MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ÉCOLE NATIONALE SUPÉRIEURE DE MANANGEMENT
ENSM. Pôle Universitaire de KOLÉA

MÉMOIRE DE FIN D'ÉTUDES

Master en Management stratégique et système d'information

Un essaie des l'élaboration une cartographie des risques-IT (information technology).

Cas : Le Centre National des Transitions et du Système d'Information des Douanes Algérie (CNTSI).

Elaboré par :
AMALOU NADA

Encadré par :
TOUMI DJAMILA

Année 2020 _ 2021

Résumé

L'environnement risque zéro demeure idéal et n'existe pas en réalité, mais il est possible de minimiser les risques qui se manifestent quotidiennement. Afin d'y procéder, une étude approfondie été élaborée au Centre National des Transmissions et Système d'Information des Douanes Algériennes communément appelé CNTSID, visant à déterminer l'ensemble des risques existants, calculer l'impact des risque IT tout en utilisant des méthodes qualitatives. L'objectif des efforts consacrés à ce projet, c'est d'élaborer une cartographie des risques, laquelle on peut exploiter ultérieurement pour décider quelle conduite à tenir et quelle approche à suivre. Les menaces sont là, les risque sont omniprésents, les vulnérabilités sont également au rendez-vous.

Mot clés : risque, risques-IT, cartographie, cartographie des risques-IT.

Abstract

The zero risk environment remains ideal and does not exist in reality, but it is possible to minimize the risks that occur daily. In order to do so, a thorough study was developed at the National Center of Transmissions and Information System of Algerian Customs commonly called CNTSID, aiming to determine all existing risks, calculate the impact of IT risks while using qualitative methods. The objective of the efforts devoted to this project is to develop a risk map, which can be used later to decide what conduct to hold and what approach to follow. The threats are there, the risks are omnipresent, the vulnerabilities are also there.

Key words : risk ,IT-risk, IT-risk mapping.

ملخص

تظل بيئة الخطر الصفري مثالية ولكنها غير موجودة بالفعل ، لذلك يجب التقليل من المخاطر التي تنشأ على أساس يومي و من أجل القيام بذلك ، تم إجراء دراسة معمقة في المركز الوطني للنقل ونظام المعلومات للجمارك الجزائرية ، بهدف تحديد جميع المخاطر التكنولوجية الحالية ، وحساب تأثير مخاطر تكنولوجيا المعلومات مع استخدام الأساليب النوعية. الهدف من الجهد المبذول في هذا المشروع هو تطوير خريطة المخاطر ، والتي يمكن استخدامها لاحقًا لتقرير ما يجب القيام به والنهج الذي يجب اتباعه. التهديدات موجودة ، والمخاطر منتشرة في كل مكان ، ونقاط الضعف حاضرة أيضًا.

الكلمات المفتاحية: خطر، مخاطر تكنولوجيا المعلومات، تخطيط مخاطر تكنولوجيا المعلومات.

Remerciements

Tout d'abord, je tiens à remercier Dieu Tout-Puissant de m'avoir donné La capacité et la force de bien faire ce travail.

Au terme de ce briefing, je tiens à exprimer ma profonde gratitude à ceux qui m'ont soutenu. De près et de loin rendent ce travail possible.

Je tiens à remercier Mr. ch. Chouaib, mon encadreur chez CNTSI, pour son Convivialité et conseils, et me donner l'opportunité de développer mon apprentissage, et Accueillez-moi avec grand intérêt, qui m'a fourni toutes les informations et éléments nécessaires et coopération amicale en répondant aux questions Entretien avec eux.

Je tiens également à remercier mon tuteur de mémoire, Mme T. Djamila pour sa disponibilité, compréhension et participation aux travaux de suivi de mon mémoire.

Je remercier nos professeurs, qui nous ont apporté une solide formation tout de mong de mes études, et qui par leurs compétences je me soutenue.

Merci beaucoup à mes fréres (MOUNA, MUSTAPHA, FARES) et amies ou voisins et cousins pour sa présence, son écoute, sa confiance en moi et surtout son soutien constant et ses encouragements pendant tous les moments difficiles que j'ai passés.

Enfin, ce travail est présent grâce à ma famille qui sont présent durant tout le long de mon parcours avec leurs soutient, sacrifices et prières.

Mon cher papa MOUHOUB, ma cher Mama FARIDA, j’espère vraiment que vous pouvez être fière de moi, ma grand-mère maternelle FATIMA qui a été toujours là pour moi et m’a apporter de l’amour, BILAL merci pour tout et surtout ta compréhension et ton soutient.

Table des matières

LISTES DES FIGURES

LISTE DES TABLEAUX

LISTE D'ABREVIATIONS :

IT	Information Technology
SI	Système d'Information
CNTSID	Centre National des Transmissions et du Système d'Information des Douanes .
WAN	Wide Area Network
IPS	Inspecteur principal aux sections.
IPOC ou IPCOC	Inspecteur principale au contrôle des opérations commerciales.
CID	Chef d'Inspection Divisionnaire.
TPD	Titre de passage en douanes (un document pour identification des véhicules entrants ou sortants du territoire national).
NIF	Numéro d'Identification Fiscale (un identifiant national unique pour chaque opérateur commercial utilisé pour l'identification de ce dernier au niveau des impôts).
RC	Registre de Commerce : un document nécessaire et indispensable pour tout opérateur commercial exerçant une activité commerciale dans un contexte légal.

INRODUCTION GENERALE

Contexte général :

Depuis le début du 20 eme siècle, la gestion des risques connait une véritable révolution culturelle. Elle est devenue une discipline managériale transversale. C'est la capitale dans toute décision.et de plus en plus un volet important de la stratégie d'organisation. Elle nous aide à éviter les situations qui peuvent contrarier l'atteinte des objectifs de chaque organisation.

L'un des objectifs de tout organisation est d'assurer son activité dans les meilleures condition d'efficacité, d'efficience, de qualité et de conformité ; mais au quotidien tout ne se passe pas toujours comme prévu à cause des risques avec des impacts importants remettant en arrière le bon fonctionnement de l'organisation, une bonne gestion des risques est le médicament qui fait diminuer cette incertitude *« un problème bien identifié est à moitié solutionné ».*

Le grand risque en ce moment c'est le risque du SI (système d'information) qui lie l'information l'informatique, la première est devenue une marchandise et un or blanc, la deuxième est la technologie la plus récente et en même temps la plus risquée.

Problématique et motivation :

IT-risk cartography (la cartographie des risques) offre des risques uniques : matériel, logiciel, les applications, les intégrations, …un revers, une limitation, un risque ou une erreur informatique peut avoir un impact sur toute la façade de l'organisions .et pour CNTSI, étant une organisation dans une position qui demande d'être toujours à jours en ce qui est risque, risque informatique consiste un levier primordial pour sa survie et son développement.

La question principale relative à cette recherche sera donc formulée ainsi :

*****Quelle est la démarche adéquate pour l'élaboration d'une cartographie des risques?

Sous question :

-comment peut-on structurer la cartographie des risques informatiques pour le CNTSID ?

Plan du mémoire

Globalement, notre mémoire se compose de trois chapitres suivis d'une conclusion générale. Il est structuré comme suit :

Chapitre1 : Revue de littérature et cadre conceptuel : Le premier chapitre présente les différents travaux sur lesquels s'appuie notre recherche, ainsi que la définition et l'introduction de divers concepts liés à nos thèmes de recherche.

Chapitre2 : cadre méthodologique : dans le deuxième chapitre nous présenterons d'abord l'organisation d'accueil et décrirons sa structure à travers l'organigramme et à travers le Centre National des Transmissions et du système d'information Center. Ce chapitre s'intéressera également aux méthodes et techniques de collecte d'informations qui permettent de répondre à nos questions de recherche.

Chapitre 3 : la cartographie des risques informatiques : ce dernier chapitre sera consacré à la présentation des résultats obtenus, relatives à la cartographie des risques IT (information technologie), et notre modelé d'identification et d'évaluation des risques informatique et les différentes étapes suivies pour répondre à notre problématique et une analyse des résultats est faite afin d'arriver à résoudre la problématique.

CHAPITRE 1 : REVUE DE LITTERATURE ET CADRE CONCEPTUL

1 La revue de la littérature :

Cette partie sera réservé aux travaux réalisés par les chercheurs, les scientifiques, les doctorants dans ce domaine, nous allons présenter au mieux leur résultats ayant traité même sujet que nous choisissions de faire une recherche, que ce soit un travail de mémoire au pour l'intérêt d'une entreprise.

1.1 La cartographie des risques technologiques :

Selon « saint-gérand Thierry» et « Eliane Propeck-Zimmermann » qui ont réalisé une étude sur (nouvelle perspective de la cartographie des risques technologique) , ils ont mentionner que le risque est une éventualité et les conséquences peuvent être variable et pour cela dise que il faut une évaluation complète des risque en différente étapes et au différentes paramètres . saint-gérand et Eliane notent que c'est difficile de prendre la mesure d'un risque lie au dysfonctionnement d'un système technique dont la probabilité est très faible mais le potentiel catastrophiques est très élevé .une base de donnée adaptées aux risque permet une production et visualisation de l'information plus complète et le cartographie permet d'avoir une vue globale des risque sur un format maniable et précise , et représente de façon claire et harmonisé les informations ,et à la fin établir une carte de synthèse des risques délimitant et hiérarchisant des risques .

1.2 Le management des risques par l'analyse globale des risques :

Les chercheurs déclarent que le risque est couvert des éventualités, et le risque met en jeu deux notion ; qualitative : l'exposition du système en danger « situation dangereuse » « situation accidentelle » ou quantitative : « mesure » en termes de probabilité et de gravité. Et ils insinuent sur Le couple (proppabilité/gravité) est indissociable et disent que c'est une variable bidimensionnelle.

