peuvent avoir divers sources ou facteurs. Selon la nature de la source du risque, il y a les risques humains, environnementaux et technologiques

- **Risques humains :**

Les risques humains sont ceux causés par les hommes. BARTHELEMY (2004 : p87) dans son discours sur les atteintes sur un actif matériel affirme que : l'intrusion, la fraude et la malveillance sont les risques dont la source est une personne ayant la volonté de nuire et dont l'objet du risque est généralement un matériel (endommagement ou vols de bien). Plus précisément, il distingue :

- l'intrusion : il s'agit de l'accès des personnes non autorisées dans locaux ;

- la malveillance : il peut s'agir d'un détournement de mot de passe (un informaticien peut détourner le mot de passe d'un utilisateur à son insu afin de bénéficier de tous les privilèges qui lui sont accordés) ;

- la fraude : la fraude concerne tous les salariés de l'entreprise, seuls ou en collusion avec des complices externes à l'entreprise ;

- vols : il s'agit des détournements d'actifs informatiques ;

- endommagement : il s'agit de la destruction du matériel informatique. Il peut être volontaire (sabotage) en raison de la mauvaise foi ou involontaire (maladresse ou erreur de manipulation).

Complétons ces sources de risques avec CALE & al. (2007 : p57) qui considèrent comme risques de source humaine, les erreurs humaines (erreur de conception, erreur de programmation, erreur de configuration et erreur par négligence).

Rajoutons à cette catégorie, le social engineering (les pirates, hacker, cracker) et le phishing (technique utilisée par les pirates pour se faire passer pour un organisme connu auprès de leur victime).

- **Risques environnementaux :**

On distingue les variations brutales d'humidité et de température dans cette catégorie (Deleuze, 2013 : 299).

Les sinistres et l'électricité sont également sources de risques environnementaux. En effet, pour BARTHELEMY (2004 : p72), les sources naturelles de risque sont diverses. Il pensait que c'était une catastrophe, une inondation, un mouvement de terre, un tsunami, une éruption volcanique, un tremblement de terre, une explosion, etc. Quant aux risques apportés par l'électricité, ils proviennent généralement des surtensions, des sous-tensions et des coupures de courant.

Les concepteurs de matériaux électroniques doivent tenir compte de la menace de l'électricité et de la poussière pour les matériaux informatiques lors de la conception. D'une manière générale, les équipements électroniques près de la mer vieilliront plus rapidement en raison de la brise.

- **Risques technologiques :**

Ce sont les risques causés par tout ce qui est lié à l'aspect technologie de l'entreprise. Ils peuvent affecter les données, les logiciels mais aussi les informations stockées par l'entreprise. Dans cette rubrique il y a les malwares, les spams, les atteintes à la disponibilité des services.

Les malwares : Pour CALE & al. (2007 : p43), « malware » est utilisé pour désigner l'ensemble des programmes malveillants qui peuvent être utilisés par les pirates afin de commettre leurs méfaits. Les principaux malwares sont :

- le virus informatique : similaire à un virus biologique qui se fixe à l'intérieur d'une cellule, le virus informatique est un logiciel qui s'introduit dans les programmes des utilisateurs, se reproduit et contamine le plus grand nombre de leurs fichiers. Les cinq (05) catégories de virus existant sont les virus du secteur d'amorçage ou boot sector, les virus d'application, les virus furtifs, les virus flibustiers et les virus polymorphes ou mutants ;

- vers informatique : contrairement au virus, un vers est un programme autonome qui n'utilise pas de support (vecteur) pour se propager car il se déplace dans les réseaux informatiques grâce à sa capacité de duplication ;

- cheval de Troie : c'est un logiciel qui se présente sous une forme bénigne en apparence (jeux, utilitaire, etc.) mais qui recèle en lui un grand péril pour l'utilisateur qui l'installera sur ma machine. Dès lors que l'utilisateur se servira du logiciel, le logiciel effectuera avec toute la discrétion possible des vols ou destructions de données par exemple et ceci à l'insu de

l'utilisateur du logiciel. Il est généralement employé dans les cas de chantage, d'espionnage commercial/industriel, détournement de fond, et de prise de contrôle à distance, relais spam etc. La bombe logique est un type particulier du cheval de Troie qui s'active à un moment précis et cause par la suite un maximum de dégâts (formatage du disque dur, corruptions des données, etc.) au sein du système dans lequel il a réussi à s'introduire ;

- back door : il s'agit d'une fonctionnalité insérée dans un logiciel ou système d'exploitation par un développeur ou autre logiciel dans le but d'accéder à certaines fonctions sans devoir s'authentifier au préalable ;

- logiciels espions : il s'agit des logiciels utilisés pour voler des données. On distingue les spywares (petits logiciels s'installant à l'insu des utilisateurs), les key logger (petit programme qui enregistre secrètement les informations tapées au clavier des ordinateurs par les utilisateurs) et l'adware (collecteur d'informations personnelles pour transmettre aux sociétés faisant le marketing en ligne) selon CALE & al. (2007 : p44).

Les spams :

Le spam ou pourriel désigne l'envoi massif de courriers publicitaires dans les boîtes aux lettres électroniques des personnes sans leurs approbations d'après CALE & al. (2007 : p55).

Les atteintes à la disponibilité des services (déni de service) :

Le déni de service est un type d'attaque ayant pour but de rendre indisponible un service ou bien d'en détériorer la qualité afin de l'empêcher de répondre aux demandes légitimes d'après CALE & al. (2007 : p66).

### C. Gestion des risques informatiques :

Afin de mieux comprendre cette partie du contenu, il est nécessaire d'introduire au préalable le sens de la gestion des risques :

#### a. Définition de la gestion des risques :

La gestion des risques se définit comme un ensemble de moyens, de comportements, de procédures et d'actions adaptés aux caractéristiques de chaque entreprise, permettant aux managers de maintenir les risques à un niveau acceptable pour l'entreprise. Cette gestion poursuit principalement quatre (04) objectifs :

- Créer et protéger la valeur et les actifs de l'organisation ;
- Assurer les processus décisionnels et organisationnels pour favoriser l'atteinte des objectifs ;
- Favoriser la cohérence des actions et des valeurs organisationnelles ;
- Mobiliser et organiser les collaborateurs autour d'une vision partagée des risques clés et les sensibiliser aux risques inhérents.

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

### b. La politique de gestion des risques informatiques :

La politique de gestion des risques informatiques est généralement incluse dans la politique de sécurité informatique.

Il s'agit d'un document qui présente les buts et les orientations du management.

Une politique de sécurité informatique contient quatre (04) thématiques clés que sont :

- ✓ La gestion des risques fondée sur l'évaluation et la réduction des risques ;
- ✓ La qualification de l'information fondée sur une classification de l'information destinée à adapter le niveau de protection de celle-ci ;
- ✓ La conformité des systèmes avec les politiques et standards de sécurité en vigueur
- ✓ La sensibilisation à la politique de sécurité SI fondée sur une communication adéquate auprès de chaque employé (en modes « push et pull ») selon le CIGREF (2009 : p120).

La politique de gestion des risques informatiques formule les objectifs du dispositif de gestion des risques en cohérence avec la culture de l'organisation, le langage commun utilisé, la démarche d'identification, d'analyse et de traitement des risques et le cas échéant, le seuil de tolérance (HERVE, 2014 : p06).

### c. Les acteurs de la gestion des risques informatiques :

Les principaux acteurs de la gestion des risques informatiques sont : la Direction Générale, le Risk Manager, le RSSI.

#### i. La Direction Générale (DG) :

Selon GREUNING & al. (2004 : p33), il est de la responsabilité de l'équipe dirigeante, et de la Direction Exécutive de définir les orientations stratégiques et de les suivre en ce qui concerne la gestion des risques au sein de l'organisation.

En effet, la Direction Générale fait partager à toute l'entreprise la vision d'une gestion rigoureuse et efficace du risque, donne l'impulsion de celle-ci et crée les conditions de mise en œuvre du processus de management des risques. Il est également de sa responsabilité d'instaurer une bonne culture de gestion des risques au sein de l'entreprise sur le giron de la gouvernance des risques avec pour objectif principal, la maîtrise des risques.

#### ii. Le Risk Manager (RM) :

Selon le CLUSIF- AMRAE (2006 : p04), le RM est chargé de concevoir les méthodes et les outils de gestion des risques (cartographie des risques, etc.), d'élaborer et de mettre en œuvre la politique et le plan d'assurance de l'entreprise, de conseiller les métiers sur les mesures de prévention, de protection, de détection et de réaction face au risque.

#### iii. Le responsable de la sécurité des systèmes d'information (RSSI) :

Le RSSI (responsable de la sécurité des systèmes d'information) est chargé de prévenir les risques dès leur phase de développement, de proposer des plans d'action de réduction et de contrôle des risques, de suivre la mise en place des actions décidées, de rendre compte à la

Direction Générale et de communiquer sur la sécurité du SI avec le ou les Directeurs en charge des SI (CLUSIF-AMRAE, 2006 : p04).

### d. Méthodes de gestion des risques liés au système d'informatique

Le tableau ci-dessous présente les différentes méthodes les plus fréquentes :

Tableau 1 :Différentes méthodes de gestion des risques informatiques (source moi-même )

| **Méthode de type « Analyse des risques»** | **Méthode de type « Approche par les processus»** |
|---|---|
| • **MARION**<br>• **MEHARI**<br>• **MADS-MOSAR**<br>• **EBIOS RM** | • **Approche d'ISRM**<br>• **Approche du DSIS**<br>• **Approche de COBIT**<br>• **Norme BS7799** |

**Dans cette partie on a choisi la méthode EBIOS RM :**

### i. Définition de la méthode EBIOS Risk Manager (EBIOS RM) :

Il s'agit d'une méthode numérique d'évaluation et de traitement des risques. Il fournit une boîte à outils adaptable dont l'utilisation varie selon les objectifs du projet et est compatible avec les normes en vigueur en matière de gestion des risques 3 et de sécurité numérique. EBIOS RM peut évaluer les risques numériques et déterminer les mesures de sécurité à mettre en œuvre pour les maîtriser. Il peut également vérifier les niveaux de risque acceptables et s'inscrire dans un processus d'amélioration continue à long terme. Enfin, cette méthode peut fournir des ressources et des arguments utiles pour la communication et la prise de décision au sein de l'organisation et de ses partenaires

La méthode EBIOS RM peut être utilisée à plusieurs fins :

• Établir ou renforcer des processus de gestion des risques numériques au sein de l'organisation ;

• Évaluer et traiter les risques liés aux projets numériques, notamment en vue d'obtenir une certification de sécurité ;

• Définir le niveau de sécurité que le produit ou le service doit atteindre en fonction du cas d'utilisation attendu du produit ou du service et des risques à traiter, par exemple, afin d'obtenir une certification ou une approbation.

Elle s'applique aux organisations publiques et privées, quels que soient leur taille, leur secteur d'activité et que leurs systèmes d'information soient en cours de développement ou existent déjà.

### ii. Une démarche itérative en 5 ateliers :

La méthode EBIOS Risk Manager adopte une méthode de gestion des risques numériques, partant du plus haut niveau, et atteignant progressivement les fonctions métiers et techniques en étudiant les scénarios de risques possibles. Il vise à réaliser l'intégration entre « conformité » et « scénario » en positionnant ces deux méthodes complémentaires là où elles apportent la plus grande valeur ajoutée. Cette méthode se caractérise par la pyramide de gestion des risques numériques

La méthode de conformité peut déterminer le fondement de sécurité sur lequel repose la méthode des scénarios pour développer des scénarios de risque particulièrement ciblés ou complexes. Cela suppose que les accidents et les risques environnementaux soient traités a priori par des méthodes de conformité au sein du socle de sécurité. Par conséquent, comme décrit dans la méthode EBIOS RM, l'évaluation des risques par scénario se concentre sur les menaces délibérées.

