Comment assurer la sécurité des données de l'entreprise ?

Marion Salendres

Mémoire de stage

Comment assurer la sécurité des données de l'entreprise ?

Présenté par : Marion Salendres

Entreprise d'accueil : HM. Clause
Rue Louis Saillant, 26800 Portes-lès-Valence

Date de stage : du 01/04/19 au 30/08/19

Tuteur entreprise : Antoine Le Tourneurs
Tuteur universitaire : Sabine Carton

Master 1 FI
Master Management des Systèmes d'Information (MSI)
2018 – 2019

Limagrain
de la terre à la vie

HM • CLAUSE

Mémoire de stage

Comment assurer la sécurité des données de l'entreprise ?

Présenté par : Marion Salendres

Entreprise d'accueil : HM. Clause
Rue Louis Saillant, 26800 Portes-lès-Valence

Date de stage : du 01/04/19 au 30/08/19

Tuteur entreprise : Antoine Le Tourneurs
Tuteur universitaire : Sabine Carton

GRENOBLE iae Graduate school of Management

Master 1 FI
Master Management des Systèmes d'Information
2018 - 2019

UNIVERSITÉ Grenoble Alpes

Avertissement :

Grenoble IAE, au sein de l'Université Grenoble Alpes, n'entend donner aucune approbation ni improbation aux opinions émises dans les mémoires des candidats aux masters en alternance : ces opinions doivent être considérées comme propres à leur auteur.

Tenant compte de la confidentialité des informations ayant trait à telle ou telle entreprise, une éventuelle diffusion relève de la seule responsabilité de l'auteur et ne peut être faite sans son accord.

RÉSUMÉ

Pour conclure la première année de Master Management des Systèmes d'Information à l'IAE de Grenoble, j'ai réalisé un stage de cinq mois au sein de l'entreprise HM. Clause et de l'équipe Data Analytics du département Business Solution Delivery de Limagrain IT, sous la tutelle d'Antoine Le Tourneurs, du 1er avril au 30 août 2019.

HM. Clause est une Business Unit de Limagrain, un groupe spécialisé dans les semences de grandes cultures, les semences potagères et les produits céréaliers.

Ma principale mission de stage consiste notamment à concevoir les spécifications fonctionnelles et techniques d'une application web de gestion des droits d'accès.

Dans ce mémoire, je présenterai mes missions de stage et je tenterai de répondre à une problématique liée à la sécurité des données dans une entreprise. Je m'appuierai sur des recherches documentaires afin d'apporter des solutions à cet enjeu devenu majeur pour les entreprises.

MOTS CLÉS : Sécurité des systèmes d'information, politique de sécurité des données, perte de données de l'entreprise, gestion des droits d'accès, Limagrain IT.

REMERCIEMENTS

Je tiens à remercier dans un premier temps, M. Antoine Le Tourneurs, mon tuteur de stage à HM. Clause, de m'avoir accueillie durant ces cinq mois de stage et de m'avoir accompagnée dans mes missions au sein du département Data Analytics de Limagrain IT.

Je souhaite lui adresser ma gratitude pour m'avoir rapidement intégrée au sein de l'entreprise, pour le partage de son expertise, pour le temps qu'il m'a consacré et pour la confiance qu'il m'a accordée en m'accueillant dans son bureau ainsi qu'au cours de ses déplacements.

Je tiens aussi à remercier l'ensemble du personnel de HM. Clause, pour leur accueil chaleureux, l'aide qu'ils m'ont apportée et l'ambiance qu'ils ont instaurée tout au long de mon stage.

Enfin, je remercie également Mme Sabine Carton, ma tutrice à l'IAE, pour son aide et ses conseils concernant la rédaction de ce rapport.

SOMMAIRE

INTRODUCTION 9

A. LE GROUPE LIMAGRAIN 9

B. HM. CLAUSE 10

C. DIAGNOSTIC STRATEGIQUE DU GROUPE LIMAGRAIN 10

I. Profil de la société 10

II. Le modèle des 5 forces de Porter 11

PARTIE 1 - PRESENTATION DES MISSIONS ET DU PROBLEME RENCONTRE 14

A. ENJEU RENCONTRE : LA SECURITE DES DONNEES 15

B. MA PRINCIPALE MISSION DE STAGE 16

C. PRESENTATION DU GANTT 18

PARTIE 2 - ANALYSE DE LA SITUATION ET DES SOLUTIONS PROPOSEES 20

A. RECHERCHE DOCUMENTAIRE SUR LE PROBLEME POSE 21

I. La perte de données, garantir la sécurité des systèmes d'information 21

II. La sécurité des données en quelques chiffres 21

III. Les causes du problème 22

IV. Les impacts et conséquences sur l'entreprise 23

B. DES SOLUTIONS AU PROBLEME RENCONTRE 24

I. La mise en place d'une politique de sécurité des données 24

II. Les solutions techniques de protection des données 25

PARTIE 3 - RESULTATS OBTENUS 27

A. PLAN D'ACTION ET PRATIQUES PROPOSEES 28

B. MISE EN PRATIQUE DES SOLUTIONS 28

C. BILAN SUR LE SUIVI DU GANTT 29

CONCLUSION 30

BIBLIOGRAPHIE 31

SITOGRAPHIE 32

TABLES DES FIGURES 34

INTRODUCTION

Je présenterai dans un premier temps le groupe Limagrain, ainsi que l'une de ses filiales, HM. Clause et je ferai ensuite un diagnostic stratégique du groupe coopératif.

A. LE GROUPE LIMAGRAIN

Limagrain est un groupe coopératif français, fondé dans la plaine de Limagne en 1942 par des agriculteurs, afin de maîtriser la fourniture des semences nécessaires à leurs exploitations. La coopérative a ainsi permis le développement de l'activité de ses agriculteurs, d'abord grâce à la production de semences de maïs.

Aujourd'hui, la coopérative Limagrain est la maison-mère d'un groupe mondial qui crée et produit des variétés végétales et commercialise des semences de grandes cultures (maïs, blé, etc.), des semences potagères (tomate, carotte, melon, etc.) et des produits céréaliers (pains Jacquet, Savane) aux agriculteurs, aux industries agroalimentaires et aux consommateurs.

Limagrain est le 4ème semencier mondial, la deuxième société de transformation en produit boulanger français et le troisième en produit pâtissier français avec les marques Jacquet et Brossard. Le groupe a développé ses activités dans 56 pays et compte plus de 10 000 salariés dans le monde.

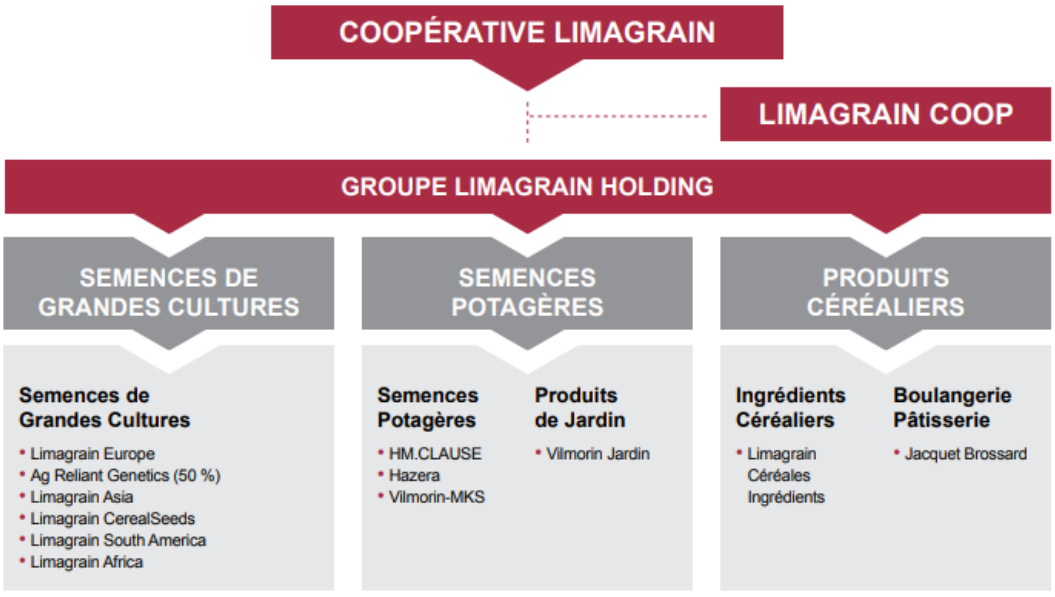


***Figure 1** : Schéma des différentes filiales de Limagrain (source : Limagrain.com)*

B. HM. CLAUSE

HM. Clause est une Business Unit de Limagrain, spécialisée dans la recherche, la production et la commercialisation de semences potagères. C'est en 2008 que les deux sociétés Harris Moran aux Etats-Unis et Clause en France sont regroupées en une même Business Unit sous le nom de HM. Clause.