1.2.1 L'appréciation des risques :

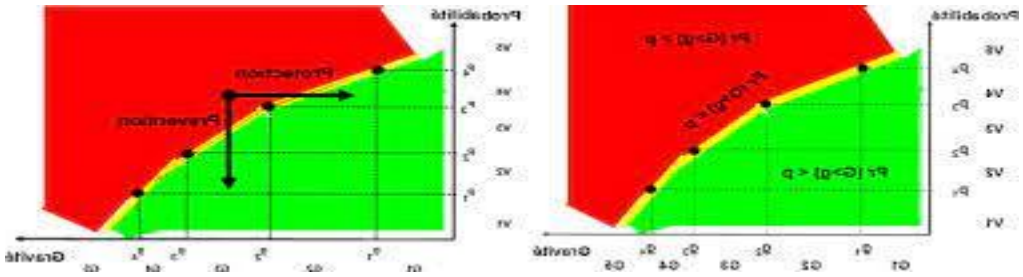
Les chercheurs notent que l'ensemble des étapes d'identification et d'évaluation des risque comme ;

L'identification : est faite en utilisant un ensemble d'outils méthodologiques traitant de façon complémentaire de la nature des événements, de leurs localisations spatiale et temporelle.

L'évaluation : est faite, d'une part, sur l'incertitude de l'occurrence Description d'un scénario d'accident. Échelle d'index de vraisemblance ou de valeurs de probabilité et, d'autre

part, sur les conséquences en utilisant une échelle d'index de gravité ou de valeurs de pertes et d'efforts.

Figure 1 Diagrammes d'acceptabilité des risques.



La source : *Le management des risques par l'analyse globale des risques*. (s. d.). [Graphe]. (2013)

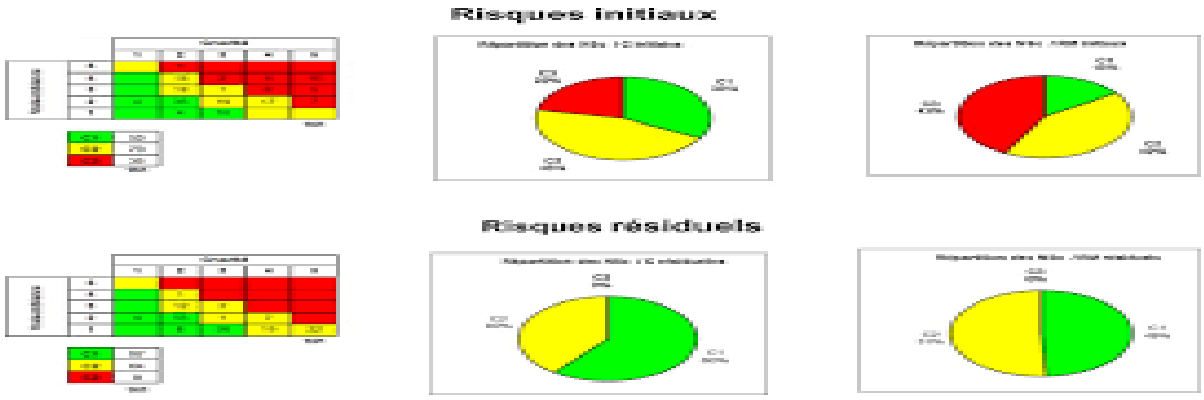
Les docteurs de la recherche donnent la maitrise de risque une importance et ils ont dites sur elle :

1.2.2 La maitrise des risques :

Est associée directement aux actions de réduction et de contrôle faites sur les composantes du risque. Le processus de réduction des risques est basé sur 3 points :

- Risque acceptable en l'état.
- Risque tolérable sous contrôle.
- Risque inacceptable.

Figure 2 Nombres de scénarios et répartition des criticités par risques initiaux et résiduels



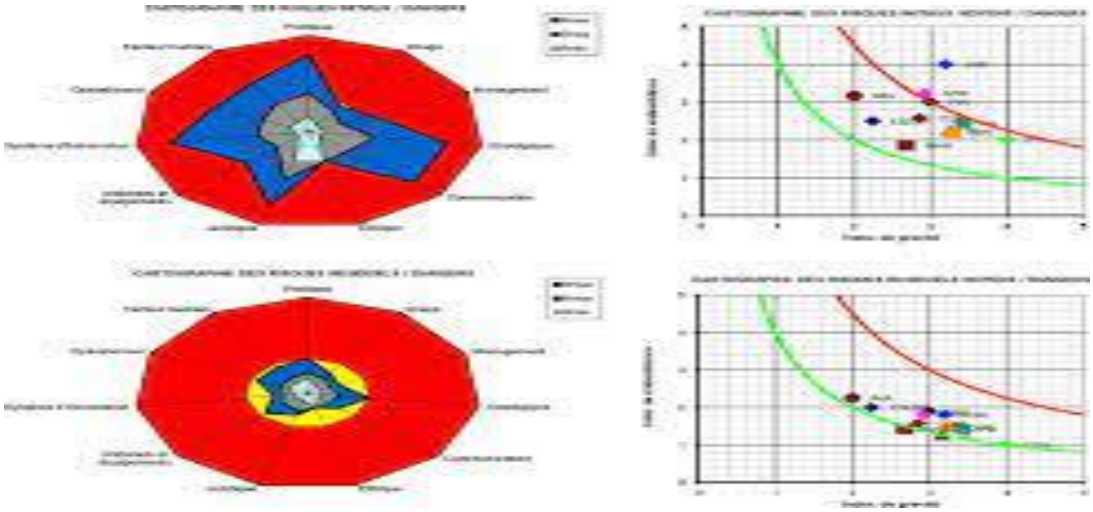
Source : *Le management des risques par l'analyse globale des risques*. (s. d.). [Graphe]. (2013)

1.2.3 La méthode l'AGR :

Les chercheurs ont montré que la méthode AGR (analyse globale des risques) qui permet d'apprécier et de maîtriser les risques d'activités de nature différente La spécificité tient à la nature du système considéré et de la cartographie des dangers considérés et non au processus d'analyse proprement dit. Il en est de même des cartographies des risques comme le visualise.

Élaboration de la cartographie des dangers : qui couvre les quatre grandes catégories suivantes : les dangers externes au système ; les dangers de gouvernance du système ; les dangers liés aux moyens techniques du système ; les dangers liés aux études et production du système. Éléments d'évaluation et de décision : d'après les chercheurs quatre échelles permettent d'évaluer les risques et d'orienter leur gestion qui sont : Gravité, incertitude, perte, effort.

Figure 3 Cartographie des risques initiaux et résiduels par danger



Source : le management des risques par l'analyse globale des risques. (s. d.-b). [Graphe].

Et à la fin disent que La mise en œuvre d'une analyse globale des risques nécessite la connaissance macroscopique mais consolidée du système, de ses vulnérabilités et des interactions avec une liste pertinente de dangers préalablement définis. (L'importance de l'information).

1.3 Sécurité informatique pour la gestion des risques :

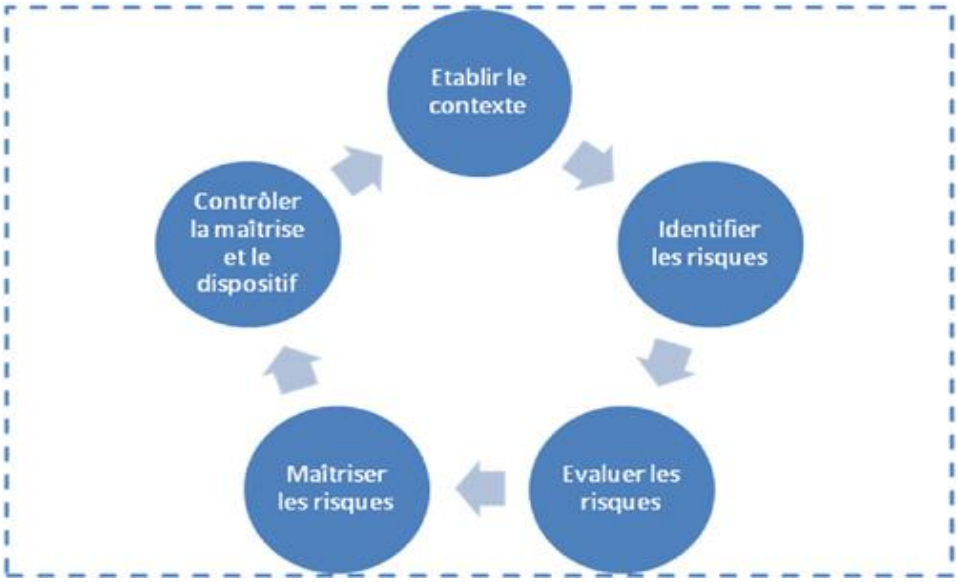
FREDERIQUE VALLEE , réalise une étude sur les risques informatiques des les systèmes d'informations et les méthodes et les enjeux existé pour sécuriser le système d'entreprise, le docteur « Frédérique Valée » définit que la sécurité doit couvrir les évènements de nature aléatoire (danger)ou volontaire (menace) .Et Frédérique a cité que l'arrivé de l'informatique a mis les entreprise au cœur du système d'information dont aucune entreprise ne pourrait plus se passe maintenant et federique ajoute que la généralisation d'internet à encore accentué et complexifié cette relation de dépendance entre l'entreprise et son système d'information. Mais Federique fait l'accent sur si ces systèmes sont insuffisant protégé provoque des catastrophes.

D. Frédérique considéré que la technologie informatique étant assez différent des autres technologies il dit car elle est rapidement apparue indispensable de disposer de technologie spécifique adaptée à la gestion des risques de ces systèmes informatiques ou programmé

Frédérique Vallée montre que la composante informatique des système peut produit directement ou indirectement divers incidents plus en moins grave , et pour cela **la sécurité innocuité** dans le cadre de le sureté de fonctionnent du système faire avec traitement des aspects matériels , logiciel , humain et intentionnels , et la **sécurité confidentielle** concerne la manipulation non autorisé de l'information et il ajoute que l'analyse des risques qui doit déterminer ensuite en fonction des viabilité du système ,si les menace sont pertinentes c'est-à-dire elle correspond bien à un besoin de protection et pour cela il faut la maitrise des risques dans une démarche classique :

Identification, évaluation, réduction \acceptation

Figure 4 Processus pour une gestion globale des risques



Source : la gestion globale des risques dans les entreprises. (s. d.). [Graphe].