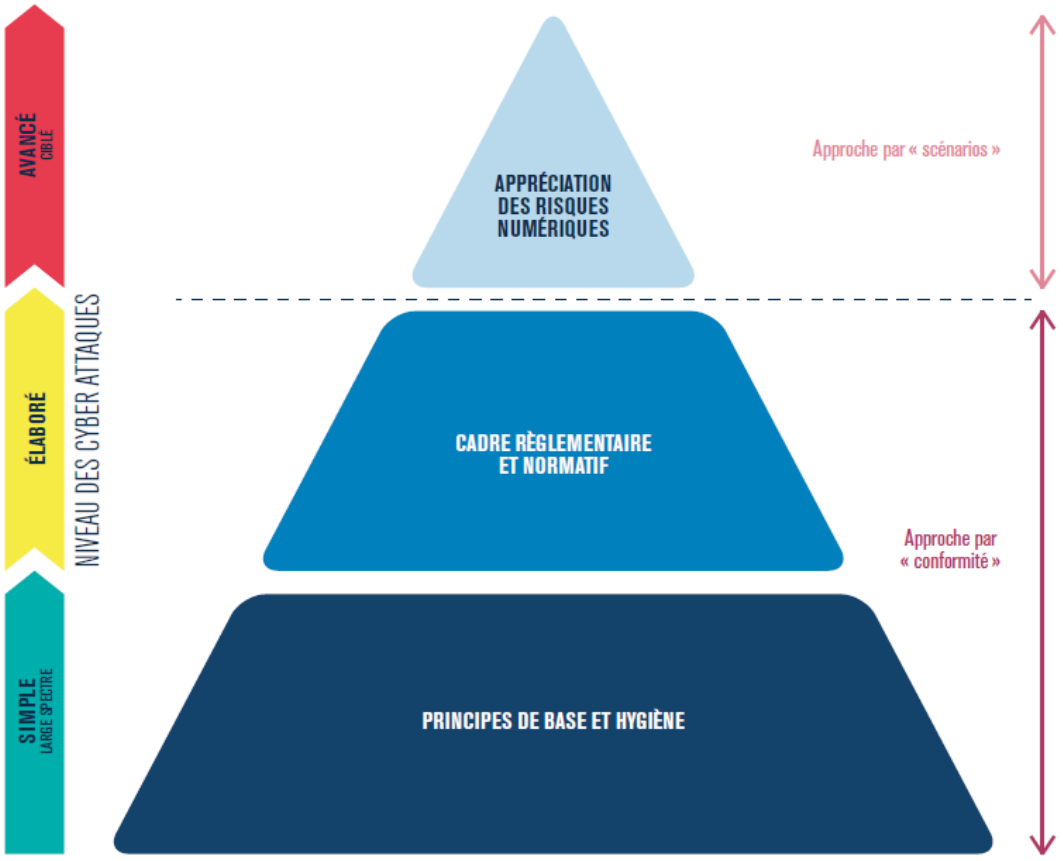



Figure 1 :Pyramide du management du risque numérique( Source Guide méthode Ebios RM )

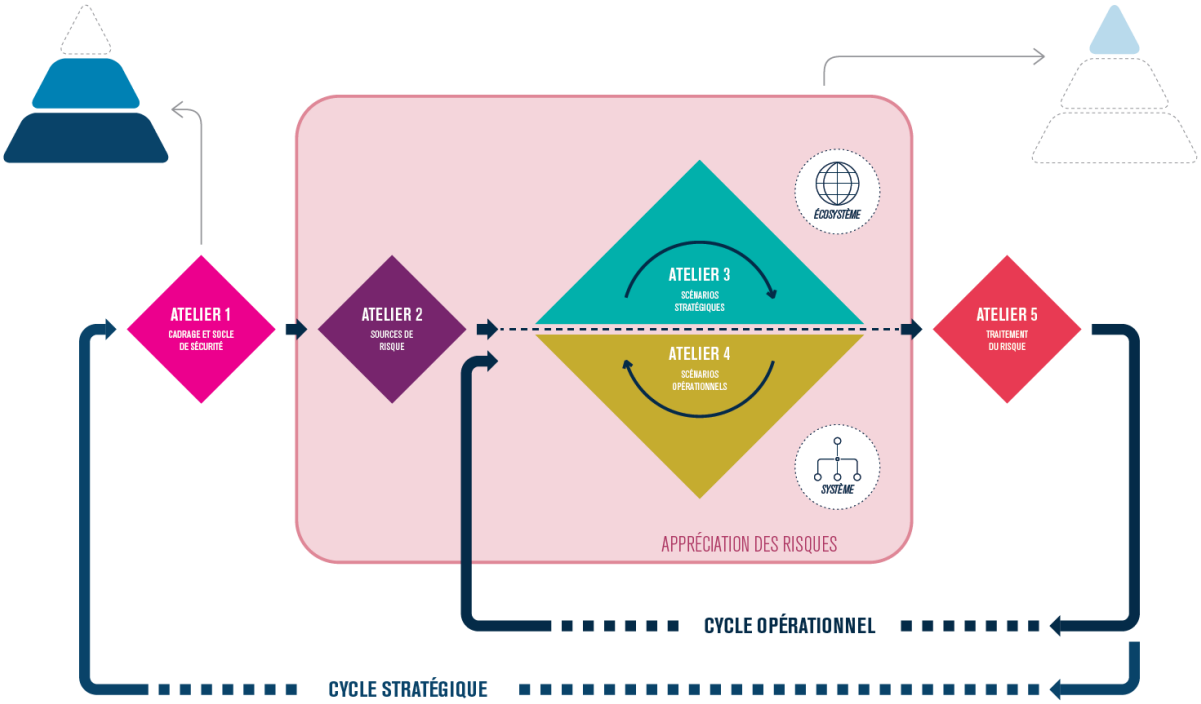



Figure 2:Une démarche itérative en 5 ateliers ( Source Guide méthode Ebios RM )

**Technique d'administration réseau :**

Cette technologie permet aux administrateurs réseau d'assurer une gestion efficace du réseau, c'est-à-dire qu'elle permet aux administrateurs réseau de planifier et de définir des plans de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité du réseau.

## 2. Notions générales sur le plan de reprise d'activité

### a. Définition Plan de reprise d'activité PRA :

Un plan de reprise d'activité peut être défini comme un ensemble de mesures préventives définies en cas de situation critique imprévue pouvant affecter le système d'information de l'entreprise. Par exemple, il peut s'agir d'un dysfonctionnement ou d'un dysfonctionnement provoqué par une attaque de pirate informatique ou une catastrophe (catastrophe naturelle, inondation, incendie). Le PRA ne doit pas être confondu avec le PCA (Plan de Continuité d'Activité). Ce dernier vise à assurer la meilleure disponibilité de l'infrastructure informatique. En ce qui concerne le PRA, il décrit l'ensemble des processus visant à assurer la reprise des activités le plus rapidement possible après une interruption partielle ou totale. Il prend la forme de documents écrits pour préciser progressivement les actions à mener face aux différents types d'incidents.

**b. Les plans PRA existants :**

Tableau 2 : Les plan existants(élaboré par nos soins)

| Nom français | Nom anglais | Objectif |
|---|---|---|
| Plan de reprise d'activité (PRA) | Disaster Recovery Plan (DRP) | • Fournir les procédures<br>• Détaillées nécessaires pour faciliter la reprise des activités à partir d'un autre site. |
| Plan de continuité d'activité<br><br>(PCA) | Business Continuity Plan (BCP) | • Fournir les procédures nécessaires pour maintenir les activités essentielles suite à une importante perturbation. |
| Plan de continuité des<br><br>opérations (PCO) | Continuity of Operations plan (COOP) | • Fournir les procédures et les capacités nécessaires pour transférer et maintenir les fonctions stratégiques et essentielles d'une organisation vers un autre site. |
| Plan de communication de crise (PCC) | Crisis Communications Plan<br><br>(CCP) | • Fournir les procédures nécessaires pour diffuser les rapports de situation aux employés et au public. |
| Plan de réponse aux incidents informatiques (PRII) | Cyber Incident Response Plan (CIRP) | • Fournir les stratégies pour Détecter, répondre, et limiter les conséquences d'une action malveillante. |
| Plan d'intervention d'urgence (PIU) | Emergency Response Plan<br><br>(ERP) | • Fournir les procédures nécessaires pour réduire au minimum les pertes en vies humaines et protéger les biens contre des dommages, en cas de menace physique. |

### c. Les objectifs du Plan de Reprise d'activité :

Le processus à déployer est lié aux caractéristiques de l'entreprise et de ses départements d'activité.

Ainsi, pour certaines entreprises ayant l'informatique comme cœur de métier, le plan de relance sera particulièrement stratégique.

Cependant, les objectifs de la PRA sont généralement les mêmes :

- Réduisez les temps d'arrêt pour les activités en cours
- Former et éduquer tous les employés
- Minimiser les dommages matériels
- Mettre en œuvre des opérations de sauvegarde des données (backup)
- Protéger l'infrastructure informatique (serveurs, équipements informatiques)

### d. Le contenu du Plan de Reprise d'activité

Le plan de reprise d'activité ne sera pas vrai au période de l'catastrophe. Il s'agit de définir l'ensemble des approches requises en cas discontinuité strictement également celles qui permettent de délibérer ces dernières.

Le PRA doit plus nettoyer lequel dispositifs doivent être mis en lieu dans tourner la sécurité et l'intégrité du système d'information, par constitution :

- Présence de détecteurs d'intrusion physique
- Présence en nombre suffisant de détecteurs d'incendie et de dégât des eaux
- Systèmes de ventilation pour limiter les risques de surchauffe
- Systèmes de restauration et de sauvegarde des données
- Formation des usagers

Bref, le PRA est un document indispensable qui doit être rédigé par le DSI et son équipe, quels que soient la taille et le domaine d'activité de l'entreprise. Celui-ci doit être le plus détaillé possible et faciliter le déploiement de mesures pour reprendre les activités efficacement et rapidement dans des situations souvent inattendues et d'urgence

# CHAPITRE 2 : CADRE MÉTHODOLOGIQUE ET CONTEXTE ORGANISATIONNEL

La validité de toute étude repose sur la méthodologie qui est suivie pour la conduire. En particulier, cette méthodologie concerne les démarches utilisées pour obtenir les principaux matériaux de l'étude, c'est-à-dire les données et les procédures relatives à leur traitement. Dans ce chapitre, deux sections existent. La première section consiste à voir le cadre méthodologique de la recherche, par ailleurs, On a les raisons et les objectifs de choix de thème, le paradigme de l'étude, le choix du type d'étude, les instruments de mesure, la collecte des données et la méthode de traitement des données, la deuxième section présenter l'organisme d'accueil.

## Section n°01 : La méthodologie de recherche

### 1. Les raisons et les objectifs de choix de thème

On a choisi le thème « Mise en place d'une démarche de gestion des risques informatiques au sein de la direction Technologies de l'Information en utilisant la méthode EBIOS RM » pour plusieurs raisons :

- C'est un sujet intéressant qui conduit les responsables à chercher une politique pour assurer une gestion des risques informatiques efficace dans l'organisation ;
- En plus, est un sujet d'actualité surtout avec le taux élevé des risques informatiques dans l'organisation ;
- Montrer le rôle de gestion des risques dans l'anticipation des risques informatiques.

Nos objectifs principaux qui nous poussent à choisir ce thème :

- Maintenir un niveau élevé de motivation concernant le sujet ;
- Avoir des informations courantes sur le sujet ;
- Identifier, formaliser et implémenter des standards et des procédures de gestion des risques et former tous les acteurs à leur utilisation ;
- Intégrer la dimension culture du risque lié aux SI dans l'élaboration de la cartographie des risques et sensibiliser la direction, le personnel de façon à favoriser l'émergence de cette culture et d'un cadre normatif de gestion de risque au sein de la direction informatique ;
- Analyser le niveau de contribution actuel de gestion des risques dans la direction liée au système informatique afin de proposer des axes d'amélioration

### 2. Paradigme de l'étude

La démarche globale de cette recherche repose sur une approche hypothético-inductive en utilisant spécifiquement un paradigme constructiviste, reposant sur l'idée que notre image de la réalité, ou les notions structurant cette image, sont le produit de l'esprit humain en interaction avec cette réalité, et non le reflet exact de la réalité elle-même, selon Jean-Michel Besnier, (2005 : p 44).

Selon Gauthier (1993 : p132), le chercheur « doit proposer une logique de démonstration des preuves qui permettra de voir si un dossier est favorable ou défavorable aux hypothèses construites ainsi que les significations que les gens attribuent à leurs expériences ». C'est pourquoi la perception des acteurs est sollicitée par des données fiables afin de faire une exploitation empirique de l'objectif principal de recherche.

## 3. Approche méthodologique

La recherche s'inscrit dans une recherche qualitative en sciences de gestion. Il se concentre sur la recherche interventionnelle unique au sein des organisations publiques. L'approche qualitative est la plus appropriée car elle permet de comprendre et de répondre à la question initiale : Quelle est la meilleure façon d'assurer une meilleure gestion des risques informatiques au sein du Bureau des technologies de l'information ?
Les méthodes qualitatives permettent également de considérer :

- La richesse des mots utilisés par les acteurs organisationnels. Comme Huber man et Miles (1991) l'ont souligné, les mots ont des caractéristiques « évocatrices », « spécifiques » et « significatives » plus convaincantes que les « chiffres ».

