REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ **S**AAD **D**AHLAB **B**LIDA 1

Faculté des Sciences
Département : Informatique

Mémoire de Fin d'Etude pour l'Obtention du Diplôme de Master en Informatique

OPTION : Sécurité des Systèmes d'Information

Présenté par :
BENABDELOUAHEB Lyna Fairouz
TORKI Hadjer

Thème:

Mise en place d'une PSSI pour la société HUBBARD ALGERIE

Organisme d'accueil : la société HUBBARD ALGERIE.

Mme BOUSTIA	**Présidente**
Mme AROUSSI	**Examinatrice**
Mme ARKAM Meriem	**Promotrice**
MRE N.TEKFA	**Encadreur**

Promotion : 2019-2020

Remerciements

En tout premier lieu, nous remercions « Dieu »le tout puissant qui nous a donné la sagesse, santé et force pour faire ce modeste travail.

C'est avec un grand plaisir que nous expriment nos profondes gratitudes et nos sincères Remerciements à notre promotrice : Mme ARKAM Meriem. Nous lui exprime nos reconnaissances pour ses précieux conseils qui nous ont permis de bénéficier de son expérience et d'acquérir de nombreuses connaissances tout le long de ce travail.

Nous tenant à exprimer notre gratitude à Mme BOUSTIA, enseignant chercheur et responsable de notre spécialité, qui nous a encadrés efficacement tout au long de notre cycle master.

Nous remercions aussi, le Groupe de la société HUBBARD ALGERIE à sa tête monsieur Nadjib TEKFA, qui nous ont bien accueille et qui ont tous fait pour que notre séjour dans leur établissement soit agréable.

Également nos sincères remerciements Aux membres de jury :

- Mme N.BOUSTIA

-Mme S.AROUSSI

Qui nous ont fait l'honneur d'apprécier et de juger ce travail.

Dédicaces

Que ce travail témoigne de mes respects à :

Mes parents

Dédié à l'âme de mon défunt père, que Dieu ait pitié de lui, et à ma chère mère qui m'ont appris à tenir la plume et à écrire ces mots, je m'incline devant vous tous mes respects et appréciation, je prie le bon dieu de la bénir, de veiller sur elle, en espérant qu'ils seront toujours fiers de moi.

A mes frères et sœurs

Houssem, Sabrina, khawla, Elkhansa,badiss,Rayane,Younes et la petite Chams et ma belle-sœur Mouna

Je prie dieu de vous bénir une vie pleine d'amour, succès et du bonheur, J'espère que chacun de vous réussira dans son domaine, que dieu vous protège, je suis tellement fière de vous**.**

A mon mari Haroun

Tous les mots ne suffisent pas pour exprimer à quel point je suis reconnaissante, et merci de m'avoir supporté dans mes difficiles moments, d'être à mes côtés, merci d'être dans ma vie.

A ma belle famille

Je remercie infiniment ma belle-mère et mon deuxième papa Abdelkader pour leurs courages, soutien et énergie qui m'ont aidé à poursuivre mon travail.
Mon beau-frère abdelbasset et sa petite famille, Et mes belles sœurs.

A mon fils mon âme bidjad abdelkarim
A mon ange Ayane et ma princesse Elia

A mes proches amies Lamiss, Lynda et Dina
Ma gratitude et mes sincères remerciements pour leur soutien, leurs encouragements et les bons moments qu'on a partagé.

Hadjer

Dédicaces

Au nom du dieu le clément et le miséricordieux louange à ALLAH le tout puissant.

Je dédie ce modeste travail en signe de respect, reconnaissance et de remerciement :

A mes chers parents

Ma maman : qui a œuvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour toute son assistance et sa présence dans ma vie, reçois à travers ce travail aussi modeste soit-il, l'expression de mes sentiments et de mon éternelle gratitude.

Mon papa : qui peut être fier et trouver ici le résultat de longues années de sacrifices et de privations pour m'aider à avancer dans la vie. Puisse Dieu faire en sorte que ce travail porte son fruit ; Merci pour les valeurs nobles, l'éducation et le soutient permanent venu de toi.

A mes chers frères et sœurs

Brahim, Aissa, Ismail, Naima et Amel qui n'ont cessé d'être pour moi des exemples de persévérance, de courage et de générosité.

A mon professeur *monsieur* Amior mahammed taher**,** merci pour ton aide précieuse dans ce travail.

Et enfin à tous ceux et celles qui sont chers pour moi.

LYNA FAIROUZ

Résumé

Les systèmes d'informations sont des outils de partage et d'échange incontournables aux bénéfices des employés, des professionnels.il est donc crucial de garantir leur sécurité, leur disponibilité et leur confidentialité pour maintenir de la confiance.

La politique de sécurité ne se limite pas à la protection contre la perte, l'indisponibilité ou la divulgation de données personnelles ou administratives, elle permet de créer un espace de confiance entre les professionnels, et fournir un ensemble de contrôles pour protéger les données contre de telles menaces.

Dans le cadre de notre projet de mise en place d'une politique de sécurité d'un système d'information (PSSI) dériver des exigences de sécurité, nous avons réussie à aboutir à la phase la plus essentiel, celle du document PSSI du système actuel de l'entreprise, en analysant une politique de mesures de sécurité, de lignes directrices pour leur réalisation, d'une stratégie globale de gestion de la sécurité et de la mise en œuvre des politiques sur les principaux mécanismes de sécurité.

Mots clés

Mesures de sécurité, menaces, exigences de sécurité.

Abstract

Information systems are essential Tools for sharing and exchange for the benefit of employees and professionals, so it is imperative to ensure their security, availability, and confidentiality in order to maintain trust.

The security policy is not limited to protection from loss, lack of availability or disclosure of personal or administrative data, it allows creating space of confidence between professionals, and providing a set of controls to protect data from such threats derived from security requirements.

As part of our project to prepare an information system security policy, we have succeeded in completing the most important phase, which is the document phase of the company's current system, by analyzing the security measures policy, the guidelines for its achievement, the overall security management strategy and implementing the policies on the main security mechanisms.

Keywords

Security measures, threats, security requirements.

ملخص

تعد أنظمة المعلومات أدوات أساسية للمشاركة والتبادل لصالح الموظفين والمهنيين، لذلك من الضروري ضمان أمنها وتوافرها وسريتها من أجل الحفاظ على الثقة.

لا تقتصر السياسة الأمنية على الحماية من الضياع أو عدم توفر أو الكشف عن البيانات الشخصية أو الإدارية، فهي تسمح بإنشاء مساحة ثقة بين المهنيين، وتوفير مجموعة من الضوابط لحماية البيانات من مثل هذه التهديدات المستمدة من متطلبات الأمان.

كجزء من مشروعنا لإعداد سياسة أمن نظام المعلومات نجحنا في إكمال المرحلة الأكثر أهمية، وهي مرحلة وثيقة الخاصة بالنظام الحالي للشركة، من خلال تحليل سياسة التدابير الأمنية، والمبادئ التوجيهية لتحقيقها، واستراتيجية إدارة الأمن الشاملة وتنفيذ السياسات على آليات الأمن الرئيسية.

كلمات محورية

التدابير الأمنية، التهديدات متطلبات الامن.

Tables des Matières

Listes des figures

Liste des tableaux

Liste des acronymes

Acronymes	Significations
BSI	British Standards Institution
DSI	Direction des systèmes d'information
FSSI	les fonctionnaires de sécurité des systèmes d'information
ISO/IEC	International organisation for standardisation/ International électrotechnical Commission
GP	Grands parents des poussins
PSSI	Politique de sécurité des systèmes d'information
RSSI	responsables de la sécurité des systèmes d'information
SI	Système d'information
SMSI	Système de management de sécurité d'information

Introduction générale

Les systèmes d'information font désormais partie intégrante du fonctionnement des administrations publiques, de l'activité des entreprises et du mode de vie des citoyens.

La communication, qui occupe une place de choix dans nos sociétés contemporaines à la recherche d'une productivité sans cesse croissante, nécessite la maitrise de l'information économique, sociale et culturelle et surtout avec les nouvelles technologies qui sont un outil de partage et d'échange de l'information qui est crucial de garantir leur sécurité, disponibilité, intégrité et leur confidentialité.

La protection des ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données informatisées contre les éventuelles attaques malveillantes, doit être assurée par un système de sécurité appelée « la cyber sécurité », qu'est également appelée sécurité des systèmes d'information.

Pour assurer cette sécurité, on peut utiliser des services, des mécanismes ou des procédures que l'on nomme de façon générale, des solutions ou des mesures de sécurité. Les mesures de sécurité consistent un ensemble de mécanismes, de procédures et d'autres moyens qui sont mises en œuvre, afin de réduire les risques auxquels les systèmes sont exposé.il est important de dire que les mesures de sécurité ne devraient pas être mise en place tant que l'on n'aura pas défini une politique complète en matière de sécurité de système.

En effet, même si les gouvernements dépensent chaque année beaucoup d'argent contre les attaques malveillantes, la croissance de celle-ci continue à un rythme ascendant. Il est donc recommandé d'utiliser un système de surveillance permanent.

L'installation d'un système de sécurité informatique permet d'assurer la progression et le développement de l'entreprise, et de distribuer une image positive. Ainsi la mise en place d'une politique de sécurité d'un système d'information est nécessaire pour reflète la vision stratégique de la direction de l'organisme en matière de sécurité des systèmes d'information (SSI).

Le but de ce travail s'inscrit dans ce contexte (la sécurité d'un système d'information) où l'objectif de notre travail est la mise en place d'une politique de sécurité de système d'information<<PSSI>>pour l'entreprise HUBBARD ALGERIE ; La société qu'est une

entreprise avicole spécialisée dans la production de poussins reproducteurs chair. Son but est de rendre l'Algérie moins dépendante des importations et de prévenir les embargos sanitaires ou autres

Le mémoire est organisé en trois parties :

Dans le premier chapitre intitulé <<la sécurité d'information>> nous abordons la sécurité de l'information en générale, les besoins de sécurité et objectifs de la sécurité de l'information ainsi que les terminologies relatives à la sécurité informatique nous parlons aussi à l'historique des normes de sécurité d'information précisément la norme 27002, son objectif et sa structure et ses avantages.

Dans le deuxième chapitre <<la politique de sécurité>>nous allons définir la politique de sécurité du système d'information, son contenue, son concept, son domaine d'application ainsi que son rôle et sa place dans l'entreprise. Puis nous allons expliquer pourquoi on a choisi une PSSI, nous parlèrent aussi de ces bénéfices. Nous terminerons par la démarche pour mettre en place une PSSI.

Dans le troisième chapitre nommé <<études de la politique>>, nous effectuant un questionnaire pour avoir une idée préalable de structuration générale de l'entreprise de plus nous expliquèrent pourquoi nous avant choisi de mettre en place une PSSI, puis nous allons présenter la société HUBBARD ALGERIE une présentation qui inclus une présentation générale de la société ainsi qu'une étude détaillée de ses postes de travail et des documents utilisées. Nous allons terminer le chapitre avec l'explication des objectifs de notre PSSI.

Dans le quatrième chapitre intitulé <<la mise en place de la politique de sécurité du système d'information>> en présente la politique appliqué dans l'entreprise.

Dans le cinquième chapitre intitulé << conception et réalisation du site web en respectant la politique appliquée>>, nous effectuant les diagrammes nécessaires à la modélisation du site, en utilisant le langage UML avec une présentation du site et les tables utilisées dans la base de données, aussi l'implémentation de notre site WEB qu'on a proposé à l'entreprise pour contrôler la transmission de données d'une maniéré sécurisée.

Nous terminons ce mémoire par une conclusion générale.

Chapitre 01 : La Sécurité d'Information

1. Introduction

Les systèmes d'informations aujourd'hui joue un rôle important au sein d'une entreprise, il est même indispensable à leur bon fonctionnement cela nécessite la sécurité de l'information dans l'entreprise. De ce fait nous toucherons dans ce chapitre la sécurité de l'information en générale, les besoins, les objectifs et les formes de la sécurité aussi les terminologies relatives à la sécurité.

2. Sécurité de l'information

La sécurité de l'information est un ensemble de stratégies de gestion des processus et politiques visant à protéger, détecter, recenser et contrer les menaces ciblant les informations numériques ou non [1] .

2.1 Besoins de sécurité

La sécurité du Système d'Information repose sur les critères suivants [2] :

•Confidentialité : l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisés. En clair, cela signifie que l'information n'est consultable que par ceux qui ont le droit d'y accéder.

• Intégrité : le caractère correct et complet des actifs doit être préservé. Cela signifie que l'information ne peut être modifiée que par ceux qui en ont le droit.

•Disponibilité : l'information doit être rendue accessible et utilisable sur demande par une entité autorisée.

Les besoins de sécurité s'appliquent aussi bien aux ressources du système d'information

(Postes informatiques, réseaux, applications...) qu'aux données traitées par ces ressources, donc il est nécessaire d'inventorier et de classifier ces données (défense, scientifique, gestion,

Nominative, stratégique...) afin d'en identifier le degré de sensibilité et donc le besoin de

Protection nécessaire.

2.2 Objectif de la sécurité de l'information

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger [3].

La sécurité de l'information a pour objectif de permettre la continuité des systèmes d'information, de sensibiliser ses employés et d'accroitre leur niveau d'adaptation à leurs Besoins de sécurité, de permettre la conformité avec les tierce parties et de mettre en œuvre de manière active les contrôles de sécurité technique actuelle afin de protéger la réputation, la fiabilité, les biens de l'information et afin d'avoir une continuité des activités avec le moindre d'interruption possible [3].

2.3 Terminologie relative à la sécurité informatique

Certains termes ont la nécessité d'être définit car nous allons les rencontrer souvent Dans notre projet :

Charte informatique : est un document de recommandations concernant la bonne utilisation des technologies informatiques, et qui est destiné aux employés de l'entreprise [4].

Système informatique : Le terme de système informatique recouvre à la fois la mise en œuvre et la gestion des composants de l'Infrastructure Technique *(« hardware »)* et l'ensemble des Logiciels qui guident et synchronisent leurs interactions *(« software »).* [5].

Système d'information : Il s'agit de l'ensemble des outils et moyens pour collecter, stocker, traiter et traiter l'information [6].

Sécurité informatique : est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information et pour assurer le bon fonctionnement du système et une capacité à protéger les objets en respectant la confidentialité, l'intégrité et la disponibilité de service.

Les menaces : ce sont des adversaires déterminés capables de monter une Attaque exploitant une vulnérabilité.

Les mesures de sécurité : ce sont les procédures ou techniques Permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.

Les vulnérabilités : ce sont les faiblesses et les failles de sécurité dans un ou plusieurs systèmes.

3. Les formes de la sécurité

Aujourd'hui, contrôler l'accès aux ordinateurs et au réseau est indispensable pour protéger les données personnelles et professionnelles contre les attaques internes ou externes. Donc il est nécessaire de diviser la sécurité en différents formes : Sécurité matérielle, Sécurité de l'information et sécurité organisationnelle [7].

3.1 Sécurité matérielle

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, d'où la sécurité matérielle protège les objets des vulnérabilités présentes. Elle est divisée en deux parties :

3.1.1 Sécurité physique

La sécurité physique consiste en l'usage de barrières, alarmes, serrures et autres contrôles physiques permettant de conditionner l'accès physique aux locaux, aux ordinateurs et aux équipements. Ces mesures sont nécessaires pour protéger les ordinateurs, leur contenu et les autres ressources matérielles contre l'espionnage, le vol et la destruction accidentelle ou intentionnelle [7].

3.1.2 Sécurité logique

La sécurité logique fait référence à la réalisation des mécanismes de sécurité par logiciel, elle repose sur la mise en œuvre d'un système de contrôle d'accès logique s'appuyant sur un service d'authentification, d'identification et d'autorisation, et elle repose également sur : les dispositifs mis en place pour garantir la confidentialité dont la cryptographie, une gestion efficace des mots de passe et des procédures d'authentification, des mesures antivirus et de sauvegarde des informations sensibles [7].

3.2 Sécurité de l'information

La sécurité de l'information est un ensemble de pratiques visant à protéger des données des vulnérabilités présentes soit dans le matériel ou logiciel. Elle est divisée en :

3.2.1 Sécurité des ordinateurs (sécurité des machines)

Concerne la protection des objets contre les attaques qui font usage de vulnérabilité. C'est la sécurité contre les accidents du travail liés aux machines qui se produisent notamment à cause de l'accès aux pièces en mouvement d'une machine en fonction [7].

3.2.2 Sécurité de communication

C'est la protection de l'information entre machine durant son transport des attaques actives ou passive. Par exemple : modifier ou détruire l'information … [7].

3.3 Sécurité organisationnelle

La sécurité organisationnelle est la protection des objets contre les vulnérabilités causées par les utilisateurs et les menaces contre l'organisation de la sécurité, devisée en :

3.3.1 Sécurité des utilisateurs

La sécurité des utilisateurs est la protection des objets contre les attaques des utilisateurs légitimes qui ont accès aux objets de système. Aussi si un utilisateur envoi un courrier confidentiel a la mauvaise personne [7].

3.3.2 Sécurité des opérations

La sécurité des opérations régularise de façon que toutes les autres formes de sécurité doivent être implémentées en renforcer les règles de sécurité établies dans la politique de sécurité, elle concerne aussi les vulnérabilités présentes dans l'organisation qui maintient la sécurité du système [7].

4 la norme

Une norme c'est un document qui fournit des exigences, des spécifications, des directives ou caractéristiques.

Les normes garantissent que les produits et services sont surs, fiables et de bonne qualité. Elles sont des outils stratégiques qui diminuent les couts en réduisant les déchets erreurs.

4.1 Historique des normes de sécurité d'information

Au cours des vingt dernières années les normes liées à la sécurité de l'information ont évolué ou ont été remplacées. Ces changements rendent difficile une bonne compréhension du sujet [8].

Un rappel historique de l'évolution de ces normes permet de clarifier la situation normative en matière de sécurité de l'information. Au début des années 90, de grandes entreprises britanniques se concertent pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Le résultat de cette collaboration servit de référence en la matière pour d'autres entreprises qui souhaitaient mettre en œuvre ces mesures.
En 1991, un projet de « best practices » code de bonnes pratiques, préconise la formalisation d'une politique de sécurité de l'information. Cette politique de sécurité doit intégrer au minimum huit points « stratégique et opérationnel 6» ainsi qu'une mise à jour régulière de la politique.

En 1995, le BSI publie la norme BS7799 qui intègre dix chapitres réunissant plus de 100 mesures détaillées de sécurité de l'information, potentiellement applicables selon l'organisme concerné.

En 1998, la norme BS7799 change de numérotation et devient la norme BS7799-1. Elle est complétée par la norme BS7799-2 qui précise les exigences auxquelles doit répondre un organisme pour mettre en place une politique de sécurité de l'information.

Cette nouvelle norme est fondée sur une approche de la maîtrise des risques et sur le principe du management de la sécurité de l'information.

En 2000, la norme BS7799-1, devient la norme de référence internationale pour les organismes souhaitant renforcer leur sécurité de l'information. Après avoir suivi un processus de concertation au niveau international et quelques ajouts, l'ISO lui attribue un nouveau nom, ISO/IEC 17799 : 2000.