La spécificité des systèmes programmé en terme produit, (logiciel et matériel un tout) et de même les interaction homme \logiciel intervient également fortement dans les analyses de risques des systèmes et donc prend en compte la sécurité du système globale (matériel, logiciel, homme).

Federique cite que l'information est ressource stratégique et en effet les systèmes d'informations occupent une place plus en plus importante dans tout le processus de décision, le moyen informatique gère cette information permet d'améliorer sa compétitivité mais ils posent en parallèle le problème du maintint de la disponibilité intégrité la preuve et la confidentialité des donnée.

Et ce problème est difficile et c'est permis les facteurs de risque, et federique propose aux entreprises de faire simulation d'attaque des ressources informatique (prise de connaissance, vérification technique, préparation d'attaque, attaque)

L'auteur a cité quelque méthode pour l'analyse du risque comme EBIOS MARION MEHARIE.

Et ajout comme solution la protection des réseaux d'Enterprise et faire cryptologie.

2 Le cadre conceptual:

Cette partie est faite pour décrire et expliquer les différents concepts de notre recherche d'apes le thème choisi à étudier, voici les concepts pertinents lui concorder :

2.1 Le risque et notion associé :

*Un **risque** peut être vu comme « un **danger**, inconvénient plus ou moins probable **selon** lequel (un individu, un acteur) est exposé » (Larousse, 2003) .

*le risque aussi « une situation dont l'occurrence est incertaine et dont la réalisation affecte les objectifs de l'entreprise qui le subit » (Barthélémy, 2000).

*Selon petit ' Robert' " le risque est une éventualité d'un événement ne dépendant pas exclusivement de la volonté des parties et pouvant causer la perte d'un objet ou tout autre dommage »

*. Pour 'Amaud', « le risque peut être défini comme un danger d'insolvabilité des contreparties et de non-recouvrement auquel la banque doit faire face en allouant une quote-part de ses fonds propres, appelés capital économique ».

*Les auteurs 'B. Marois 'et 'L.S. Olivier' définissent le risque pesant sur toute organisation comme « un aléa qui peut être bénéfique ou néfaste à l'entreprise ». Selon ces deux auteurs, la manifestation d'un risque n'a donc pas d'incidence forcement négative. Ils nous signalent qu'il faut aussi distinguer la notion du risque de celle d'incertitude.

La première est une évaluation de la probabilité d'occurrence d'un événement associé à un enjeu ; la seconde est le degré du doute dans cette évaluation. L'incertitude croit avec l'ignorance, c'est à dire le manque d'information.

'Hapman' et 'Cooper' définissent le risque comme une exposition a la possibilité de pertes ou gains économiques ou financier ; physique dommage, blessures ou retards dus à l'incertitude associée à la poursuite d'une ligne de conduite.

Source de risque : tout élément qui, seul ou combiné à d'autres, est susceptible d'engendrer un risque.

Événement : occurrence ou changement d'un ensemble particulier de circonstances.

Une conséquence : peut-être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects, sur l'atteinte des objectifs et peuvent être exprimées de façon qualitative ou quantitative.

Vraisemblance : possibilité que quelque chose se produise
Note 1 à l'article: Dans la terminologie du **management du risque** , le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article : Le terme anglais « likelihood » (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme « probability » (probabilité) qui est utilisé à la place. En anglais, cependant, le terme « probability » (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme « vraisemblance » est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme « probability » (probabilité) dans de nombreuses langues autres que l'anglais.

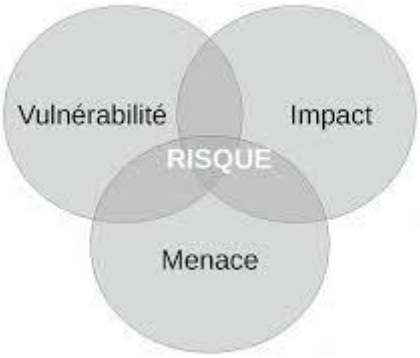
Moyen de maîtrise : action qui maintient et/ou modifie un risque

Note 1 à l'article : Un moyen de maîtrise du risque inclut, sans toutefois s'y limiter, n'importe quels processus, politique, dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient un risque.

Note 2 à l'article : Un moyen de maîtrise du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

Selon ISO 27000 une **menace** : est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation (**définition selon** la norme de sécurité des systèmes d'information.

Figure 5 la gestion de la sécurité.



La source : La gestion de la sécurité « guide de bonne pratique ». (s. d.). [Graphe]. resinfo.

2.1.1 La définition du risque dans la norme ISO 9001

Un risque est souvent utilisé lorsqu'il n'existe qu'une possibilité de conséquences négatives. Comme défini précédemment, le risque peut être un effet positif. Il est rarement utilisé comme tel.

Le risque qualité peut être une atteinte et même un dépassement des objectifs fixés. La gestion de ces risques via une approche préventive est un élément fondamental de la norme ISO 9001 version 2015. L'approche est une des nouveautés de l'ISO 9001 pour laquelle il est important de bien cibler les risques qui vont être intégrés au SMQ.

2.1.2 La définition du risque dans la norme ISO 31000 :

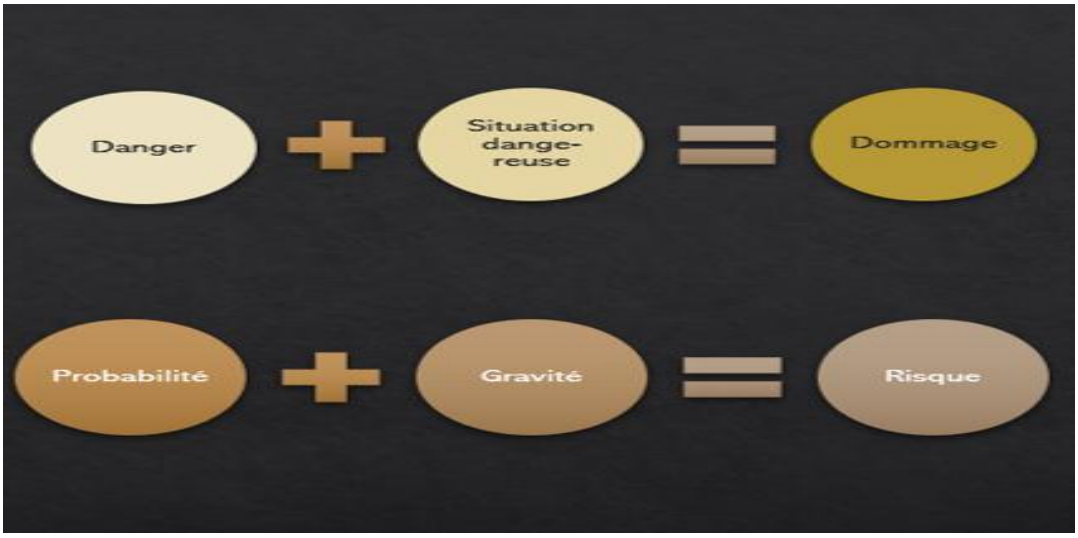
Est effet de l'incertitude sur des objectifs. Le management du **risque** est donc un outil pour contrôler les menaces et les effets négatifs et pour mettre à profit les opportunités et les effets positifs. Effet de l'incertitude sur les objectifs

Note 1 à l'article : Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces.

Note 2 à l'article : Les objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux.

Note 3 à l'article: Un risque est généralement exprimé en termes de sources de risque , événements potentiels avec leurs conséquences et leur vraisemblance .

Figure 6 Définitions : Risque & Notions associées



La source : *les risques : définition,types,évaluation*. (s. d.). [Graphe].

- **Danger** : la cause d'un risqué

Situation dangereuse : la situation qui expose les gens/l'environnement/la société/… au danger.

- **Gravité** : l'ampleur des dommages potentiels.
- **Probabilité d'occurrence** : « à quel point il est probable de subir le dommage.

Selon Svensson (2002), la vulnérabilité est la propension pour les facteurs de risques à prendre
Le pas sur les outils et pratiques de maîtrise des risques, et causant ainsi des conséquences graves.

Il existe de nombreux risques en sécurité du système d'information, qui évoluent d'année en année.et comme l'***informatique*** joue un rôle de premier plan ***dans*** les ***entreprises et les organisations et tout le gouvernement,*** le risque le plus importants et l'élément majeur de tout organisme c'est bien le risque informatique (IT-RISK).

2.2 Le « risque informatique »

Selon la banque de France :
*correspond au **risque** de perte résultant d'une organisation inadéquate, d'un défaut de fonctionnement, ou d'une insuffisante sécurité du système d'information.

« La technologie de l'information ou le **risque informatique** est essentiellement une menace pour vos données d'entreprise, vos systèmes critiques et vos processus d'entreprise. Il s'agit du risque associé à l'utilisation, à la propriété, à l'exploitation, à l'implication, à l'influence et à l'adoption de l'informatique au sein d'une organisation ».[1]

« Le risque informatique, le risque technologique ou le **risque cybernétique** :

Sont tous les risques liés aux technologies de l'information . Alors que l'information est depuis longtemps considérée comme un atout précieux et important, l'essor de l'économie du savoir et la révolution numérique ont conduit les organisations à devenir de plus en plus dépendantes de l'information, du traitement de l'information et en particulier de l'informatique. Divers événements ou incidents qui compromettent en quelque sorte peut donc avoir des impacts négatifs sur l' organisation de processus métier ou mission, allant d'une échelle sans importance à catastrophique. L'évaluation de la probabilité ou de la probabilité de divers types d'événements / incidents avec leurs impacts ou conséquences prévus, s'ils se produisent, est un moyen courant d'évaluer et de mesurer les risques informatiques. Les méthodes alternatives de mesure du risque informatique impliquent généralement d'évaluer d'autres facteurs contributifs tels que les menaces, les vulnérabilités, les expositions et la valeur des actifs »[2].

« Le potentiel d'un résultat commercial négatif imprévu impliquant une défaillance ou une mauvaise utilisation de l'informatique »[3].