- Rechercher des faits socio-économiques à travers la littérature, des entretiens semi-directifs et des observations dans le « milieu naturel ».

Ces deux raisons permirent de mieux cerner la complexité du phénomène à étudier. Quant au choix d'une recherche-intervention, comme stratégie de recherche, tel qu'elle est définie par Savall et Zardet (1995 : p104) « Cette recherche s'organise autour d'un processus d'interactivité cognitive entre les acteurs de l'entreprise et l'équipe de recherche », donc la RI consiste à aider, sur le terrain, à concevoir et à mettre en place des modèles, outils et procédures de gestion adéquats, à partir d'un projet de transformation plus ou moins complètement défini, avec comme objectif de produire à la fois des connaissances utiles pour l'action et des théories de différents niveaux de généralité en sciences de gestion selon (Albert DAVID,2000), semblé la plus appropriée pour aborder la question centrale de recherche.

## 4. Délimitation du périmètre d'investigation

Les investigations sur terrain n'ont pas concerné toutes les structures de l'organisation. Le choix était sélectif. Concrètement cela concernait la Direction Informatique (DI) qui s'occupe du système informatique au sein de la Direction Technologies de l'information.

## 5. Recueil des données

Pour mener à bien la recherche, On a mobilisé trois approches, à savoir : l'observation participante, l'étude documentaire et les entretiens, que nous présenterons successivement selon le principe de triangulation

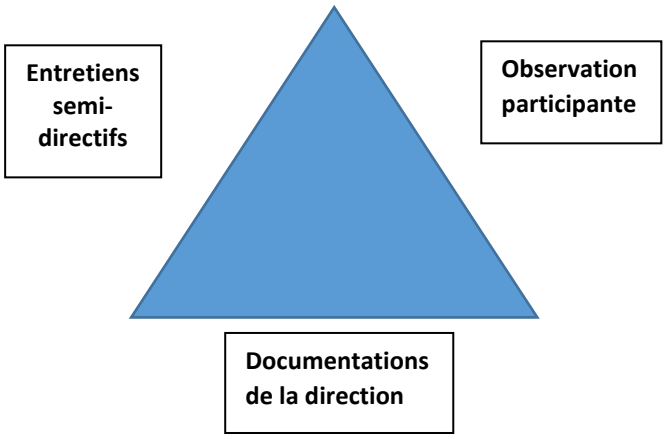



Figure 3: Triangulation de trois principales sources de données (source nous-même)

- **L'entretien** :

L'entretien est considéré comme principal mode de collecte de données primaires dans la recherche. Selon (Thiétart et Coll 2007), « l'entretien est une technique destinée à collecter, dans la perspective de leur analyse des données discursives reflétant notamment l'univers mental conscient ou inconscient des individus ». On a opté pour l'entretien semi-directif ; qui permet de centrer le discours des acteurs interviewés autour de différents thèmes définis au préalable dans un guide d'entretien ; avec les différents acteurs intervenants dans la gestion des risques informatiques au sein de la DTI y inclut les responsables de chaque sous-direction et chef de bureau.

- **L'observation participante :**

L'observation est la deuxième source de données. Elle peut être définie comme étant « une technique de collecte de données primaires visibles et audibles ». (Marie Laure et autre, 2008 p. 140).

On considère que cette source d'information n'est pas une source de données mineur par rapport à l'entretien mais elle revête toute l'importance nécessaire à la complémentarité des documentations de la direction.

Observation participante de les données. En effet, l'objet de la recherche qui est axé sur la gestion des risques à oblige à étudier ce dernier sur le vif de l'action.
Les observations ont été réalisées au fur et à mesure de l'avancement des investigations commençant par l'observation des faits et des dires qui permis de formaliser la problématique jusqu'à l'achèvement de l'étude.

- **Collecte de documents :**

La documentation est la troisième source de données que mobilisée, le rôle des documents consiste essentiellement à corroborer des informations et à augmenter la validité des autres sources.

Nos principaux supports documentaires sont : les sites, et les livres.

En effet, la confrontation des trois sources d'information (l'entretien, l'observation et la documentation de la direction) permet de comparer entre ce qu'on dit (données issues des entretiens), ce qu'on fait (données issues de l'observation) et ce qu'on écrit (données issues de la documentation).

### 6. Les Avantages et les obstacles de la recherche

➢ **Les Avantages :**

- Décrire le domaine de la recherche scientifique.
- Mettre en pratique les connaissances acquises dans le cursus scolaire (ENSM) en passant de la théorie à la pratique.
- Comparer les connaissances scientifiques acquises à l'école avec la situation réelle sur le lieu de travail de l'organisation.
- Bénéficier des connaissances des cadres supérieurs. Il en va de même pour la possibilité d'apprendre à le faire.
- Acquérir des compétences en gestion et présentation des données.

➢ **Les obstacles :**

- La durée limitée du stage.
- La confidentialité des données à son influencé sur le niveau de détails perçu lors remplissages des questionnaires.
- Le manque des ouvrages qui traite le thème.

## Section n°02 : Présentation de l'organisme d'accueil

### 1. Présentation de la SONATRACH

Sonatrach est la plus grande compagnie pétrolière et gazière en Algérie et en Afrique. Il comprend l'exploration, la production, le transport par pipeline, le traitement et la commercialisation d'hydrocarbures et de leurs dérivés. Sonatrach adopte une stratégie diversifiée et développe des activités dans les domaines de la production d'électricité, des énergies nouvelles et renouvelables, du dessalement, de la recherche et de l'exploitation minière.

Poursuivant une stratégie internationale, Sonatrach est présente en Algérie et dans de nombreuses régions du monde : Afrique (Mali, Niger, Libye, Égypte), Europe (Espagne, Italie, Portugal), Amérique latine (Pérou) et États-Unis. Le volume des exportations s'élevait à près de 561 milliards de dollars américains, Sonatrach se classe au premier rang en Afrique et au 12e rang mondial. C'est également le quatrième exportateur mondial de gaz naturel liquéfié, le troisième exportateur de gaz de pétrole liquéfié et le cinquième exportateur de gaz naturel.

- 1ère Compagnie Africaine,
- 14ème Compagnie pétrolière Mondiale,

- 13ème Compagnie Mondiale concernant les hydrocarbures liquides (réserves et production)
- 6ème Compagnie Mondiale en matière de Gaz Naturel (réserves et production)
- 5ème exportateur mondial de Gaz Naturel
- 4ème exportateur mondial de GNL
- 3ème exportateur mondial de GPL

Que veut dire le mot SONATRACH ?

SO : SOCIETE

N'A : NATIONALE

TRA : TRANSPORT

C : COMMERCIALISATION

H : HYDROCARBURE

**Société Nationale du Transport et de la Commercialisation des Hydrocarbures.**


Figure 4 : Logo de l'entreprise SONATRACH(Profil/Site de SONATRACH, 2021)

## 2. Organigramme de la SONATRACH

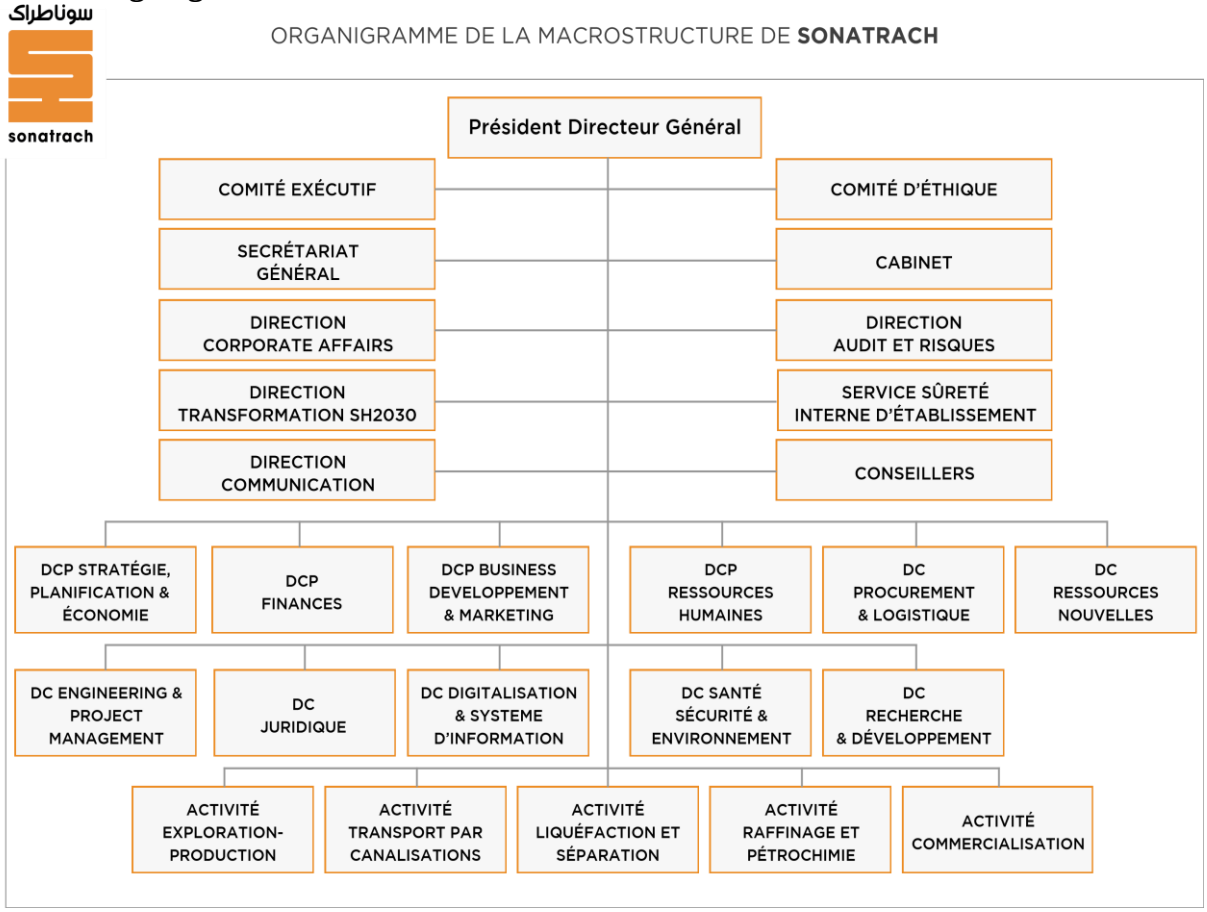



Figure 5:Organigramme du SONATRACH(Profil/Site de SONATRACH, 2021)

## 3. Politique de sécurité SI de SONATRACH

Mesures de contrôle à mettre en œuvre :

1. Le service responsable de l'ISM doit formuler des politiques globales et spécifiques pour la sécurité de l'information, et stipuler clairement le contrôle et les exigences de la sécurité de l'information ;

2. La politique générale de sécurité de l'information doit être cohérente avec les exigences de la stratégie de l'organisation ;

3. Le service responsable du GSI doit s'assurer que les contrôles et les exigences contenus dans la politique de sécurité sont mis en œuvre ;

4. La politique globale de sécurité de l'information doit être confirmée par le comité de sécurité de l'information et approuvée par le premier responsable de l'organisation, s'il existe un comité de sécurité de l'information ;

5. La direction s'assure que la politique de sécurité est diffusée aux parties concernées (employés et tiers de l'organisation) ;

6. Les politiques de sécurité doivent être examinées et mises à jour à des intervalles de temps réguliers, ou en cas de modification des exigences législatives, réglementaires et normatives pertinentes. Toute mise à jour doit être documentée et adoptée par la Direction ;

7. Les politiques de la sécurité de l'information doivent être déclinées du présent référentiel, et peuvent être soutenues par les normes, les standards et les bonnes pratiques en matière de sécurité de l'information.