Le siège social de HM. Clause est basé à Portes-lès-Valence dans la Drôme, où j'ai eu l'opportunité de réaliser mon stage. L'entreprise est présente sur 5 continents, répartis en 3 hubs : EMEA (Europe, Moyen-Orient, Afrique), AMPA (Amériques et Pacifique) et ASIA et regroupe plus de 2800 professionnels.

C. DIAGNOSTIC STRATEGIQUE DU GROUPE LIMAGRAIN

I. PROFIL DE LA SOCIETE

Limagrain est un groupe coopératif qui crée, produit et commercialise des semences potagères et de grandes cultures et qui s'est progressivement internationalisé. Le groupe s'organise en 13 Business Units, qui couvrent toutes les activités opérationnelles du groupe et favorisent une proximité et une excellente connaissance des différents marchés, produits et clients sur les 5 continents.

Limagrain mène une stratégie d'internationalisation, développant sa présence à l'international, notamment grâce à des partenariats et des prises de participation dans des entreprises. Le groupe mène aussi une stratégie de diversification, l'offre s'adapte en fonction des spécificités locales et son activité est diversifiée, de la génétique à l'agroalimentaire.

Le progrès fait aussi partie des valeurs fondatrices du groupe et il s'appuie sur un fort investissement en recherche (environ 14% du CA), visant à assurer une meilleure croissance. Elle permet notamment de mettre au point des variétés de semences plus performantes en termes de rendement, de résistance et d'adaptation aux climats et territoires.

Cette stratégie d'internationalisation, de diversification et ses investissements en recherche permettent à Limagrain de renforcer sa position concurrentielle sur les marchés mondiaux.

En effet, sur le marché, Limagrain est :

- Le 4e semencier mondial.
- Le n°2 mondial en semences potagères, avec un portefeuille de produits très diversifié de plus de 30 espèces pour les maraîchers et les conserveurs.
- Le n°1 mondial en semences de tomate, carotte, melon, chou-fleur et courgette.
- Le n°6 mondial en semences de grandes cultures, avec 2 espèces stratégiques (le maïs et le blé) et des espèces régionales (le tournesol, le colza, l'orge, le riz, le soja).

Le marché des semences représente près de 35 milliards d'euros en 2017. C'est un secteur porteur, notamment grâce à l'augmentation de la population mondiale qui induit un

accroissement des besoins alimentaires en matières premières agricoles, ainsi que l'utilisation croissante des semences commerciales.

II. LE MODELE DES 5 FORCES DE PORTER

Le modèle des cinq forces de Porter permet d'analyser le marché des semences ainsi que la position concurrentielle de l'entreprise en prenant en compte cinq dimensions : l'intensité de la concurrence, la menace des nouveaux entrants, la menace des produits de substitution, le pouvoir de négociation des clients, et le pouvoir de négociation des fournisseurs.

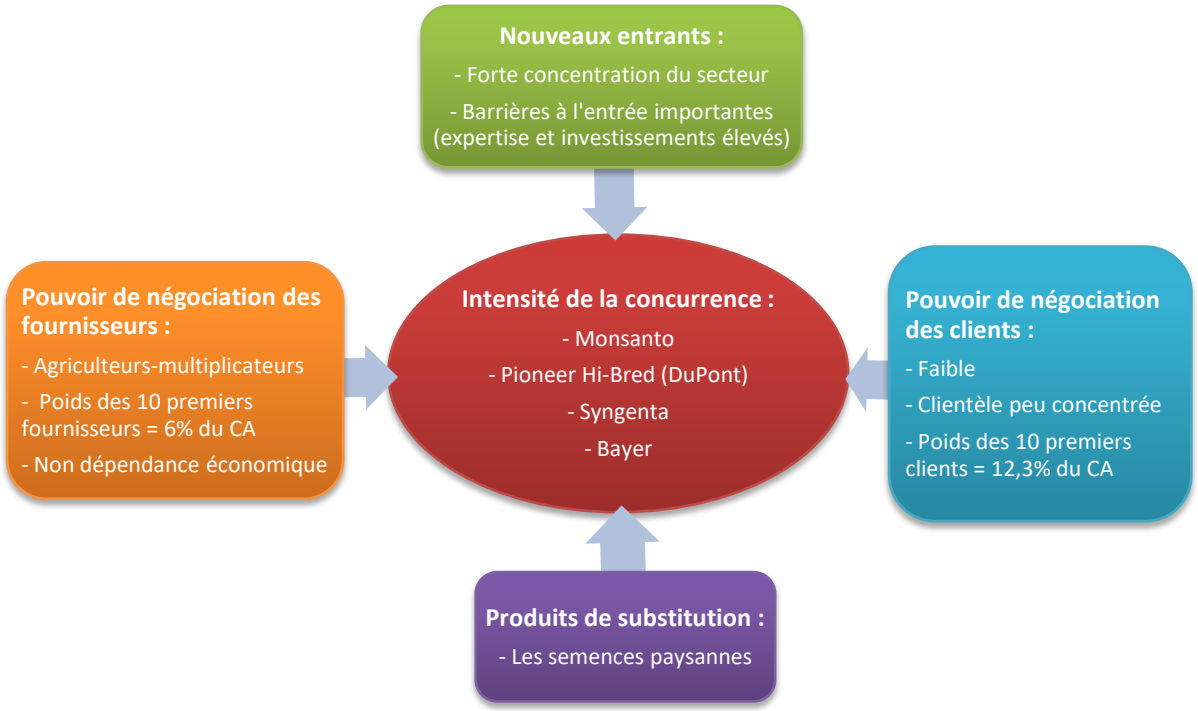


Figure 2 : *Représentation du modèle des 5 forces de Porter pour Limagrain*

- **L'intensité de la concurrence :**

Les principaux concurrents de Limagrain sont des groupes agrochimistes comme Bayer-Monsanto (aux Etats-Unis), Pioneer Hi-Bred (filiale de DuPont aux Etats-Unis), Syngenta (société suisse).
Le marché mondial des semences est de plus en plus concentré. En effet, les nombreuses fusions et acquisitions ont réduit le nombre d'acteurs et modifié la hiérarchie du classement mondial. Les cinq premières entreprises semencières représentent plus de la moitié du marché mondial des semences commerciales.

- **La menace des nouveaux entrants :**

La menace de nouveaux entrants potentiels est relativement faible car l'entrée sur le marché des semences est difficile, étant donné la puissance des principaux opérateurs, la forte

concentration du secteur et compte tenu des barrières importantes à l'entrée. En effet, les recherches en génétique et le développement de biotechnologies requièrent une expertise et un investissement initial élevé.

- **Le pouvoir de négociation des clients :**

Il existe plusieurs types de clients sur le marché :

- La clientèle d'agriculteurs, par l'intermédiaire de réseaux de distribution adaptés aux pays visés et aux espèces commercialisées
- Les maraîchers, producteurs de légumes pour le marché de frais, et indirectement les transformateurs spécialistes de la conserve et de la surgélation.
- Réseaux de distribution de produits de jardin (jardineries, grandes surfaces et bricolage, grandes surfaces alimentaires).

Le portefeuille de clients est relativement large, la clientèle est peu concentrée. En effet, le poids des 10 premiers clients est de 12,3% du chiffre d'affaires en 2018, et de 8,3% pour les 5 premiers clients. Le risque de chute d'activité ainsi que le pouvoir de négociation des clients est donc relativement faible.

- **Le pouvoir de négociation des fournisseurs :**

La production de semences est gérée par un réseau international d'agriculteurs-multiplicateurs sélectionnés. Ce réseau produit une grande quantité de graines, à partir de semences mères d'une variété, qui est ensuite reprise par le semencier. Un cahier des charges strict est établi entre semenciers et multiplicateurs et permet d'assurer l'approvisionnement. De plus, une partie des approvisionnements en semences est assurée au travers de la coopérative Limagrain.
Le poids des 10 premiers fournisseurs est de 6% du CA, et de 4,1% pour les 5 premiers.
Le groupe s'assure donc de sa non-dépendance économique à l'égard des fournisseurs.

- **La menace des produits de substitution :**

Les semences paysannes (ou de ferme) sont un produit de substitution. Ce sont des variétés de semence issues des mises en culture par un agriculteur, qu'il va ensuite sélectionner et multiplier, avant de les replanter.
Cependant, ces semences paysannes ne correspondent pas aux critères d'homogénéité et ne figurent donc pas sur le catalogue officiel autorisant leur commercialisation.
La menace des produits de substitution est donc faible.

La stratégie de diversification, d'internationalisation et les forts investissements en recherche de Limagrain permet au groupe de s'adapter à l'environnement concurrentiel et de garder sa place de quatrième semencier mondial.