En 2002, le BSI fait évoluer la norme BS7799-2 en s'inspirant des normes ISO 9001:2000 et ISO 14001 : 1996. La norme adopte définitivement une approche de management de la sécurité de l'information.

En 2005, l'ISO/CEI adopte la norme BS7799-2 sous la référence ISO/CEI 27001 : 2005 en y apportant quelques modifications pour se rapprocher le plus possible du principe de « système de management » développé par les normes ISO 9001 et ISO14001. L'ISO/IEC 27001: 2005 spécifie les exigences pour la mise en place d'un SMSI (système de management et de sécurité de l'information).

En 2007, dans un souci de clarification, l'ISO renomme la norme ISO/IEC 17799 :2005 en changeant sa numérotation pour ISO/IEC 27002. La norme se greffe à la famille des normes ISO/IEC 2 700x toujours en développement.

Aujourd'hui les organismes disposent de deux normes qui se sont imposées comme référence des SMSI, l'ISO/CEI 27001 :2005 qui décrit les exigences pour la mise en place d'un SMSI et l'ISO/CEI 27002 qui regroupe un ensemble de bonnes pratiques «best practices» pour la gestion de la sécurité de l'information.

Autour de ces deux normes viennent s'articuler d'autres normes de la même famille, ISO/CEI 2700x, encore en développement pour certaines.

4.2 La norme ISO 27002

La norme ISO/CEI 27002 (*Technologies de l'information – Techniques de sécurité – Code de pratique pour la gestion de la sécurité de l'information*), issue de l'ISO/CEI 17799, est un code de bonne pratique qui couvre les aspects techniques, organisationnels, sociaux et juridiques de la sécurité de l'information, en complément des exigences de certification décrites dans la norme NF ISO/CEI 27001[9].

La sécurité de l'information est définie au sein de la norme comme la «préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information».

4.3 Objectifs de la norme

La norme ISO/CEI 27002 nous fournira les lignes directrices fondamentales qui nous aideront à initier, à mettre en œuvre, à maintenir et à améliorer le management de la sécurité de l'information au sein d'une organisation. Les mesures de sécurité de l'information qui sont énumérées dans la norme sont conçues pour nous aider à identifier et à répondre aux exigences spécifiques dans une approche formelle d'appréciation des risques. ISO/CEI 27002 nous permettront aussi d'acquérir les connaissances nécessaires pour assurer aux organisations que leurs actifs informationnels précieux sont protégés par une norme internationale reconnue [10]. Les entreprises qui adoptent l'ISO/IEC 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

Elle présente une série de contrôles (39 objectifs de contrôle)qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité.

4.4 Structure de la norme

La norme ISO 27002 se compose de 18 chapitres dont 4premiers introduisent la norme et les 14 chapitres suivants couvrent le management de la sécurité autant dans ses aspects stratégiques que dans ses aspects opérationnels [11].

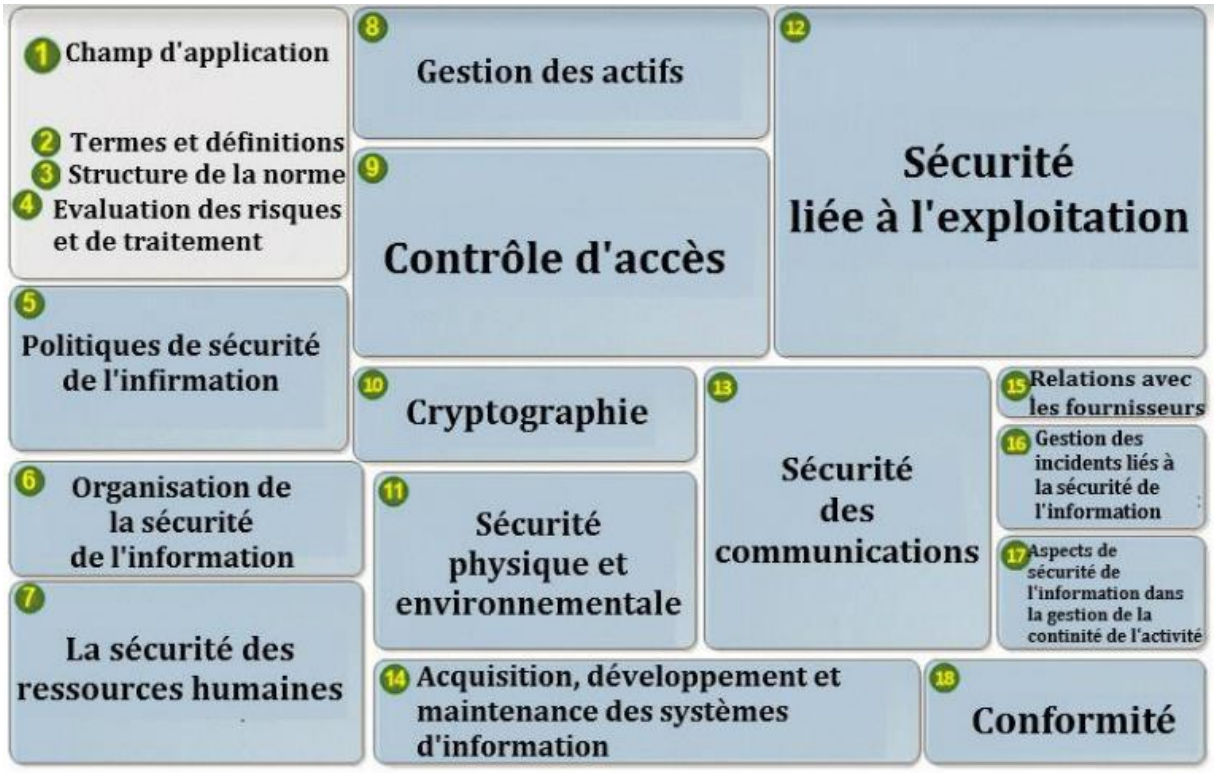


Figure 1 : structure de la norme ISO 27002

Ces 18 chapitres sont organisés comme suit dans le tableau suivant :

Chapitres	**Champ d'application**	La norme donne des recommandations pour la gestion de la sécurité des informations pour ceux qui sont chargés de concevoir, mettre en œuvre ou maintenir la sécurité.
	Termes et définitions	Cette page définie la préservation de la confidentialité, l'intégrité et la disponibilité de l'information ».
	Structure de la présente norme	Cette page explique que la norme contient des objectifs de contrôle
	Évaluation des risques et de traitement	couvre le sujet de la gestion des risques. Elle donne des directives générales sur la sélection et l'utilisation de méthodes appropriées pour analyser les risques pour la sécurité des informations.
	Politiques de sécurité de l'information	Il existe deux mesures de sécurité. Elles concernent la composition des politiques de sécurité et leurs revues périodiques.

	Organisation de la sécurité de l'information	L'information Il n'existe aucun lien particulier entre les différentes mesures de sécurité abordées dans ce chapitre. Elles sont toutes organisationnelles.
	La sécurité des ressources humaines	Il existe un certain nombre de mesures de sécurité à prendre auprès du personnel avant son embauche, pendant sa présence dans l'organisme, puis à son départ.
	Gestion des actifs	Ce chapitre aborde les actifs d'information au sens large du terme comme les supports physiques ; Responsabilités relatives aux actifs, Classification de l'information, Manipulation des supports.
	Contrôle d'accès	L'objectif de cette catégorie est de contrôler l'accès aux informations des installations de traitement, d'information et des processus commerciaux.
	Cryptographie	Il existe deux mesures de sécurité: ○Politique de chiffrement : cette mesure conseille de chiffrer les informations en fonction de leur sensibilité ○Gestion des clés : les conséquences liées à la divulgation des clés ou à la perte de celles-ci sont telles qu'il convient de les protéger de façon adéquate.
	Sécurité physique et environnementale	○ Mesure de sécurité des salles machines et des autres locaux de l'organisme. ○ Sécurité des équipements.
	Sécurité liée à l'exploitation	Ce chapitre aborde de très nombreux domaine : voici les plus importants : ○ Protection contre les codes malveillants. ○ Journalisation. ○ Gestion des vulnérabilités techniques.
	Sécurité des communications	Ce chapitre traite des mesures relatives à la sécurité des réseaux

	Acquisition, développement et maintenance des systèmes d'information	Il est convenu de mettre en place des mesures pour assurer la sécurité des services réseaux.
	Relations avec les fournisseurs	Il s'agit d'un des points le plus important de la norme. ○ Relations avec les fournisseurs : Il est conseillé de rédiger une politique de sécurité destinée aux fournisseurs. ○ Gestion de la prestation de service : Le fournisseur doit être en mesure d'apporter la preuve qu'il respecte ses engagements en matière de sécurité
	Gestion des incidents liés à la sécurité de l'information	Ce chapitre évoque toutes les mesures liées à la gestion des incidents de sécurité de l'information.
	Aspects de la sécurité de l'information	Dans la gestion de la continuité de l'activité Il est recommandé de réaliser un plan de continuité (PCA) ou de reprise (PRA), qui doit être testé et mis à jour.
	Conformité	Il est conseillé d'identifier les législations applicables dans le pays où se situe l'organisme. Des textes peuvent formuler des exigences concernant la sécurité des systèmes d'information que l'organisme se doit de respecter sous peine de poursuites judiciaires ou de pénalités contractuelles.

Tableau 1 : signification de la structuration de la norme ISO 27 002

4.5 Les avantages de la norme ISO/CEI 27002

La certification PECB ISO/IEC 27002 démontre que vous avez [10] :

- Compris la mise en œuvre des mesures de sécurité de l'information en conformité avec le cadre et les principes de la norme ISO/CEI 27002.
- Compris la relation entre les différentes composantes des mesures de sécurité de l'information, y compris la responsabilité, la stratégie, l'acquisition, la performance, la conformité et le comportement humain.

- Obtenu les compétences nécessaires pour accompagner une organisation dans la mise en œuvre et la gestion des mesures permanentes de sécurité de l'information selon l'ISO/CEI 27002.
- La capacité à effectuer une évaluation périodique des risques dans une organisation.
- La capacité à aider les organisations à améliorer leur position en matière de sécurité de l'information.
- La capacité à rédiger et à mettre en œuvre des stratégies d'optimisation des coûts.

5 Méthodologies de gestion des risques

La gestion du risque en informatique consiste à analyser les dangers potentiels qui pèsent sur un système d'information afin de pouvoir les prévenir ou les traiter rapidement si Besoin. Il s'agit d'envisager tous les risques afin de prendre en compte les mesures nécessaires, améliorer la sécurité générale du système et de l'optimiser.
Il existe plusieurs méthodes d'appréciations des risques, nous avons retenu deux qui figurent Parmi les plus utilisées MEHARI et EBIOS.

5.1 MEHARI

La méthode MEHARI (Méthode harmonisée d'analyse des risques), portée par l'association loi 1901 CLUSIF (Club de la sécurité de l'information français), respecte les lignes directrices tracées par la norme ISO 27005:2009 et permet une intégration dans une démarche complète qui permet d'être utilisée aussi dans le cadre d'un Système de Management de la Sécurité de l'information (ISO 27001:2005) grâce à sa capacité à impliquer et sensibiliser la Direction de l'entité comme les responsables opérationnels [12].

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

Scénarios de risque est déterminé à partir des niveaux de potentialité et d'impact, et la structure de la méthode permet de sélectionner les mesures de sécurité susceptibles de traiter

(réduire son niveau) chaque risque au mieux des ressources de l'organisation [12].

5.2 EBIOS

La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est un outil complet de gestion des risques SSI conforme au RGS (Référentiel Général de Sécurité).

Créée en 1995 par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), Portée maintenant par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et régulièrement mise à jour, la méthode EBIOS bénéficie de ses 20 ans d'expérience dans le domaine de la gestion du risque. Elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI [12].

5.3 choix de la méthodologie

Les deux méthodes sont conformes aux exigences techniques, environnementales et légales auxquels se réfère notre travail. D'où le choix entre les deux méthodes n'était pas facile. Nous avons choisissiez la méthode EBIOS car elle bénéfices ses expériences dans le domine de gestion des risque et elle permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information que notre travail qui représente la mise en œuvre de la politique de cette dernière.

6 conclusion

Cette partie de notre travail nous a permis d'avoir une vision globale de la sécurité de l'information avec ses objectif et besoins aussi la norme 27002 qui nous avons mis en place pour réaliser notre politique et dans le chapitre suivant nous touchons notre sujet de mémoire a savoir la politique de sécurité des systèmes d'information.

Chapitre 02 : La Politique de Sécurité

1. Introduction

L'objectif de ce chapitre est de présenter les notions de base d'une politique de la sécurité informatique Nous commencerons par la définition du politique de sécurité informatique Ensuite nous parlerons de ce qu'elle contient et son domaine d'application aussi le rôle, les bénéfices, avantages et inconvénients de la PSSI De plus nous parlerons de la place de la PSSI dans le référentiel documentaire de l'entreprise d'application On sitars aussi pour quoi et comment mettre en place la PSSI.

2. Définition de la politique de sécurité de système d'information

Une politique de sécurité de système d'information est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie [13].

À distinguer de la charte informatique, qui est un document de recommandations concernant la bonne utilisation des technologies informatiques, et qui est destiné aux employés de l'entreprise [13].

3. le contenu une PSSI

D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, référentiel réglementaire, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme [14] .

4. Concepts manipulés

4.1 Principe de sécurité

Les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la SSI en vue de l'élaboration d'une PSSI [14].

4.2 Règle de sécurité

Les règles de sécurité définissent les moyens et les comportements définis dans le cadre de la PSSI. Elles sont construites par déclinaison des principes de sécurité dans un environnement et un contexte donné.

4.3 Domaines d'application

La portée de la réalisation d'une PSSI couvre les besoins du secteur public et du secteur privé.

Appliqué aux ministères, il est plus particulièrement destiné aux acteurs de la voie fonctionnelle SSI, tels que les fonctionnaires de sécurité des systèmes d'information (FSSI) ou autorités qualifiées, afin de mettre en place une PSSI, conformément aux instructions interministérielles et pour satisfaire les besoins de leurs métiers.

Appliqué aux autres types d'organismes, il s'adresse plus particulièrement aux responsables de la sécurité des systèmes d'information (RSSI) et propose une approche pour l'application des actions de sécurité conformes à l'état de l'art en matière de principes de protection appliqués aux systèmes d'information.

De façon plus globale, s'adresse aux personnes qui ont la responsabilité de définir ou de faire évoluer une organisation de la sécurité au sein d'un organisme, public ou privé. Il apporte une aide à la préparation d'un projet de définition et/ou de déploiement d'une PSSI applicable à l'ensemble des systèmes d'information de l'organisme ou à un système d'information spécifique.

Il est finalement destiné à l'ensemble des acteurs de l'organisme dans un but de sensibilisation et d'adhésion aux principes.

5. Champs d'application de la PSSI

La Politique de Sécurité des Systèmes d'Information (PSSI) peut s'appliquer à la totalité ou à une partie du système d'information de l'organisme.

La PSSI [14] :

- s'applique à un système existant ou à développer.

- concerne toute personne ayant accès au système d'information de l'entreprise qu'il soit interne ou externe à l'organisme (sous-traitant, stagiaire, prestataire).

- concerne l'ensemble des aspects du système d'information (l'organisation, l'environnement physique, le développement, l'exploitation, la maintenance…).

-Elle couvre aussi l'ensemble des systèmes d'information de l'administration, de l'organisme ou de l'entreprise.

6. Place de la PSSI dans le référentiel documentaire

La PSSI est un élément de la politique générale de l'organisme et elle est en accord avec le schéma directeur du système d'information et la stratégie de sécurité de l'information.

Bien qu'elle puisse concerner l'ensemble des systèmes d'information de l'organisme, elle peut également être restreinte à un système d'information particulier, par exemple lié à un métier de l'organisme ou à un système transversal (messagerie, intranet…). Dans ce cas, il peut exister plusieurs PSSI dans un organisme ou une entreprise. Elles devront être cohérentes entre elles. Cette cohérence est assurée grâce à la formalisation d'une PSSI globale [14].

Les autres politiques sont alors des déclinaisons de la PSSI dans un environnement métier ou technique particulier, pour des instances spécialisées ou des cas particuliers.

Pour élaborer une PSSI adaptée à l'organisme, il est recommandé de réaliser une analyse des risques spécifiques au contexte afin d'en ajuster les règles de sécurité.

7. Rôle de la PSSI

La sécurité du système d'information est devenue un facteur indispensable au bon fonctionnement de l'organisme [14].

Par ailleurs, l'utilisation croissante des systèmes d'information pour des applications variées a fait prendre conscience à la communauté des utilisateurs qu'il ne suffisait pas de mettre en œuvre les moyens de communication les plus performants, mais que ces derniers devaient être fiables et sûrs (disponibilité, intégrité, confidentialité et parfois preuve).

La PSSI constitue un document de référence de sécurité du système d'information (SSI).

Celle-ci est là pour définir les objectifs à atteindre, les acteurs associés ainsi que les moyens accordés pour parvenir aux cibles.

L'autre but de la PSSI est de définir et expliquer la vision stratégique de la DSI en termes de sécurité du SI. Elle informe l'ensemble des acteurs des enjeux, des choix face à la gestion des risques.

8. La raison de mettre en place une PSSI :

Face aux menaces qui pèsent sur les systèmes d'information, l'usager exige une protection adaptée des informations et des services de traitement, d'archivage et de transport de l'information. La sécurité est donc devenue l'une des dimensions essentielles de la stratégie de l'organisme et elle doit être prise en compte dès la conception d'un système d'information afin d'assurer la protection des biens et des personnes et du patrimoine de l'organisme. Ainsi, la sécurité des systèmes d'information vise en particulier à protéger les composantes suivantes du patrimoine :

- le patrimoine matériel, composé des biens matériels nécessaires au fonctionnement de ses activités ; ce patrimoine est essentiellement composé des technologies de l'information et de communication (serveurs, réseau, postes de travail, téléphonie...).

- le patrimoine immatériel et intellectuel, composé de toutes les informations concourant au métier de l'organisme (données scientifiques, techniques, professionnelles, administratives…).

- les informations relatives aux personnes (physiques et morales) avec qui l'organisme est en relation, dont la destruction, l'altération, l'indisponibilité ou la divulgation pourrait entraîner des pertes ou porter atteinte à son image de marque voire entraîné des poursuites judiciaires [14].

9. Les bénéfices d'une PSSI

La PSSI offre les bénéfices suivants [14] :

- une vision stratégique de la gestion des risques globaux, dont la SSI, visant à informer les maîtrises d'ouvrage des enjeux et susciter la confiance dans le système d'information,

- la mise en évidence des objectifs, obligations et engagements de l'organisme vis-à-vis de ses usagers et partenaires en fonction des lois applicables, ainsi que les principes de sécurité régissant la protection de son propre patrimoine,

- la sensibilisation aux risques menaçant les systèmes d'information.

- une aide aux Directeurs de programmes et chefs de projet pour intégrer la sécurité aux nouveaux services du système d'information.