Selon (the standard in Security Ratings) « la gestion des risques informatiques est définie comme les politiques, les procédures et la technologie qu'une organisation adopte afin de réduire les menaces, les vulnérabilités et les conséquences qui pourraient survenir si les données ne sont pas protégées ».[4]

[1] https://www.nibusinessinfo.co.uk/content/what-it-risk consulté le 02 mai 2021
[2] https://cioindex.com/the-cio-network/ Consulté le 29 avril 2021
[3] https://www.gartner.com/en/information-technology/glossary/it-risk consulté le 30 avril 2021
[4] https://www.bitsight.com/third-party-risk-management consulté le 30 avril 2021

2.3 La cartographie

Selon le dictionnaire « Larousse » : Ensemble des opérations ayant pour objet l'élaboration, la rédaction et l'édition de cartes. Représentation spatiale d'une réalité.
Selon les universités de France : *La cartographie* a pour but la conception, la préparation et la réalisation des cartes. Sa vocation est la représentation du monde sous une forme graphique.

2.3.1 La cartographie des risques

La cartographie des risques est un outil fondamental pour le responsable du management du risque, elle présente l'avantage d'illustration, à un instant donné, les résultats des analyse menées. (Sutra, G. (Éd.). (2018). Qu'est-ce qu'une cartographie des risques ? Dans définition (réviser éd., Vol. 3, p. 9). Afnor.)

« La cartographie des risques est un outil de management utilisé dans une démarche d'étude et de gestion du risque. Elle consiste à recenser les risques et à les synthétiser sur un document dans lequel ils seront placés en tenant compte de leurs impacts s'ils survenaient et de leurs fréquences hypothétiques »[5].

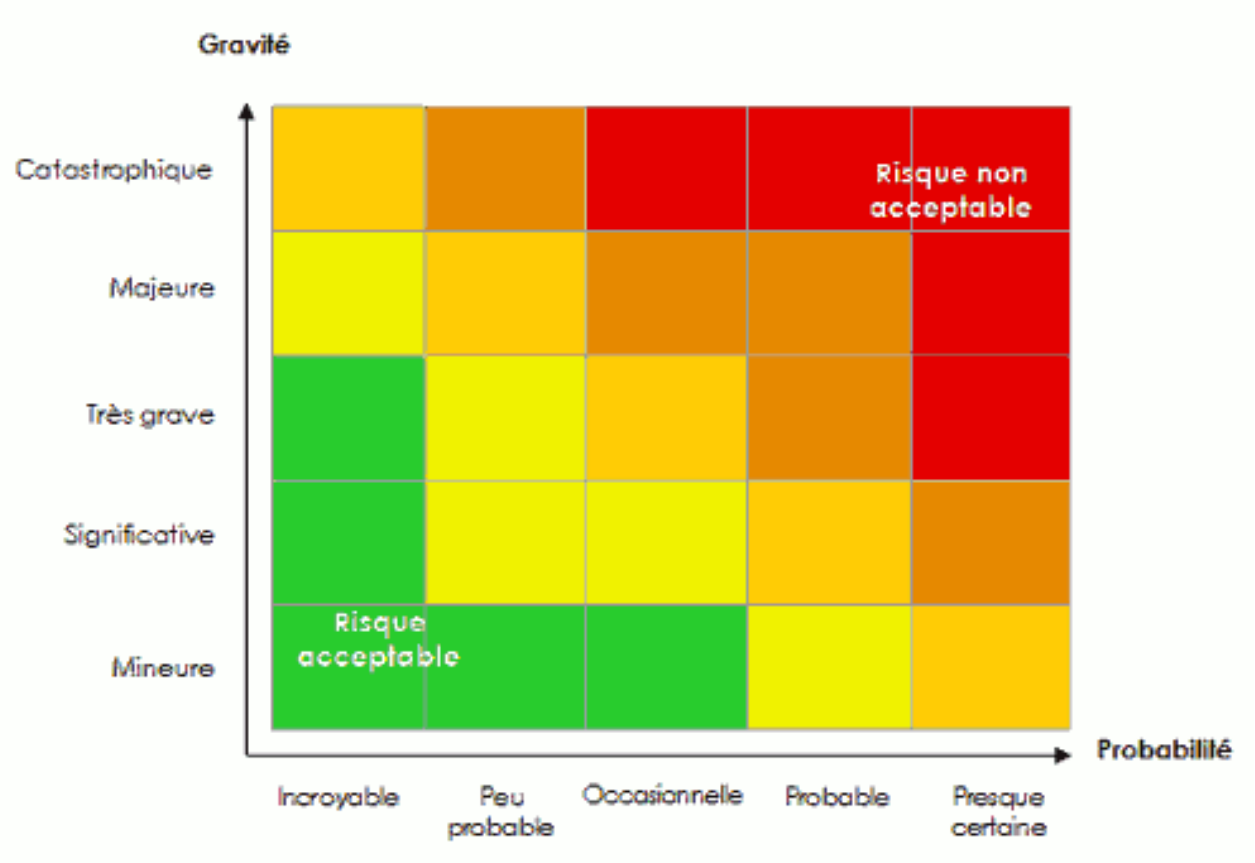
« La cartographie des risques est un levier indispensable au pilotage des risques et constitue le socle de la stratégie de gestion des risques. Elle peut être mise par tout type d'organisation, qu'elle soit privée ou publique ».

*La cartographie des risques permet d'appréhender l'ensemble des facteurs susceptibles d'affecter les activités et leur performance. L'objectif est de mettre alors en place les actions nécessaires afin de se prémunir au maximum des conséquences juridiques, humaines, économiques et financières que représentent les risques identifiés.

*La cartographie des risques implique d'investiguer de façon approfondie l'ensemble des processus managériaux, opérationnels et support que les activités nécessitent de mettre en œuvre. Elle nécessite également d'identifier les rôles et responsabilités de chaque acteur, à chaque étape des processus »[6].

[5] https://sdes.fr/fiches-pratiques/la-cartographie-des-risques-pourquoi-est-ce-un-outil-indispensable/ consulté le 01 mai 2021
[6] https://www.preventica.com/dossier-cartographie-risques-definition. Consulté le 30 mai 2021

Figure 7 Exemple d'une cartographie des risques



La source : Comment faire une cartographie des risque? (s. d.). [Graphe].

Conclusion

Nous avons conclu qu'il existe de nombreux auteurs, articles, livres et personnes qui s'intéressent à la cartographie des risques, et cela devient très important à mesurer que l'organisation se développe, donc la cartographie des risques met l'accent sur l'identification des problèmes possibles. Évaluer les risques à traiter et mettre en œuvre des stratégies pour faire face à ces risques. Les entreprises qui ont identifié des risques seront mieux préparées et réagiront de manière plus rentable.

CHAPITRE 2 : LE CADRE METHODOLOGIQUE

Dans ce chapitre, l'objectif est de mieux cerner sur la démarche méthodologique et description des techniques et étapes de collecte et traitement de données utilisé pour réaliser notre travail e recherche. Et une description de l'organisme d'accueil « CNTIC » sera présentée étant considéré qu'elle a une bonne direction informatique et étant besoin d'une cartographie des risque IT.

1 Presentation de l'organisme d'accueil:

1.1 Le centre national des transmissions et du système d'information des Douanes Algériennes (CNTSID

Le centre est un service extérieur compétences nationale de la direction générale des douanes Placé sous l'autorité du directeur général des douanes et dirigé par un directeur de centre, le centre a pour missions :

- De participer à la définition de la politique de la direction générale des douanes en matière d'exploitation et d'utilisation des technologies de l'information et de la communication et d'élaborer les programmes annuels de sa mise en œuvre.
- De collecter les besoins des services des douanes en matière de technologies de l'information et de la communication, de confectionner les cahiers des charges techniques et fonctionnels y afférents et de suivre l'exécution des programmes et des contrats d'acquisition.
- De promouvoir le système de dédouanement en ligne et les e-procédures.
- D'Etablir des interfaces avec les systèmes d'informations des autres intervenants de la chaine logistique du commerce international.
- D'Etudier les conditions d'implantation des stations des transmissions et du système d'information et de leur fonctionnement continu sur l'ensemble des services des douanes.
- D'établir la nomenclature technique du matériel et des Equipements des technologies de l'information et de la communication et de définir les normes de leur utilisation en douanes.
- De définir et de préciser le régime de travail en matière d'exploitation et d'utilisation des technologies de l'information et de la communication et, de veiller à son application.
- De veiller à la sécurité des technologies de l'information et de la communication en douane.

- De procéder aux vérifications périodiques des installations et logiciels des technologies de l'information et de la communication et de superviser les mouvements du matériel et des Equipements et, de veiller à leur utilisation optimale.