Afin de rester concurrentielles dans leur domaine, les organisations ont un besoin croissant de maîtriser leurs données, elles collectent et exploitent au quotidien des données nombreuses et diversifiées. On les appelle aussi Data ou encore le Big Data, elles concernent les clients, les fournisseurs ou encore les employés de l'entreprise.

Dans le contexte actuel de la Business Intelligence, où un grand volume de données circule et joue un rôle primordial dans la prise de décisions et le fonctionnement de l'entreprise, la sécurité des données représente un nouveau défi majeur.

Ce constat me permet donc de poser la problématique suivante, à laquelle j'apporterai une réponse dans ce rapport : **Comment assurer la sécurité des données de l'entreprise ?**

Dans une première partie, je présenterai mes missions de stage et la problématique liée à la sécurité des données à laquelle j'ai choisi de répondre. Je ferai ensuite une analyse du problème et je proposerai des axes de solution à ce dernier. Enfin, une troisième partie exposera des recommandations portant sur la sécurité des données d'une entreprise ainsi que les solutions mises en œuvre dans le groupe Limagrain.

PARTIE 1

-

PRESENTATION DES MISSIONS ET DU PROBLEME RENCONTRE

Dans cette partie, je présenterai l'enjeu de la sécurité des données dans une entreprise, ainsi que la mission principale de mon stage. J'annoncerai ensuite les différents axes de résolution de ce problème. Enfin, je présenterai en détails les tâches liées à ma mission de stage, illustrées par un diagramme de Gantt.

A. ENJEU RENCONTRE : LA SECURITE DES DONNEES

C'est au sein du département Data Analytics de Limagrain IT que j'effectue mon stage et l'une de mes missions est de concevoir une application de gestion des droits d'accès aux outils de reporting.

Comme dans de nombreuses entreprises actuelles, les données se situent au cœur des stratégies et sont un outil majeur d'aide à la décision.

Les nouveaux besoins des utilisateurs du business changent, ils utilisent de plus en plus de rapports et tableaux de bord et nécessitent de nouveaux outils de reporting. Les utilisateurs font part de leurs besoins auprès des départements BI, ils ont notamment besoin d'utiliser des données organisationnelles, mais avant tout d'avoir accès aux données, dans un contexte agile et collaboratif.

Grâce aux outils de reporting BI mis en place dans l'entreprise, les métiers sont plus indépendants, ils peuvent analyser l'information, gérer et traiter les données en interne et ainsi prendre des décisions rapidement, par exemple à travers des tableaux de bord adaptés aux besoins de chaque métier. Cela leur permet d'associer la gestion opérationnelle et décisionnelle. Ces outils permettent aux métiers de réaliser eux-mêmes des requêtes pour accéder rapidement aux informations dont ils ont besoin, avec des données significatives pour le business.

Cette demande croissante d'accès aux données nécessite une amélioration des modèles de sécurité BI. Pour répondre à ces besoins, il est nécessaire d'accéder aux données de plusieurs processus et Business Units, afin d'effectuer des corrélations entre elles. Cela implique une certaine collaboration entre les métiers et non un stockage des données en silos[1].

La BI repose sur les concepts de couche sémantique et de la sécurité à l'accès aux données. La couche sémantique est une couche orientée métier entre la base de données et l'utilisateur final, c'est-à-dire une interface qui emploie un langage qui parle au business.

Quant à la sécurité d'accès aux données, elle correspond d'abord au contrôle d'accès aux données basé sur les zones géographiques par exemple, mais aussi au contrôle des droits dans les applications, qui dépendent des différents rôles dans l'organisation (administrateur, utilisateurs simples, etc.).

Dans ce contexte où la data est au centre de la stratégie d'entreprise, un besoin de sécurisation et de protection des données s'impose et la mise en place d'un contrôle d'accès aux données est nécessaire.

[1] *Un silo de données est un référentiel de données fixes maintenu sous le contrôle d'un seul service déterminé de l'entreprise, et qui se trouve isolé des autres services.*

Au sein de Limagrain, l'équipe BSD Data Analytics gère les contrôles d'accès en définissant les droits d'accès des sujets (les utilisateurs) sur les objets (bases de données, tableaux de bord, rapports, etc.). En effet, il est nécessaire de limiter l'accès aux données de chaque utilisateur du business. Une absence de limites pourrait conduire à une fuite de données confidentielles, comme des informations sur les clients ou des produits, ou encore des données financières. Toute perte de données qu'elle soit accidentelle ou intentionnelle, pourrait impacter négativement l'activité de la société et ses résultats.

C'est pourquoi la sécurité informatique est devenue essentielle dans toute entreprise, et afin de protéger les données et les infrastructures informatiques, les entreprises mettent en place des politiques de sécurité et des techniques de protection des données. Dans ce rapport, nous allons notamment aborder une composante importante de la sécurité des systèmes d'information : le contrôle d'accès.

B. MA PRINCIPALE MISSION DE STAGE

Ma mission m'amène à concevoir une application web de gestion des droits d'accès des utilisateurs reporting des trois Business Units potagères de Limagrain (HM.Clause, Vilmorin et Vilmorin Jardin). Mon rôle consiste notamment à rédiger les spécifications fonctionnelles et techniques de l'application.

Actuellement, l'équipe Data Analytics du département BSD (Business Solution Delivery) de Limagrain IT est chargée de répondre aux demandes d'accès des utilisateurs par le biais du ticketing (*voir Annexe 1 : Exemple de ticket de demande d'accès*). Les utilisateurs créent des tickets sur la plateforme MyHelpDesk, dans lesquels ils adressent à l'équipe des demandes d'accès aux différents objets de reporting (Analysis Services Cubes, Reporting Services Reports, applications QlikView).

L'équipe gère tout d'abord les droits d'accès au niveau de l'objet (*par exemple : les rapports RS pour le domaine des ventes, ou le cube pour le domaine finance*). Ce niveau de droits d'accès est géré via des groupes de l'Active Directory[2] (groupes AD) dédiés, il existe un groupe AD par objet et domaine. L'équipe reporting crée des tickets IWS pour demander à ajouter des utilisateurs dans les groupes AD.

Pour affiner la sécurité, c'est à dire gérer les droits d'accès au niveau des données ou périmètres (ce niveau de sécurité est aussi appelé Row Level Security) (*ex : autoriser Paul à voir les données pour la France uniquement*), l'équipe remplit des tableaux excel qui indiquent quel utilisateur a accès à quel périmètre, puis les tables de sécurité des entrepôts de données (DWH) sont alimentées par des jobs SQL qui reprennent ces tableaux excel.

Cependant, plusieurs problèmes se posent :

- Cette procédure est peu pratique et génère une perte de temps. En effet, le nombre de demandes d'accès est important.
- La gestion des droits d'accès est manuelle et pourrait être automatisée.

[2] *Limagrain utilise l'Active Directory (AD) qui est un annuaire permettant de centraliser des informations relatives aux utilisateurs de l'entreprise. L'AD fournit des mécanismes d'identification et d'authentification et sécurise ainsi l'accès aux données.*

- Les demandes de droits d'accès sont souvent mal définies et ont besoin de précisions. Les utilisateurs qui font des demandes d'accès omettent parfois de spécifier à quel domaine ou pour les données de quelle société il souhaite avoir accès.
- Avant d'accorder un accès, l'équipe Reporting doit demander l'accord des Domain Leader ou des Key Users. En effet, seul le business sait qui a besoin de quel accès.
- La gestion des droits d'accès n'apporte pas de valeur ajoutée à l'équipe qui pourrait se consacrer à d'autres tâches.

L'équipe Reporting souhaite donc faire développer une application web pour permettre aux Domain Leaders d'administrer les droits eux-mêmes.

J'ai eu l'opportunité de prendre part au processus de conception d'une application web de gestion des droits d'accès reporting à travers les étapes suivantes : l'analyse du besoin des utilisateurs, la rédaction des spécifications fonctionnelles et techniques, et enfin la phase de test.

Je présenterai ces étapes dans la partie suivante à travers un diagramme de Gantt, et je détaillerai chacune des tâches.

Par la suite, la partie 2 exposera une analyse du problème posé issue de ma recherche documentaire ainsi que différentes solutions et bonnes pratiques qu'une entreprise peut mettre en œuvre pour sécuriser ses données. Je proposerai notamment dans ce rapport des pistes de résolution telles que la mise en place d'une politique de sécurité des données ou d'outils techniques.