## 4. Organisation de l'Activité Commercialisation

### ❖ Missions essentielles de l'Activité Commerciale :

- La définition, l'élaboration et la mise en œuvre de la politique et des stratégies de commercialisation et de valorisation des hydrocarbures primaires et transformés, à l'international et sur le marché national, dans le cadre des objectifs stratégiques de SONATRACH ;
- La définition des stratégies de maîtrise des risques de marché, de contreparties et des risques opérationnels (réglementaires, environnementaux, etc.) ;
- L'approvisionnement du marché national en produits pétroliers et gazeux ;
- La sécurisation des marchés traditionnels de la Société et la consolidation de sa position dans son rôle d'exportateur capable de fournir la flexibilité requise à des conditions compétitives ;
- La recherche continue de nouveaux débouchés en vue de la diversification et/ou la promotion des exportations et la recherche de la meilleure valorisation des produits exportés y compris les quantités additionnelles ;
- La conduite des négociations avec les clients étrangers et nationaux ;
- La participation aux négociations commerciales avec les partenaires ;
- La gestion des contrats de vente et d'achat ainsi que les contrats d'importation des hydrocarbures ;
- La participation à la génération d'une plus-value sur les segments internationaux de valorisation industrielle des ressources en hydrocarbures de SONATRACH ;
- La coordination avec les Activités de la Société afin d'optimiser la commercialisation et la valorisation des produits ;
- La gestion des contrats de Processing du Pétrole Brut à l'international ;
- La contribution et le support en expertise nécessaire au développement des activités de la Société, ainsi que des filiales du groupe à l'échelle nationale et internationale ;
- Le reporting auprès de la Direction Générale de SONATRACH et des instances de tutelle.

### ❖ Organisation de l'Activité Commerciale :

L'Activité Commercialisation est composée des structures suivantes :

- Une Division Commercialisation Pétrole Brut et Produits Pétroliers ;
- Une Division Commercialisation Gaz ;
- Une Division Ventes Marché National ;

- Une Coordination Unités Portuaires ;
- Une Direction Transport Maritime ;
- Une Direction Etudes, Planification et Performances ;
- Une Direction Finances ;
- Une Direction Ressources Humaines ;
- Une Direction Technologies de l'information ;
- Une Direction Juridique ;
- Une Direction Moyens Généraux ;
- Un Département Contrôle Interne ;
- Un Assistant Sûreté Interne d'Etablissement ;
- Une Cellule HSE ;
- Deux Conseillers.

❖ **Organigramme de l'activité commercialisation :**

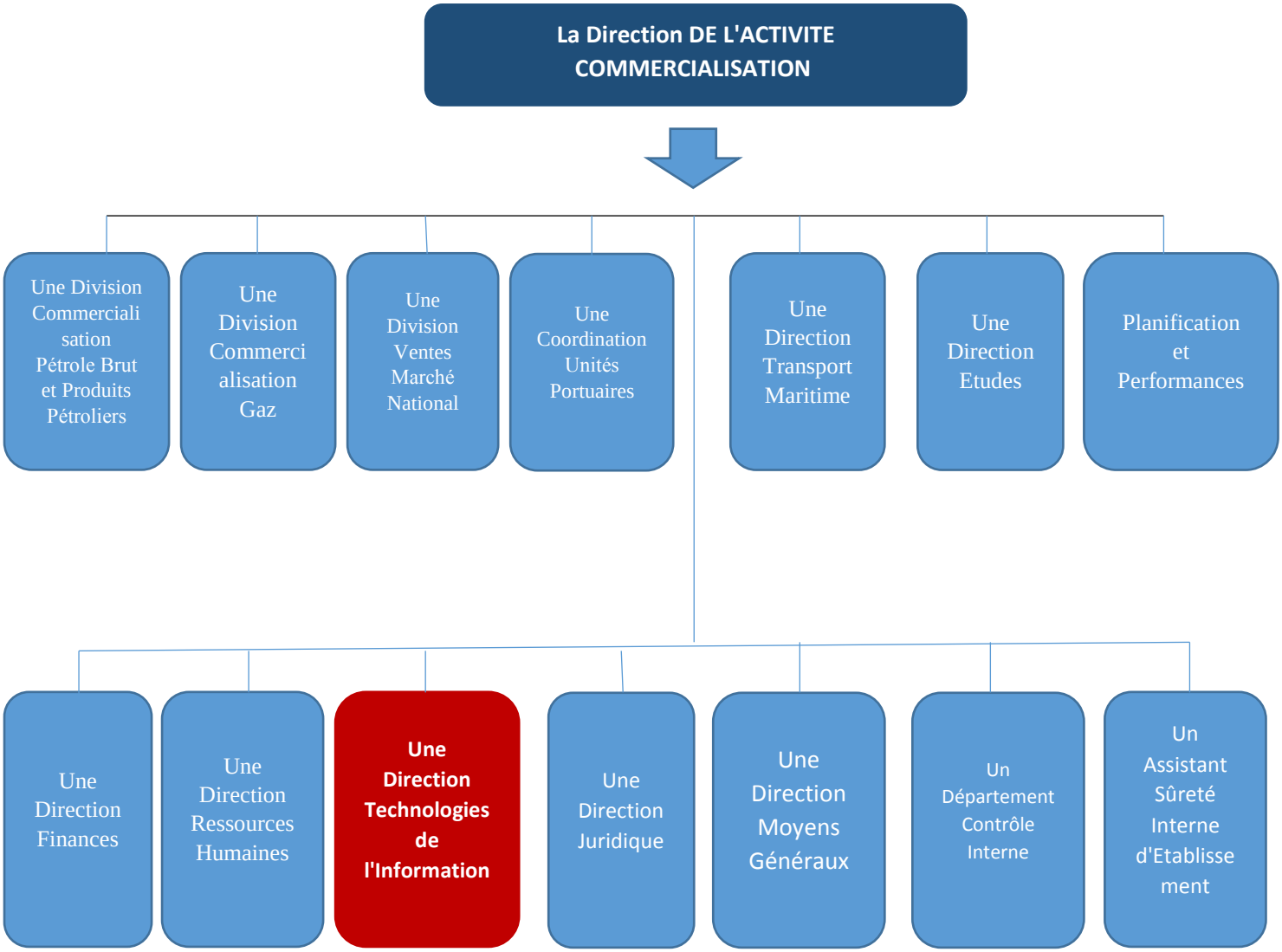



Figure 6: Organigramme de l'activité commercialisation . (Source moi-même)

### 5. Direction Technologies de l'Information

La Direction Technologies de l'Information est organisée comme suit :

- ✓ Un Département Solutions Métiers ;
- ✓ Un Département Réseaux et Systèmes ;
- ✓ Un Département Sécurité des Systèmes d'Information.

❖ **Missions essentielles**

- L'exploitation, le développement et le maintien en conditions opérationnelles des plateformes d'infrastructures réseaux, télécommunications, WAN et des solutions COE pour les structures de l'Activité Commercialisation, y compris pour les Unités Portuaires et les services ventes Skikda, Alger et Arzew
- La mise en œuvre des politiques et des stratégies de la Société en matière de normes et standards, de systèmes d'information et des technologies de l'information
- La contribution à la construction, au déploiement et à la mise en œuvre de l'ERP, de la Business Intelligence et de toutes les solutions informatiques
- L'intégration et la convergence des solutions IT business, en conformité avec le programme de Digitalisation de SONATRACH
- Le développement et le maintien en conditions opérationnelles des solutions spécifiques à l'Activité tout en veillant sur l'intégrité, la cohérence et la sécurité des données
- La gestion optimale du Datacenter mis sous la responsabilité de l'Activité
- L'appui, le conseil et l'assistance aux structures de l'Activité en matière de technologies de l'information, de systèmes d'information et des télécommunications
- L'élaboration et le suivi de la réalisation des prévisions budgétaires du volet technologies de l'information et télécommunications du Plan Annuel et PMT de l'Activité
- Le reporting régulier à la hiérarchie et à la DC DSI

## 6. Cartographie applicative du système d'information de SH COM

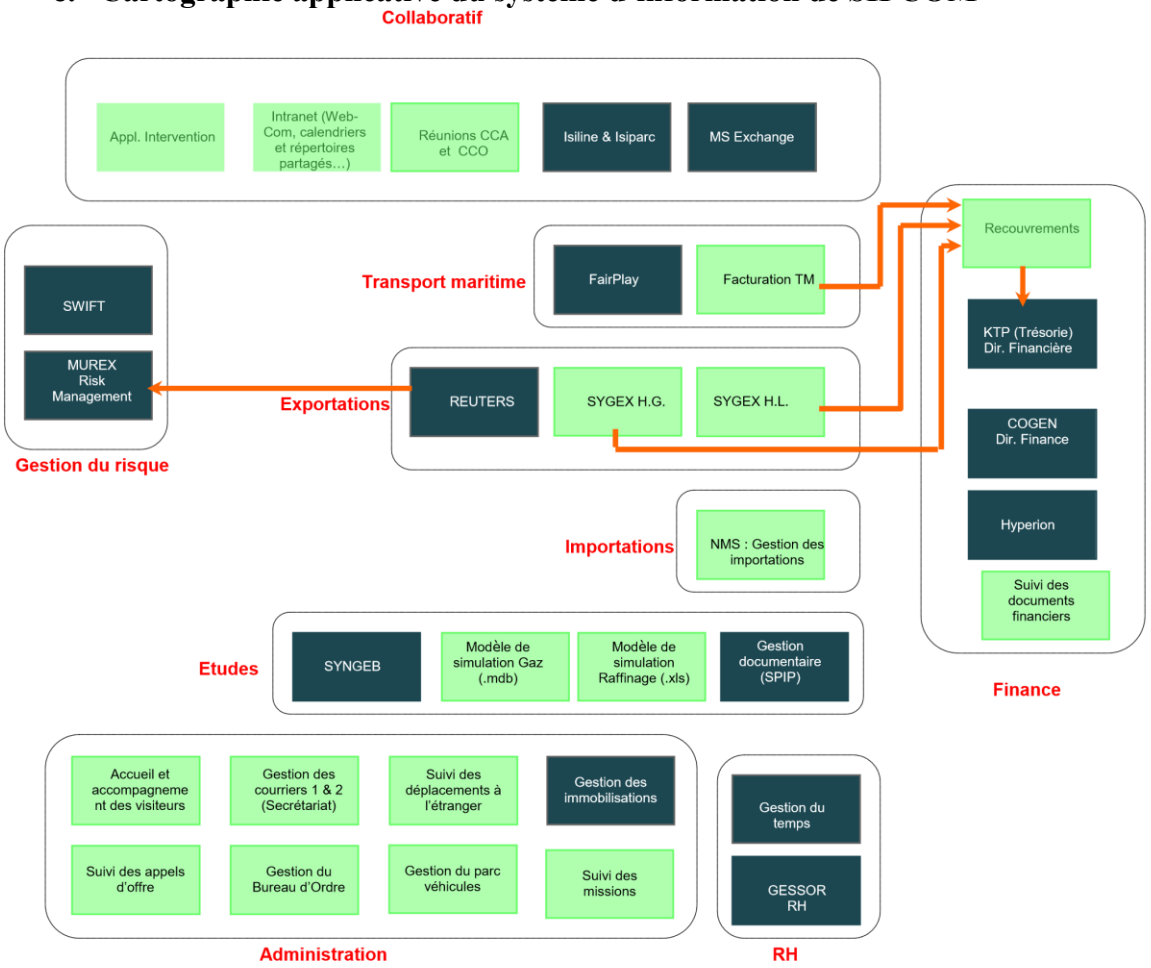



Figure 7:Cartographie applicative de l'activité Commercialisation (élaboré par nos soins sur la base des documents de l'entreprise)

# CHAPITRE 3 : RÉSULTATS ET DISCUSSION

**Section 1 : Identification des risques majeurs spécifiques au SI**
**Risques :**

- Gestion non maîtrisée des licences informatiques
- Allocation des ressources non optimisée concernant des projets informatiques
- Accès non autorisé à des données confidentielles
- Mauvaise gestion des habilitations suite aux mouvements de personnel
- Risque d'erreurs liées à une mauvaise utilisation et connaissance du système d'information
- Risque lié à l'appauvrissement et la perte de connaissance des outils informatiques
- Risque d'accès illicite au système / piratage de fichiers commerciaux
- Risque d'accès à l'information stratégique par des personnes internes/externes au service et à la société
- Erreurs générées par les outils informatiques supportant la maintenance des équipements
- Obsolescence de vieilles applications
- Perte de continuité de services informatiques
- Manque d'agent de sécurité
- Le personnel agit sans suivre des règles
- Tout le monde peut accéder facilement à toutes les données
- Un équipement non répertorié ne fonctionne pas correctement
- Utilisation d'un équipement au-delà des besoins légaux

**Menaces :**

- Perte ou altération des preuves empêchant toute investigation
- Intrusion de personne
- Menaces physiques (Incendies, inondations, tremblements de terre...)
- Défaillance des prestations de tiers
- Interruption des activités métiers
- Accès non autorisé
- Abus de droits
- Reniement d'actions

**Section 2 : Modélisation du système étudié en méthode EBIOS RM**
**Atelier 1 : cadrage et socle de sécurité**

Le premier atelier vise à identifier l'objet de l'étude, les participants aux ateliers et le cadre temporel. Au cours de cet atelier, les missions, valeurs métier et biens supports relatifs à l'objet étudié. Les événements redoutés associés aux valeurs métier et évalue la gravité de leurs impacts. Le socle de sécurité et les écarts.