1.2 Les moyens techniques du CNTSID:

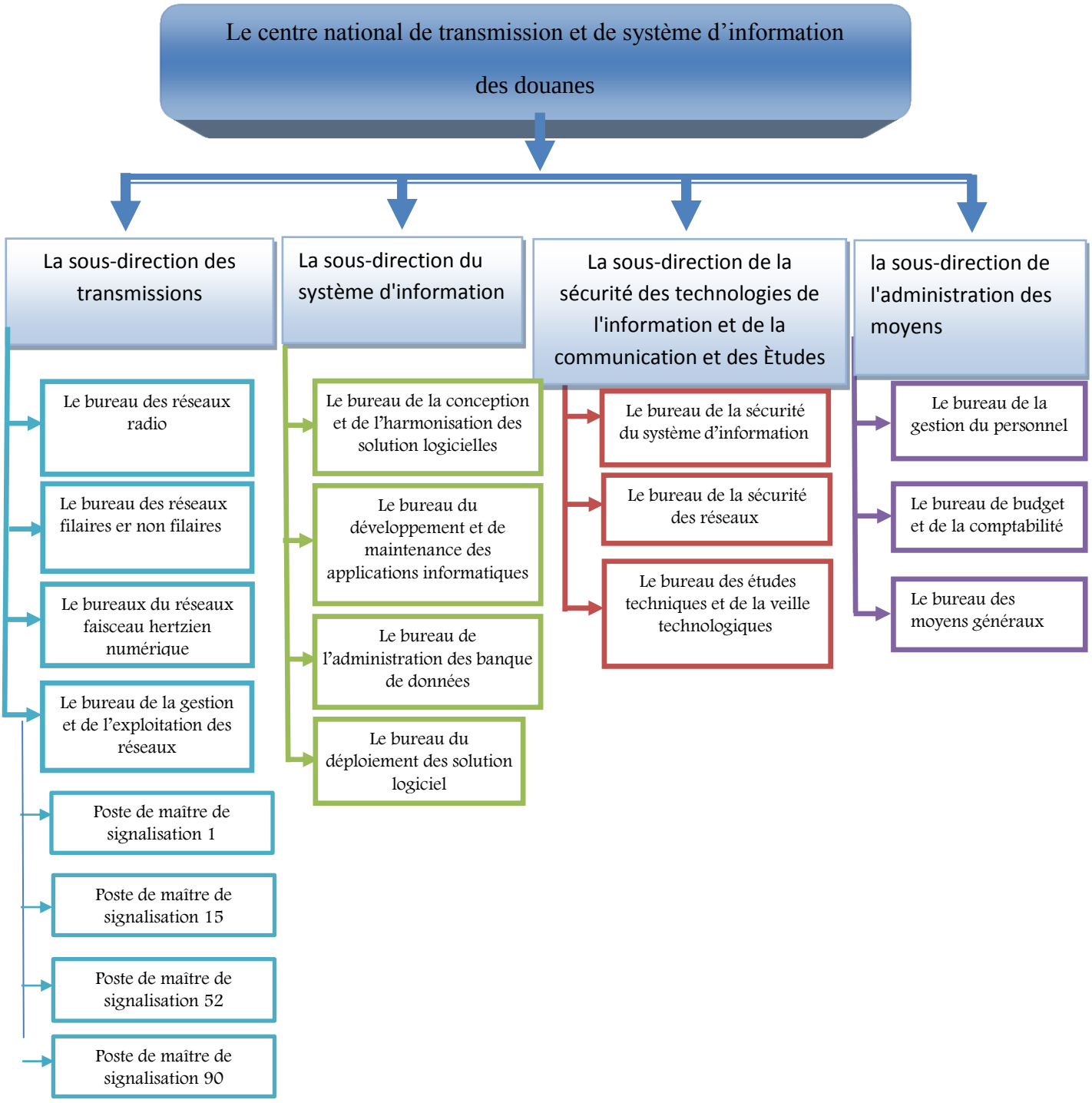
Le CNTSI structuré autour de plusieurs salles particulièrement informatisées ainsi que de postes clients répartis dans les différents bureaux qui compose :

- Un centre de calcul qui a pour fonction de consolider et de mettre a jours toutes les bases de données ainsi que de prendre en charge les besoins en terme d'automatisation.
- Une salle de développement au sein de laquelle sont conçues toutes les applications nécessaires au fonctionnent.
- Au niveau matériel, de nombreux terminaux esclaves, PC et imprimantes, quelques serveurs ainsi qu'un jeu de modems, multiplexeurs, routeurs.

Tous les sites douaniers tendent vers une informatisation généralisée visant à garantir :

- Une efficacité optimale des différents acteurs qui doivent interagir sur le système d'information (SI) des Douanes Algériennes.
- La transparence de la gestion des évènements douaniers.
- Les possibilités de contrôle rapide et efficaces sur tout le territoire Algérien.
- La maitrise du suivi des mouvements de marchandises.
- Une visibilité permanente et la plus précise possible des statistiques sur le commerce extérieur.

Le centre est organisé en quatre (4) sous-directions :



Source : document de l'entreprise

A - La sous-direction des transmissions : est chargée

- d'effectuer les opérations d'installation des Equipements des technologies de l'information et de la communication ; de gérer et d'exploiter les réseaux des télécommunications et de veiller l'application et au respect des règles de l'exploitation, conformément aux prescriptions en vigueur ; d'assurer la maintenance des équipements des technologies de l'information et de la communication de l'administration des douanes ; d'Evaluer l'ensemble des activités qui lui incombent et d'en Établir un bilan annuel assorti de propositions de mesures d'amélioration.

B **- La sous-direction du système d'information** : est chargée

- de veiller l'harmonisation des logiciels et équipements des technologies de l'information et de la communication avec ceux des institutions de l'Etat dans l'optique de leur interopérabilité et mutualisation ; de codifier, de développer et d'administrer les banques de données du système d'information des douanes ; de collecter et d'optimiser les données destinées l'Élaboration des statistiques et l'information Economique, stratégique et décisionnelle ; de développer et de maintenir les logiciels d'automatisation de l'activité de l'administration des douanes aussi bien de métier que de soutien ; de développer les sites intranet et internet des douanes et de veiller leur mise à jour continue et automatique ; d'assurer la maintenance des logiciels utilisés par l'administration des douanes ; d'Évaluer l'ensemble des activités qui lui incombent et d'en Etablir un bilan annuel assorti de propositions de mesures d'amélioration.

C - **La sous-direction de la sécurité des technologies de l'information et de la communication et des études :** est chargée

- d'Etudier, d'Elaborer et de veiller l'exécution des procédures de sécurité arrêtées en matière de technologies de l'information et de la communication, notamment celles relatives au système d'information et aux centres radioélectriques ; d'initier et d'élaborer toute étude technique relative l'appropriation et au développement des technologies de l'information et de la communication en douane ; d'Évaluer l'ensemble des activités qui lui incombent et d'en établir un bilan annuel assorti de propositions de mesures d'amélioration.

D - La sous-direction de l'administration des moyens : est chargée

- De gérer le personnel et de proposer les mesures qui en permettent la stabilité et la motivation ; de gérer les moyens du centre ; d'Évaluer l'ensemble des activités qui lui incombent et d'en Etablir un bilan annuel assorti de propositions de mesures d'amélioration.

2 Cadre methodologies:

Il existe plusieurs méthodes de collecte de donnée nous basons sur :

2.1 La description et observation :

Difficile de définir une bonne stratégie dans un contexte totalement risquer ; La connaissance et la bonne compréhension de l'environnement de travail sont fondamentales pour produire une analyse des risques de qualité.

Plus généralement, **tous les outils de description** seront le socle de notre analyse des risques ; et plus la description sera complète et précise, plus nous pourrons détecter un grand nombre de risques.

Et par Gaspard Claude (**2019).**L'observation est une technique fréquemment utilisée pour mener une étude qualitative. Elle permet de recueillir des données verbales et surtout non verbales.

2.2 L'entretien et les questions scientifique

L'entretien /l'interview

- Selon **Pierre Romelaer** (2005) est une méthode de recherche et d'investigation. Par le biais de cette méthode, l'enquêteur cherche à obtenir des informations sur les attitudes, les comportements, les représentations d'un ou de plusieurs individus dans la société.

- Et le **Geneviève Imbert** (2010) Définit L'entretien comme une des méthodes qualitatives les plus utilisées dans les recherches en gestion. Un entretien de recherche n'a rien de commun avec une discussion dans laquelle on se laisse porter par l'inspiration du moment.
- **Gérald Boutin (1997)** dit que la collecte de données au moyen de l'entretien. Mais ce type d'investigation demande une préparation adéquate de la part de l'intervieweur, en particulier : développer l'art de la communication, connaître les caractéristiques des clientèles visées, savoir conduire un entretien, savoir analyser et interpréter les résultats et, enfin, rédiger un rapport de recherche.

Et pour ce ci la bonne démarche est bien rédigée les questions.

2.3 La documentation :

Consiste en la consultation et la lecture de document officiel concernant le sujet de recherche.

L'AFNOR définit ;

La documentation comme l'ensemble des techniques permettant le traitement permanent et systématique de documents ou de données, incluant la collecte, le signalement, l'analyse, le stockage, la recherche, la diffusion de ceux-ci, pour l'information des usagers.

La documentation est donc l'action de sélectionner, de classifier, d'utiliser, et de diffuser des documents. Par extension, la documentation désigne l'ensemble des renseignements et des documents.

Une documentation informatique est un système informatique qui fournit à la demande des réponses supposées pertinentes, sélectionnées dans un ensemble de connaissances préalablement mémorisées.

Et pour notre recherche voici dans le tableau ci-dessous les personnes interviewées :

Tableau 1 : listes des personnes interviewées

Nom & Prénom	**Poste**	**Formation de Base**	**Expérience Professionnelle (Années)**
Mme ACHOURI Leila	Sous Directrice de sécurité des systèmes d'information au CNTSID	Ingénieur en Informatique	27
Mr MAARICHE Layachi	Chef de Bureau Audit, Etude et Veille Technologique	Ingénieur en Informatique	20
Mr CHABIL Chouaïb	Administrateur système chargé de la sécurité des S.I	Ingénieur en Informatique	04

Source : Réalisé par nous-même.