De plus, l'élaboration ou la révision d'une PSSI est l'occasion de repenser dans une démarche structurée et à finalité opérationnelle, la sécurité du système d'information en commençant par l'organisation mise en place pour répondre à ce besoin en modifiant la culture de l'organisme.

D'autre part c'est un document général diffusable qui :

- satisfait les objectifs de sécurité identifiés pour l'organisme.

- doit être connu de l'ensemble des acteurs internes,

-doit, après validation par l'autorité responsable, être largement diffusé, sous une forme simplifiée à l'ensemble du personnel.

10. la mise en place une PSSI

La mise en place d'une PSSI doit être menée sous la forme d'un projet PSSI et la démarche à adopter consiste à établir un référentiel de l'organisme croisée avec une analyse des risques SSI, donc l'objectif de la méthode consiste à construire un document de politique comprenant des éléments stratégiques et des règles de sécurité pour notre système d'information.

La validation successive des différentes phases vise à faciliter l'implication de la DSI et l'adhésion de tous les intervenants.

Le phasing projet se découpe alors logiquement en 5 grandes phases :

Phase 0 : préalables

Cette phase préliminaire doit permettre la présentation du projet au niveau de la Direction générale et de faire valider ainsi ses objectifs et les moyens qu'il convient d'y consacrer.

Tâche 1 : organisation projet

Tâche 2 : constitution du référentiel

Phase 1 : élaboration des éléments stratégiques

Elle doit obligatoirement identifier et prendre en compte le périmètre d'étude, le contexte, les enjeux et orientations stratégiques, le référentiel réglementaire, l'échelle de besoins, les besoins de sécurité des biens à protéger et les origines des menaces. Elle est composée de 6 taches

Tâche 1 : définition du périmètre de la PSSI

Tâche 2 : détermination des enjeux et orientations stratégiques

Tâche 3 : prise en compte des aspects légaux et réglementaires

Tâche 4 : élaboration d'une échelle de besoins

Tâche 5 : expression des besoins de sécurité

Tâche 6 : identification des origines des menaces

Phase 2 : sélection des principes et rédaction des règles

Le travail de cette phase consiste à sélectionner, concevoir, préparer, documenter et valider la déclinaison des principes généraux d'une PSSI et des choix stratégiques de l'organisme. Ce travail se traduit en l'élaboration d'un corpus de règles directement applicables.

Tâche 1 : choix des principes de sécurité

Tâche 2 : élaboration des règles de sécurité

Tâche 3 : élaboration des notes de synthèse

Phase 3 : finalisation

La finalité de cette phase est de conduire une étape ultime de validation de la PSSI et du plan d'action associé par la direction générale. Elle est composée de deux taches

Tâche 1 : finalisation et validation de la PSSI

Tâche 2 : élaboration et validation du plan d'action

Phase 4 : Application du plan d'action

Le plan type d'une PSSI figure en phase 3. D'une manière générale, il doit évoquer

Les points suivants :

- pourquoi protéger et susciter la confiance : enjeux, aspects réglementaires, menaces.

- que protéger : biens à protéger et échelle de besoins.

- qui protège : organisation, responsabilités et gestion de la SSI.

- comment protéger : ensemble cohérent et opérationnel de règles de sécurité

- quand protéger : considération de l'ensemble du cycle de vie [15].

Phase 0	Phase 1	Phase 2	Phase 3
cette tâche consiste à définir l'organisation du "projet PSSI" afin d'élaborer le cadre de réalisation.	cette tâche consiste à décrire les domaines d'activités à couvrir et à affiner le périmètre, notamment les échanges entre les domaines et l'extérieur du périmètre. Le champ d'application de la politique de sécurité du système d'information.	cette tâche consiste à sélectionner les principes de sécurité qu'il conviendra de développer et instancier en règles de sécurité lors de la tâche suivante.	L'objectif de cette phase est de produire le document validé exprimant la Politique de Sécurité des Systèmes d'Information de l'organisme.
cette tâche consiste à identifier le référentiel documentaire de l'organisme (SI, SSI, aspects Déontologiques et contractuels) qui servira de base à la suite de la démarche.	cette tâche consiste à présenter les enjeux et orientations stratégiques liés au périmètre de la PSSI. Elle permet aussi d'identifier les contraintes générales pesant sur l'organisme.	cette tâche consiste à instancier les principes de sécurité retenus en règles de sécurité selon les Éléments contenus dans la note de cadrage et la note de stratégie de sécurité. Chaque principe de sécurité retenue doit être déclinée en une ou plusieurs règles	Cette phase consiste à assurer l'application de la PSSI au système d'information de l'organisme.

		de sécurité adaptées au contexte du périmètre de la PSSI.	
	cette tâche consiste à présenter l'ensemble du référentiel légal, réglementaire et contractuel applicable au périmètre de la PSSI.	cette tâche consiste à synthétiser le travail effectué afin d'en obtenir la validation, ce qui permettra ensuite de finaliser la PSSI.	La PSSI doit être complétée par un plan d'action pour assurer sa mise en œuvre.
	cette tâche consiste à définir une échelle de mesure utile à l'expression des besoins de sécurité pour les domaines d'activités identifiés dans la PSSI ou les fonctions et informations identifiées dans les études de sécurité dans le périmètre de la PSSI.		
	L'objectif de cette tâche est d'identifier de manière générale les besoins de sécurité associés à chaque domaine		
	cette tâche consiste à identifier et caractériser les origines des menaces qui pèsent sur le périmètre de la PSSI.		

Tableau 2 : schématisation des taches des 4 phases du projet

11 Conclusion

Dans ce chapitre nous avons présenté des généralités sur la politique de la sécurité des systèmes d'information. Dans la prochaine partie nous allons entamer l'étude et la mise en place de notre politique.

Chapitre 03 : Etudes de La Politique

1. Introduction

Même si la mise en place d'une politique de sécurité du système d'information n'est pas encore applique àtoutes les entreprises en Algérie, ils n'en demeurent pas moins que plusieurs d'entre elle l'on applique et d'autre tentent de le faire. Que ce soit des grands ou des petites entreprises la PSSI accompagne le changement informatis é.

Dans le chapitre pr ésent on expliquera pourquoi on choisit de faire une politique de sécurité du système d'information. Puis nous abordèrent la présentation de la société Hubbard Algérie. Ensuite on entamera l'étude détail du projet. Nous conclurons ce chapitre par l'objectif de notre PSSI.

2. Le choix du projet d'une politique de sécurité du système d'information

La Politique de Sécurité du Système d'Information est mise au sein de n'importe quelle entreprise, peu importe sa taille, le nombre de collaborateurs ou encore son cœur de métier.

Les risques qui p èsent sur le SI n écessitent de cadrer les actions mises ou à mettre en place pour en r éduire les effets. Ce cadre se place au niveau strat égique dans l'entreprise, en ce sens que les dirigeants doivent y être associ és [16].

Nous avant choisie de mettre en place une PSSI pour la soci ét é HUBBARD ALGERIE parce qu'elle est un document qui exprime les orientations de l'équipe de direction de l'organisme. Et comme la soci ét é est on évolution quotidien un tel document lui sera d'un très grand aide parce qu'il constitue un outil de communication que ce soit pour l'équipe interne ou vers l'extérieur ainsi que la PSSI informe sur les choix faits par l'entreprise en termes de SSI.

3. Présentation de la société d'Hubbard Algérie

3.1 Pr ésentation g én érale

La soci ét é HUBBARD ALGERIE est une entreprise avicole sp écialis ée dans la production de poussins reproducteurs chair. Son but est de rendre l'Algérie moins d épendante des importations et de pr évenir les embargos sanitaires ou autres. Afin de contribuer àla s écurit é alimentaire du pays. Elle met… à la disposition de ses éleveurs la meilleure génétique, la plus adapt ée aux besoins du march é alg érien et qui ne cessons d'évoluer avec lui.

La soci ét é propose une tr ès haute qualit é de poussin produit conformes aux normes internationales. Elle bénéficie de la génétique et de l'appui du Géant avicole le Groupe Aviagen.

HUBBARD ALGERIE s'inscrit dans la lignée des groupes économique qui contribuent à l'amélioration de la productivité nationale et à l'abaissement des coûts de revient de la filière en accompagnant ses éleveurs dans le management de leur volaille.

3.2 Organigramme de l'entreprise

Au sein d'une entreprise, l'organigramme est un schéma représentant les liens organisationnels, fonctionnels et hiérarchiques de la structure. Un organigramme vous permettra d'avoir une vue d'ensemble de la répartition des fonctions et postes au sein d'une entité[17].

En général, le terme organigramme représente un ou plusieurs schéma(s) de la hiérarchie entre les divers employés d'une entreprise. Grâce à ce graphique, vous pouvez identifier les directions et services liés [17].

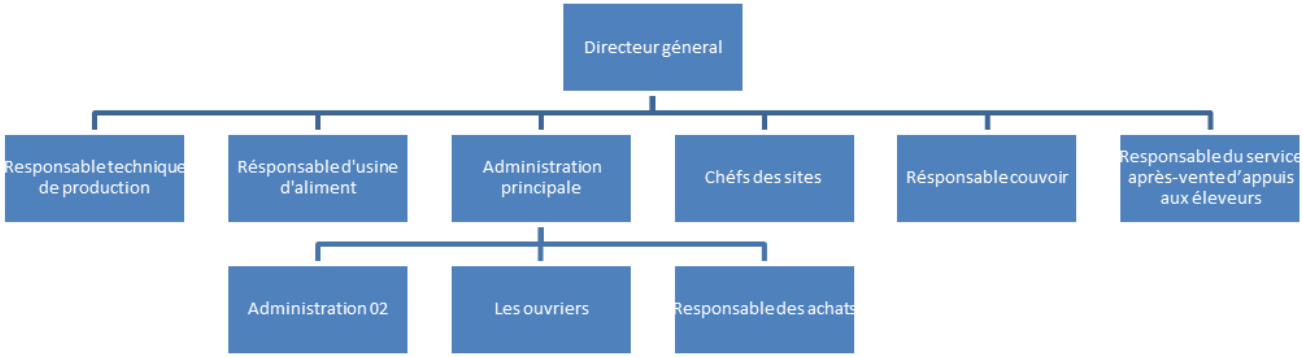


Figure 2 : Organigramme de la société HUBBARD ALGERIE

3.3 Champs d'application de la PSSI dans l'entreprise

Avant de mettre en place une PSSI il est nécessaire de clairement identifier le cadre de la mise en œuvre de la PSSI. Est-elle applicable à l'ensemble du système d'information de l'organisme ? Est-elle applicable à l'extérieur de l'entreprise ?

Dans le cas de la société HUBBARD ALGERIE le document s'applique à tous les employés de l'organisation, y compris les employés temporaires, les visiteurs ayant un accès temporaire aux services et les clients ayant un temps d'accès limité aux services.

4. Etude détaille

Dans le cadre de la réalisation de notre politique de sécurité et pour avoir une idée préalable de la structuration générale de l'entreprise, nous avons effectués un questionnaire sur 100 employés.

Le résultat de manière de sauvegarde de données informatique est présenté dans le graphe suivant :

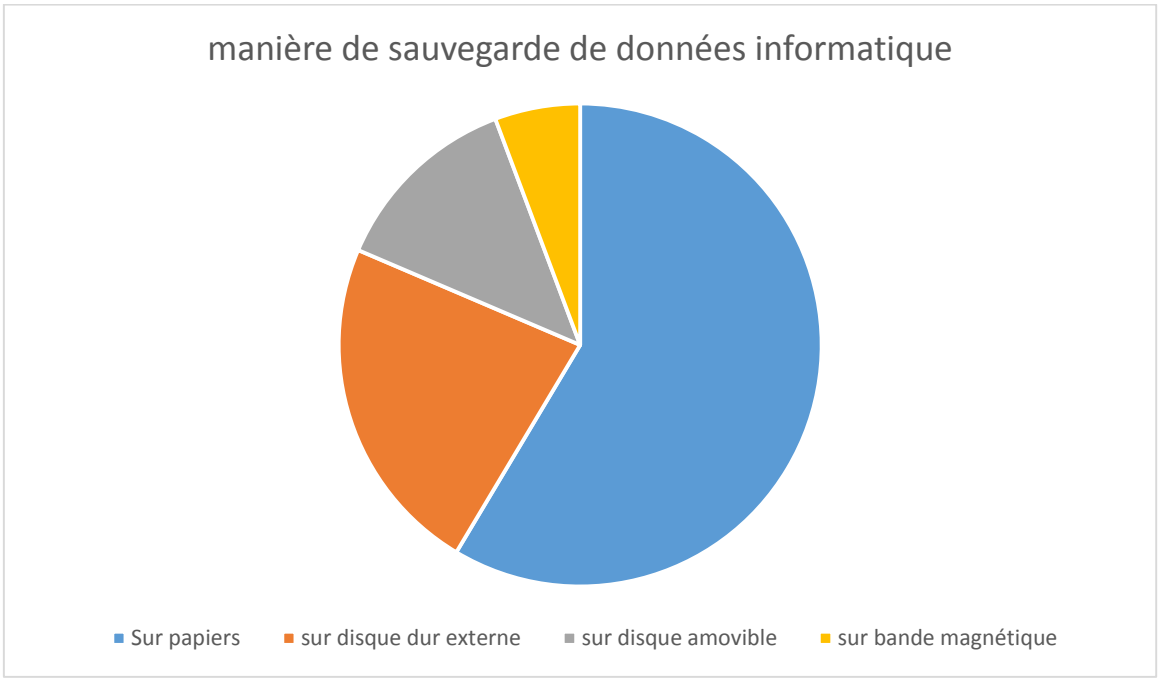


Figure 3 : graphes par secteurs représente la manière de sauvegarde de données informatique

4.1 Etude des postes de travail

Un poste de travail est un employé physique ou moral caractérisé par les taches qu'il accompli et par les ressources qu'il dispose.

Les postes de travail qui intervient dans la société sont :

- Directeur général
- Responsable technique de production
- Responsable d'usine d'aliment
- Administration principale
- Chefs des cites
- Responsable couvoir
- Responsable du service après-vente d'appuis aux éleveurs
- Les ouvriers
- Responsable des achats
- Administration 02

4.2 Etude des documents

Pour l'étude des documents on a besoin de deux études :

A/ Etude de la forme :

- Désignation
- Emetteur
- Récepteur
- Nature
- Rôle
- Nombre d'exemplaire

B/ Etude détaillée

Pour chaque rubrique dans le document en détermine

- Désignation
- Type/taille
- Observation (répétitif, calculable,…)

Les documents utilisés par l'entreprise sont :

- Fiche de transfert
- Fiche journalière
- Détails des mises en place des GP
- Rapport de réception des poussins GP
- Fiche de semaine poussinière
- Fiche de semaine de production
- Synthèse des pesses
- Fiche semaine -détail production
- Fiche usine
- Contrat
- Demande de congé
- Titre de congé
- …..

5 L'objectif de notre PSSI

Dans le cadre de notre travail, notre objectif est de rédiger et de mettre en place une politique de sécurité du système d'information simple, cohérente et facile à comprendre.

Son objectif est d'offrir une vision stratégique de la gestion des risques globaux et mettre en évidence les objectifs, obligations et engagements de l'organisme via ces employées et ces clients.

6 Analyse des risques

L'analyse de risque est l'une des premières étapes et forme le principal moyen d'optimiser la sécurité. La gestion du risque a depuis fort longtemps été intégrée aux entreprises de tous genres. Maintenant que les ordinateurs sont entrés dans les entreprises, le risque informatique doit être pris en considération. De plus, l'informatique étant maintenant en charge de plusieurs opérations critiques, si ce n'est toutes, le risque informatique devient l'un des principaux risques de l'entreprise d'aujourd'hui. Après avoir mesurer la maturité de l'entreprise en termes de sécurité du système d'information aux bons pratiques de la norme ISO 27002, nous allons à présent nous intéresser à l'analyse des risques en identifiant les risques.

Etude de contexte	Système : Biens essentiels : les données Biens support : notre site proposé
Etude des événements redoutés	Événements redoutés : ne pas avoir une trace exacte du travail à cause des informations différentes Impacts : on n'a pas les informations exactes à remplir dans les fichiers et les rapports du travail
Etude de scénario de menaces	Source de menace : Les employés Menace : - modifications des données

Etude des risques	Les risques : Perte des données une différence des données entre le bon de livraison remplit par le responsable de la production et la fiche journalière remplie par le responsable du couvoir
Etude de mesures de sécurité	- proposition d'un site web pour contrôler la transmission de données d'une maniéré sécurisée

Etude de contexte	Système : Biens essentiels : manque de contrôle du carburent Biens support : le groupe d'électricité
Etude des événements redoutés	Événements redoutés : une panne dans le groupe d'électricité Impacts : il a un impact sur la continuité du travail voir même l'arrêt du travail
Etude de scénario de menaces	Source de menace : l'électricité/ manque de contrôle du carburent Menace : une masse d'électricité/le réservoir de carburent est vide
Etude des risques	Les risques : le groupe pend feu un retardement dans le travail
Etude de mesures de sécurité	- la continuité du contrôle, chaque responsable avant le début de son travail doit vérifier le groupe d'électricité.

Etude de contexte	Système : Biens essentiels : l'aliment à utiliser Biens support : site de production d'aliment
Etude des événements redoutés	Événements redoutés : manque d'aliment Impacts : un retardement de travail
Etude de scénario de menaces	Source de menace : le non contrôle du stocke Menace : l'aliment à utiliser n'est pas disponible donc pas possible de terminer le travail
Etude des risques	Les risques : retardement du travail
Etude de mesures de sécurité	-un contrôle continu du stockage pour éviter les retardements de travail.