- **NOTE :** l'atelier 1 permet de suivre une approche par « conformité », correspondant aux deux premiers étages de la pyramide du management du risque numérique et d'aborder l'étude du point de vue de la « défense ».

Tableau 3 : Identifier l'objet de l'étude (élaboré par nos soins sur la base des documents de l'entreprise)

| **Mission** | **Identifier** | | | | |
|---|---|---|---|---|---|
| **Dénomination de la valeur métier** | **DTI** | | | **Le développement et le maintien des plateformes d'infrastructures réseaux** | **Traçabilité et control** |
| **Nature de la valeur métier** | **Processus** | | | **Processus** | **information** |
| **Description** | **Le développement et le maintien l'intégrité, la cohérence et la sécurité des données** | | | | **Informations permettant d'assurer le contrôle qualité** |
| **Entité ou personne responsable(interne ou externe )** | **Informaticienne** | | | | |
| **Entité ou personne responsable** | **Serveurs bureautique Internes** | **Serveurs bureautique externes** | **Responsable Métier** | | **Serveurs bureautique Internes** |
| **Description** | **Serveurs bureautiques permettant de stocker l'ensemble des données** | **Serveurs bureautiques permettant de stocker une partie des données** | **Ensemble de machines et équipements informatiques** | | **Serveurs bureautiques permettant de stocker l'ensemble des données relatives à la traçabilité et au contrôle, pour les différents processus** |
| **Entité ou personne responsable(interne ou externe )** | **DSI** | **DSI** | **DSI** | | **DSI** |

**Atelier 2 : Sources de risque**

- Identifier les sources de risque (SR) et leurs objectifs visés (OV),

Tableau 4 : Identifier les couples SR /OV(élaboré par nos soins sur la base des documents de l'entreprise)

| **Sources** | **Objectifs visés** |
|---|---|
| **Hacktiviste** | **Accès non autorisé à des données confidentielles** |
| **Concurrent** | **Un concurrent veut voler des informations en espionnant les travaux de DTI en vue d'obtenir un avantage concurrentiel** |
| **Hacktiviste** | **Accès non autorisé** |
| **Cyber _ terroriste** | **Accès illégitime à des informations confidentielles** |

- Évaluer les couples SR/OV

Tableau 5 : Évaluer les couples SR/OV(élaboré par nos soins sur la base des documents de l'entreprise)

| **Sources** | **Objectifs visés** | **Motivation** | **Ressources** | **Activité** | **pertinence** |
|---|---|---|---|---|---|
| **Hacktiviste** | **Accès non autorisé** | ++ | + | ++ | **Moyenne** |
| **Concurrent** | **voler des informations** | +++ | +++ | +++ | **Elevée** |
| **Hacktiviste** | **Accès non autorisé** | ++ | + | + | **Faible** |
| **Cyber _ terroriste** | **Accès illégitime à des informations confidentielles** | + | ++ | + | **Faible** |

**Atelier 3 : Scénarios stratégiques**

Acquérir une vision claire de l'écosystème et établir une cartographie de menace numérique :

- On a identifié les parties prenantes externes de la société :

Tableau 6 : Les parties prenantes externes de l'écosystème(élaboré par nos soins sur la base des documents de l'entreprise)

| **Catégorie** | **Partie prenante** |
|---|---|
| **Clients** | **C1 - Un carburant** |
| **Clients** | **C2 - l'industrie pétrochimique** |
| **Clients** | **C3 - combustibles** |
| **Partenaire** | **P1 - entreprise pétrolière** |
| **Partenaire** | **P2 - compagnie aérienne** |
| **Partenaire** | **P3 - le transport maritime** |
| **Prestataires** | **F1 – Fournisseurs industriel** |
| **Prestataires** | **F2- Fournisseurs de matériel** |
| **Prestataires** | **F3 - le prestataire informatique** |

L'évaluation de chaque partie prenante a permis d'établir la cartographie de menace numérique ci-après :

C1

C2

C3

P1

P2

P3

F1

F2

F3

Niveau de manace

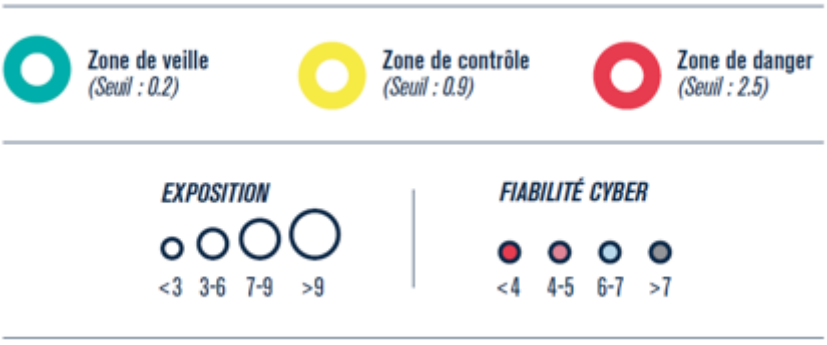



Figure 8: La cartographie de menace numérique(élaboré par nos soins sur la base des documents de l'entreprise)

Tableau 7 : La cartographie de menace numérique(élaboré par nos soins sur la base des documents de l'entreprise)

| Catégorie | Nom | Dépendance | Pénétration | Maturité cyber | Confiance | Niveau menace |
|---|---|---|---|---|---|---|
| **Clients** | **C1** | **1** | **1** | **1** | **3** | **0 ,3** |
| **Clients** | **C2** | **1** | **1** | **2** | **3** | **0,2** |
| **Clients** | **C3** | **1** | **2** | **2** | **3** | **0,3** |
| **Partenaire** | **P1** | **2** | **1** | **1** | **2** | **1** |
| **Partenaire** | **P2** | **2** | **1** | **2** | **4** | **0,25** |
| **Partenaire** | **P3** | **3** | **3** | **2** | **2** | **2,25** |
| **Prestataires** | **F1** | **4** | **2** | **2** | **3** | **1,3** |
| **Prestataires** | **F2** | **4** | **3** | **2** | **3** | **2** |
| **Prestataires** | **F3** | **3** | **4** | **2** | **2** | **3** |

« Un concurrent veut voler des informations en espionnant les travaux de DTI en vue d'obtenir un avantage concurrentiel ». Les trois voies d'attaque suivantes ont été considérées comme pertinentes.

Le concurrent vole les travaux de recherche :

En créant un canal d'exfiltration de données portant directement sur le système d'information de la DTI.

En créant un canal d'exfiltration de données sur le système d'information l'industrie pétrochimique.

En créant un canal d'exfiltration de données passant par le prestataire informatique.

- Le scénario stratégique associé est représenté ci-après. Il est de gravité 3 (grave) selon la cotation effectuée lors de l'atelier 1 sur les valeurs métier

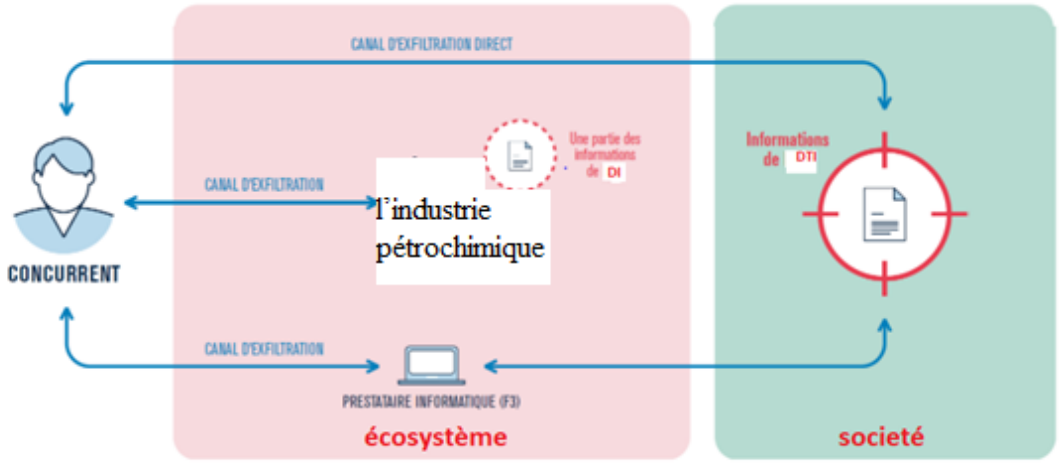



Figure 9 : Scénario stratégique(élaboré par nos soins sur la base des documents de l'entreprise)

En synthèse, scénarios stratégiques ont été retenus :

Tableau 8 : Résultat scénario stratégique(élaboré par nos soins sur la base des documents de l'entreprise)

| **Sources de risque** | **Objectifs visés** | **Chemin d'attaque stratégiques** | **Gravité** |
|---|---|---|---|
| **Concurrent** | Un concurrent veut voler des informations en espionnant les travaux de DTI en vue d'obtenir un avantage concurrentiel | Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données :<br><br>1. portant directement sur le système d'information de DTI ;<br><br>2. sur le système d'information du l'industrie pétrochimique (P2), qui détient une partie des travaux ;<br><br>3. passant par le prestataire informatique F3. | 3<br><br>Grave |

- Définir des mesures de sécurité sur l'écosystème :

Tableau 9 : Les mesures de sécurité sur l'écosystème(élaboré par nos soins sur la base des documents de l'entreprise)

| **Partie prenante** | **Chemin d'attaque stratégiques** | **Mesure de sécurité** | **Menace initial** | **Menace résiduelle** |
|---|---|---|---|---|
| **F2 Fournisseurs de matériel** | **Arrêt de production par compromission de l'équipement de maintenance** | **Réduire le risque de piégeage des équipements de maintenance utilisés sur le système industriel. Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site (permet de réduire la pénétration des fournisseurs de 3 à 2).** | **2** | **1.3** |
| **F3 - le prestataire informatique** | **Vol d'informations en passant par le prestataire informatique** | **Accroitre la maturité cyber du prestataire (2 → 3) : Audit de sécurité (à inclure dans le contrat) ; Suivi du plan d'action interne. Renforcer la protection des données de DTI. Solutions à investiguer: chiffrement, cloisonnement du réseau DTI.** | **3** | 2 |
| **P3** | **Vol d'informations sur le système d'information du laboratoire** | **Diminuer la pénétration des laboratoires (3→ 2) : limitation des données transmises au laboratoire au juste besoin (mauvaise habitude actuelle de « tout » diffuser).** | **3** | **2** |

L'application des objectifs ci-dessus devrait permettre sous 9 à 12 mois de réduire le risque, avec une cartographie de menace numérique résiduelle comme suit :

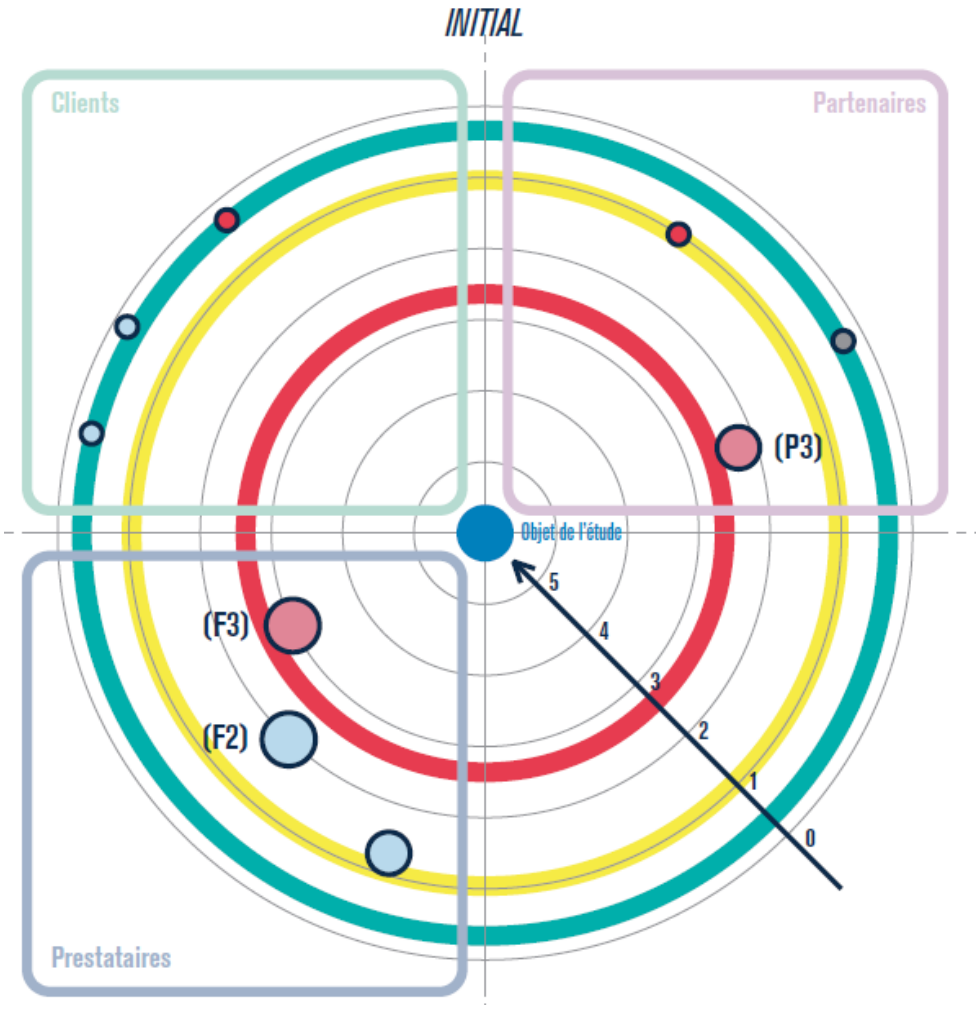



Figure 10:Cartographie de menace numérique initial(élaboré par nos soins sur la base des documents de l'entreprise)