C. PRESENTATION DU GANTT

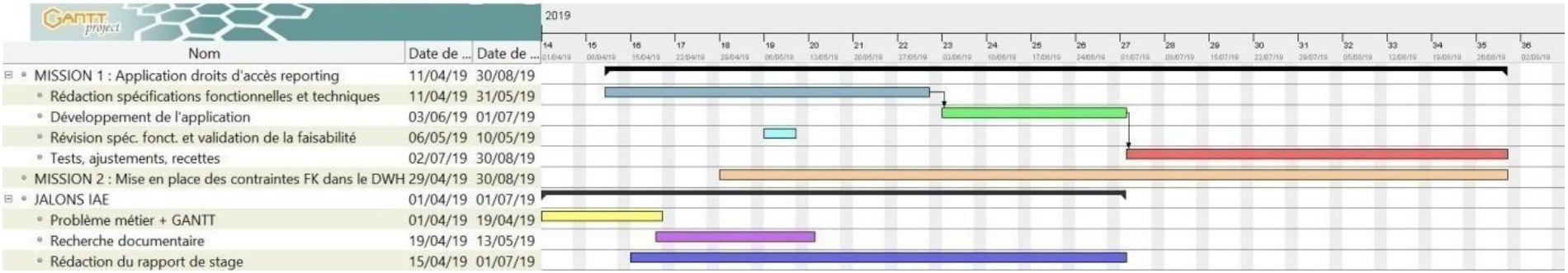


***Figure 3** : Diagramme de Gantt initial*

J'ai édité ce diagramme de Gantt à l'aide du logiciel Gantt Project.

Ma mission principale 'Application droits d'accès reporting' se rapporte à la conception d'une application de gestion des droits. Il s'agit de rédiger les spécifications fonctionnelles et techniques d'une application Web pour gérer les droits d'accès des utilisateurs reporting des Business Units potagères (HM.Clause, Vilmorin et Vilmorin Jardin).

Cette mission se décompose en plusieurs étapes :

1) Dans un premier temps, il m'a fallu comprendre les procédures et le fonctionnement de la gestion des droits reporting actuelle. En effet, j'ai pu traiter des tickets de demande d'accès (*voir Annexe 1*) et répondre à la demande de certains utilisateurs en leur donnant accès à différents objets reporting (Analysis Services Cubes, Reporting Services Reports, applications QlikView).

2) Par la suite, j'ai effectué une maquette des pages de l'application grâce à l'outil Userform d'Excel VBA. Il s'agit d'avoir une première idée de ce à quoi ressemblerait l'application, et de visualiser les différentes pages et les fonctionnalités de l'application (*voir Annexe 2 : maquette de l'une des pages de l'application de gestion des accès).*

3) En parallèle, j'ai rédigé les spécifications fonctionnelles et techniques (cette étape est indiquée sur le diagramme de Gantt, du 11/04/19 au 31/05/19).
    - Les spécifications fonctionnelles permettent de décrire en détail les services que l'application va fournir, les aspects métier de l'application ainsi que les parties fonctionnelles de l'interface et leur action, notamment les formulaires, les boutons, les listes, etc.
    - Les spécifications techniques vont décrire les choix techniques répondant aux besoins et aux spécifications fonctionnelles, elles concernent par exemple l'architecture de l'application et reprennent les contenus et détails des fonctionnalités ainsi que des pistes de solutions techniques.

    Ces spécifications fonctionnelles et techniques sont destinées aux développeurs, qui s'appuieront sur ces dernières pour démarrer la phase de développement de l'application web (l'étape de développement est indiquée sur le diagramme du 03/06/19 au 01/07/19).

    Le document des spécifications de l'application est révisé lors de réunions avec le lead developer (indiquées sur le diagramme de Gantt du 06/05/19 au 10/05/19).

4) Enfin, la dernière étape de ma mission est la phase de recette ou test, que je réaliserai après le développement de l'application (cela correspond à la phase 'tests, ajustements, recettes' que j'ai indiquée comme durant du 02/07/19 au 30/08/19)

Sur le diagramme de Gantt ci-dessus est aussi indiquée une MISSION 2 concernant la mise en place des contraintes Foreign-Keys dans le DataWareHouse. Il s'agit de créer des clés étrangères, qui permettront de gérer des relations entre plusieurs tables et de garantir la cohérence des données.

Enfin, les jalons IAE correspondent aux différentes dates de rendu des livrables :

- Elaboration du problème métier et réalisation du diagramme de Gantt
- Liste des ouvrages de la recherche documentaire liée au problème métier
- Finalisation et rendu du présent rapport de stage.

PARTIE 2

-

ANALYSE DE LA SITUATION ET DES SOLUTIONS PROPOSEES

A. RECHERCHE DOCUMENTAIRE SUR LE PROBLEME POSE

I. LA PERTE DE DONNEES, GARANTIR LA SECURITE DES SYSTEMES D'INFORMATION

Dans les entreprises de toute taille, l'outil informatique prend de l'ampleur, les processus métiers se dématérialisent et les données sont au cœur de leur fonctionnement et de leur organisation. Les organisations sont amenées à gérer des volumes de données de plus en plus importants. L'analyse et l'exploitation de ces informations évoluent et progressent, notamment avec l'arrivée des outils de Business Intelligence. En effet, les données des entreprises jouent un rôle important en fournissant aux collaborateurs et chefs d'entreprise des outils clés dans la prise de décision et les stratégies d'entreprise.

Dans ce contexte où les volumes de données sont en croissance permanente et prennent une place importante, la sécurisation des données devient une préoccupation et un enjeu majeur pour les entreprises. L'essor du télétravail, la mobilité des employés ou encore la collaboration ouverte nécessitent des précautions accrues en matière de protection des données. Il devient essentiel pour l'entreprise d'adopter ou de redéfinir des stratégies de sécurité pour lutter contre la perte ou le vol de données et pour protéger les informations de l'entreprise.

Cependant, il est difficile de garantir la sécurité de ces informations et de gérer les risques de fuite ou de corruption des données.

Plusieurs scandales concernant des fuites de données éclatent d'ailleurs chaque année, et cela peut coûter très cher aux entreprises, notamment lorsqu'il s'agit de données personnelles. Dans ce cas, l'entreprise risque une pénalité qui peut s'élever jusqu'à 4% de son chiffre d'affaires.

II. LA SECURITE DES DONNEES EN QUELQUES CHIFFRES

Une perte de données peut être de plusieurs natures : elle peut être due à une erreur humaine, une panne du système ou encore une cyber-attaque.

Selon le site datahealthcheck.com, les principales causes de perte de données en 2018 sont les suivantes :

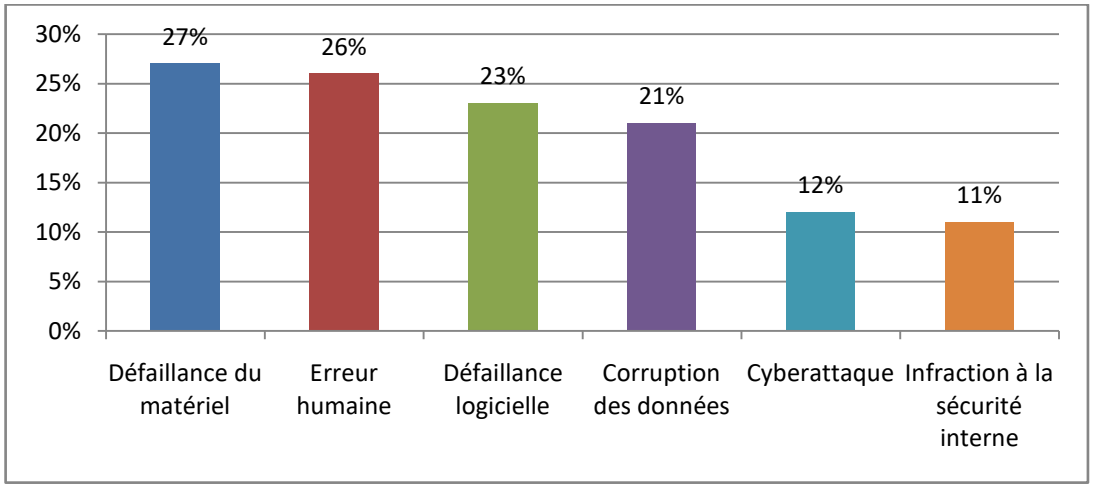


Figure 4 : *Graphique des principales causes de perte de donnés, selon le site DataBarracks.com*

On peut constater que les principales causes de la perte de données sont liées à des problèmes internes à l'entreprise. Ces chiffres suggèrent que les entreprises devraient davantage renforcer leur stratégie de sécurité des données, et mener des examens réguliers de la sécurité des systèmes.

Les pertes de données peuvent avoir des conséquences très coûteuses, et environ 80% des entreprises ont fait faillite l'année après avoir perdu une grande partie de leurs données. Connaitre ces risques devrait inciter les entreprises à mettre en place des systèmes de sécurité d'autant plus efficaces.

De plus, Kaspersky a constaté dans un rapport sur les budgets de sécurité informatique que le coût moyen d'une cyber-attaque ou d'une violation de données serait d'environ 1,2 million de dollars. Cet impact financier est en augmentation depuis 2016.