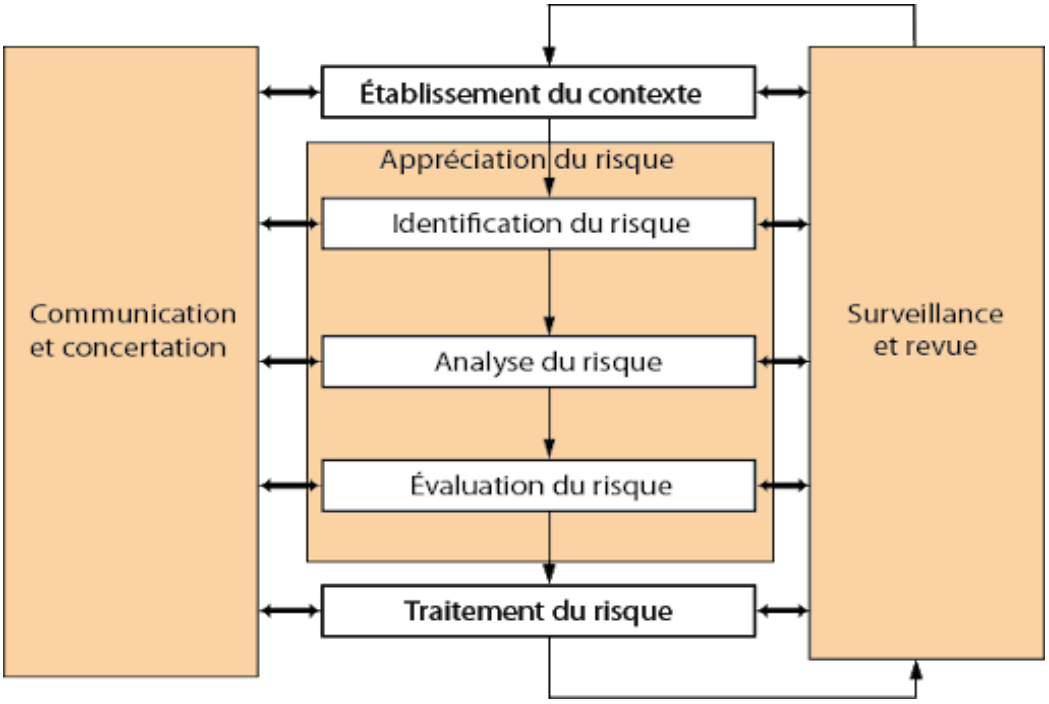
Suit a la crise sanitaire qui a rendu la façon de travaille différente, la majore partie des informations dont avions besoin ont été collecté par mon tuteur .

2.4 Planification de la cartographie :

Le plant qu'on a suivi c'est :

Plan de gestion des risques : il s'agit d'un processus documenté qui décrit les méthodes utilisées par votre entreprise ou votre équipe pour identifier et résoudre les risques .

Figure 8 :processus de gestion de risque



Source : *Le processus global de gestion des risques*. (s. d.). [Graphe]. http://gpp.oiq.qc.ca/. https://lh3.googleusercontent.com/proxy/8_2v9ciOHa-ie2snxe2fSOrDoTIKRq6hTsZPF7Wo6ER_5Ku1hJaekfEsvqCfFRYKRKwYRqAjOlPOAM5Y0dGMw6cmg6e5K8RaNBI

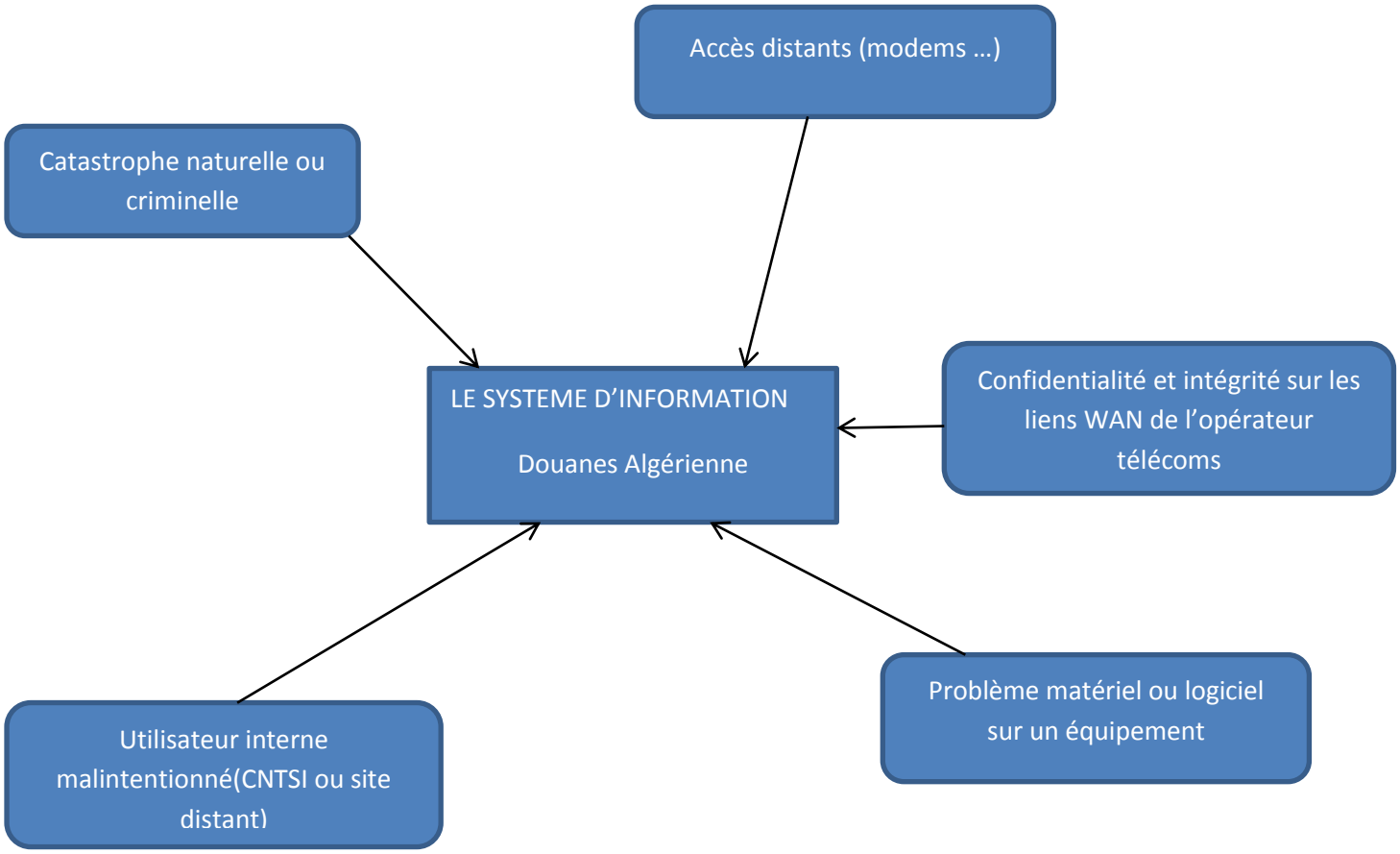
CHAPITRE 3 : LA CARTOGRAPHIE DES RISQUES INFORMTIQUE

1 Présentation de l'ensemble de donnée :

1.1 La gestion des risques dans CNTSI *:*

La gestion des risques joue un rôle important dans la réalisation de notre projet, et la cartographie des risques est un moyen de gérer les points intrinsèquement sensibles. Et ça ce qu'on va faire dans CNTSI dans leurs système d'information qui peut avoir diverses risques plus au moins probable.

Figure 9 : risques et menaces portant sur le SI de CNTSI des Douanes Algérienne



Source : Réalisé par nous-même

2 La cartographie des risques-it :

Tableau 2:cartographie des équipements informatiques

Actifs	Priorité	Description du risque	Catégorie du risque	Probabilité du risque	Gravité du risque
Serveurs BD	1	-Des utilisateurs interne à privilège minimum peuvent détourner le Shell et devenir super utilisateur -perte des données -vol des données	Risque cybernétique	Très probable	Élevé
Serveurs de rapatriement de données	1	Détournement de données durant le transite sur le réseau faiblesse des algorithmes de cryptage	Risque cybernétique	Peux probable	Moyen
Serveur web	1	-Des pirates utilisent des scans pour détecter des failles sur serveur web - attaques XSS, injection SQL, redirection et renvoie non valide	Risque cybernétique	Moyennement probable	Élevé
Serveur de développement	1	Un utilisateur interne mal intentionné qui peux détruire des fichier critique de développement	Risque cybernétique	Peux probable	Élevé
Poste de travail et serveurs	1	Des pirates déploient un virus de demande de rançon causant l'indisponibilité du system	Risque cybernétique	Peux probable	Élevé
Support de transmission	1	Un désastre naturel détruit des surcuits de communications avec les sites distants	Risque environnemental	Peux probable	Élevé

Messagerie électronique professionnel	1	Une attaque de spams Des virus	Risque cybernétique	Très probable	Élevé

Source : Réalisé par nous-même.

Tableau 3 : liste d'applications

Dédouanemant	Déclaration Dépôt (ips) Suivi déclaration Recevabilité(IPOOC) Liquidation inspecteur) Module utilité (IPS)
Contentieux	
Comptabilité	Caisse Receveur TPD Bon d'enlèvement
Control	Control CID
GRH	
Tarif	Cour Sui nif +RC Déclaration en devis Taxations forfaire Manifeste

Source : Réalisé par nous-même.

-D'abord ils répondent plus aux besoins de l'actualité (technologie dépasser)

Les applications sont développées avec le langage 4GL :

- C'est un langage procédural non orienté objet (la maintenance et la modification nécessite beaucoup de temporelle.

- Dépond d'une technologie de base donnée obsolète.

- Manque de support et documentation.

- Son interface graphique, multibase.

Tableau 4 : classification des ressources

	Besoin		
	Contrôle d'accès et authentification	**Confidentialité et intégrité**	**Disponibilité**
Serveur Base de Donnée	Fort	Fort	Fort
erveur de rapatriement de données	Fort	Fort	Fort
Serveur web	Fort	Fort	Fort
Serveur de développement	Fort	Fort	Fort
Sarveur statistique	Fort	Fort	Fort
Station travail et serveurs	Moyen	Faible	Faible
Serveur impression	Moyen	Moyen	Faible
Datacenter primaires	Fort	Fort	Fort
Messagerie électronique professionnel	Moyen	Moyen	Fort
Autre équipements réseau et infrastructures (routeurs, Switch, …)	Fort	Faible	Fort

Source : Réalisé par nous-même.

Contrôle d'accès et authentification : Cette notion implique qu'il est nécessaire, pour certaines ressources, de faire en sorte qu'elles ne soient accessibles que par un groupe d'utilisateurs bien déterminées.

Confidentialité et intégrité : La nature sensible de certaines données implique qu'il est nécessaire de porter une attention particulière à la confidentialité et à l'intégrité de ces dernières. Elle sur de l'intégrité certaine données signifier être sûr que ces données n'ont pas été altérées/modifier. La notion de confidentialité est souvent complémentaire elle signifie lorsqu'elle est nécessaire que qui conque intercepterait les données dont il est est question ne pourrait les interpréter. Si la condition précédente est remplie (maitrise de contrôle d'accès), alors le risque de perte du caractère confidentiel des données peut être pris lors du transfert des données d'un point à un autre (classiquement d'une machine à une autre)

Disponibilité : la non disponibilité de certaines ressources clefs peut avoir des incidences grave sur l'ensemble du fonctionnement du SI. Pour cela est nécessaire de prévoir des scenarii catastrophes liés à ces ressources particulières.