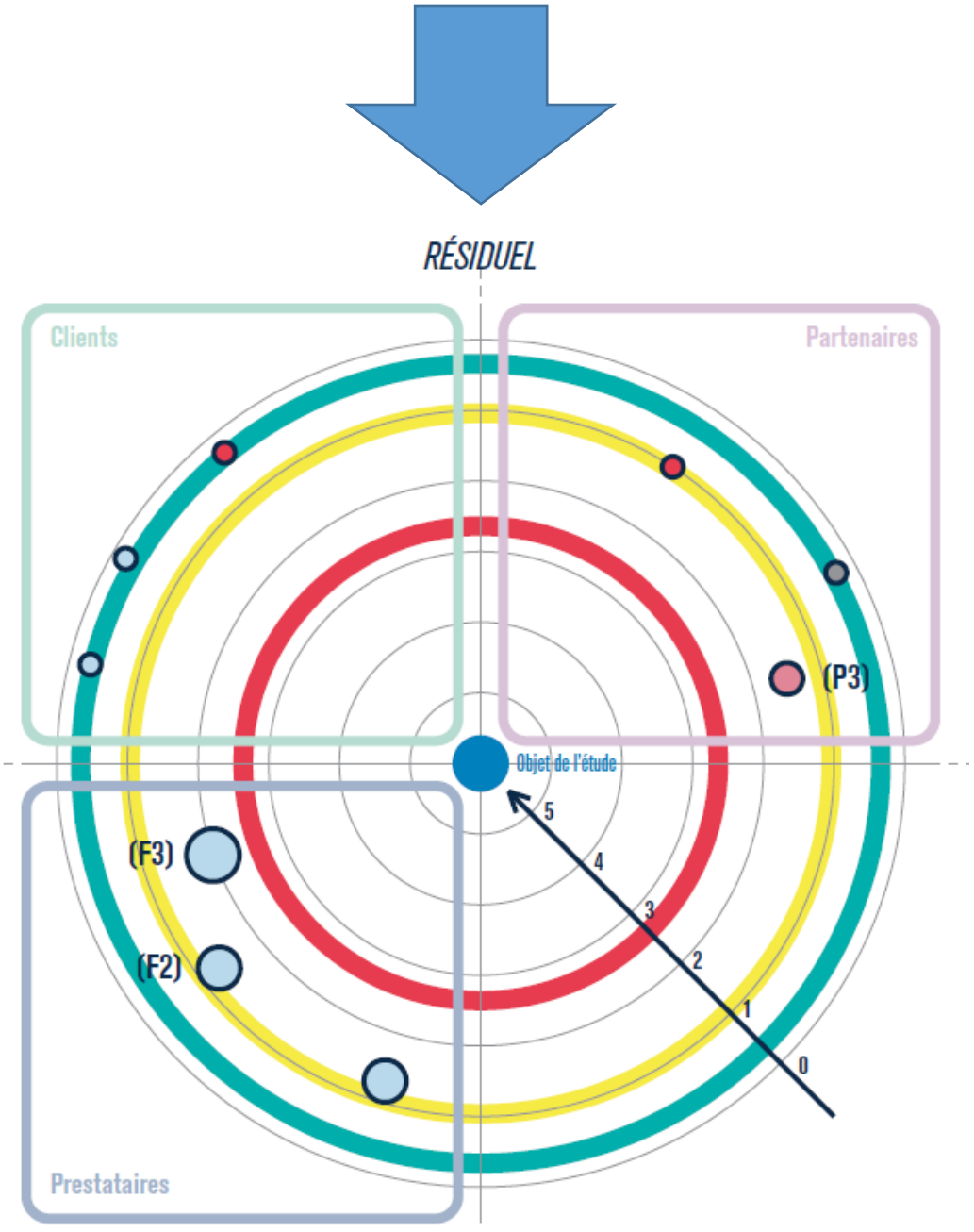



Figure 11:Cartographie de menace numérique résiduelle(élaboré par nos soins sur la base des documents de l'entreprise)

**Atelier 4 : Scénarios opérationnels**

Scénario opérationnel relatif au chemin d'attaque « Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données portant directement sur le système d'information de la DTI : la Direction Technologies de l'Information (de l'entreprise de SONATRACH) » :

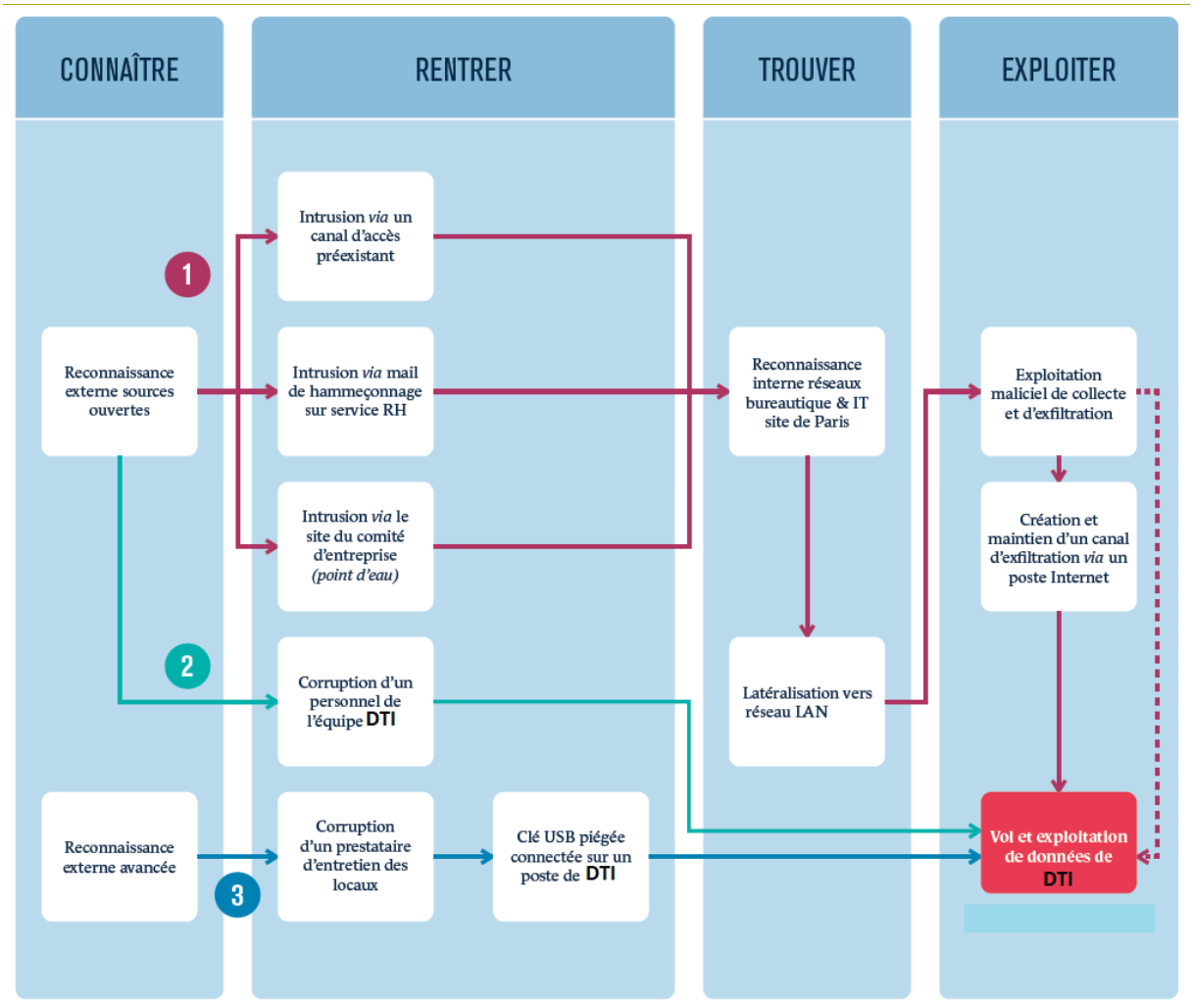



Figure 12 : Scénario opérationnel(élaboré par nos soins sur la base des documents de l'entreprise)

- L'attaquant s'introduit dans le système d'information par une attaque ciblée sur la messagerie du service des ressources humaines en piégeant le site du comité d'entreprise ou en exploitant un canal caché préexistant. Il accède ensuite aux données stratégiques de DTI du fait notamment de l'absence de cloisonnement entre les réseaux internes puis les exfiltre en utilisant le canal caché voire un canal légitime.

- ❖ L'attaquant corrompt un salarié de l'équipe DTI qui récupère ensuite facilement les informations depuis son poste de travail, dans la mesure où aucune action de supervision n'est réalisée.

- ❖ L'attaquant corrompt un personnel d'entretien des locaux et lui demande de brancher une clé USB préalablement piégée sur un poste de travail de DTI. Cette opération est facilitée par le fait que l'entretien des locaux est réalisé en dehors des heures ouvrées, que le personnel d'entretien a accès librement au bureau d'études et que les ports USB ne sont soumis à aucune restriction.

- ➢ **Echelle de vraisemblance globale d'un scénario opérationnel :**

Tableau 10: Echelle de vraisemblance globale d'un scénario opérationnel(élaboré par nos soins sur la base des documents de l'entreprise)

| ➢ **Chemins d'attaque stratégique (associés aux scénarios opérationnelle** | **VRAISEMBLANCE GLOBALE** |
|---|---|
| **Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données portant directement sur le système d'information de la DTI** | **V3**<br><br>**très VRAISEMBLANCE** |
| **Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données sur le système d'information du laboratoire, qui détient une partie des travaux** | **V2**<br><br>**VRAISEMBLANCE** |
| **Un concurrent vole des travaux de recherche en créant un canal d'exfiltration de données passant par le prestataire informatique** | **V4**<br><br>**Quasi certain** |
| **Un hacktiviste perturbe la production en provoquant un arrêt de la production industrielle par compromission de l'équipement de maintenance du fournisseur de matériel** | **V2**<br><br>**VRAISEMBLANCE** |
| **Un hacktiviste perturbe la distribution en modifiant leur étiquetage** | **V1**<br><br>**Peu VRAISEMBLANCE** |