Les données les plus concernées par ces menaces peuvent être de plusieurs types. Selon le site Quantic.fr, ce sont principalement :

- Des informations personnelles à 22%
- La propriété intellectuelle à 19%
- Des données sensibles de l'entreprise à 12%
- Des informations d'authentification à 11%
- Des données financières d'entreprise à 6%
- Des numéros de compte à 4%

On constate avec ces chiffres que les informations personnelles et la propriété intellectuelle sont des données à risque. La propriété intellectuelle est un atout majeur pour l'entreprise et un moyen efficace pour garder une place concurrentielle. Celle-ci correspond en effet à des données très sensibles et protégées par des droits d'auteur, ce sont par exemple des savoir-faire, des secrets commerciaux, des marques ou des brevets. Ces données nécessitent donc une protection particulièrement efficace. La fuite ou le vol de ces données sont souvent dus à des pirates informatiques ou à des abus de privilèges, par exemple dans le cas où une personne malveillante venait à transmettre les données sensibles volées à des concurrents de l'entreprise.

III. LES CAUSES DU PROBLEME

Comme indiqué plus tôt, les erreurs humaines constituent l'une des causes principales de la perte de données dans une société. La fuite de données peut être intentionnelle, par exemple lorsqu'un collaborateur interne à l'entreprise partage des informations confidentielles, vole des documents ou le matériel informatique de l'entreprise (ordinateurs portables, périphériques de stockage). Ces pertes de données peuvent aussi être accidentelles, dues à une négligence de la part d'un salarié, suite à de fausses manipulations, des suppressions par erreur, l'utilisation de systèmes ou de sites peu sécurisés, ou encore l'oubli d'une session ouverte.

Très souvent, ces fuites de données sont dues à une politique de sécurité qui n'est pas assez contraignante, par exemple des contrôles d'accès qui ne sont pas assez limités ou des solutions pas assez sécurisées.

Le problème est que les employés ont parfois accès à des données qui ne leur sont pas nécessaires, cela est justement un principe contraire à la sécurité des systèmes d'information. La majorité des utilisateurs des données de l'entreprise sont des utilisateurs simples, des employés. Mais il existe aussi des utilisateurs privilégiés qui possèdent des accès plus étendus, comme les administrateurs. Ce type d'utilisateur dispose d'un plus grand champ d'action et peut donc causer plus de risques.

Bien sûr, les attaques cybercriminelles et les actes malveillants représentent aussi un risque pour la sécurité de l'entreprise et peuvent causer des pertes des données.

Egalement, des catastrophes et évènements naturels peuvent représenter un risque pour les données et perturber le fonctionnement de l'entreprise, comme des incendies ou des dégâts des eaux.

IV. LES IMPACTS ET CONSEQUENCES SUR L'ENTREPRISE

La perte de données peut avoir des conséquences économiques importantes pour les entreprises. Si les risques de vol ou de fuite des données n'étaient pas bien anticipés et que des solutions n'étaient pas mises en place, l'activité de l'entreprise pourrait s'arrêter partiellement ou totalement, et engendrer une perte de temps et des dommages financiers importants, voire une faillite dans le pire des cas.

En effet, perdre une partie ou la totalité des informations de l'entreprise peut avoir une incidence grave sur le chiffre d'affaires, et les coûts induits dépendent surtout du type de problème qui a causé la fuite de données, par exemple une erreur humaine, une défaillance du système ou encore le plus couteux, une cyber-attaque. A cela s'ajoute le coût de la mise en place d'un nouveau système de sécurité informatique, de la récupération des données ou de potentielles poursuites judiciaires.

De plus, la perte des données pourrait aussi porter atteinte à l'image de l'entreprise, notamment auprès de la clientèle, par exemple si l'attaque visait les informations personnelles des clients, qui pourraient perdre leur confiance en l'entreprise. Aussi, une fuite de données peut perturber les processus métier et engendrer un retard sur les commandes ou empêcher de fournir un produit aux clients.
Les salariés peuvent eux-aussi se trouver en difficulté face à la perte de leurs données informatiques, voire subir un ralentissement de la productivité, puisqu'ils sont de plus en plus dépendants des données dans leur travail quotidien.

B. DES SOLUTIONS AU PROBLEME RENCONTRE

I. LA MISE EN PLACE D'UNE POLITIQUE DE SECURITE DES DONNEES

La lutte contre la fuite de données dans l'entreprise peut intégrer plusieurs solutions comme la mise en place d'une stratégie de sécurité des données en accord avec les spécificités et les pratiques de l'entreprise, l'application de bonnes pratiques de sécurité, les techniques Data Loss Prevention, la sauvegarde et restauration des données ou encore la gestion des contrôles d'accès.

Dans un premier temps, il est nécessaire de définir une politique de sécurité des données composée d'un ensemble d'orientations en termes de sécurité.

La rédaction d'une politique de sécurité informatique permet de déterminer le périmètre des données les plus sensibles et essentielles à l'activité de l'entreprise, et qui nécessitent donc une protection et une sécurisation efficace. La charte informatique permet notamment de mettre en œuvre les solutions de surveillance des accès et de sensibiliser davantage les utilisateurs.

Des solutions de protection peuvent être mises en place dans l'entreprise en fonction de ses besoins, et du coût de la mise en place de ces solutions par rapport au coût que représenterait une perte de données. Il faut par exemple cibler les services qui ont réellement besoin d'une protection des données et que celle-ci soit adaptée à leur utilisation spécifique.

Avant le déploiement de ces solutions, l'entreprise doit s'assurer que les utilisateurs sont sensibilisés au besoin de protection de l'information et former ces derniers à l'utilisation des nouveaux outils et à leur nécessité. Cette première étape permettra aux collaborateurs d'adopter plus facilement les bonnes pratiques de sécurité et de les responsabiliser en les informant sur la confidentialité et les conséquences encourues par l'entreprise en cas de divulgation de données sensibles.

Les principaux objectifs de la sécurité des données sont les suivants :

- L'intégrité : les données doivent être exactes et complètes et ne pas être altérées (intentionnellement ou accidentellement)
- La confidentialité : l'information est accessible uniquement pour les utilisateurs autorisés (notions de droits et permissions), les données doivent être inaccessibles aux personnes indésirables.
- La disponibilité : elle consiste à garantir l'accès rapide et régulier aux services et aux ressources du système d'information, qui doit être permanant et sans faille.
- L'authentification : Elle assure l'identité de l'utilisateur. Seuls des utilisateurs autorisés ont accès aux ressources de l'entreprise, en prouvant leur identité avec un code d'accès ou un mot de passe par exemple. Cela permet de gérer les droits d'accès aux données.

II. LES SOLUTIONS TECHNIQUES DE PROTECTION DES DONNEES

Plusieurs solutions peuvent être mises en place et appliquées afin d'éviter la perte ou la corruption des données de l'entreprise.

Il existe des outils tels que le chiffrement ou cryptage, qui rendent la donnée illisible pour une personne qui ne possède pas la clé privée permettant d'y accéder. De cette façon, même si les données venaient à être dérobées, leur confidentialité serait assurée.

La sécurité des systèmes d'information comprend une composante importante qui consiste à garantir les droits d'accès aux données de l'entreprise, par exemple grâce à la mise en place d'un système d'authentification et d'un contrôle d'accès. C'est notamment cette technique que je vais aborder dans cette partie.

Le contrôle des droits d'accès consiste à contrôler si un utilisateur possède les droits requis pour accéder à un objet. Les techniques de contrôle d'accès implémentées doivent être conformes à la politique de sécurité de l'entreprise. L'entreprise peut être amenée à contrôler la conformité des règles de contrôle d'accès et la validité des identités, notamment lorsque la sécurité et les systèmes viennent à évoluer. Par exemple, un salarié qui aurait quitté l'entreprise ou changé de poste ne doit plus bénéficier des mêmes droits d'accès.

Dans un premier temps, la CNIL conseille de limiter les accès aux stricts besoins de l'utilisateur, c'est-à-dire ne pas lui attribuer de droits trop importants. Pour cela, la CNIL recommande de définir des profils d'habilitation, en séparant les tâches et domaines de responsabilité. Ces précautions permettent d'éviter d'accorder trop de privilèges à un utilisateur, ou encore de donner des droits d'administrateurs à des personnes qui n'en ont pas besoin par exemple.

Il est aussi nécessaire de supprimer les permissions d'accès des utilisateurs lors de leur départ de l'organisation ou lors d'un changement d'affectation.

Enfin, réaliser des revues annuelles de ces habilitations permettra de modifier les droits de certains utilisateurs qui ne correspondent plus à leurs fonctions, voire d'identifier et de supprimer les comptes non utilisés.

Dans l'ouvrage *Sécurité informatique: pour les DSI, RSSI et* administrateurs *(Chapitre 2 - les différents volets de la protection du SI),* les auteurs expliquent que le propriétaire d'un objet peut attribuer à des utilisateurs des droits d'accès à cet objet. Il existe plusieurs types de droits d'accès :

- Les droits d'accès en consultation (lecture)
- Les droits d'accès en modification (écriture, destruction, création)
- Les droits d'accès en exécution (exécution d'un programme ou d'une commande).