Tableau5 : classement des risques

Type de risque	Situation dangereuse	Niveau de gravité	Niveau de probabilité	Priorité
Environnemental	-La climatisation : système de refroidissement à usage domestique -pas de système de DAI (**détection** automatique **d'incident**). -risque naturel (tremblement de terre, inondation …).	Très grave	Peu improbable	Risque négligeable
Logiciel	-Un système d'exploitation obsolète : RHEL version 6 .2 . -Des port tcp/udp inutilement ouverts. -Base de données contenant quelles que tables qui manquent de clés primaires ce qui engendre la présence d'informations incohérentes. -Absence d'un contrôleur de domaine pour le déploiement de solutions centralisées.	Grave	Certain	Risque à suivre
Financière	-Difficulté en matière d'acquisitions des solutions logicielles dues au manque de ressources budgétaire.	Peu grave	Fort probable	Risque à traiter
Ressource humain	L'utilisation des mots de passe contenant des mots dictionnaire. –manque de formation et de sensibilisation .	Grave	Fort probable	Risque à traiter

Source : Réalisé par nous-même.

On a utilisé NMAP(pour scanne des réseaux) pour prend l'exemple d'une adresse IP est 152 .1.4.2 et voici quelques ports qui étaient ouvert au moment du scan :

Tableau 6: une liste de ports ouverts sur 154.1.4.2

Ports TCP	APLICATIONS
9	Discard
37	Time
111	SunRPR
512	Exec
513	Login
631	Ipp

Source : Réaliser par nous-même .

Chaque port ouvert correspond à un service applicatif et représente de ce fait une porte d'entrée potentielle pour un pirate.

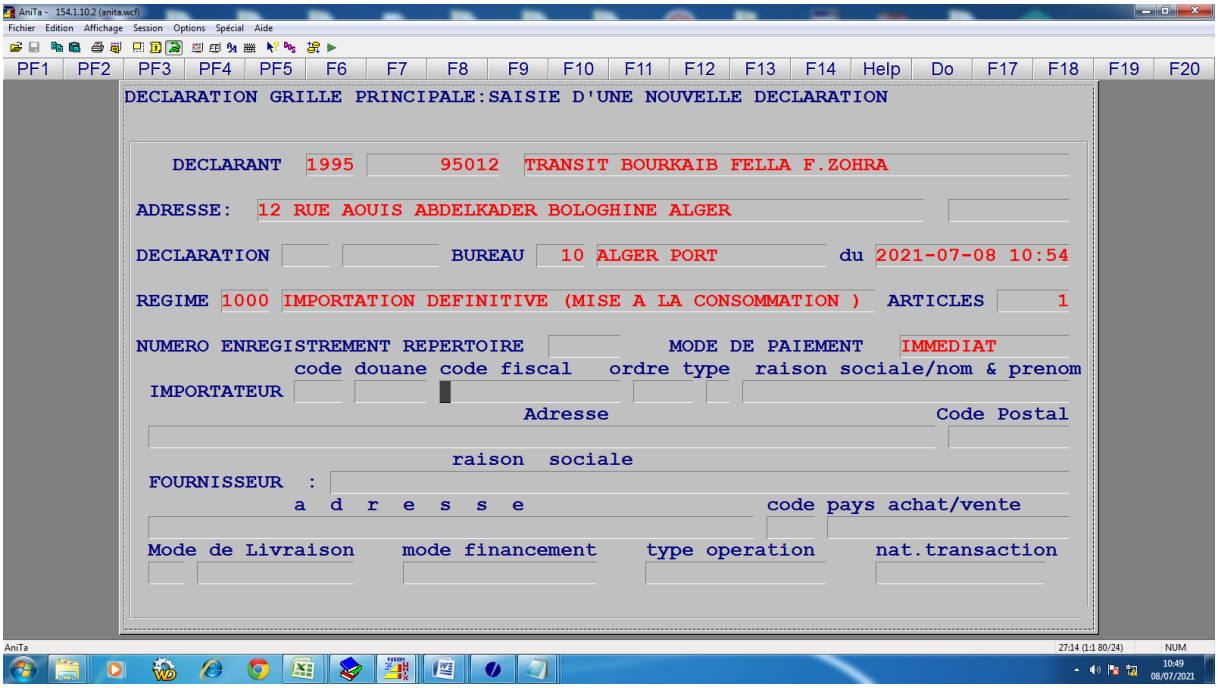
Une port d'entrée pour :

- Obtenir d'avantage d'information sur le système.
- Provoque un déni de service sur l'application.
- Obtenir un accès à des données normalement non accessible.
- Obtenir un accès au système globale avec des droits plus ou moins privilégies.

Le centre utilise « Anita » qui est pour le Web donne une nouvelle vie à nos applications de texte, offrant une apparence graphique et des fonctionnalités.

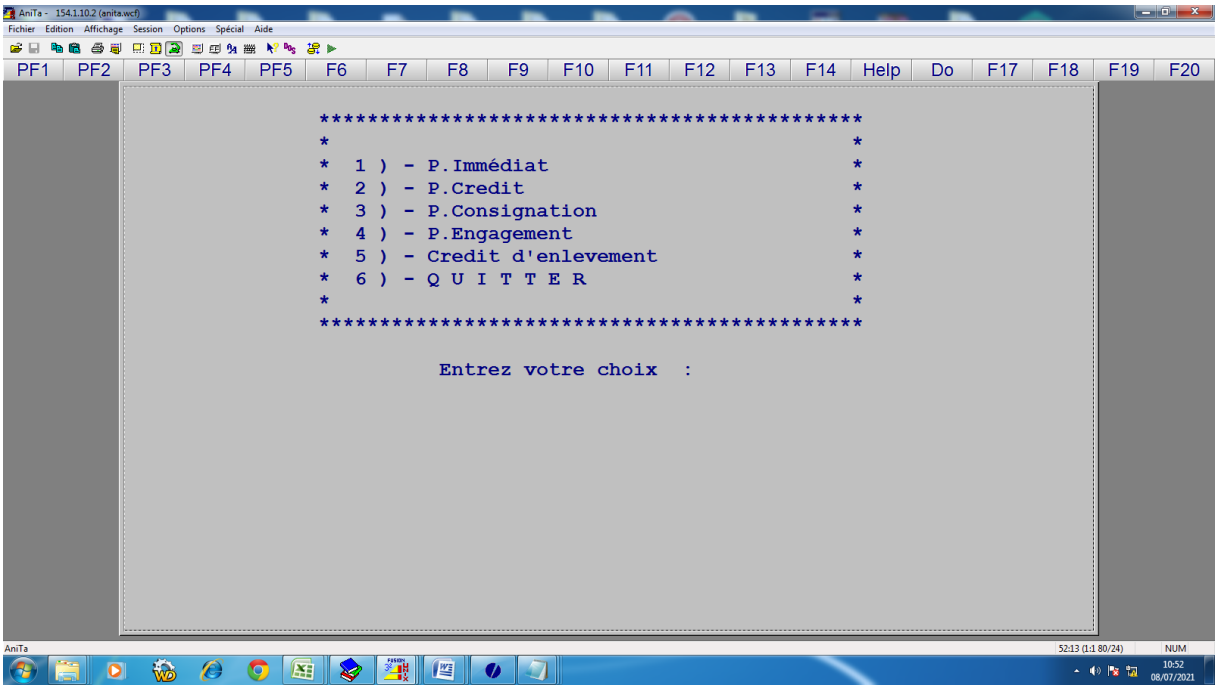
Certaines fonctions ont été adaptées et développées selon les besoins. Voici quelques captures d'écran pris au lieu de stage :

Choix 1 : déclaration



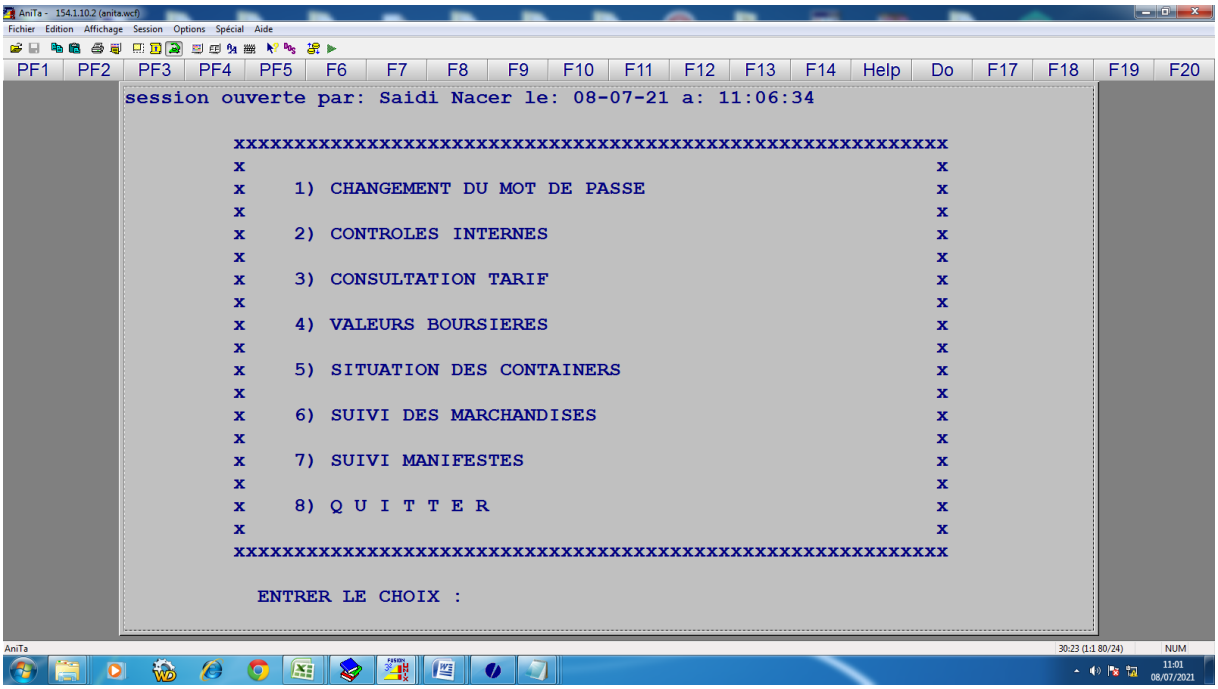
Source : capturée depuis l'ordinateur de l'administrateur