**Atelier 5 : Traitement du risque**

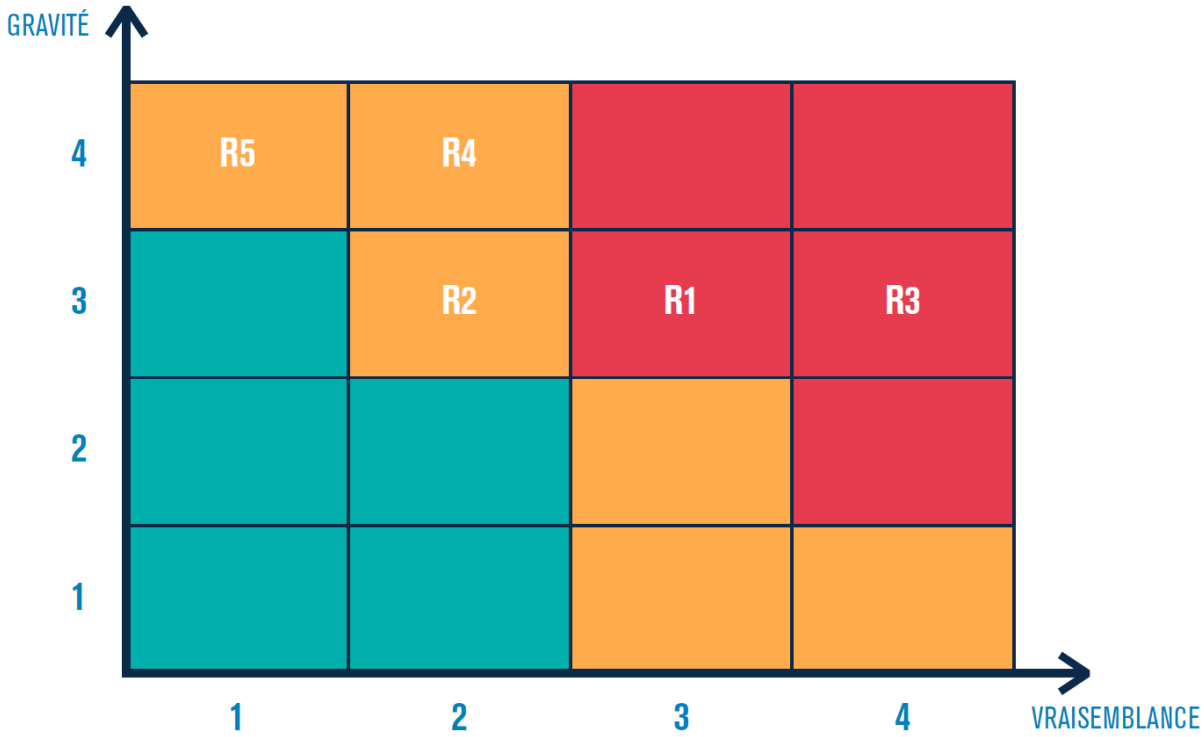



Figure 13 : Traitement du risque(élaboré par nos soins sur la base des documents de l'entreprise)

**Scénarios de risques :**

R1 : Un concurrent vole des informations de DTI grâce à un canal d'exfiltration direct

R2 : Un concurrent vole des informations de DTI en exfiltrant celles détenues par l'industrie pétrochimique

R3 : Un concurrent vole des informations de DTI grâce à un canal d'exfiltration via le prestataire informatique

R4 : Un hacktiviste provoque un en compromettant l'équipement de maintenance du fournisseur de matériel

R5 : Un hacktiviste perturbe la distribution en modifiant leur étiquetage

Tableau 11: Mesures de sécurité(élaboré par nos soins sur la base des documents de l'entreprise)

| Mesure de sécurité | scénarios des risques associés | Responsable | Freins et difficultés de mise en œuvre | Cout complexité | échéance | Statut |
|---|---|---|---|---|---|---|
| **Gouvernance** | | | | | | |
| **Sensibilisation renforcée au hameçonnage par un prestataire spécialisé** | **R1** | **RSSI** | **Validation indispensable** | **+** | | **En cours** |
| **Audit de sécurité technique et organisationnel de l'ensemble du SI bureautique** | **R1 ,R5** | | | **++** | | **En cours** |
| **Mise en place d'une procédure de signalement de tout incident de sécurité ayant lieu chez un prestataire** | **R2,R3, R4** | **RSSI** | | **++** | | **A lance** |
| **Audit de sécurité organisationnel des prestataires. Mise en place et suivi des plans d'action consécutifs** | **R2,R3, R4** | **RSSI** | | | | **En cours** |
| **Protection** | | | | | | |
| **Protection renforcée des données de R&D sur le SI (pistes : chiffrement, cloisonnement)** | **R1,R3** | **DSI** | | **+++** | **3 mois** | **En cours** |
| **Renforcement du contrôle d'accès physique au bureau** | **R1** | | | **++** | **9 mois** | **Terminé** |
| **Dotation de matériels de maintenance administrées par la DSI et qui seront mis à disposition du prestataire sur site** | **R4** | **DSI** | | **+++** | **3 mois** | **A lancé** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Renforcement de la sécurité du système industriel selon les recommandations ANSSI** | | | | | **12 mois** | **A lance** |
| **Défense** | | | | | | |
| **Surveillance renforcée des flux entrants et sortants (sonde IDS). Analyse des journaux d'évènements à l'aide d'un outil.** | **R1** | **DSI** | **Achat d'un outil, budget à provisionner** | **+++** | **9 mois** | **En cours** |
| **Résilience** | | | | | | |
| **Mise en place du plan de continuité d'activité** | **R4, R5** | **Equipe continuité d'activité** | | **++** | **3 mois** | **A lance** |

**Section 3 : L'implémentation de la sécurité du système d'information**

1. **Schéma de l'architecture globale du site SONATRACH la COM :**

Le schéma ci-dessous illustre l'architecture globale du site SONATRACH la COM :

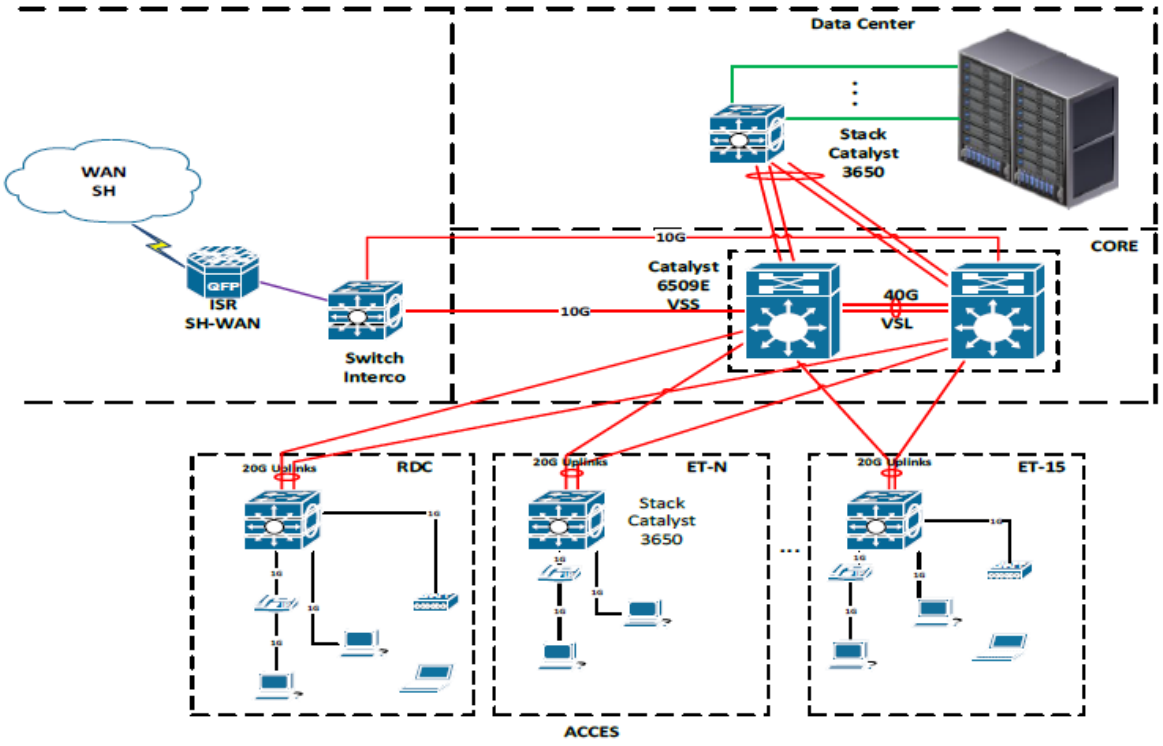



Figure 14 : Architecture Data Centres Sonatrach COM(élaboré par nos soins sur la base des documents de l'entreprise)

2. **Schéma de l'architecture cible après implémentation des Firewall du site SONATRACH la COM :**

L'architecture cible consiste à installer deux firewalls entre les différents réseaux (Data Center – LAN et le réseau Intercom)

Le schéma ci-dessous illustre l'architecture cible après implémentation des firewalls du site SONATRACH COM :

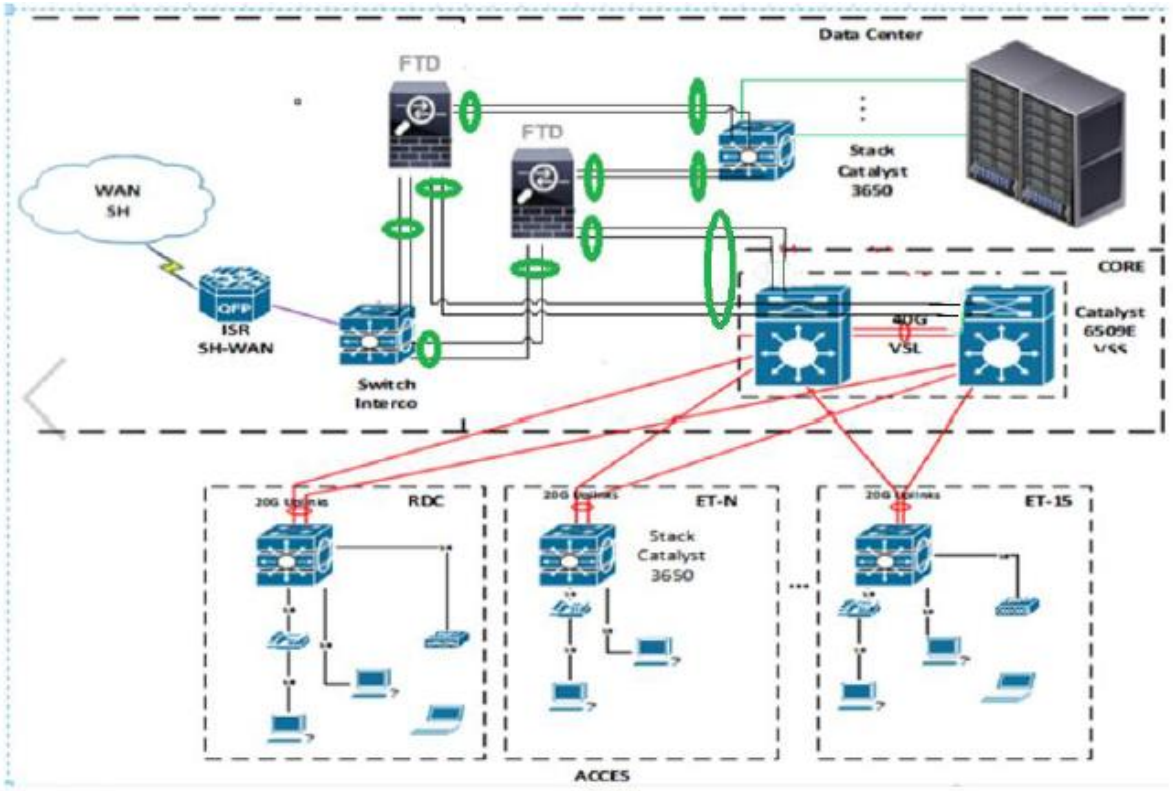



Figure 15: Architecture cible du site SONATRACH COM(élaboré par nos soins sur la base des documents de l'entreprise)

Les éléments de l'architecture cible sont comme suit :

• Le firewall seront positionnés entre les réseaux LAN, Data Center et le réseau Interco

• Les liens d'interconnexion existants entre le (Data Center – Interco) et (LAN – Interco) seront redirigés vers les deux firewalls

• Un bridge port sera créé au niveau des firewalls pour l'interconnexion des réseaux LAN – Data Center et Interco


Figure 16 : Un pare-feu, représenté par un mur de briques

### 3. Description de l'équipement :

Le Firewall implémenté permet de créer des pare-feu logiques distincts pour une flexibilité de déploiement et une optimisation des ressources. Inspecte rapidement le trafic Web crypté, bénéficie d'une visibilité sur les applications, détecte et bloque les intrusions sur le réseau, déployé des VPN évolutifs et profite d'une protection intégrée contre les attaques. Mette les dispositifs en grappe pour garantir les performances et la haute disponibilité.