Chaque objet est donc associé à une liste de contrôle d'accès énumérant les utilisateurs autorisés et leurs droits.

L'utilisateur souhaitant obtenir des droits d'accès doit avant tout être authentifié, c'est-à-dire que le système de contrôle d'accès doit vérifier que l'identité de l'utilisateur est authentique (par exemple grâce à un mot de passe). L'authentification permet d'assurer la légitimité d'un accès à une ressource. En effet, les procédures d'identification et d'authentification des utilisateurs sont nécessaires avant toute stratégie de protection.

Il est aussi nécessaire d'appliquer le principe de séparation des privilèges, c'est-à-dire attribuer à chaque utilisateur seulement les privilèges dont il a besoin. Le plus haut niveau de privilège permet à l'administrateur de créer, détruire ou modifier des fichiers, lancer ou interrompre des programmes par exemple… Les utilisateurs ordinaires ont quant à eux des droits d'accès en création, écriture et en destruction à leurs propres données, et des droits d'accès en lecture pour les données partagées.

Afin d'assurer une bonne administration de la sécurité, les systèmes doivent garder trace de toutes les actions significatives et enregistrer l'identité des auteurs de ces évènements.

L'identité de l'utilisateur détermine ses privilèges et ses droits d'accès à telles ou telles données. Cependant, pour que cette identité soit correctement administrée et qu'elle ne soit pas usurpée, son authenticité doit être vérifiée.

Les utilisateurs accèdent à diverses applications fonctionnant sur des systèmes différents, et doivent souvent saisir leurs paramètres de connexion (identité) à plusieurs reprises. C'est dans ce contexte qu'un service d'authentification unique ou Single Sign-On (SSO) est mis en place. Le SSO est un système d'identification centralisé qui permet d'utiliser un seul et même login pour toutes les applications, et donc à l'utilisateur de ne se loguer qu'une seule fois. L'objectif du SSO est notamment d'avoir un référentiel centralisé des identités et mots de passe auquel les applications s'adressent pour vérifier l'identité d'un utilisateur.

Ce principe d'authentification unique a plusieurs avantages pour l'entreprise. Il permet notamment d'offrir un accès simplifié aux applications et donc un certain confort aux employés. Il limite aussi les risques au niveau de la sécurité, car il n'est plus nécessaire de retenir plusieurs mots de passe mais un seul. Aussi, le SSO permet de gérer et de limiter l'accès des utilisateurs au réseau, en une seule fois, c'est-à-dire qu'un utilisateur ne pourra accéder qu'aux applications auxquelles il a un droit d'accès.

Cependant, ce service peut aussi avoir un inconvénient. En effet, il peut être risqué de pouvoir se connecter à plusieurs applications à la fois avec un même identifiant, si celui-ci venait à être corrompu. Pour pallier ce problème, il est nécessaire de mettre en place des mots de passe forts voire une authentification à deux facteurs.

PARTIE 3

-

RESULTATS OBTENUS

A. PLAN D'ACTION ET PRATIQUES PROPOSEES

La mise en place d'une politique de sécurité des données efficace consiste à mettre en œuvre un plan d'action. Il a pour objectif de protéger la société et ses données informatiques en anticipant les risques qui pourraient survenir, comme une panne de réseau, une menace extérieure ou intérieure.

- La première étape consiste à préparer un plan de sécurité des données en amont : Il faut évaluer les risques et menaces, leurs conséquences et les vulnérabilités de l'entreprise concernant son système d'information et ses données. Il convient aussi de prévoir les mesures à mettre en place en cas de menace ou d'attaque et les bonnes pratiques utiles à la sécurisation des données.

- Il est ensuite nécessaire de définir le périmètre sensible, c'est-à-dire quelles données sont particulièrement essentielles ou confidentielles et nécessitent une protection renforcée. Un audit des données peut être mené dans l'entreprise et permettra de définir des catégories de données et le niveau de protection qu'elles nécessitent.

- Une fois que ces objectifs de sécurité sont fixés, l'entreprise doit choisir les moyens qu'elle mettra en place pour sécuriser ses données, comme l'installation d'un pare-feu, d'un contrôle d'accès, de serveur de sauvegarde, etc. Ces mesures de protection seront adoptées en fonction des coûts que l'entreprise souhaite engager pour garantir la sécurité de ses données.

- Enfin, il faut maintenir une communication efficace avec les services et les salariés de l'entreprise vis-à-vis des règles de sécurité informatique et diffuser aux collaborateurs les procédures et les réactions à adopter en cas de problème. Ces règles peuvent concerner l'utilisation des logiciels, de sites internet, le matériel informatique, etc.

B. MISE EN PRATIQUE DES SOLUTIONS

Limagrain a en effet mis en pratique ces solutions. L'entreprise a par exemple identifié et évalué les principaux risques liés au système d'information ; ils concernent la disponibilité, l'intégrité et la confidentialité des données. Ces risques pourraient notamment provenir d'une défaillance du système d'information ou des infrastructures informatiques (data centers, réseaux) mais aussi de la perte de données, qu'elle soit accidentelle ou intentionnelle. Ces menaces ont été identifiées comme pouvant avoir un impact important sur les activités ainsi que les résultats de Limagrain.

Pour prévenir ces risques et protéger ses données, le groupe applique une gestion du risque. Par exemple, les données considérées comme les plus sensibles sont hébergées dans des data centers hautement sécurisés chez des prestataires reconnus et l'entreprise s'assure de la consolidation des infrastructures informatiques.

Aussi, Limagrain IT communique régulièrement sur les risques liés à la sécurité des données auprès de ses salariés et collaborateurs, notamment à travers des mails, des réunions sur le sujet, ou des rubriques sur l'intranet de ses différentes filiales (*voir Annexe 3 : Articles de la rubrique sécurité sur l'intranet de HM.Clause*).

C. BILAN SUR LE SUIVI DU GANTT

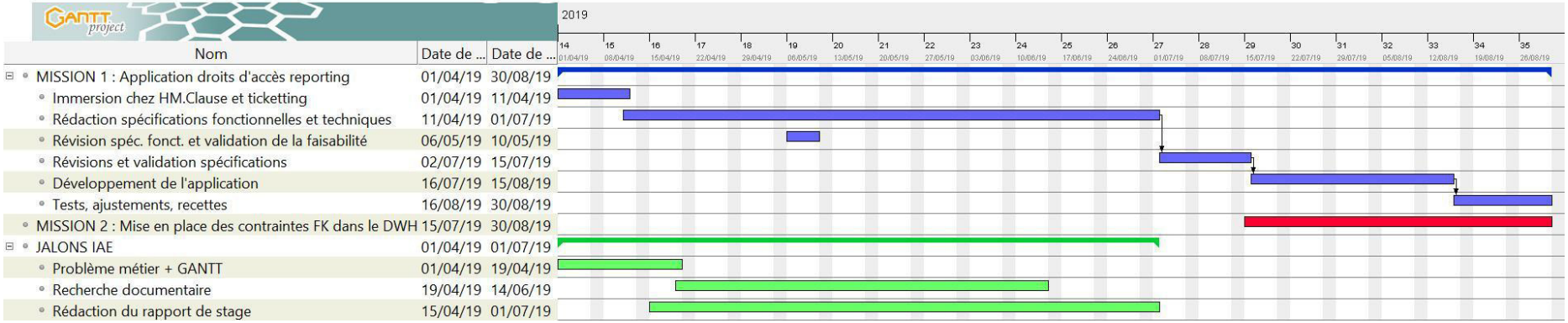


Figure 5 : *Diagramme de Gantt rectifié*

Certaines tâches indiquées dans le diagramme de Gantt initial ont évolué ou ont été reportées. J'ai donc effectué un nouveau diagramme de Gantt.

La rédaction des spécifications fonctionnelles et techniques a été menée du 11 avril au 01 juillet et n'a pas terminé le 31 mai comme indiqué sur le diagramme de Gantt initial. En effet, cette tâche a demandé plus de temps que prévu. Il était difficile d'évaluer le temps que prendrait la réalisation des spécifications de l'application web au début du projet car de nombreux ajustements relatifs aux fonctionnalités ont été nécessaires. Nous avons d'ailleurs regroupé les spécifications de l'application en trois lots, afin d'en optimiser le développement et de s'assurer qu'au moins le premier lot soit opérationnel avant mon départ.

Le développement de l'application, que j'avais planifié début-juin dans le diagramme de Gantt, démarrera en réalité à la mi-juillet. Cette date a été fixée en fonction des disponibilités du développeur qui se consacrera au développement de l'application. La phase de recettage pourra démarrer lorsque le développement de l'application sera terminé.