7 Application de la norme ISO 27002

Le tableau suivant présent les résultats du questionnaire effectué à propos de l'application de la norme ISO 27002 selon les mesures de sécurité

Objectif	**Article**	**Mesure**	**Question posé**	**réponse**
Montrer l'importance de la sécurité de l'information	**5-politique de sécurité**			
	5-1 politiques de sécurité de l'information	Un document de politique de sécurité de l'information doit être approuvé et appliqué au sein de l'organisme	Est-ce que votre organisme applique un document de politique de securité de l'information ?	**non**
	6-organisation de la sécurité d'information			
	6-1 Organisation Interne			
Garantir le bon fonctionnement de la sécurité de l'information au sein de l'organisme	**6-1-1 rôle et responsabilité**	Toutes les responsabilités doivent être définies et attribuées	Lors l'application des rôles et responsabilités si les employés respectent les lois et aura une communication ?	**Oui**
	6-1-2 séparation des taches	Les taches doivent être séparé pour éviter le mauvais usage ou modification des parties non autorisés	Au sein de l'organisme les taches sont –ils séparés ?	**Non**
	6-1-3 les relations au sein de l'organisme entre les groupes et les autoritaires	Relations entre les groupes et les autoritaires doivent être tenus	Les contacts entre les groupes sont –ils maintiens ?	**Oui**
	6-2 Appareils Mobile et Télétravail			
Assurer la sécurité des appareils mobiles et télétravail	**6-2-1 politique de sécurité des appareils mobiles et télétravail**	Une politique et mesures de sécurité doivent être adoptées pour gérer les risques découlant d'utilisation des appareils mobiles et protéger les informations consultées ou stockées	Y'a-t-il une mesure ou bien une politique qui gère les risques découlant de l'utilisation des appareils mobiles et télétravail	**Non**
	7-sécurité de ressources humaines			
	7-1	**Avant l'embouche**		

Les employés connaissent leurs responsabilités et fonction attribuées		Sensibilisation aux lois, réglementaires et éthiques du travail	Lors le recrutement si les critères spécifiques à la mission de travail sont pris en compte ?	**Oui**
	7-2Pendant la durée De contrat			
Assurer que les salaries assure leurs responsabilités		Les salaries doivent applique les règles de sécurité de l'information	Si les employés appliquent le réglementaire de travail ?	**Oui**
	7-3 rupture ou Modification de Contrat de Travail			
Protéger les intérêts de l'organisme		Les responsabilités liées à la rupture, modification de contrat de travail doivent être définie, communiquer et appliquer	En cas de modification si les responsabilités sont communiquées à l'employées ?	**Non**
	8- gestion des actifs			
	8-1 responsabilités Relatives aux Actifs			
Identifier les actifs de l'organisme pour une bonne protection de l'information		Les responsabilités doivent être dressé et tenu à jour	Les actifs concernant l'information sont-ils identifiés ?	**Oui**
	8-2 utilisations Correcte des actifs			
		Les règles d'utilisation correcte de l'information doivent être mise en œuvre	Est-ce que vous respectez les réglementaire de bonne utilisation de l'information ?	**Oui**
	8-3 manipulations Des supports			
Empêcher la divulgation, modification, retrait ou destruction non autorisé de l'information		Les supports doivent être protégés contre l'accès non autorisés et les erreurs d'utilisation lors du transport	Vos informations confidentielles sont-elles protéger contre l'accès non autorisé?	**Oui**
Limiter l'accès à l'information	**9- contrôle d'accès**			
	9-1 exigences Relatives aux Contrôle D'accès			
		Une politique de contrôles d'accès doit être établie	Avez-vous élaboré une politique de contrôle d'accès ?	**Non**
	9-2 gestions de l'accès utilisateur			

		Une procédure d'enregistrements des utilisateurs doit être établie	Avez-vous élaboré une procédure d'enregistrement des utilisateurs ?	**Non**
Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, intégrité et disponibilité de l'information	**10- cryptographie**			
	10-1mesures Cryptographiques			
		Une politique d'utilisation des mesures de cryptographie doit être élaborée et mis en œuvre	Existe –il Une politique d'utilisation des mesures de cryptographie ?	**Non**
Empêcher tout accès physique non autorisé	**11- sécurité physique et environnementale**			
	11-1 zones sécurisées			
		Les zones sécurisées doivent être protégées par des contrôles pour que le personnel autorisé puisse admis	Les zones sécurisées sont-ils protégées par des contrôles d'entrée pour que le personnel autorisé puisse admis	**Oui**
	11-2 sécurités des équipements			
		Les matériels doivent être localisés et protégés de manière à réduireles risques	L'équipement est ils protégé contre les pannes d'alimentation et d'autres interruptions ?	**Non**
Assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants	**12-sécurité liée à l'exploitation**			
	12-1 protection contre les codes malveillants			
		Des mesures de détection de codes	Existent-ils des contrôles pour protéger contre les	**Non**

		malveillants doivent être mise en œuvre	codes malveillants ?	
Enregistrer les évènements	**12-2 journalisations**			
		Des journaux d'évènements enregistrant les activités des utilisateurs	Existent-ils Les journaux d'évènements qui enregistrent les activités des utilisateurs ?	**Non**
Empêcher toutes exploitations des vulnérabilités techniques	**12-3 gestions des Vulnérabilité technique**			
		Des informations contres de la vulnérabilité technique des systèmes d'information doivent être connues	Des informations contres de la vulnérabilité technique des systèmes d'information, sont-ils identifiés ?	**Non**
	13-Sécurité des communications			
	Des mesures relatives à la sécurité des Réseaux. » il n'existe pas un réseau dans l'organisme »			
Mettre en place des mesures de sécurité Recommandent de protéger les transactions contre les erreurs et les traitements incomplets.	**14-Acquisition, développement et maintenance des systèmes d'information**			
		Mettre en place des mesures pour assurer la Sécurité des services réseaux.	Les modifications apportées aux systèmes pendant le développement sont-elles contrôlées par l'utilisation des procédures de contrôle des modifications ?	**Non**
La protection des actifs accessible aux fournisseurs	**15-Relations avec les fournisseurs**			
	15-1 Relations avec les fournisseurs			

		Rédiger Une politique de sécurité destinée aux fournisseurs	Les exigences en matière de sécurité de l'information pour atténuer les risques associés à l'accès des fournisseurs aux actifs de l'organisation sont-elles définies et documentées ?	**Non**
	15-2 Gestion de la prestation de service			
		Le fournisseur doit être en mesure d'apporter la preuve qu'il respecte ses engagements en matière de sécurité	L'organisation vérifie, contrôle et surveille-t-elle les services des fournisseurs ?	**Oui**
Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information.	**16-Gestion des incidents liés à la sécurité de l'information**			
		La gestion des incidents de sécurité de l'information.	Des procédures de gestion sont- elles établies pour assurer une réponse rapide, efficace aux incidents de sécurité de l'information ?	**Non**
Garantir la disponibilité des moyens de traitement de l'information	**17-Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité**			
		Réaliser un plan de continuité (PCA) ou de reprise (PRA) L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information	Existe-il un plan de continuité (PCA) ou de reprise (PRA) ? L'organisation a-t-elle déterminé ses exigences en matière de sécurité de l'information et la	**Non** **Oui**

			continuité de la gestion de la sécurité ?	
Éviter toute violation des exigences de sécurité.	**18-Conformité**			
		Toutes les exigences légales, réglementaires et législatives être explicitement définies, documentées et mises à jour pour chaque système d'information	les exigences légales, réglementaires, contractuelles et législatives pertinentes sont-elles explicitement identifiées, documentées ?	**Oui**

Tableau 3 : application de la norme ISO 27002 selon les mesures de sécurité

8 Conclusion

Dans ce chapitre nous avons expliqué pourquoi nous avant choisie de mettre en place une PSSI, nous avant aussi présenté d'une manière général et détaillé la société HUBBARD ALGERIE.

Chapitre 04 : Mise en place de la Politique

-

Politique de sécurité du système d'information d'Hubbard Algérie

Version 1.0

Historique des versions		
Date	**Version**	**Evolution du document**
	1.0	Publication de la première version de la politique de sécurité du système d'information d'Hubbard Algérie

1. GENERALITES

1.1 Objet

Cette politique de sécurité du système d'information implique la sécurité d'Hubbard Algérie. Elle se compose d'objectifs de sécurité, de lignes directrices pour leurs réalisations, d'une stratégie globale de gestion de la sécurité et de la mise en œuvre des politiques sur les principaux mécanismes de sécurité. La politique de sécurité du système d'information est conforme aux directives, modèles et termes de l'entreprise.la norme ISO 27001 est utilisée pour les termes de sécurité de l'information.

1.2 Champs d'application

Ce document s'applique à tous les employés de l'Organisation, y compris les employés temporaires, les visiteurs ayant un accès temporaire aux services et les clients ayant un temps d'accès limité aux services. Le respect des politiques de ce document est obligatoire pour cette circonscription.

1-3 Personnel couvert

Les rôles sont définis comme:

- secrétariat
- chefs des sites
- chef couvoir
- Responsable technique de production
- Responsable d'usine d'aliment
- Les ouvriers
- Responsable des achats
- Responsable du service après-vente d'appui aux éleveurs.

1.4 Objectif de la politique de sécurité du système d'information

La politique de sécurité établit les lignes directrices et les procédures concernant les actifs que les employés d'Hubbard Algérie doivent connaître et respecter comme principal moyen d'atteindre les objectifs de sécurité. La politique de sécurité est la base de la planification, de la conception, de l'exécution et de la gestion de la sécurité. Son objectif est de protéger l'Organisation et les utilisateurs dans toute la mesure du possible contre les menaces à la sécurité qui pourraient compromettre leur intégrité, leur confidentialité, leur réputation et leurs résultats commerciaux.

1.5 Objectifs de sécurité

1.5.1 La sécurité des actifs doit être maintenue dans la mesure où Hubbard Algérie pourrait fonctionner normalement et sans interruption en cas de menaces les plus probables, pour atteindre ses objectifs commerciaux.

1.5.2 Les mesures de sécurité doivent être économiquement justifiées et leur effet perturbateur sur les opérations et le personnel d'Hubbard Algérie doit être aussi réduit que possible.

1.5.3 La conformité à la législation en matière de sécurité (y compris les informations personnelles, les lois et règlements de l'État et les exigences en matière de santé et de sécurité des travailleurs et les exigences de sécurité incendie) doit être assurée. Pour répondre à cette exigence, certains objets et processus doivent être protégés avec des mesures supérieures au niveau de la sécurité moyenne si nécessaire.

1.6 Principes de sécurité

1.6.1 Les autorisations d'utilisation des biens sont accordées aux travailleurs en fonction des besoins liés au travail.

1.6.2 Pour les biens de l'entreprise, elles ont décide quoi faire selon la situation.

2. ORGANISATION ET INFRASTRUCTURE DE SÉCURITÉ

2.1 Responsabilités

2.1.1 Les employés sont responsables des biens qui leur sont confiés pour le travail.

2.1.2 Les employés sont financièrement responsables.

2.1.3 Le responsable des machines est responsable du bon fonctionnement des machines du couvoir.

2.1.4 Le responsable des moyens généraux s'occupe des achats et des missions.

2.2 Remplacement temporaire des personnes responsables

2.2.1 Le poste de secrétariat et celui du responsable technique doivent être remplis en tout temps. Des efforts devraient être faits pour éviter la disparition simultanée d'un titulaire de rôle. Lorsque cela n'est pas possible, La secrétaire ou le responsable technique nomme un adjoint pour la période d'absence temporaire correspondante et lui donne des instructions.

2.3 Notification des incidents

2.3.1 Tous les incidents de sécurité réels et présumés doivent être signalés immédiatement.

2.3.2 Les incidents de sécurité générale doivent être signalés, selon la situation, soit au directeur général ou à l'administration principale ou au responsable des moyens généraux soit à contacter immédiatement les autorités compétentes.

2.4 Politique de sécurité supplémentaire

Les responsables des sites ont le droit d'imposer des dispositions supplémentaires et des politiques détaillées sur les objets et mécanismes de sécurité, si elles ne sont pas incompatibles avec cette politique de sécurité.

3 ÉVALUATION DES RISQUES ET GESTION DES RISQUES

3.1 Risque résiduel acceptable

3.1.1 Le risque résiduel acceptable est décidé une fois par an.

3.2 Test de conformité de la sécurité

3.2.1 L'administration principale teste la conformité de la sécurité à la politique de sécurité au hasard au moins une fois par mois.

3.2.2 L'administration principale effectue un audit interne pour vérifier la conformité à la sécurité de base au moins une fois par an.

3.2.3 L'audit externe est effectué si nécessaire, mais au moins une fois tous les trois ans.

3.3 Assurances

3.3.1 Dans les présentes conditions, l'assurance est économiquement justifiée pour Hubbard Algérie.

4 ATOUTS PHYSIQUES ET D'INFORMATION

4.1 Actifs critiques

Cette politique de sécurité vise principalement la sécurité des actifs répertoriés dans cette section.

4.1.1 Infrastructure

Les articles suivants doivent répondre au niveau moyen de disponibilité et d'intégrité:

- Locaux et bâtiments
- infrastructure technique, distribution d'énergie et autres systèmes d'utilité générale
- équipement et outils utilisés pour l'entretien, la restauration et d'autres activités de soutien dans les locaux
- parking
- voitures.

4.1.2 Données et documentation

Pour l'activité d'Hubbard Algérie, en particulier les types de données suivants sont importants sur le plan de la sécurité:

4.1.2.1 Données commerciales avec une confidentialité moyenne: plan de mise en élevage, contrats, plans de vente dont la divulgation pourrait raisonnablement affecter le fonctionnement normal et la compétitivité d'Hubbard Algérie.

4.1.2.2 Données autoproduites dont l'intégrité et la disponibilité sont essentielles: les résultats intermédiaires et finaux de la production interne.

4.1.2.3 Données autoproduites pour lesquelles la confidentialité est importante: données d'entrée, intermédiaires et de résultats couverts par un secret professionnel ou un accord de confidentialité.

4.1.2.4 Données du personnel qui sont confidentielles: y compris les fichiers sur les travailleurs, les contrats, les registres, les données de paie, les données de santé…

4.1.2.5 Traiter les données de gestion avec des exigences de confidentialité: plans de travail détaillés et affectations des travailleurs et données administratives sur les mécanismes de sécurité.

4.1.2.6 Données auxiliaires nécessitant disponibilité et intégrité: données de gestion de l'infrastructure, documentation de l'équipement et de l'infrastructure, documentation professionnelle.

4.1.3 Matériel

L'intégrité et la disponibilité du matériel suivant sont importantes:

Couvoir :

- incubateur et éclosoir
- chariot et plateaux
- climatiseur
- thermomètre.

Bâtiments :

- ventilateur
- coulions
- abreuvoirs
- mangeoire
- la sonde
- chauffage.

4.1.4 Systèmes de communication

La disponibilité et l'intégrité des équipements de communication suivants sont importantes:

- téléphones, y compris les téléphones portables.
- modems, réseaux sans fil et autres équipements de communication de données.

4.1.5 Logiciel

4.1.5.1La disponibilité, l'intégrité et la légalité des logiciels commerciaux et autodidactes sont importantes.

4.1.5.2 Le logiciel spécial développé…. Contient le logiciel aux fins de l'entreprise.

4.1.5.3 Logiciel spécial acheté

4.1.5.4 Obtenir des logiciels gratuits uniquement à partir de sources fiables.

4.1.6 Matériaux

Pour assurer la disponibilité des équipements et la continuité des processus, il faut prévoir un approvisionnement de chaque mois pour les matériels suivants:

- papier
- toner d'imprimante
- Clés USB
- Produits de nettoyage
- Produits de désinfections.-

Un approvisionnement de 6 mois pour les bons d'achats.

4.1.7 Médicaments et vaccins :

Pour assurer la disponibilité des médicaments et vaccins et pour la continuité du programme de vaccination, il faut prévoir un approvisionnement d'un mois.

4.1.8 Autres actifs

La disponibilité et l'intégrité sont importantes pour les ressources suivantes:

- Les tenues de travail
- Les balances
- Les meubles.

4.2 Comptabilité des actifs

4.2.1 Les actifs d'information énumérés à la section 4.1, à l'exception de ceux de (4.1.6) doivent être identifiés, documentés, évalués quantitativement ou qualitativement, et répertoriés.

4.2.2 Lors de l'évaluation du prix des actifs, il faut tenir compte à la fois de la valeur monétaire des actifs et des éventuels dommages indirects liés à des incidents de sécurité (destruction, dommages, exposition) entraînant un ralentissement des processus de travail, des atteintes à l'image publique, etc.

5 RISQUES ET FAIBLESSES

Pour la planification, la mise en œuvre et la gestion de la sécurité, les risques suivants seront considérés comme typiques et les mesures de sécurité doivent être basées sur cette sélection.

5.1 Risques spontanés

- Feu
- Orage
- Tremblement de terre
- Dégâts dus à l'eau (eaux pluviales, conduites internes)
- Erreur humaine
- Fluctuations de la qualité de l'énergie et panne de courant
- Erreur matérielle
- Perte de personnel.

5.2 Attaques

- Vol
- Virus
- Interception de la communication orale
- Comportement délibéré de violation de la sécurité des travailleurs, attaques internes.

6 POLITIQUES DE MESURE DE SÉCURITÉ

La mise en œuvre et la gestion des mécanismes de sécurité de base doivent respecter les politiques et directives suivantes.

6.1 Politique d'accès

6.1.1 L'accès aux ressources est basé sur les rôles, selon les exigences du poste.

Pour des raisons sanitaires relatives au travail :

6.1.2Passage de la zone propre vers la zone sale.

6.1.3 L'accès aux bâtiments ne se fait pas sans mesures de désinfection.

6.1.4 L'accès aux réunions ne peut être que par autorisation.

6.1.5 Passage du lot le plus jeune vers le plus âgé.

6.2 Politique de cryptographie

6.2.1 Pour accéder aux ressources interne sur le réseau public et pour la transmission de données confidentielles sur le réseau public, seules des connexions sécurisées doivent être utilisées : connexions VPN, connexions SSL / HTTPS.

6.2.2 Toutes les données confidentielles sur les ordinateurs transportés en dehors du périmètre de l'entreprise (ordinateurs portables pour le travail à domicile), toutes les données confidentielles sur les disques durs ou clés USB doivent être cryptées. Les clés de chiffrement doivent être dupliquées dans une sauvegarde sécurisée.

6.3 Politique de suppression

6.3.1 Tous les documents papier inutiles contenant des données confidentielles doivent être détruits avec une déchiqueteuse.

6.3.2 Les supports retirés et / ou jetés des supports de stockage d'archives doivent être détruits physiquement.

6.3.3 Pour supprimer des données secrètes hautement confidentielles du disque, une suppression sécurisée doit être utilisée.

6.4 Politique d'environnement de travail

6.4.1 Le nouveau logiciel doit être testé avant l'utilisation et confirmé comme approprié.

6.4.2 Aucune donnée réelle ne doit être utilisée pour les tests et les démos.

6.5 Politique de l égalit é

6.5.1 Tous les biens doivent être acquis l également.

6.5.1 Toutes les utilisations des biens devraient être l égales.

7 SÉCURITÉ DE LA COMMUNICATION

7.1 Courrier électronique

7.1.1 Si vous recevez une pièce jointe d'un inconnu, ne l'ouvrez pas. Détruisez-la sur le champ. Méfiez-vous aussi des pièces jointes envoyées par des proches si vous n'en attendez pas : leurs comptes de messagerie sont peut-être infectés ou leurs adresses de courriel falsifiées

7.1.2 Au lieu de cliquer sur un lien, ouvrez un nouveau navigateur et tapez l'adresse.

7.1.3 Ne donnez pas votre adresse électronique à des sites à qui vous ne faites pas confiance.

7.1.4 utiliser plusieurs adresses email différentes afin de séparer vos activités professionnelles et personnelles.

7.1.5 rester prudent lorsque vous naviguez sur le WIFI public.

7.1.6 vérifier l'adresse de l'expéditeur en cas de données sensibles à fournir.

7.1.7 En cas d'adresse de courrier suspecte, faites une recherche sur Internet pour vérifier si d'autres personnes la connaissent et s'ils l'ont identifiée comme étant sérieuse ou non.

7.2 Appels téléphoniques

7.2.1 La transmission d'informations confidentielles par téléphone doit être évitée, en particulier avec les téléphones portables.

7.3 Fax

7.6.1 Le fax d'Hubbard Algérie ne peut être utilisé que par du personnel autorisé et seulement pour le travail.

7.4 Échange de données à l'aide d'un support amovible

7.4.1 Les données transférées à l'aide d'un périphérique de stockage portable ou d'une clé USB ne doivent contenir aucune donnée cachée.