### 4. Description des fonctionnalités et support :

- Identification et contrôle des applications sur n'importe quel port, pas seulement les ports standard (y compris les applications utilisant http ou d'autres protocoles) ;
- Identification des techniques d'évasion et des contournements : proxy, accès distant, applications dans un tunnel chiffré ;
- Déchiffrements des flux SSL sortants ;
- Possibilité de contrôle des différentes fonctions d'une même application (ex. : SharePoint Admin face à SharePoint Docs) ;
- Détection des menaces dans les applications collaboratives autorisées (ex. : SharePoint, Box.net, MS Office Online…) ;
- Protéger en temps réel contre les menaces embarquées dans les applications ;
- Visibilité sur les menaces avec indication de compromission par utilisateur ou flux ;
- Possibilité de gérer le trafic inconnu avec des règles et ne pas simplement les laisser passer ;
- Identification et contrôle des applications partageant une même connexion ;
- Assurer le même contrôle et la même visibilité sur les utilisateurs distants que sur les utilisateurs Internes ;
- Assurer une sécurité simple du réseau, pouvoir contrôler les applications ne doit pas ajouter de Complexité ;
- Fournir le même débit et les mêmes performances malgré l'activation de tous les contrôles Applicatifs ;
- Protection contre les attaques DOS/DDOS (Denial of service) ;

- Prise en charge de menaces avec détection, blocage, suivi, analyse et remédiation contre les logiciels malveillants et les menaces émergentes manqués par d'autres couches de sécurité ;
- Visibilité sur les menaces avec indication de compromission par utilisateur ou flux ;
- Qualité de service QoS, réservation de bande passante ;
- Assurer le VPN Ipsec site à site ;
- Support de Translation d'adresses (NAT) ;
- Routage Statique et Dynamique RIP, OSPF, BGP ;
- Assurer la protection IPS type NGIPS avec prévention contre les menaces ;
- Ajustement des règles IPS ;
- Visibilité et contrôle applicatif granulaire permettant de lancer un filtrage IPS spécifique pour une analyse approfondie ;
- Classification utilisateur par contexte et par profile ;
- Authentification LDAP, AD, Radius et Tacacs+ ;
- Possibilité de Clustering Active/Passive et Active/Active ;
- Définition des polices de sécurité ;
- Analyse et corrélation des évènements ;
- Remédiation et correction des règles de sécurité ;
- Monitoring et Reporting intégrés, Tableaux de bord et rapports granulaires ;
- Log des évènements en local et/ou vers un serveur SysLog externe ;
- Interface Web multilingue supportant le français ;
- Gestion via une interface Web (HTTP/HTTPS) ou CLI (Console/SSH/Telnet) ;
- Support de la solution d’une année avec possibilité de renouvellement
- Identification des techniques d’évasion et des contournements : proxy, accès distant, applications dans un tunnel chiffré ;
- Déchiffrements des flux SSL sortants ;

5. **Identifier les risques propres à l'activité Commercialisation, avec un exemple d'actions :**

Tableau 12: Identifier les risques propres . (Élaboré par nos soins sur la base des documents de l'entreprise)

| N° | Risque | Action |
|---|---|---|
| 1 | Incident dans les locaux informatiques (ou défaillance des servitudes des locaux informatiques) entraînant l'indisponibilité de tout ou partie du système d'information. | Mise aux normes de la salle informatique |
| 2 | Incapacité à restaurer une application dans délai acceptable pour les métiers en cas de panne serveur | Redondance des serveurs, serveurs de secours |
| 3 | Perte des liens télécoms (liens physiques) entre le siège de l'activité Commercialisation et le groupe Sonatrach | Mise en place d'une double adduction télécoms au siège de l'activité Commercialisation |
| 4 | Perte des liens télécoms entre les Unités Commerciales et l'activité commercialisation | Mise en place de deux liens télécoms distinct |
| 5 | Indisponibilité du réseau informatique de l'activité commercialisation | Redonder les équipements (cœur de réseaux) |
| 6 | Perte de données informatique | Sensibilisation des utilisateurs à la problématique de sauvegarde des données |
| 7 | Divulgation d'informations confidentielles suite à un vol ou la perte du matériel<br>Sécuriser les postes de travail de prêt | Installation d'outils de sécurisation (anti-virus, anti-spyware) |
| 8 | Accès illégitime à des informations confidentielles | Renforcement de la politique de gestion des mots de passe pour les applications sensibles |
| 9 | Incapacité à assurer la détection, le traitement et le suivi des incidents d'exploitation et de sécurité | Définition et mise en place d'un processus de gestion des incidents d'exploitation et/ou de sécurité |

- Documentez toutes ces actions dans un plan de reprise après sinistre (DRP) structuré et planifié. Chaque mesure est liée à la personne responsable, les principaux obstacles et difficultés dans le processus de mise en œuvre, le coût et le délai. Le PRA favorise le niveau de maturité SSI d'une organisation et permet une gestion progressive des risques résiduels

# CONCLUSION

Le numérique devient une composante universelle et vitale de notre société qui transforme de manière irréversible les dimensions politique, économique, sociale et culturelle des organismes comme des individus.

Dans ce contexte, il nous semble nécessaire d'étudier les enjeux d'élaboration d'un plan de reprise d'activité au sein du système d'information, notamment en utilisant la méthode EBIOS risk manager. D'où le titre : « Utiliser la méthode EBIOS RM pour mettre en œuvre des méthodes de gestion des risques informatiques au sein de la direction informatique »

Notre principale préoccupation est d'étudier dans quelle mesure des solutions de reprise d'activité peuvent être mises en œuvre dans les systèmes d'information de l'entreprise ; des solutions qui permettent aux administrateurs de ne pas avoir à se soucier de la récupération des données en cas de sinistre informatique.

Pour y parvenir, nous avons utilisé la méthode EBIOS RM (expression des exigences et identification des objectifs de sécurité), qui nous permet d'évaluer les risques numériques et de déterminer les mesures de sécurité à mettre en œuvre pour les maîtriser. Il peut également vérifier les niveaux de risque acceptables et s'inscrire dans un processus d'amélioration continue à long terme.

La méthode EBIOS RM est une méthode d'analyse de risques que nous avons appliquée au cours de ce travail ; elle analyse les risques en passant par cinq ateliers qui sont : Cadrage et socle de sécurité, sources de risque, scénarios stratégiques, scénarios opérationnels, traitement des risques.

Par conséquent, la solution a simplement confirmé notre hypothèse initiale selon laquelle la mise en œuvre d'un plan de reprise après sinistre est sans aucun doute l'une des solutions phares de l'entreprise pour une récupération de données flexible et facile.

Ce qui a amenés à discuter de la dernière technologie des plans de reprise après sinistre au chapitre 1. Étudier l'organisation cible, la gestion des risques, et enfin la mise en œuvre de la solution qui adoptée dans la troisième partie.

Dans l'ensemble, nous pensons que la technologie de continuité de service dans le réseau est encore dans l'ombre, car si les activités de restauration sont inévitables pour les entreprises de toute taille, il existe très peu de documents liés aux activités de restauration.

Des solutions peuvent exister, mais elles doivent sensibiliser chaque participant au risque et changer la mentalité de chaque hiérarchie en conséquence. Il s'agit de repenser la relation entre la technologie et les hommes dans un dialogue disciplinaire. Il s'agit de la logique de départ de l'intégration, de la confrontation et de la tension permanente dans un esprit constructif.

# REFERENCES BIBLIOGRAPHIQUES

**OUVRAGES :**


- Angers Maurice. (1999) Initiation pratique à la méthodologie des sciences humaines. Casbah, Alger
- DELMOND Marie-Hélène, PETIT Yves et GAUTIER Jean-Michel (2008), Management des systèmes d'information, 2ème édition, Editions Dunod, Paris,
- MONACO Laurence (2014), Les carrés DCG 8 : Système d'information de gestion 2014-2015, Editions Guialino, Paris,
- DESROCHES Alain, LEROY Alain, et VALLEE Frédérique (2007), La gestion des risques, 2ème édition, Editions Lavoisier, Paris,
- Marie de Fréminville · (2019) La cyber sécurité et les décideurs : Sécurité des données et confiance numérique
- BARTHELEMY Bernard (2004), Gestion des risques : méthode d'optimisation globale, Editions d'Organisation, Paris,
- Massimiliano Albanese, Ross Horne, Christian W. Probst ·( 2019) Graphical Models for Security
- VOLLE Michel (2004), Lexique du système d'information, Club des maitres d'ouvrage des systèmes d'information & Michel VOLLE,
- Jean-Marie Flaus · (2019) Cybersécurité des systèmes industriels - Page 231
- Mohamed Boucadair, Christian Jacquenet (2020) Design Innovation and Network Architecture for the Future Internet


**Revues et articles :**


- Futuribles n°354-juillet-août 2009, Vers l'apocalypse ? Gérard Donnadieu.
- La Tribune, 26 janvier 2006, Frédéric Hastings, « le Risk Manager s'installe dans une approche globale des risques ».
- BAPST Pierre Alexandre, BERGERET Florence (2002), Pour un management des risques orienté vers la protection de l'entreprise et la création de la valeur ajoutée (deuxième partie), Revue française de l'audit interne, N°162 : 31-33.
- Les Echos, dossiers L'Art de la gestion des risques.

**Site Web :**


- AMRAE-CLUSIF (2006), RM et RSSI : Deux métiers qui s'unissent pour la gestion des risques liés au système d'information, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-RM-RSSI-GESTION-DES-RISQUES.pdf, p04.

- **NIST (2002), Risk Management guide for IT,http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30**

- **https://blog.advancia-itsystem.com/plan-de-reprise-d-activite-pra/#.YR_Xt477TIW**

- **https://www.syloe.com/glossaire/systeme-dinformation/**

- http://www.rffst.org/images/6/60/Fiche_Double_approche_systemique_pluridisciplinaire_RFFST.pdf

# ANNEXES

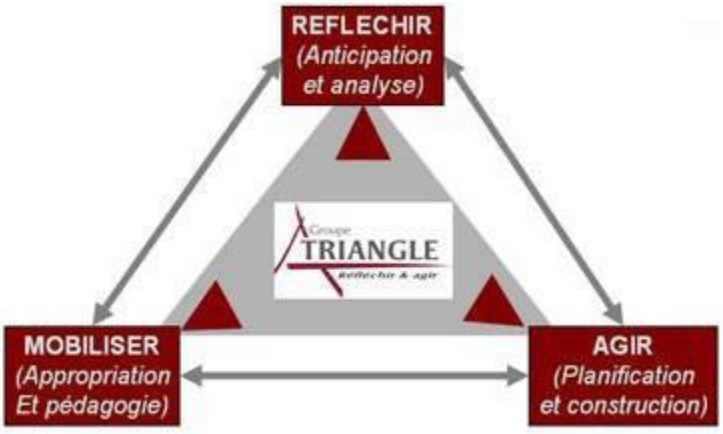
# ANNEXE A – GUIDE D'ENTRETIEN

**Guide d'entretien**

L'objectif de ce guide d'entretien ceci afin de répondre à notre problématique d'assurer une meilleure gestion des risques au sien de la Direction Technologies de l'Information.

| **Thématiques /axes** | **Questions posées** |
|---|---|
| **Système informatique dans la direction** | 1) Pouvez-vous nous décrire brièvement vos activités de service ?<br>2) Parlez-moi du système informatique de gestion ?<br>3) Le travail du département informatique est-il coordonné avec le travail des autres départements de l'Administration générale ?<br>4) Existe-t-il une charte informatique ? Est-il mis à jour régulièrement ?<br>5) Existe-t-il une politique informatique ? Est-il mis à jour régulièrement ?<br>6) Existe-t-il une politique de sécurité informatique ? |
| **Gestion des risques informatiques dans la direction** | 6) La direction dispose-t-elle d'une unité de gestion des risques informatiques ?<br>7) Qui est le gestionnaire des risques informatiques ?<br>8) Pouvez-vous nous parler des méthodes de gestion des risques ?<br>9) Avez-vous une carte des risques ?<br>10) Dans le cadre de la gestion des risques informatiques, quelle méthode avez-vous choisie ?<br>11) Quel est l'objectif du système de gestion des risques informatiques ?<br>12) Quels sont les sous-systèmes qui causent un danger dans la gestion ?<br>13) Quels sont les principaux risques que vous rencontrez souvent dans le système d'information de gestion ?<br>14) Les employés sont-ils impliqués dans le processus d'identification des risques ? est-ce suffisant ?<br>15) Les employés ont-ils les qualifications et l'expérience de la gestion des risques informatiques ?<br>16) Existe-t-il un plan de communication et de sensibilisation aux risques informatiques ? |

# ANNEXE B – Le triangle Grec




Le triangle Grec (Source, Groupe Triangle Grec)

# ANNEXE C – EXEMPLE DE CARTOGRAPHIE DES RISQUES


Exemple de cartographie des risques (Source Digimind Redbook Risk Management-2010).