De plus, nous avons assisté à plusieurs réunions de révisions des spécifications avec le Lead Developer courant mai mais aussi fin juin. Lors de ces dates, nous avons fait valider la faisabilité des fonctions de l'application.

Enfin, je n'ai pas encore abordé la deuxième mission concernant la mise en place de contraintes Foreign Keys dans le Data Warehouse car la mission principale nous a demandé beaucoup de temps. Je réaliserai sans doute cette mission pendant le développement de l'application, période durant laquelle je resterai aussi à disposition pour interagir avec le développeur et répondre à ses questions concernant les spécifications de l'application.

CONCLUSION

Souhaitant m'orienter vers un Master 2 Parcours Intelligence des données l'année prochaine, je me suis dirigée vers un stage en Business Intelligence. La mission qui m'a été proposée à Limagrain IT correspondait parfaitement à mon projet d'étude, mêlant à la fois une dimension technique et fonctionnelle.

Au cours de ce stage de cinq mois, j'ai eu l'occasion de travailler en collaboration avec Antoine Le Tourneurs, au sein de l'équipe Data Analytics de Limagrain IT. J'ai eu l'opportunité de participer à une mission consistant à concevoir une application web pour la gestion des droits d'accès des utilisateurs reporting de trois Business Units potagères de Limagrain. J'ai pu mettre en œuvre des compétences acquises durant ma formation, mais surtout en acquérir de nouvelles, en contribuant à l'évolution de ce projet, de l'analyse des besoins jusqu'au recettage de l'applicatif. J'ai notamment utilisé un nouveau système de gestion de bases de données : Microsoft SQL Server Management Studio et sa suite de solutions : SQL Server Analysis Services (SSAS), SQL Server Integration Services (SSIS) et SQL Server Reporting Services (SSRS). J'ai aussi conçu l'interface d'une application web, grâce aux Userform d'Excel et au langage Visual Basic (Excel VBA).

A ce stade de mon stage, le projet n'en est qu'à l'étape des spécifications fonctionnelles et techniques et le développement de l'application web va bientôt débuter. Cependant, j'espère avoir l'occasion de tester l'application web avant mon départ, une fois son développement avancé.

Cette expérience pratique du monde professionnel a été pour moi une opportunité de découvrir le métier. Cela m'a permis d'observer le fonctionnement du système d'information et de la stratégie data d'un groupe international mais aussi d'étoffer mon expérience du travail en entreprise, en développant mes savoir-faire et savoir-être.

La rédaction de ce rapport m'a aussi permis d'en apprendre davantage sur la sécurité des données d'une entreprise, notamment à travers les diverses recherches documentaires que j'ai pu effectuer.

Enfin, je pense que cette expérience me permettra d'aborder ma deuxième année de Master avec plus d'assurance et un bagage de connaissances et de capacités plus solide.

BIBLIOGRAPHIE

- Souillé, A., Kokos, A., Billois, G., Wolfhugel, C., Bloch, L., Anzala-Yamajako, A., & Debize, T. (2016). *Sécurité informatique: pour les DSI, RSSI et administrateurs*. Editions Eyrolles.

- Lathe, M. E., *Gestion de droits d'accès dans des réseaux informatiques.* Mémoire de maitrise. *Université Laval, 2016.*

- *Réfalo, P. L. (2012). La sécurité numérique dans l'entreprise: L'effet papillon du hacker*. Editions Eyrolles.

SITOGRAPHIE

Sites WEB

- Limagrain. *Limagrain est un groupe coopératif créé et dirigé par des agriculteurs.* Disponible sur : https://www.limagrain.com/fr (consulté le 15 avril 2019).
- HM.Clause. *Site d'HM.Clause.* Disponible sur : https://hmclause.com/fr/ (consulté le 15 avril 2019)
- Vilmorin&Cie. *Les activités semences de Limagrain.* Disponible sur : https://www.vilmorincie.com/fr/ (consulté le 01 mai 2019)
- Vilmorin&Cie. *Document de référence 2017 – 2018 incluant le rapport financier annuel.* Disponible sur : https://www.vilmorincie.com/flipbook/20181030/ (consulté le 01 mai 2019)
- CommandersAct. *Les enjeux de la sécurité de la donnée dans une entreprise data-driven.* Disponible sur : https://www.commandersact.com/fr/enjeux-securite-donnee-entreprise-data-driven/ (consulté le 15 mai 2019)
- SUPINFO. Christian Tedajio Suki. *Les fondements de la Business Intelligence.* Disponible sur : https://www.supinfo.com/articles/single/6721-fondements-business-intelligence (consulté le 15 mai 2019)
- ITespresso. *Six étapes pour empêcher la perte ou le vol de données.* Disponible sur : https://www.itespresso.fr/avis-expert/six-etapes-pour-empecher-la-perte-ou-le-vol-de-donnees (consulté le 01 juin 2019)
- Present. *5 étapes pour implanter les meilleures pratiques de gestion des daccès aux données.* Disponible sur : https://blog.present.ca/fr/5-etapes-pour-implanter-les-meilleures-pratiques-de-gestion-des-acces-aux-donnees (consulté le 01 juin 2019)
- DataBarracks. *Disaster recovery and Business Continuity.* Disponible sur : https://datahealthcheck.databarracks.com/2018/dr.html (consulté le 15 juin 2019)
- Quantic. *78% des fuites proviennent de personnes internes à l'entreprise*. Disponible sur : https://www.quantic.fr/conseil/actualites (consulté le 15 juin 2019)
- Kasperky. *Rapport : Faire évoluer les budgets de sécurité informatique pour protéger les initiatives de transformation numérique.* Disponible sur : https://go.kaspersky.com/IT-securiy-economics-2018.html (consulté le 15 juin 2019)
- Data-IT. *Les risques d'une perte de données.* Disponible sur : http://www.data-it.fr/les-risques-dune-perte-de-donnees-informatiques/ (consulté le 15 juin 2019)

- ITrust. *Fuite de données : quel impact pour les entreprises ?*. Disponible sur : https://www.itrust.fr/fuite-de-donnees-quel-impact-pour-les-entreprises/ (consulté le 01 juin 2019)

- CNIL. *Sécurité : Gérer les habilitations*. Disponible sur : https://www.cnil.fr/fr/securite-gerer-les-habilitations (consulté le 15 juin 2019)

- Microsoft. *5 conseils pour mettre en place votre politique de sécurité informatique.* Disponible sur : https://experiences.microsoft.fr/business/confiance-numerique-business/politique-de-securite-informatique/ (consulté le 15 juin 2019)

Articles en ligne

- Le Libellio d'Aegis. *La stratégie de* Limagrain. Vol. 9, n° 3 – Automne 2013 Dossier AIMS 2013 – pp. 35-37. Disponible sur : http://lelibellio.com/la-strategie-de-limagrain/ (consulté le 30 mai 2019)

- Inf'OGM. *Semences : définitions, lois et marché mondial.* 2017. Disponible sur : https://www.infogm.org/faq-semences-definitions-lois-marche-mondial#nb13 (consulté le 01 mai 2019)

- WillAgri. *Classement mondial des semenciers.* Disponible sur : http://www.willagri.com/2018/11/06/classement-mondial-des-semenciers/ (consulté le 30 mai 2019)

- Inf'OGM. Frédéric Prat. *Ressemer et vendre ses semences : un droit à (re)conquérir.* 2015. Disponible sur : https://www.infogm.org/5864-ressemer-et-vendre-ses-semences-un-droit-a-reconquerir (consulté le 30 mai 2019)

- Challenges. Ontrack. *Les enjeux de la récupération de données pour les sociétés. 2019.* Disponible sur : https://www.challenges.fr/high-tech/les-enjeux-de-la-recuperation-de-donnees-pour-les-societes_644631 (consulté le 15 juin 2019)

- Informanews. Jerôme Dajoux*. La perte de données, une cause importante de faillite des entreprises*. 2017. Disponible sur : https://www.informanews.net/perte-de-donnees-cause-faillite/ (consulté le 15 juin 2019)

- Siècle Digital. Pierre-Louis Lussan. *Protéger la propriété intellectuelle des menaces internes.* Disponible sur : https://siecledigital.fr/2019/03/13/proteger-la-propriete-intellectuelle-des-menaces-internes/ (consulté le 15 juin 2019)

- IT for Business. Business intelligence et sécurité : un grand pouvoir implique de grandes responsabilités. 2017. Disponible sur : https://www.itforbusiness.fr/business-intelligence-et-securite-un-grand-pouvoir-implique-de-grandes-responsabilites-11408 (consulté le 10 juin 2019)