7.4.2 Lors de la réception des données avec un dispositif de stockage portable, une détection de virus doit être effectuée.

7.4.3 Le périphérique à livrer ne doit pas contenir de programmes ou de données étrangers.

7.5 Communication orale

7.5.1 Évitez les questions confidentielles dans les zones publiques.

8 SÉCURITÉ GÉNÉRALE

8.1 Sécurité du périmètre et des zones

8.1.1 Portes

8.1.1.1 Les portes doivent être à fermetures sécurisées.

8.1.1.2 L'entrée à un bâtiment doit être verrouillée en dehors des heures de travail.

8.1.2 Accès aux locaux

8.1.2.1 Les employés temporaires n'ont pas accès à l'administration principale pendant les heures de travail, ils n'ont le droit d'accès qu'aux locaux de leur espace de travail selon les besoins de leur fonction.

8.1.3 Autres verrous

8.1.3.1 Les clés de rechange de toutes les pièces doivent être conservées dans des armoires ignifuges verrouillées.

8.1.4 Les fenêtres

8.1.4.1 Toutes les fenêtres doivent pouvoir être fermées de façon sûre.

8.1.4.2 Les fenêtres doivent être suffisamment étanches pour éviter les dommages dus à la pluie.

8.1.4.3 Les pièces avec des fenêtres au rez-de-chaussée doivent être sécurisées.

8.1.5 Garde

8.1.5.1 Avant le début de la garde le responsable de garde doit vérifier tous les éléments nécessaires pour la continuité du travail.

8.1.6 Système d'alarme de sécurité

8.1.6.1Tout les sites doivent contenir des alarmes des sécurités.

8.1.7 Visiteurs

8.1.7.1 Les visiteurs et les clients ne sont pas autorisés à pénétrer dans l'administration principale que s'ils sont accompagnés d'un accompagnateur.

8.1.7.2 Le préposé rencontrera le visiteur ou le client à l'entrée de l'administration principale.

8.1.7.3 Les réunions auxquels participent d'autres parties ne devraient avoir lieu que dans la salle de réunion.

8.2 Sécurité des locaux

8.2.1 Désignation de la pièce

8.2.1.1 Les salles de machines, les salles d'archives et les locaux techniques doivent avoir des étiquettes compréhensibles.

8.2.2 Matériel de lutte contre l'incendie

8.2.2.1 Le nombre d'extincteurs, la disposition et la vérification doivent être conformes à la réglementation sur les incendies.

8.2.2.2 Les extincteurs dans les locaux équipés de matériel ou de distribution d'électricité doivent être à gaz ou à poudre.

8.2.2.3 Les personnels doivent être formés pour l'utilisation des extincteurs.

8.2.2.4La société externe responsable de la vérification des extincteurs fait une vérification chaque 6 mois.

8.2.3 Mesures environnementales

8.2.3.1 La salle de tri des œufs doit être climatisée tout le temps, ce qui régule la température et l'humidité de l'air.

8.2.3.2 La salle de tri poussins doit être climatisée en été et réchauffée en hiver, ce qui régule la température et l'humidité de l'air.

8.2.3.3 Les hangars d'élevage doivent être climatisés en été par le pad colin et les canons pour réchauffer en hiver, ce qui régule la température et l'humidité de l'air.

8.2.4 Sécurité des locaux

8.2.4.1 Lorsqu'ils quittent un lieu de travail, les travailleurs doivent fermer les fenêtres et verrouiller la porte.

8.2.5 Sécurité des pièces spéciales

8.2.5.1 Les salles techniques doivent être de construction à sécurité renforcée, elles doivent être équipées d'une alarme de sécurité et d'incendie et d'extincteurs à gaz. Les salles techniques doivent être verrouillées en permanence.

8.2.5.3 Les salles de distribution d'électricité doivent être équipées d'alarme incendie et d'extincteurs et fermées à clés.

8.2.5.4 Les tableaux de distribution d'électricité doivent être bien verrouillés.

8.2.5.5 La salle de stockage et le laboratoire doivent être équipés d'une alarme de sécurité et verrouillées en permanence.

8.2.6 Sécurité au travail

8.2.6.1 Il est recommandé que tous les lieux de travail respectent le principe d'une table vide, c'est-à-dire que lorsque vous quittez la pièce après le travail, retirez tous les

documents et supports de la table et d'autres emplacements visibles et verrouillez toujours l'écran de votre ordinateur.

8.2.6.2 Les documents, les supports importants et les actifs physiques de petite taille mais de valeur doivent être conservés dans une armoire ou un tiroir verrouillés.

8.2.7 Travaux d'entretien et de réparation

8.2.7.1 Le personnel externe d'entretien et de réparation n'est autorisé à se rendre sur les lieux que s'il est accompagné d'un préposé.

8.2.7.2 Les clés ou autres dispositifs d'accès ne doivent pas être remis aux réparateurs.

8.3 Sécurité physique de l'équipement

8.3.1 Équipement mobile

8.3.1.1 Les utilisateurs de téléphones portables et d'ordinateurs portables sont responsables de leur sécurité.

8.3.2 Stockage

8.3.2.1 Les clés USB doivent être étiquetées.

8.3.2.2 Les supports d'archivage doivent être conservés dans des armoires spéciales.

8.3.3 Interruptions des services techniques

8.3.3.1 Une alimentation de secours pendant la panne doit être fournie à l'aide d'un groupe électrogène.

8.4 Communication avec les autorités en cas d'incident de sécurité

8.4.1, L'employé qui découvre le danger contactera la police ou le numéro d'urgence.

8.4.2 Sur les questions d'électricité, le technicien interagit avec les autorités compétentes.

9 SÉCURITÉ DU PERSONNEL

9.1 Sélection du personnel

9.1.1 Les candidats aux postes vacants doivent être sélectionnés sur la base des exigences du poste.

9.1.2 Les antécédents de chaque candidat doivent être vérifiés du point de vue des risques de sécurité.

9.2 Procédures de nomination

9.2.1 Lors de la nomination au poste, le nouveau personnel doit lire attentivement les documents suivants et confirmer ses connaissances par sa signature :

- Contrat
- Description de l'emploi
- Politique de sécurité du système d'information
- règlement intérieur.

9.2.2 Pour les travailleurs contractuels, les exigences de sécurité appropriées doivent être incluses dans le contrat dans chaque cas.

9.2.3 Le responsable du site est responsable de l'instruction et la formation du nouvel employé.

9.3 Notification

9.3.1 Le personnel recevra des notifications via les responsables.

9.3.2 Les informations de sécurité opérationnelles sont diffusées via la liste de diffusion interne.

Dans cette liste de diffusion, les événements suivants doivent être annoncés:

- incidents de sécurité
- changements d'environnement de sécurité
- recrutement et licenciement
- modifications et ajouts au système de sécurité interne du réseau.

9.4 Formation

9.4.1 La formation à la sécurité du personnel consiste principalement à lire les guides et la politique de sécurité.

9.5 Procédures de licenciement

9.5.1 À la fin de la dernière journée de travail, le travailleur licencié doit restituer tous ses actifs à Hubbard Algérie. Le responsable de l'administration principale est responsable de la reprise de ces actifs.

.

9.5.2 A la fin du dernier jour travaillé tous les moyens d'accès (clés ou autres) doivent être remis. Le responsable de l'administration principale est responsable de la reprise.

9.5.3 Si nécessaire, les mesures des 9.5.1 et 9.5.2 sont prises immédiatement après la décision de licenciement.

9.6 Sanctions

9.6.1 En cas de violation des exigences de sécurité, le contrevenant sera poursuivi avec des sanctions allant de la réprimande au licenciement.

9.6.2 La direction d'Hubbard Algérie doit obliger le contrevenant à réparer ou à rembourser les dommages physiques causés.

9.7 Télétravail

9.7.1 Le télétravail a droit au cas par cas.

9.7.2 Le télétravail ne peut être effectué que par une communication sécurisée et en conformité avec d'autres exigences de sécurité appropriées.

10. SÉCURITÉ DES DOCUMENTS ET STOCKAGE

10.1 Archivage

10.1.1 La durée typique de conservation des documents archivés est de 7ans.

10.1.2 Dans des cas exceptionnels, qui peuvent résulter des lois correspondantes (Code de commerce, loi sur les archives, règles d'archivage), ou d'autres considérations, le temps est décidé par le chef du site.

10.2 Conservation des documents papier

10.2.1 Les documents secrets et confidentiels doivent être conservés dans un coffre-fort ignifuge.

10.2.2 Tout autre document à archiver doit être conservé dans les armoires d'archives sur des étagères, dans des dossiers et des boîtes étiquetés.

10.2.3 Les originaux des documents techniques doivent être conservés dans les archives.

10.2.4 Les autres documents non publics doivent être conservés dans des armoires ou tiroirs fermés.

10.3 Conservation des supports de stockage

10.3.1 Les supports à contenu secret doivent être conservés dans un coffre-fort.

10.3.2 Les autres supports de stockage importants doivent être étiquetés et conservés dans les archives.

10.4 Assainissement et élimination

10.4.1 Les documents obsolètes et le stockage des données à éliminer doivent être archivés et, à la fin de la période d'archivage, physiquement détruits.

10.4.2 Les clés USB doivent être nettoyées par reformatage avant de les réutiliser.

10.4.3 Les supports défectueux doivent être éliminés en cas de défauts.

10.5 Procédures de transfert et d'admission

10.5.1 Le transfert par courrier ou autre intermédiaire doit être accusé réception pour la garantie.

11. CONTINUITÉ DES AFFAIRES

11.1 Sauvegarde

11.1.1 Données et logiciels

11.1.1.1 Avoir toujours une copie des données critiques ressentes pour assurer une continuité du travail en cas de problèmes.

11.1.2 Matériel

11.1.2.1 Aucune panne de matériel ne doit être tolérée.

11.1.2.2 Le manque de contrôle du groupe électrogène ne peut être justifié en aucun cas.

11.1.3 Puissance

11.1.3.2 L'équipement, les machines et les systèmes essentiels sont sauvegardés avec des groupes électrogènes.

11.2 Urgences

11.2.1 La liste des urgences possibles devrait être revue au moins une fois par an.

11.2.3 Les ressources pour les actions imprévues doivent être prises en compte lors de l'établissement du budget.

12. GESTION DU CHANGEMENT

12.1 Surveillance de la sécurité

12.1.1 Surveillance opérationnelle

12.1.1.1 Le responsable technique de production devrait contrôler les fiches et les données une fois par semaine.

12.1.1.2 Les performances techniques doivent être surveillées hebdomadairement.

12.1.1.3 En ce qui concerne les incidents de sécurité, les éventuels changements des besoins doivent être identifiés.

12.1.1.4 En cas de modifications techniques, organisationnelles, juridiques ou autres modifications internes ou externes importantes, des modifications des besoins de sécurité y afférentes doivent être identifiées.

12.1.2 Contrôles de sécurité aléatoires

12.1.2.1 Dans les conditions normales la sécurité du groupe électrogène doit être vérifiée régulièrement.

12.1.3 Examen régulier de la sécurité

12.1.3.1 Doit être effectué au moins une fois par an.

12.2 Modification de la politique de sécurité

12.2.1 La politique de sécurité est modifiée, si les résultats de la surveillance de la sécurité l'exigent (voir 12.1).

12.2.2 La politique de sécurité du système d'information est modifiée, si le besoin survient à l'apparition d'un changement dans le référentiel de l'organisme de base.

12.2.3 Les changements de sécurité dus aux changements de la politique de sécurité sont effectués dans un délai d'un mois.

Plan d'action

Pourquoi ?

Contexte : contient des directives et des consignes à suivre pour compléter la PSSI

Buts du plan d'action : détailler les actions à faire pour sécuriser plus les zones de l'entreprise et son site web

Quoi ?		Qui ?	Comment ?	Quand ?		Où ?	Combien ?
Mettre en place un firewall	L'installation d'un pare-feu pour sécuriser les réseaux de l'entreprise	Directeur général	Budget d'achat du firewall et de celui qui l'installera	Avant la mise en ligne du site web	///	L'administration des deux zones	Une seul fois, et le contrôler à chaque fois
Utilisation d'un VPN	Utilisation d'un VPN en cas de connexion hors les réseaux de l'entreprise	Les responsables qui ont accès au site	L'installation d'une application VPN sur ces biens	L'activer Avant l'accès au site	//	sur les biens mobiles des responsables	A chaque utilisation non sécurise
Placer des barreaudages dans l'administration principale	Mettre en place des barreaudages pour sécuriser l'accès à l'administration principale	Responsable d'administration principale	L'achat et le placement des barreaudages	Dès la validation de la proposition et le déblocquement du budget	///	Le bâtiment de l'administration principale	Une seule fois

Tableau 4 : le plan d'action

Chapitre 05 : Conception d’un site en respectant la politique réalisée

Chapitre 05 : conception d'un site en respectant la politique réalisée

1. Introduction

La société HUBBARD ALGERIE se situe sur 2 sites différents, le premier situé à Ain oussara qui comporte l'administration principale ainsi que le couvoir, le deuxième site qui comporte une administration, 2 poussinières ainsi que 4 sites de production et une usine de fabrication d'aliment.

Dans leur travail quotidien y'a une très forte relation de travail entre la production et le couvoir, et les deux doivent rendre compte aux responsable technique de production pour vérifier les données. Jusqu'à aujourd'hui les données sont enregistrées sur du papier et la transmission des données se fait manuellement. Le responsable technique de production a constaté pendant un certain temps une différence des données entre le bon de livraison remplit par le responsable de la production et la fiche journalière remplie par le responsable du couvoir.

De ce fait on leurra proposée de leur faire un site web pour contrôler la transmission de données d'une manière sécurisée afin de déterminer où est le problème maintenant et d'on profiter dans l'avenir pour leur faciliter le travail.

2. Présentation du projet

Notre site se compose de 5 espaces de travail, présenté comme suit :

Acteur	Fonction
Responsable de production	Connecter chaque jour pour remplir ses bons de livraison
Responsable du couvoir	Connecter à son tour pour remplir sa fiche journalière.

Responsable technique	Connectera chaque jour pour vérifier et comparer les données enregistrer et rendre son rapport
Responsable d'administration	Qui a le droit de crée des espaces aux nouveau responsables, de vérifier la liste des responsables et de bloquer un espace on cas de problème
L'administrateur (super admin)	Ajouter d'autres administrateurs et des responsables d'administration.

Tableau 5 : espace utilisateur

3. langage de modélisation UML

Le développent de n'importe quel système d'information nécessite une démarche très importante dans le cycle de vie d'un logiciel, et la modélisation en pratique est important dans les développements des logiciels, dans notre projet nous choisit le langage de modélisation UML.

3.1 UML

UML (*Unified Modeling Language*) est né de la fusion des trois méthodes qui ont influencé la modélisation objet au milieu des années 90 : OMT, Booch et OOSE. Il s'agit d'un compromis qui a été trouvé par une équipe d'experts : Grady Booch, James Rumbaugh et Ivar Jacobson. UML est à présent un standard défini par l'Object Management Group (OMG) [15].

UML est un langage visuel constitué d'un ensemble de schémas, appelés des diagrammes, qui donnent chacun une vision différente du projet à traiter. UML nous fournit donc des diagrammes pour représenter le logiciel à développer : son fonctionnement, sa mise en route, les actions susceptibles d'être effectuées par le logiciel, etc., réaliser ces diagrammes revient donc à modéliser les besoins du logiciel à développer [18].

UML est constitué de 13 diagrammes officiels. Ces diagrammes sont tous réalisés **à partir du besoin des utilisateurs** mais seul neuf qui sont utilisés régulièrement :

- Diagramme de cas d'utilisation
- Diagramme de classe
- Diagramme de séquence
- Diagramme d'objet
- Diagramme d'état
- Diagramme de collaboration
- Diagramme de composants
- Diagramme d'activité
- Diagramme de déploiement.

Dans le cadre de notre conception, nous utilisons seulement les diagrammes suivants :

- Le diagramme de cas d'utilisation,
- Le diagramme de séquence,
- Le diagramme de classe.

3.1.1 Conception détaille

La conception de notre site web est décrite avec les diagrammes UML suivant :

3.1.1.1 diagrammes de cas d'utilisation :

Un cas d'utilisation est la description d'un ensemble de séquences d'actions qu'un système effectue pour produire un résultat observable à un acteur. Un cas d'utilisation représente une exigence fonctionnelle de votre système dans son ensemble. Les diagrammes de cas d'utilisation décrivent ce qu'un système fait du point de vue d'un observateur externe. L'accent est mis sur ce qu'un système fait, plutôt que sur la façon dont il le fait [19].

Les diagrammes de cas d'utilisation sont étroitement connectés aux scénarios. Un scénario est un exemple de ce qui arrive quand quelqu'un interagit avec le système.

Concevez une hiérarchie de cas d'utilisation :

1. En principe, vous commencez à un niveau élevé et spécifiez les principaux cas d'utilisation du système.

2. Vous déterminez ensuite les cas d'utilisation du système principal à un niveau plus granulaire.

3. Lorsque vous avez atteint le niveau désiré de granularité, il est utile d'avoir une méthode pratique de développement ou de réduction des cas d'utilisation pour comprendre la portée des vues des cas d'utilisation du système et leurs relations [19].