Menu caissier



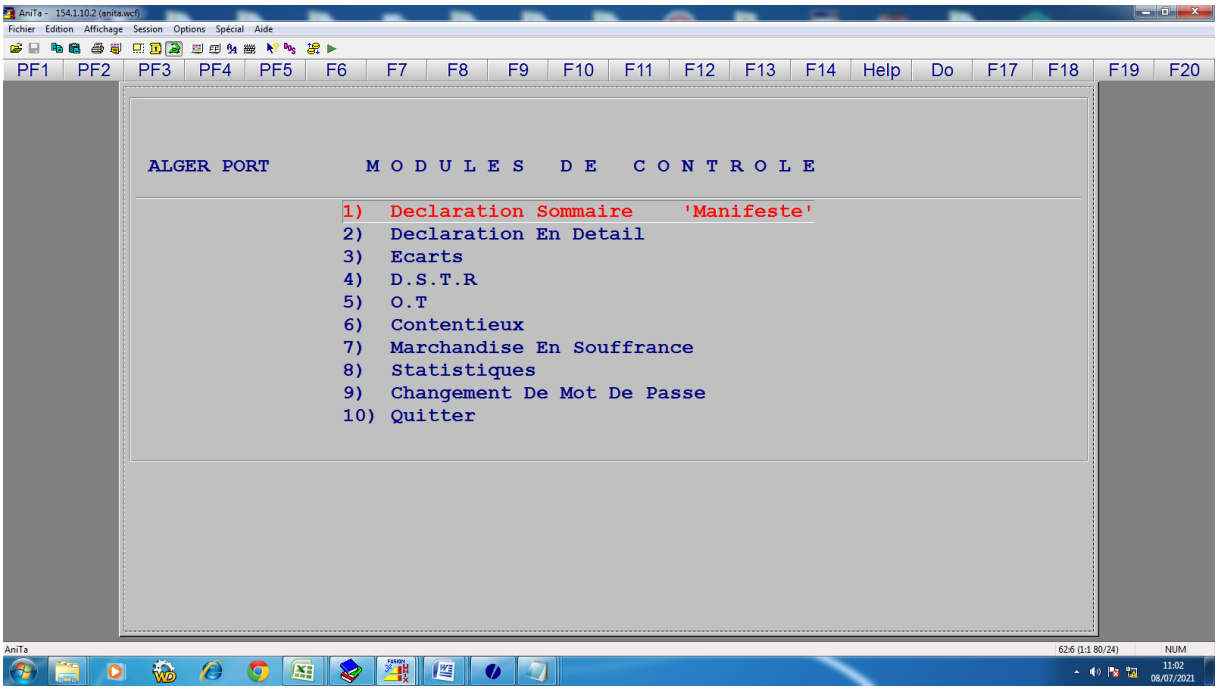
Source : capturée depuis l'ordinateur de l'administrateur

Différents modules de contrôle



Source : capturée depuis l'ordinateur de l'administrateur

Contrôle interne



Source : capturée depuis l'ordinateur de l'administrateur

Proposition de quelques solution :

- **La protection des accès physiques** : sécuriser le matériel qu'on utilise par des câbles de protection, une vérification des entrées et des sorties, de la vidéo surveillance.
- Protéger le matériel contre les **crash** et **pannes** : il est nécessaire d'utiliser du matériel de bonne qualité avec une solution de repli si besoin : **le lien de secours**
- Protection contre les **attaques informatiques** (mots de passe très sécurisés, authentification avec plusieurs étapes d'identification...).
- La **sensibilisation des collaborateurs** qui reste un levier primordial pour se prémunir des risques.
- Une **sauvegarde** de vos données efficace et fréquente, voire automatisée si possible.
- Solution antiviral centralisé (actif directoire domaine) pour facilite la politique de sécurisation.

CONCLUSION GENERALE

Dans un monde interconnecté, les entreprises se trouvent dans l'obligation de toujours chercher à être visible , sécurisé et en bon fonctionnement. les supports informatiques sont devenus une clé stratégique pour le développement de l'organisation, mais en retour, les risques que représentent les risques des technologies de l'information apparaissent.

Le point culminant de la recherche modérée que nous avons menée dans Le centre national des transmissions et du système d'informations des douane Algérienne communément appelé CNTSID, que nous tentons à travers notre étude d'élaboré une cartographie des risques-IT .

Il a fallu dans un premier temps identifier les différents équipement informatique dans le CNTSID et déterminer l'ensemble des risques existants, calculer l'impact des risque IT tout en utilisant des méthodes qualitatives , sachez aussi qu'il est possible de transférer les quantités des risques déterminées en monnaie, chose qui permettra de prendre la meilleure décision financière.

En effet , CNTSID a besoins de nouvelles technologies et de nouveaux logiciels lui permettant de s'adapter au développement et répondre à ses nouveaux besoins Cette intégration doit impliquer toutes les activités, ce qui produira des changements pour le mieux. Ceux-ci sont déterminés sur la base d'une revue de la littérature qui nous a inspirée l'approche la plus appropriée à ce sujet, car basée sur Les recherches et les résultats obtenus par les auteurs, nous sommes en mesure de mener nos propres recherches.

Il convenait de suivre une démarche de recherche qualitative pour faire une analyse déterminant des risques informatique et atteindre le résultat de la recherche , et cela par les entretiens, et la documentation.

Suite à cette analyse nous avons élaboré une cartographie des risques-IT de CNTSID, que ce soit la situation positive ou négative, ainsi que le niveau d'information et les préoccupations des employés à ce sujet.

Cette étude nous a menées à constater que les entreprises ont besoin d'être toujours à jour en ce qui est des nouvelles technologies et assurer de soumettre la politique de sécurité en pratique et c'est pour tout entreprises Algérienne,

Pour conclure, Cette expérience du projet de fin d'études nous a été très enrichissante, car nous avions concrétisé nos connaissances acquises tout au long de notre cursus, voir licence en ingénierie du logiciel et master en management stratégique et système d'information, mais également des connaissances récentes suite à notre recherche. De plus, nous avions affronté un état de crise et s'y être adaptées pour enfin aboutir à ce travail.

REFERENCE BIBIOGRAPHIQUE

ARTICLES :

- saint-gérand Thierry , Eliane Propeck-Zimmermann « Cartographie des risques technologiques majeurs: nouvelles perspectives avec les SIG » March 2002
- École centrale Paris, Grande-Voie-des-Vignes, 92295 Châtenay-Malabry cedex, France "The management of risks by the global risk analysis"17 April 2013.
- FREDERIQUE VALLEE « Sécurité informatique pour la gestion des risques » 10 avr. 2016

LIENS

https://ars.els-cdn.com/content/image/1-s2.0-S1246782013000086-gr14.jpg

http://risquesenvironnementaux.oree.org/notre-methodologie//gestion-globale-risques.html

http://gbp.resinfo.org/wp-content/uploads/2014/07/fig4.jpg

https://www.qualitiso.com/wp-content/uploads/2020/07/definition-de-risque.png

https://www.qualitiso.com/risques-definition-types-evaluation-gestion/

https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

https://www.certification-qse.com/definition-risque-qualite-qualite-iso-9001

La gestion des risques. (s. d.). manager-go. https://www.manager-go.com/gestion-de-projet/cartographie-des-risques.htm

La gestion des risques. (s. d.-b). dafmag.fr. https://www.daf-mag.fr/Definitions-Glossaire/Gestion-risques-245455.htm

gestion des risques. (s. d.). info entrepreneure. https://www.infoentrepreneurs.org/fr/guides/bl--gestion-des-risques/

Guide de pratique proffetionnel. (s. d.). gpp.oiq.qc.ca. http://gpp.oiq.qc.ca/le_processus_global_de_gestion_des_risques.htm

https://www.joradp.dz/FTP/JO-FRANCAIS/2017/F2017013.pdf

https://www.qualitiso.com/risques-definition-types-evaluation-gestion/

https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:fr

https://www.certification-qse.com/definition-risque-qualite-qualite-iso-9001

La gestion des risques. (s. d.). manager-go. https://www.manager-go.com/gestion-de-projet/cartographie-des-risques.htm

La gestion des risques. (s. d.-b). dafmag.fr. https://www.daf-mag.fr/Definitions-Glossaire/Gestion-risques-245455.htm

gestion des risques. (s. d.). info entrepreneure. https://www.infoentrepreneurs.org/fr/guides/bl---gestion-des-risques/

Guide de pratique proffetionnel. (s. d.). gpp.oiq.qc.ca. http://gpp.oiq.qc.ca/le_processus_global_de_gestion_des_risques.htm

En quoi consiste la gestion des risques ? (s. d.). redhat. https://www.redhat.com/fr/topics/management/what-is-risk-management

https://www.joradp.dz/FTP/JO-FRANCAIS/2017/F2017013.pdf

ANNEXE- guide d’entretien individuel (semi directif)

Annexe A : GUIDE D'ENTRETIENT SUR LACARTOGRAPHIE DES RISQUES-IT

- Qu'est-ce que un risque pour vous ?
- Qu'elles sont les actifs informatiques critique de centre de calcule ?
- Quelles sont les menaces principales pour le système d'information aux quelle fait face votre entreprise ?
- Existe-il une politique de sécurité comme stratégie mise en place par votre entreprise ?
- Qui doit gérer les risques dans un projet informatique ?
- Depuis votre recrutement ; y'a-t-il eu du changent comme une nouvelles technologie intégré ?