TABLES DES FIGURES

FIGURE 1 : *SCHEMA DES DIFFERENTES FILIALES DE LIMAGRAIN (SOURCE : LIMAGRAIN.COM)* 9

FIGURE 2 : *REPRESENTATION DU MODELE DES 5 FORCES DE PORTER POUR LIMAGRAIN* 11

FIGURE 3 : *DIAGRAMME DE GANTT INITIAL* 18

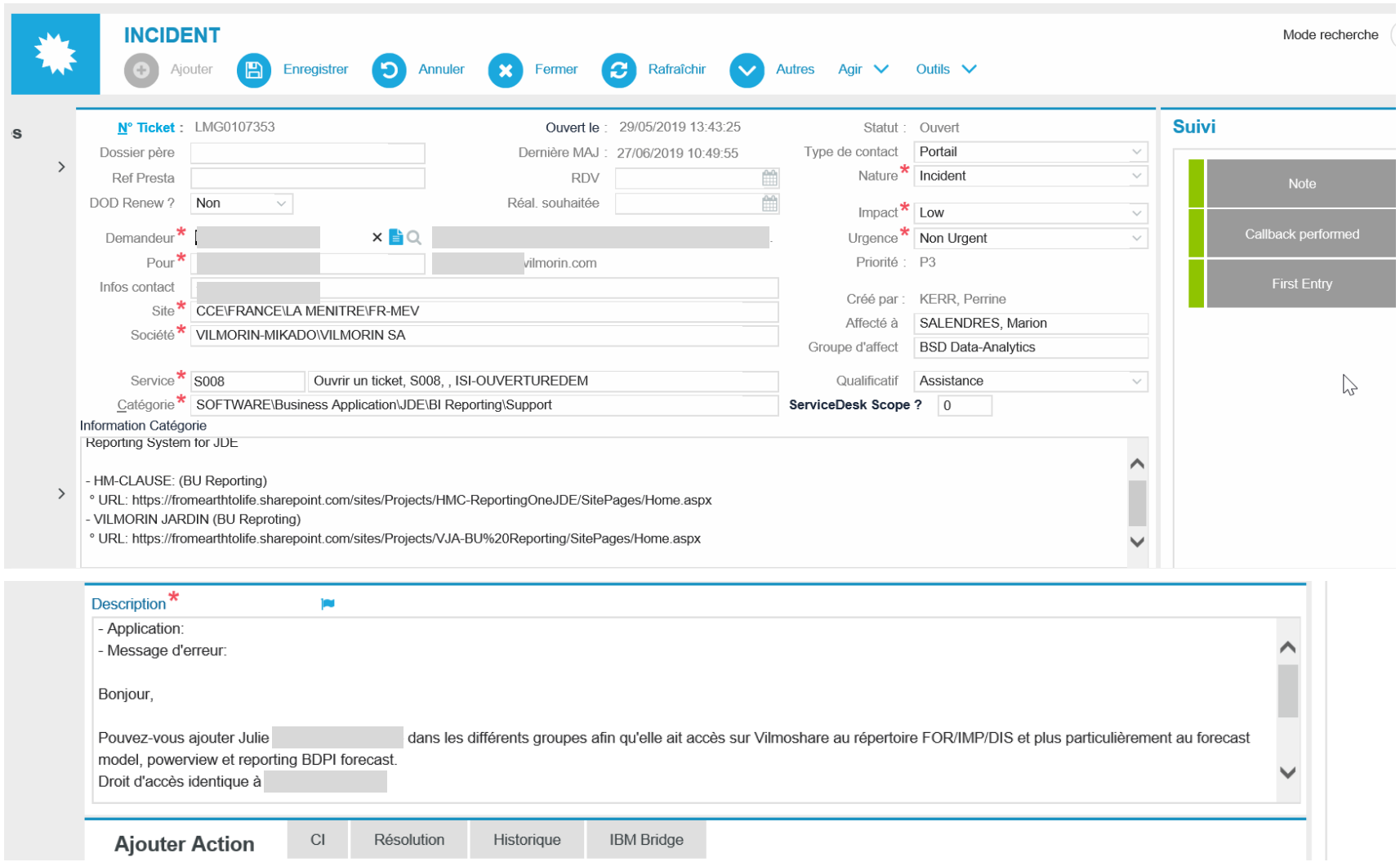
FIGURE 4 : *GRAPHIQUE DES PRINCIPALES CAUSES DE PERTE DE DONNES, SELON LE SITE DATABARRACKS.COM* 21

FIGURE 5 : *DIAGRAMME DE GANTT RECTIFIE* 29

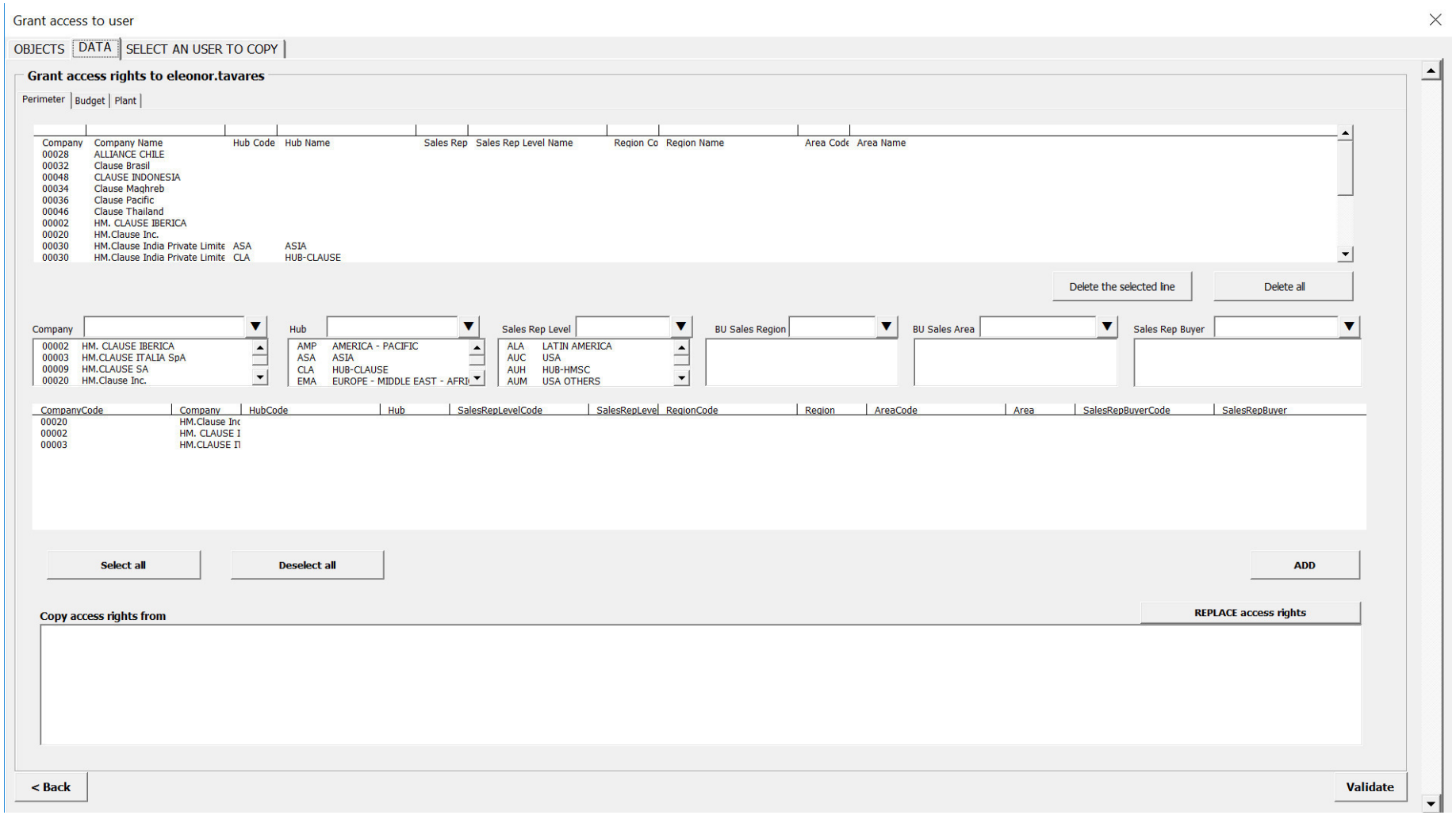
TABLES DES ANNEXES

ANNEXE 1 : EXEMPLE D'UN TICKET DE DEMANDE D'ACCES 36
ANNEXE 2 : MAQUETTE DE L'UNE DES PAGES DE L'APPLICATION DE GESTION DES DROITS D'ACCES 37
ANNEXE 3 : ARTICLES DE LA RUBRIQUE SECURITE SUR L'INTRANET DE HM.CLAUSE..... 38

ANNEXE 1 : EXEMPLE D'UN TICKET DE DEMANDE D'ACCES



ANNEXE 2 : MAQUETTE DE L'UNE DES PAGES DE L'APPLICATION DE GESTION DES DROITS D'ACCES



ANNEXE 3 : ARTICLES DE LA RUBRIQUE SECURITE SUR L'INTRANET DE HM.CLAUSE