Les diagrammes de cas d'utilisation de notre site web sont :

- Les acteurs de notre site web

Nous avons 5 acteurs dans ce site web :

- Responsable de production
- Responsable du couvoir
- Responsable technique
- Responsable d'administration
- L'administrateur (super admin)

+ Diagramme de cas d'utilisation des activités <<super admin>>

Voici ci-dessous le diagramme de cas d'utilisation des taches du super admin

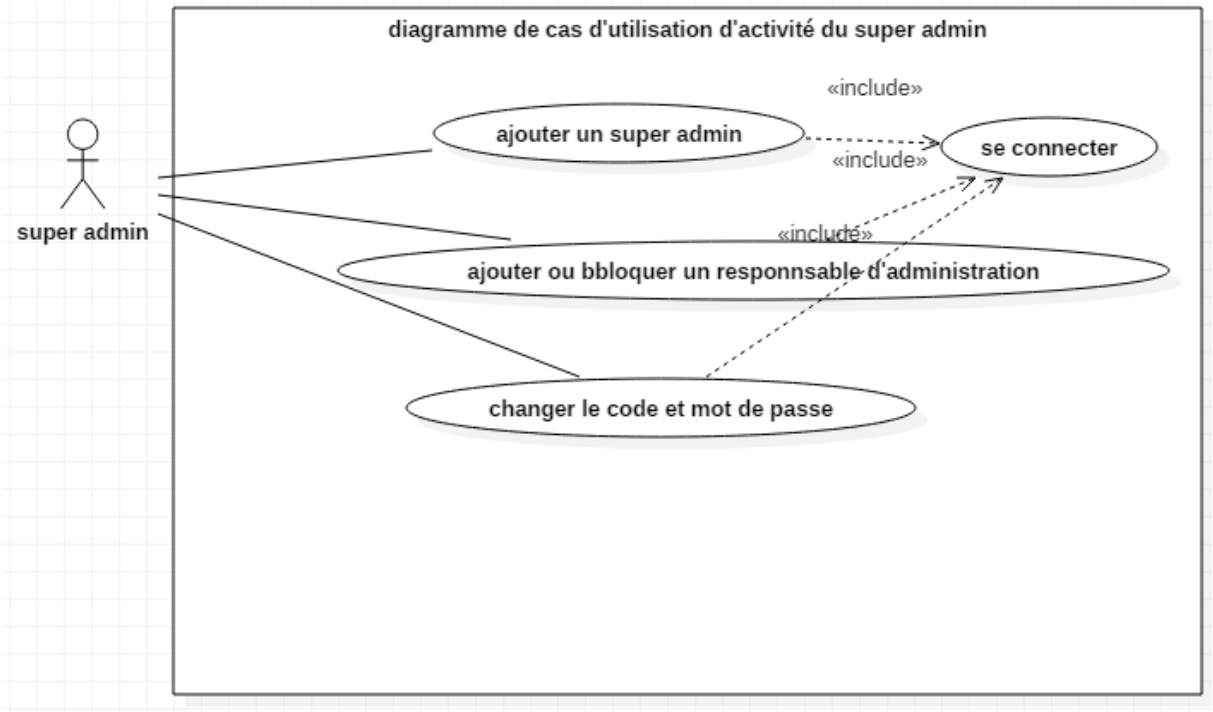


Figure 4 : diagramme de cas d'utilisation de super admin

+Diagramme de cas d'utilisation des activités <<responsable administrateur >>

Voici ci-dessous le diagramme de cas d'utilisation des taches du responsable administrateur

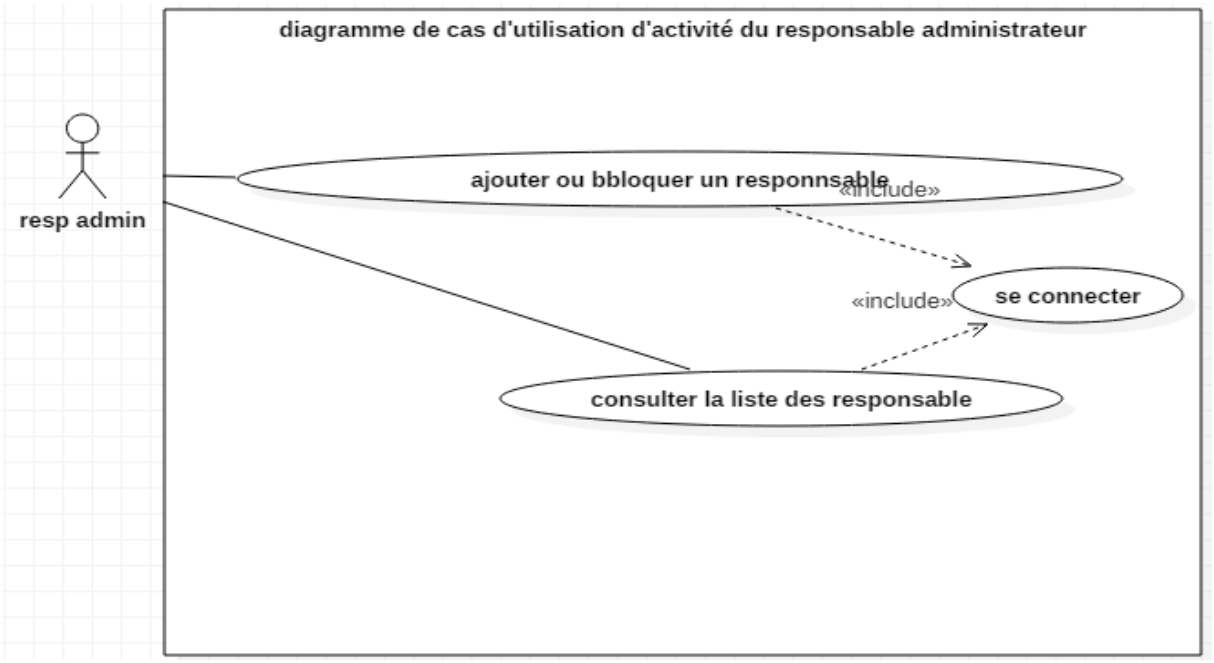


Figure 5 : diagramme de cas d'utilisation de responsable administration

+Diagramme de cas d'utilisation des activités <<responsable technique>>

Voici ci-dessous le diagramme de cas d'utilisation des taches du responsable technique

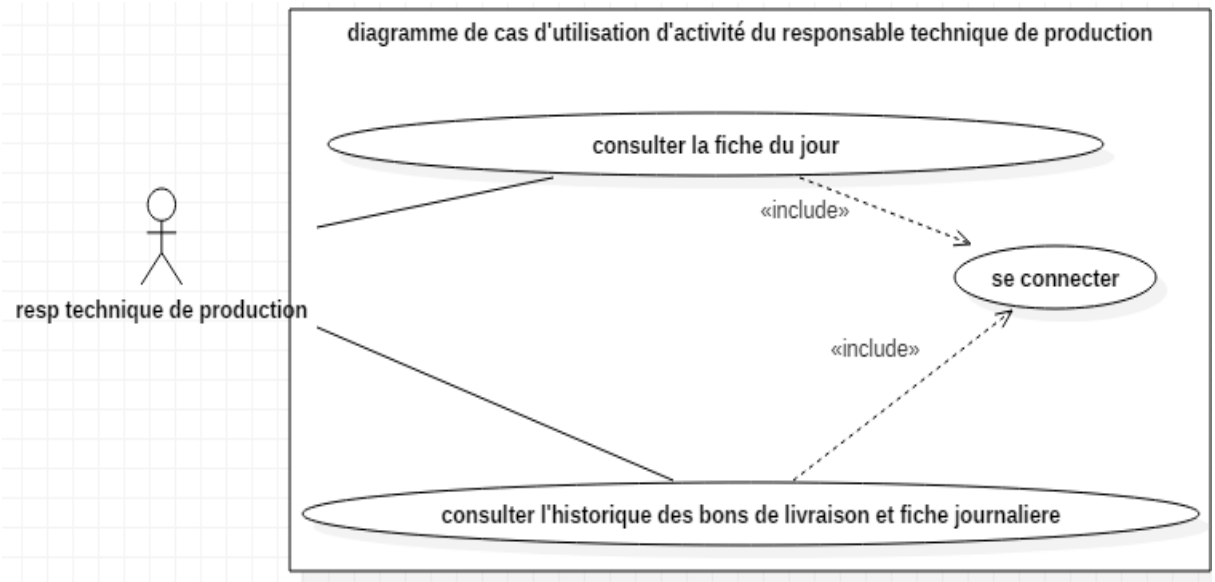


Figure 12 : diagramme de cas d'utilisation de responsable technique

+Diagramme de cas d'utilisation des activités <<responsable couvoir >>

Voici ci-dessous le diagramme de cas d'utilisation des taches du responsable du couvoir

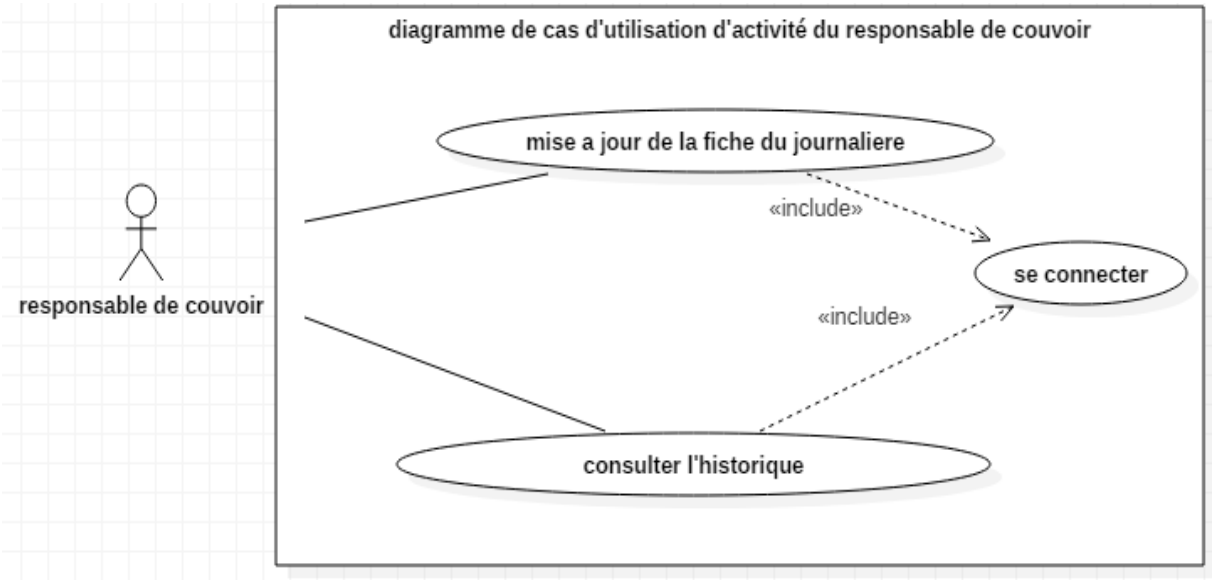


Figure 7 : diagramme de cas d'utilisation de responsable couvoir

+Diagramme de cas d'utilisation des activités <<responsable production >>

Voici ci-dessous le diagramme de cas d'utilisation des taches du responsable de production

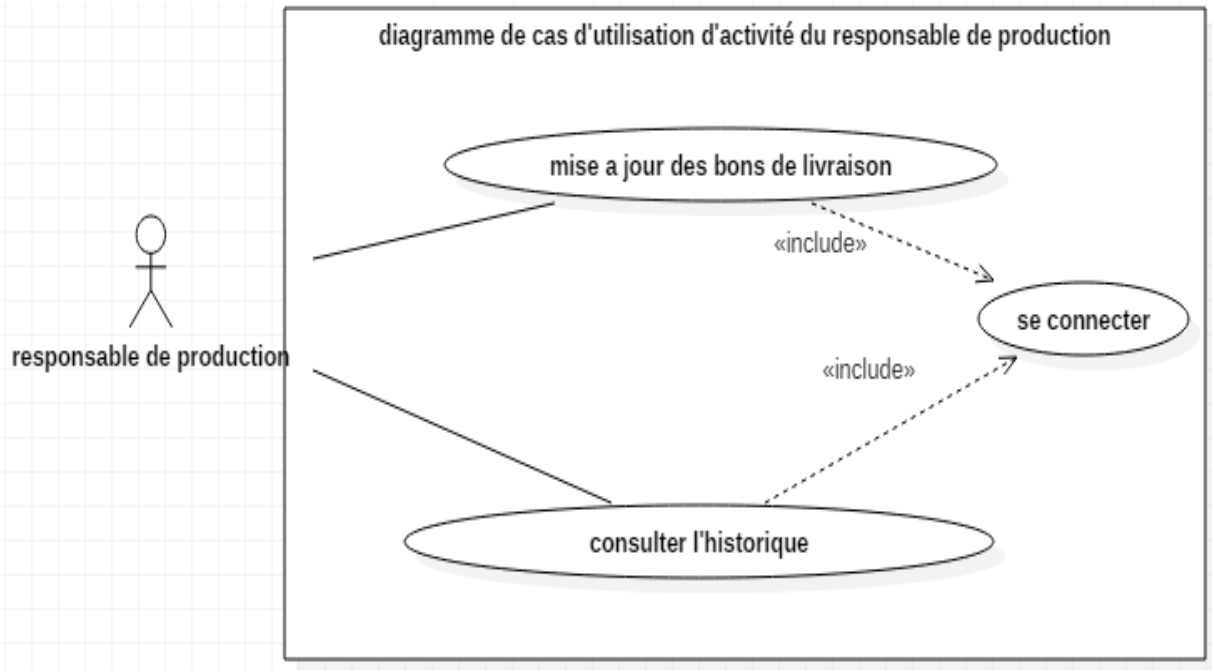


Figure 8 : diagramme de cas d'utilisation de responsable production

3.1.1.2 Diagramme de séquence :

Un diagramme de séquence est un diagramme UML (Unified Modeling Language) qui représente la séquence de messages entre les objets au cours d'une interaction. Un diagramme de séquence comprend un groupe d'objets, représentés par des lignes de vie, et les messages que ces objets échangent lors de l'interaction. [19].

Les diagrammes de séquence de notre site web sont :

- **Diagramme de séquence <<connexion >>**

Voici ci-dessous le diagramme de séquence de connexion

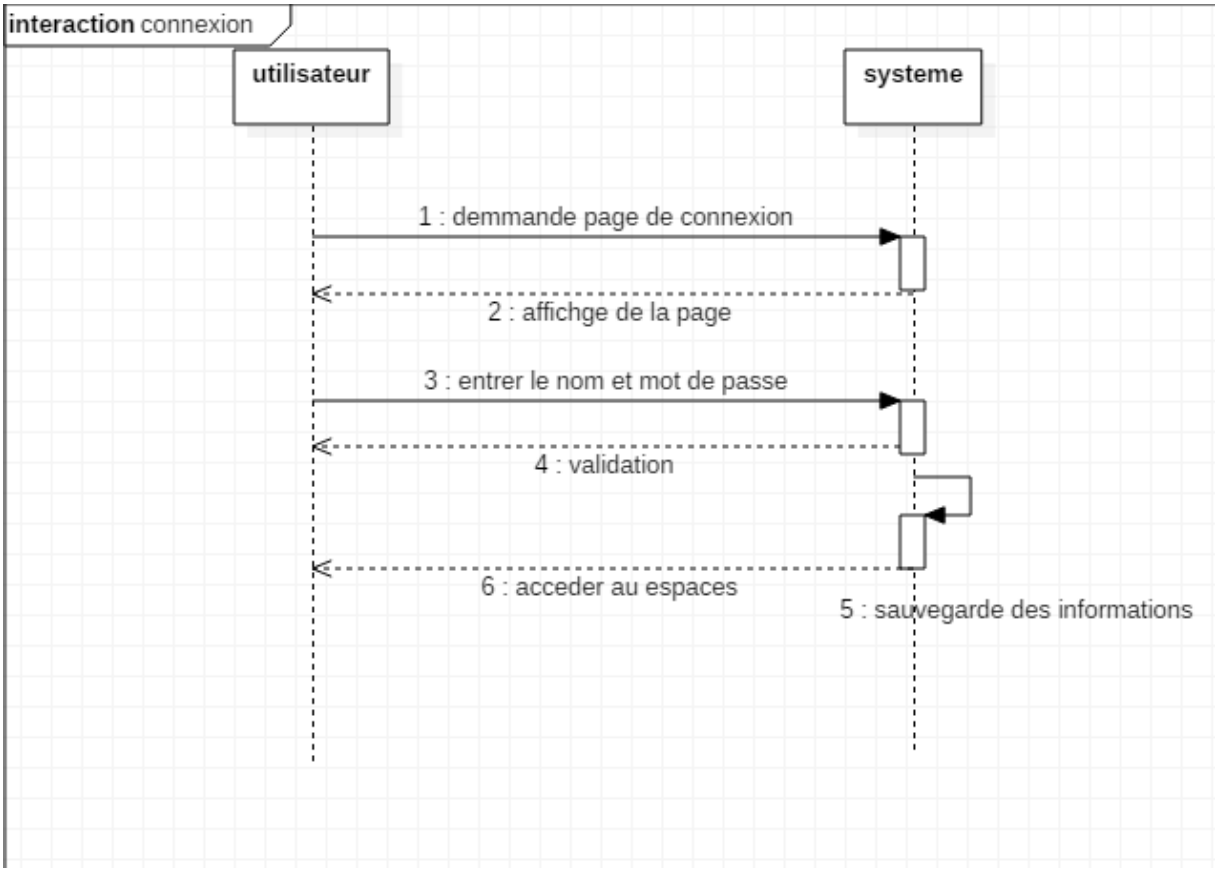


Figure 9 : diagramme de séquence connexion

- **Diagramme de séquence << Administrateur >>* créer les membres**

Voici ci-dessous le diagramme de séquence pour la création des membres

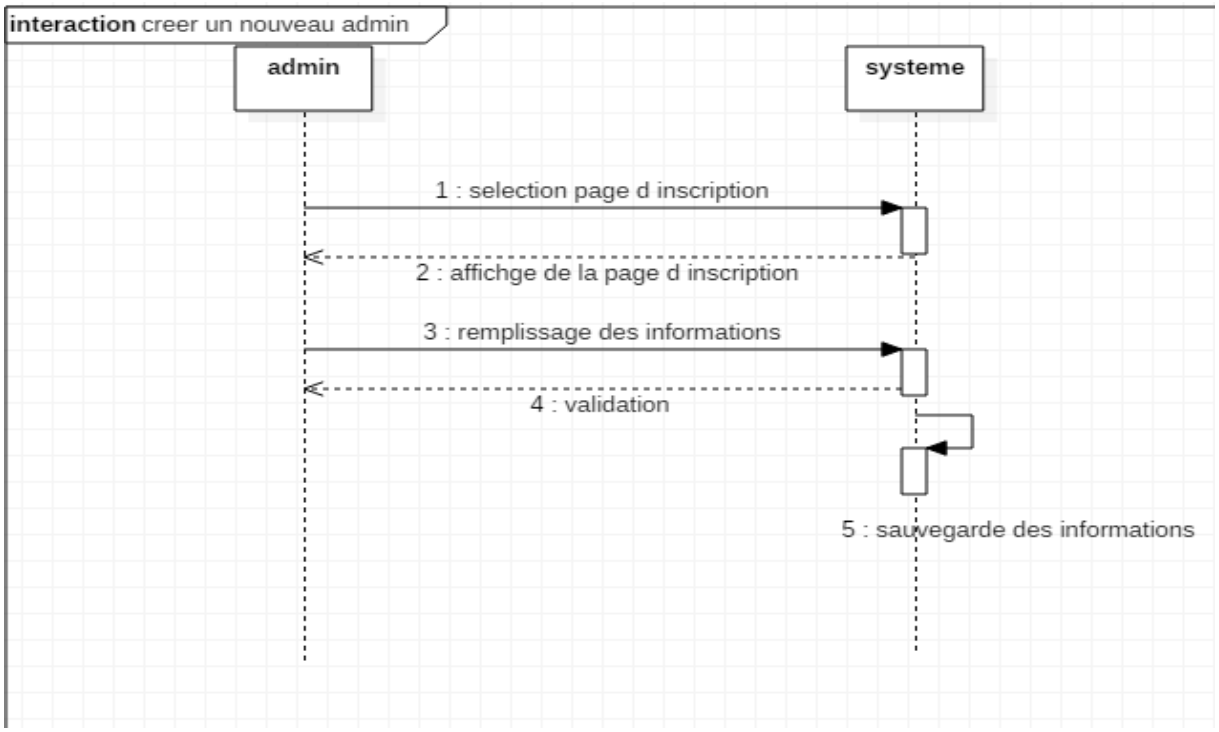


Figure 10 : diagramme de séquence créer un nouveau membre

- **Diagramme de séquence << responsable de production >>**

Voici ci-dessous le diagramme de séquence du responsable de production

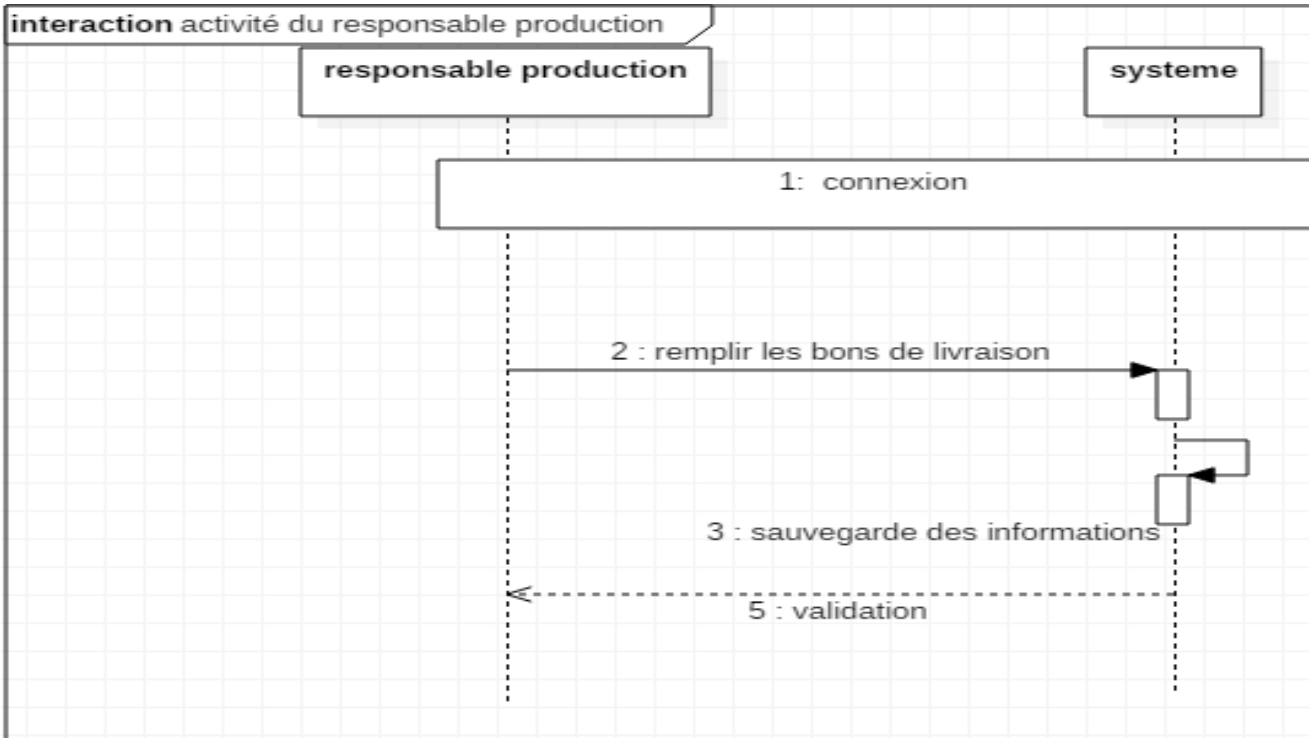


Figure 11 : diagramme de séquence tache de responsable de production

- **Diagramme de séquence << responsable technique>>**

Voici ci-dessous le diagramme de séquence du responsable technique

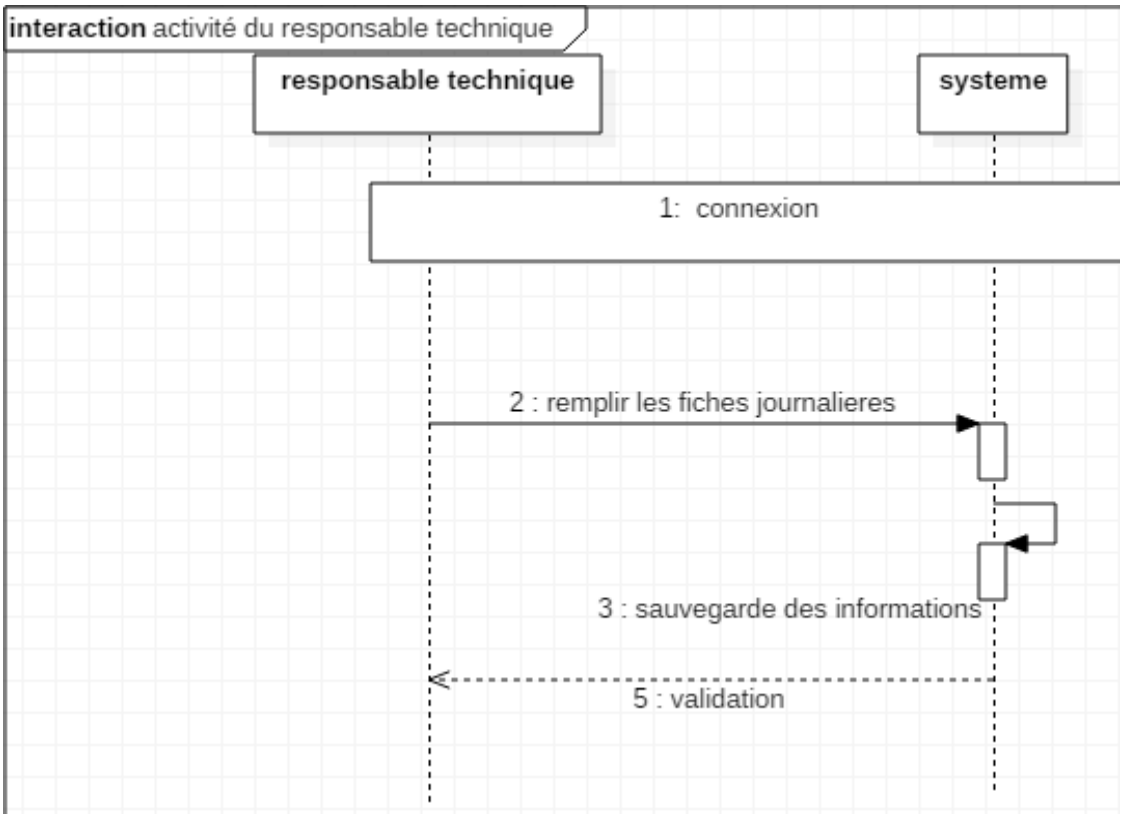


Figure 12 : diagramme de séquence tache de responsable technique

3.1.1.3 diagrammes de classes :

Un diagramme de classes fournit une vue globale d'un système en présentant ses classes, interfaces et collaborations, et les relations entre elles. Les diagrammes de classes sont statiques : ils affichent ce qui interagit mais pas ce qui se passe pendant l'interaction.

En notation UML, une classe est représentée sous la forme d'un rectangle divisé en plusieurs parties : le nom de la classe, les attributs (champs), les opérations (méthodes) [20].

Dans la Modélisation, le rectangle de la classe est divisé en compartiments distincts pour les champs, les classes internes, les propriétés, les opérations.

- **Diagramme de classe**

voici-dessous le diagramme de classe des tables représentées dans le site

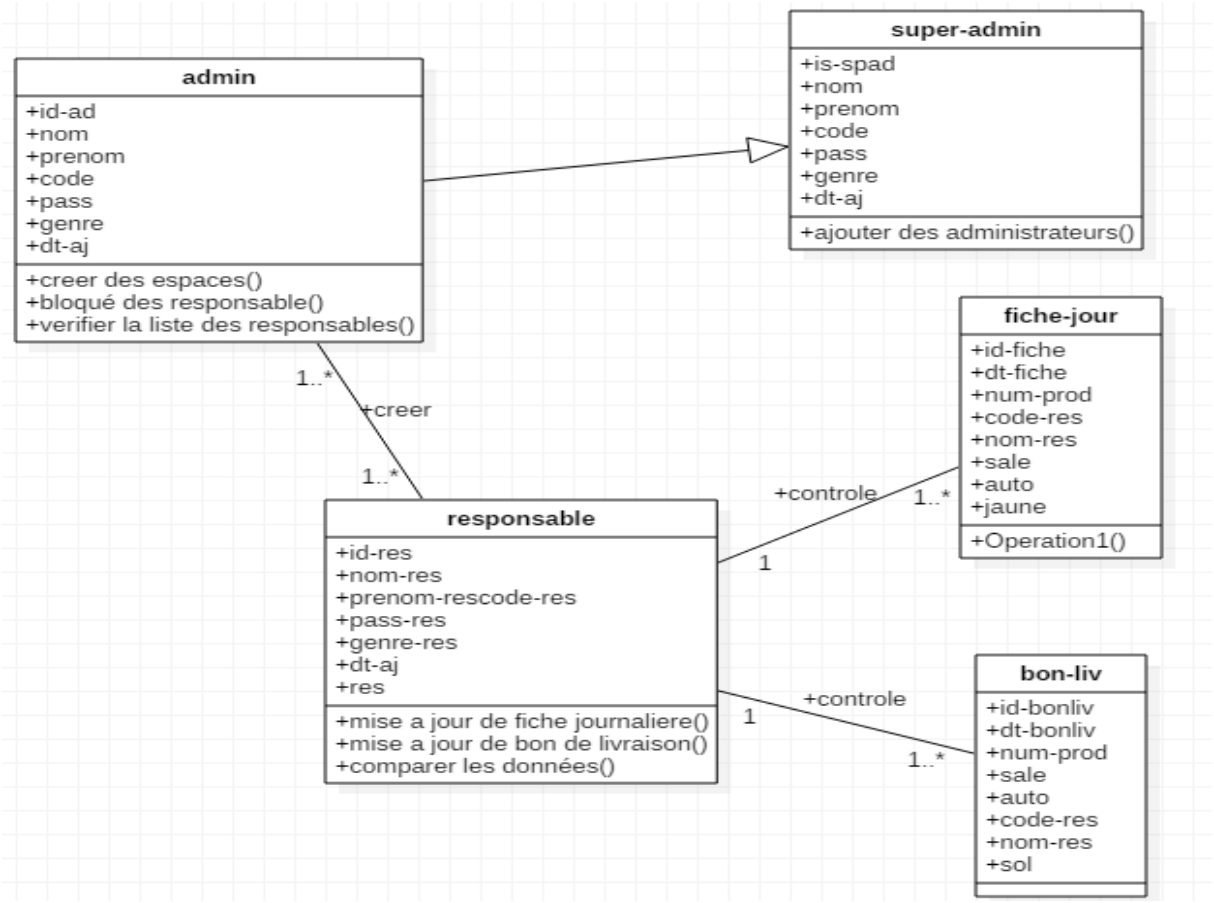


Figure 13 : diagramme de classe des tables représentées dans le site

❖ **Le dictionnaire de données**

Code	Signification	Type
Admin		
Id-ad	L'identifiant de l'admin	Int
Nom	Nom de l'admin	Varchar
Prénom	Prénom de l'admin	Varchar
Code	code de l'admin	Varchar
Pass	Mot de passe d'admin	Varchar
Genre	Genre d'admin	Varchar
Dt-aj	La date d'ajout	Date
Super_admin		
Id-spad	L'identifiant de super admin	Int
Nom	Nom du super admin	Varchar
Prenom	Prénom du super admin	Varchar
Code	codedu super admin	Varchar
Pass	Mot de passe du super admin	Varchar
Genre	Genre du super admin	Varchar
Dt-aj	La date d'ajout	Date
Res-tech		
Id-perso	L'identifiant de responsable technique	Int
Nom-res	Nom de responsable technique	Varchar
Prenom-res	Prénom de responsable technique	Varchar
Code-res	Code de responsable techniqueadmin	Varchar
Pass-res	Mot de passe de responsable technique	Varchar
Genre-res	Genrede responsable technique	Varchar
Dt-aj	La date d'ajout	Date
Res	Responsable	Varchar

Res-prod		
Id-pouss	L'identifiant de responsable poussinière	Int
Nom-pouss	Nom de responsable poussinière	Varchar
Prenom-pouss	Prénom de responsable poussinière	Varchar
Code-pouss	code de responsable poussinière	Varchar
Pass-pouss	Mot de passe de responsable poussinière	Varchar
Genre-pouss	Genre de responsable poussinière	Varchar
Dt-aj-pouss	La date d'ajout	Date
Res	Responsable	Varchar
Res_couv		
Id-couv	L'identifiant de responsable couvoire	Int
Nom-couv	Nom de responsable couvoire	Varchar
Prenom-couv	Prénom de responsable couvoire	Varchar
Code-couv	code de responsable couvoire	Varchar
Pass-couv	Mot de passe de responsable couvoire	Varchar
Genre-couv	Genre de responsable couvoire	Varchar
Dt-aj-couv	La date d'ajout	Date
Res	Responsable	Varchar
Fiche-jour		
Id-fiche	Identifiant	Int
Dt-fiche	Date de fiche	Date
Num-prod	Num produit	Varchar
Entre		Int
Sale		Varchar
Auto		Int

Sol		Int
Jaune		Int
Tri		Int
Code-res	Code responsable	Varchar
Nom-res	Nom responsable	Varchar
Prenom-res	Prenom responsable	Varchar
Bon-liv		
Id-bonliv	Identifiant de bon de livraison	Int
Dt-bonliv	Date de bon de livraison	Date
Sale		Varchar
Auto		Int
Sol		Int
Jaune		Int
Tri		Int
Code-res	Code responsable	varchar
Nom-res	Nom responsable	varchar
Prenom-res	Prenom responsable	Varchar
Num-prod	Numero de produit	Varchar

Tableau 6 : table des données

4. Réalisation du site web

Nous allons développer un site web, pour cela nous allons on décrit les logiciels et les langages de programmation utilisés, qui nous ont permis la réalisation de ce travail et qu'on a utilisé et on évoquera le système d'exploitions, ainsi nous présenterons quelques exemples des interfaces représentant la plateforme qui ont été réalisées.

4.1 Environnement de développement

Dans cette partie nous allons présenter chacun des logiciels de programmation, langage de programmation, logiciel de traitement d'image qu'on a utilisé le système d'exploitions.

4.1.1 Le système d'exploitation

L'environnement de base pour ce travail est le système d'exploitation Windows 8.1, pour obtenir des performances de fa çon plus facile, et il est li é à la machine. Donc Windows 8.1, fournit un travail plus efficace, qui offre la fiabilité et l'efficacité. Dans cette partie on va donner quelque d éfinition sur les langages de programmations qu'on va utiliser pour la r éalisation de notre travail qui sont les suivant :

4.1.2 PHP

HyperText Préprocesseur, plus connu sous son sigle PHP (acronyme récursif), est un langage de programmation principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. PHP est un langage impératif orienté objet [21].

PHP a permis de cr éer un grand nombre de sites web c él èbres, comme Facebook, Wikip édia, etc. Il est consid ér écomme la base de la cr éation des sites Internet dits dynamiques [21].

4.1.3 HTML (Hyper Text Markup Language)

C'est un langage de balise permettant le codage des pages WEB. HTML permet également de structurer sémantiquement et de mettre en forme l'interface des sites, d'inclure des ressources multim édias telles que les images, les formulaires de saisie, et les programmes informatiques. Il permet de cr éer des documents interop érables avec des équipements tr ès variés de manière conforme aux exigences de l'accessibilité du web. Il est souvent utilis é conjointement avec des langages de programmation (PHP, JavaScript…) et des formats de pr ésentation (feuilles de style en cascade) [21].

4.1.4 JavaScript

Est un langage de script orienté objet principalement utilisé dans les pages HTML. À l'opposé des langages serveur (qui s'exécutent sur le site), JavaScript est exécuté sur l'ordinateur de l'internaute par le navigateur lui-même. Ainsi, ce langage permet une interaction avec l'utilisateur en fonction de ses actions (lors du passage de la souris au-dessus d'un élément, du redimensionnement de la page…) [21].

4.1.5 CSS

Les feuille de style en cascade, généralement appelées CSS de langage informatique qui décrit la présentation des documents HTML et XML. Les standards définissant CSS sont publiés par le World Wide Web Consortium (W3C). Introduit au milieu des années 1990, CSS devient couramment utilisé dans la conception des sites web et bien pris en charge par les navigateurs web dans les années 2000 [21].

4.1.6 XAMPP

XAMPP signifie Cross-Platform (X), Apache (A), MySQL (M), PHP (P) et Perl (P).C'est un ensemble de logiciels permettant de mettre en place facilement un serveur Web et un serveur FTP. Il s'agit d'une distribution de logiciels libres (X Apache MySQL Perl PHP) facile à installer offrant une bonne souplesse d'utilisation permettent l'exploitation d'un serveur Apache, de l'SGBD MySQL et l'interpréteur PHP. XAMPP est également multi plate-forme, ce qui signifie qu'il fonctionne aussi bien sur Linux, Mac et Windows.

4.1.7 MySQL

Est un système de gestion de bases de données relationnelles (SGBDR). Il est distribué sous une double licence GPL et propriétaire [21].

Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public (applications web principalement) que par des professionnels, en concurrence avec Oracle, Informix et Microsoft SQL Server [21].

4.1.8 Bootstrap

Bootstrap est une collection d'outils utiles à la création du design de sites et d'applications web. C'est un ensemble qui contient des codes HTML et CSS, des formulaires, boutons, outils de navigation et autres éléments interactifs, ainsi que des extensions JavaScript en option.

4.1.9 Sublime text

Sublime Text 2, est un éditeur de texte avancé qui permet sur Mac, Windows et Linux, d'éditer du texte, mais aussi des scripts [22].

5. présentation des interfaces de notre site web

Au démarrage de l'application, le système affiche une interface qui représente la page d'accueil de notre application. A travers cette interface les acteurs peuvent utiliser le système chacun selon ses droits. Nous donnons une description pour chaque fenêtre ce qui concerne les différentes interfaces que constituent notre site Web.

- **Page d'accueil du site**

Cette page ci-dessous représente la page d'accueil du site web

Figure 14 : page d'accueil du site.

- **Page de connexion**

Cette page présente la page d'authentification qui permet aux utilisateurs d'accéder à leur tableau de bord.

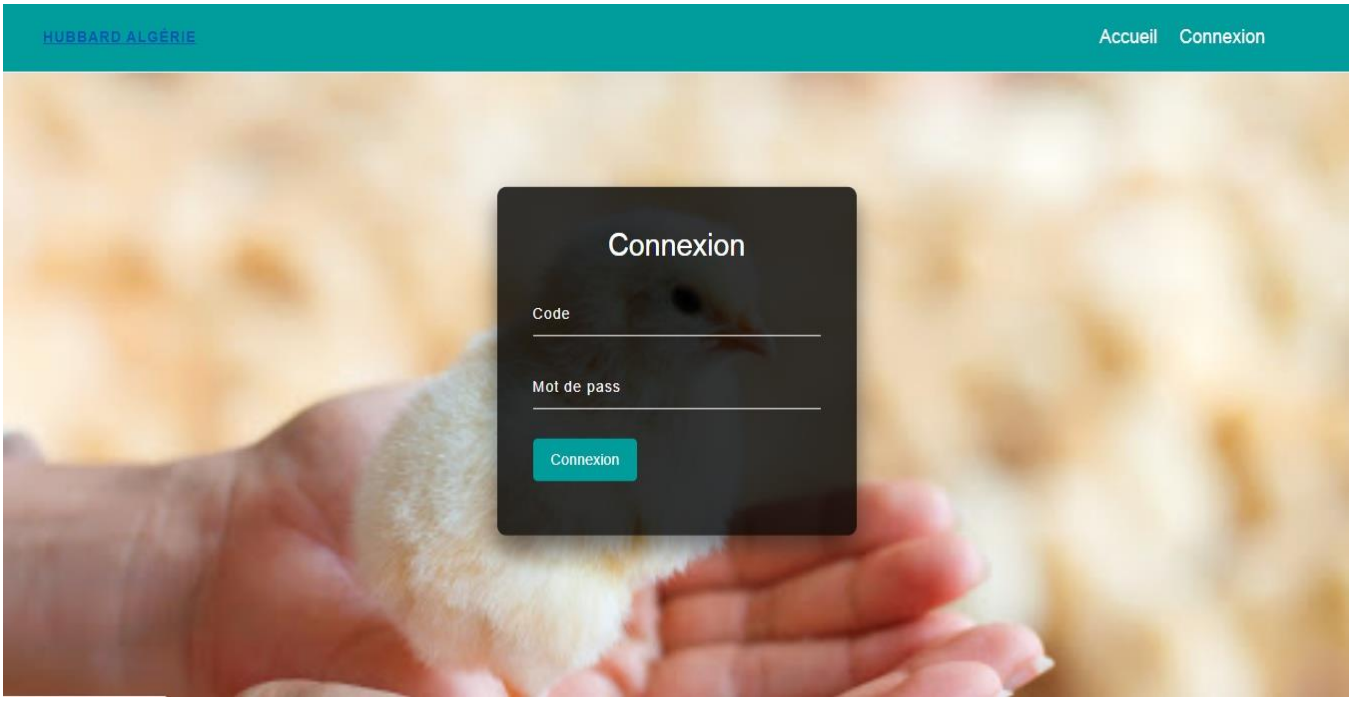


Figure 15 : Page de connexion.

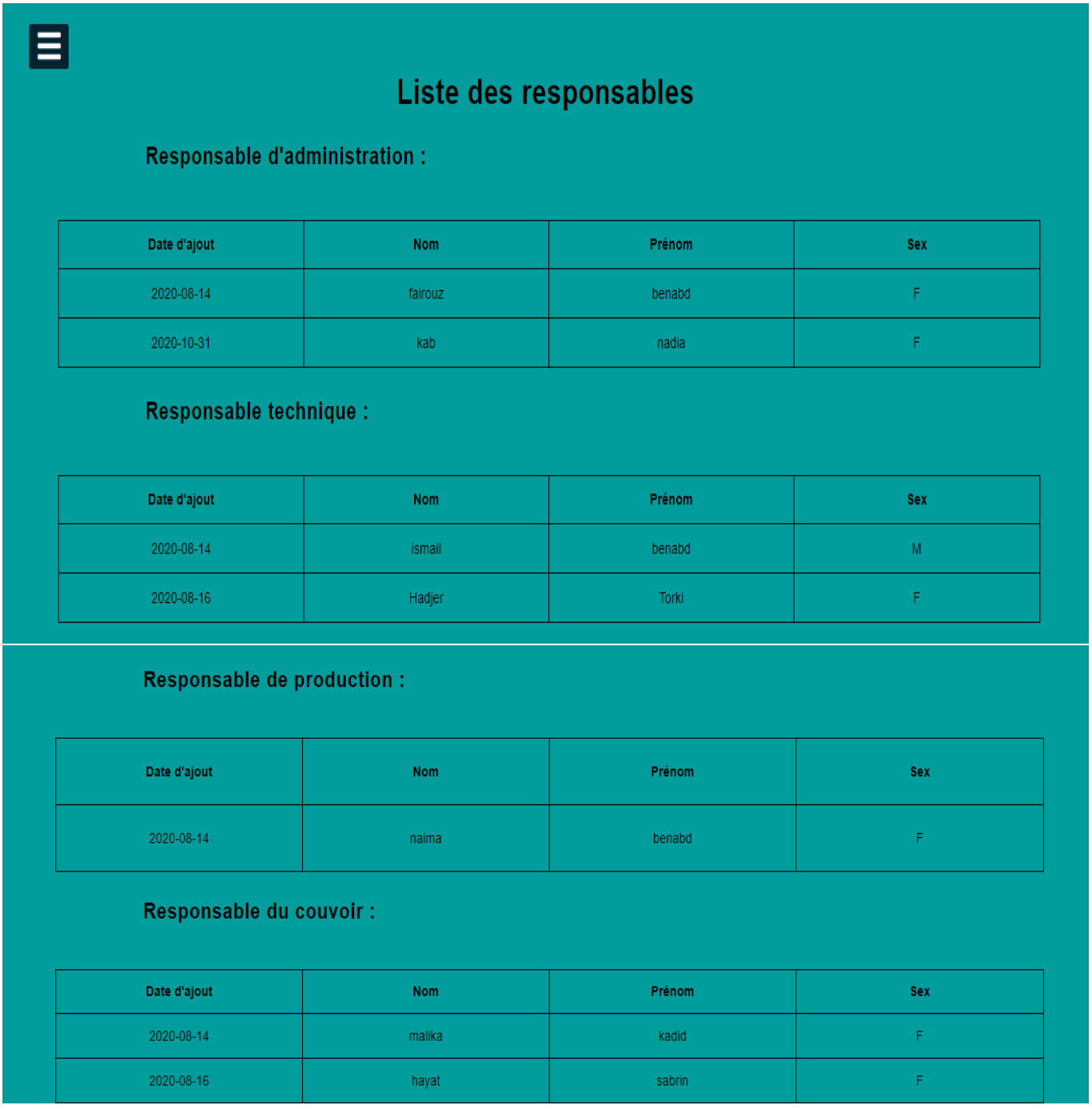
- **Tableau de bord des utilisateurs :**

Cette page représente le tableau de bord des utilisateurs. Ils ont le même tableau de bord sauf que le menu bar il change d'un espace utilisateur a un autre.

Figure 16 : Tableau de bord.

- **Page de la liste des responsables :**

Cette page ci-dessous représente la liste des responsables de l'entreprise.



Liste des responsables

Responsable d'administration :

Date d'ajout	Nom	Prénom	Sex
2020-08-14	fairouz	benabd	F
2020-10-31	kab	nadia	F

Responsable technique :

Date d'ajout	Nom	Prénom	Sex
2020-08-14	ismail	benabd	M
2020-08-16	Hadjer	Torki	F

Responsable de production :

Date d'ajout	Nom	Prénom	Sex
2020-08-14	naima	benabd	F

Responsable du couvoir :

Date d'ajout	Nom	Prénom	Sex
2020-08-14	malika	kadid	F
2020-08-16	hayat	sabrin	F

Figure 18: la liste des responsables.

- **Pages d'ajout d'un administrateur d'un responsable d'administration ou d'un responsable de site :**

Ces pages ci-dessous contient le formulaire a remplir pour ajouter un nouveau utilisateur

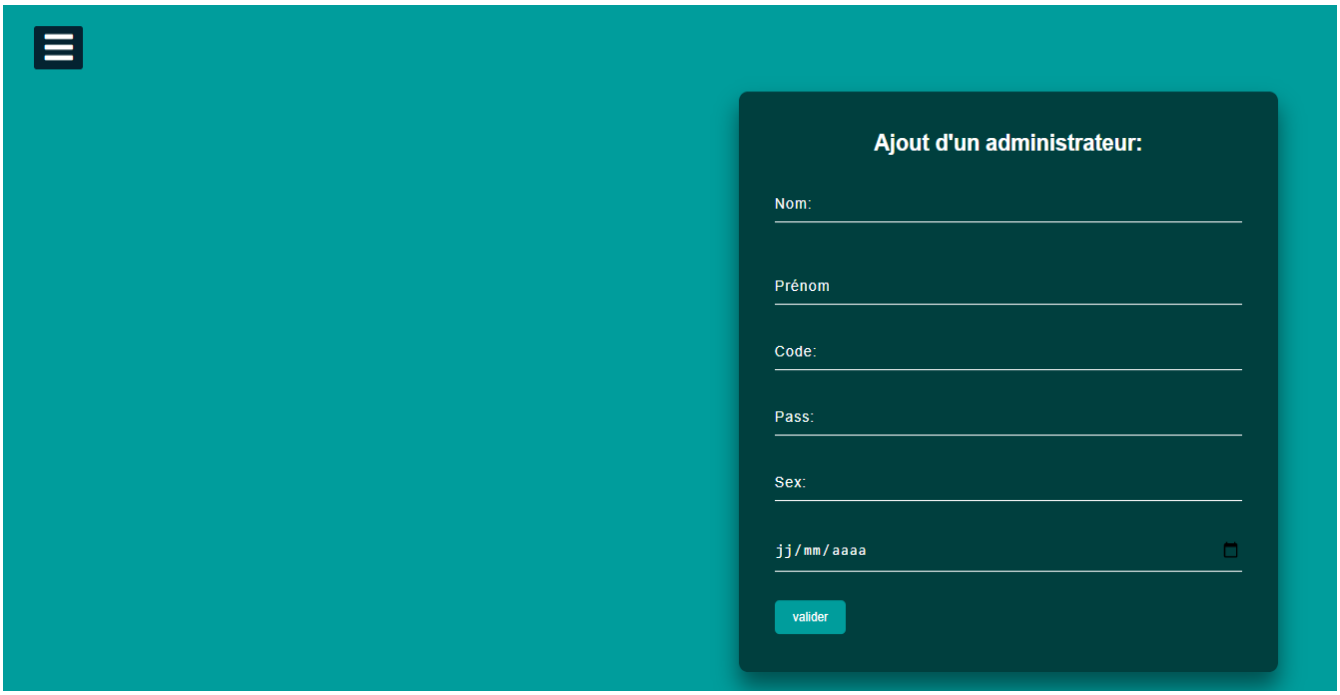


figure 19: page d'ajout d'un administrateur.

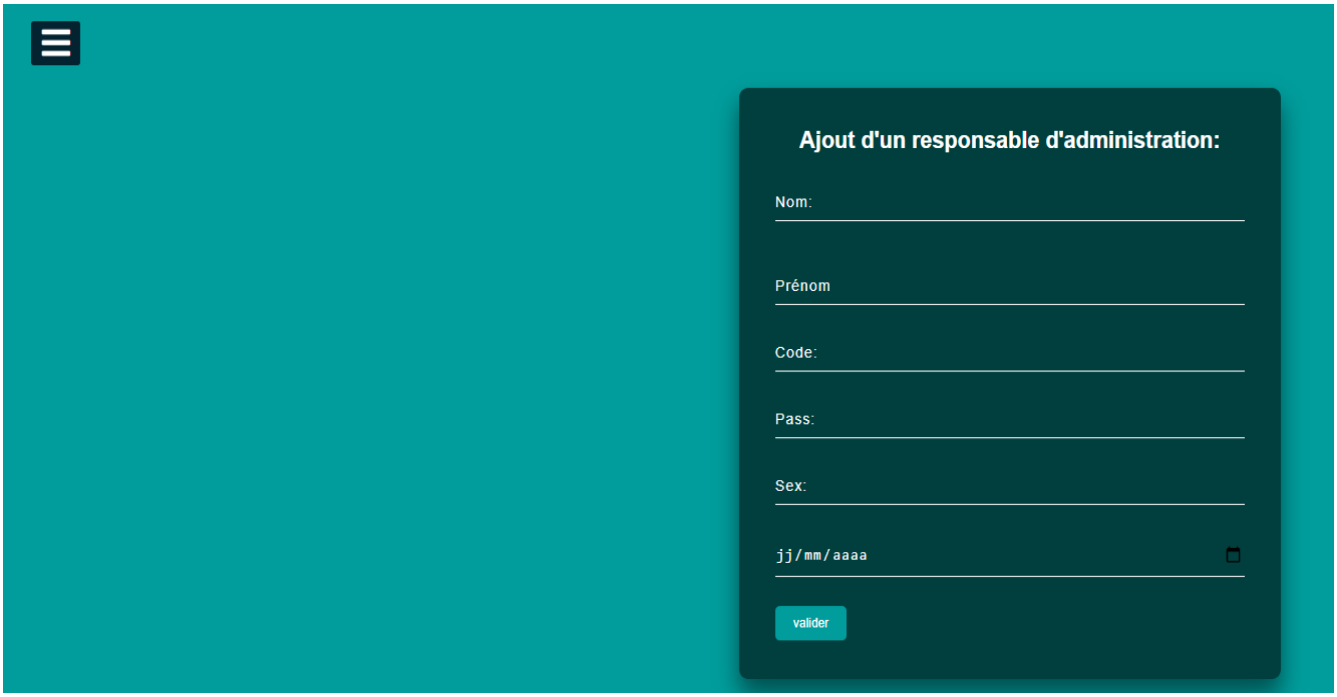


Figure 20: page d'ajout d'un responsable d'administration.

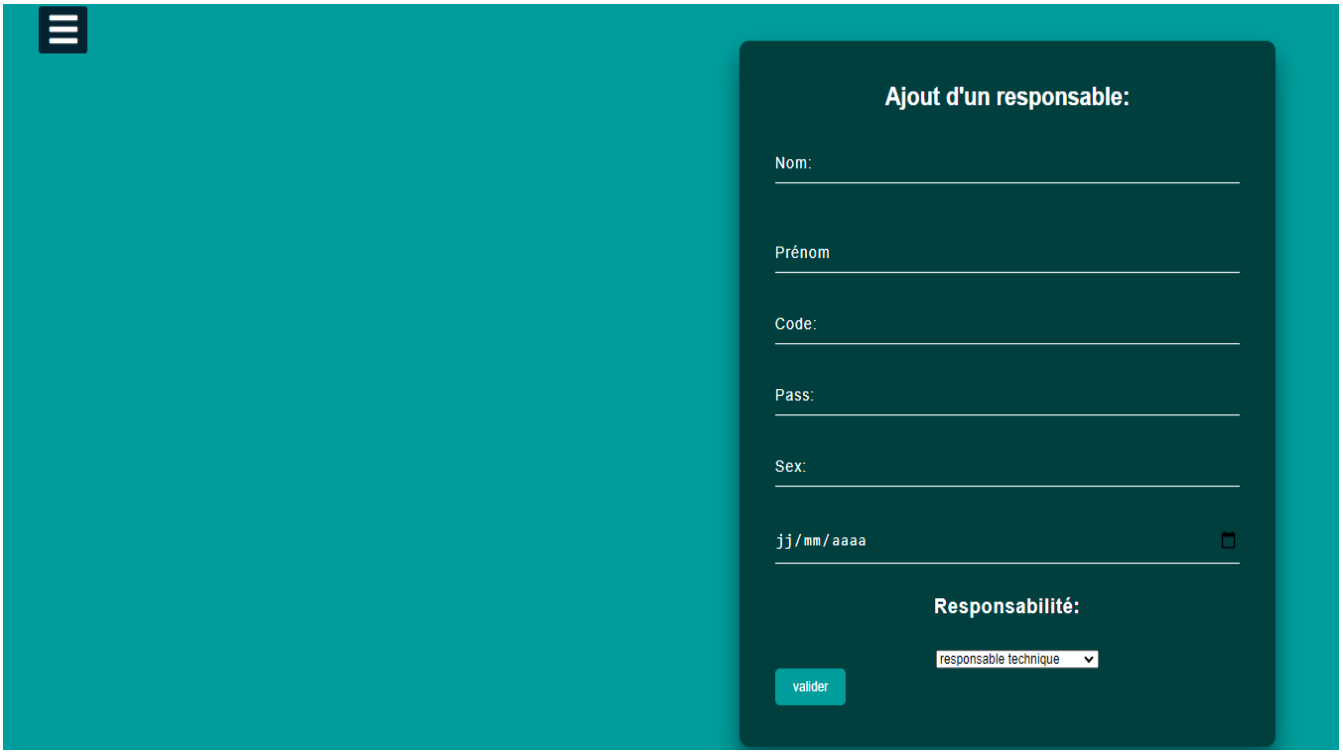


Figure 21 : page d'ajout d'un responsable de site

- **Pages de modification du code et mot de passe :**

Cette page ci-dessous représente la page de la modification du code et mot de passe de l'administrateur

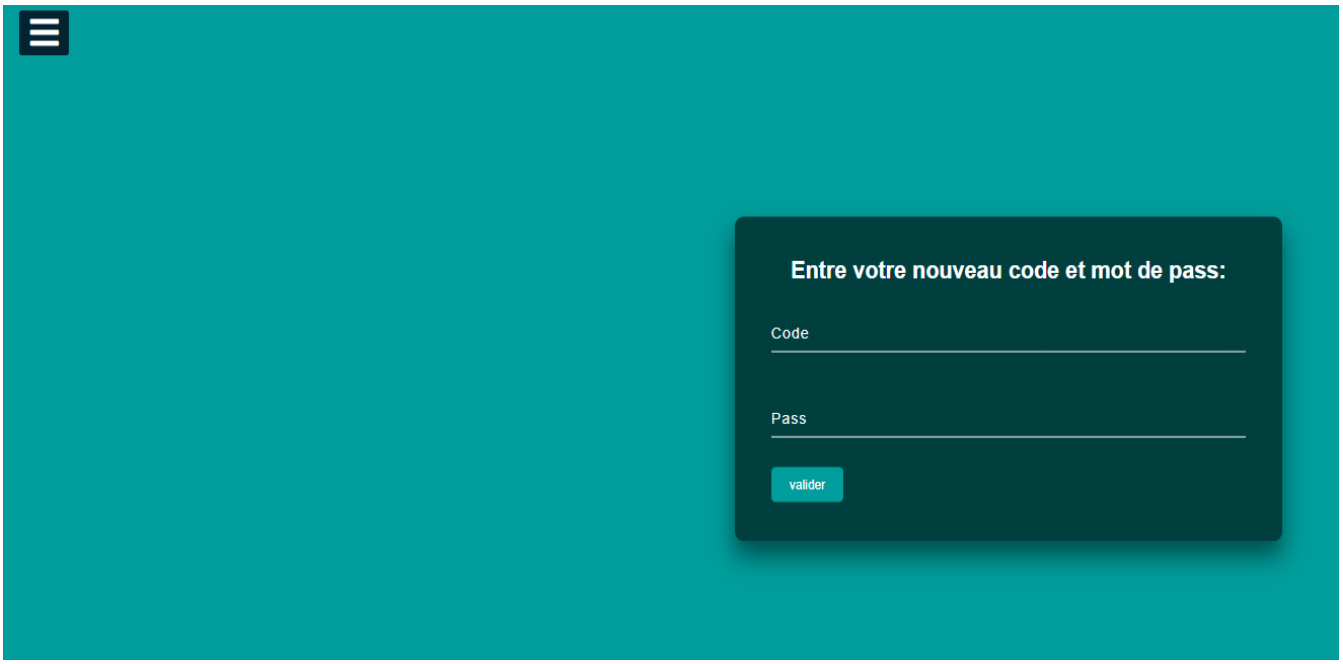


Figure 22 : page de modification du code et mot de passe de l'administrateur.

Cette page ci-dessous représente la page de la modification du code et mot de passe d'un responsable

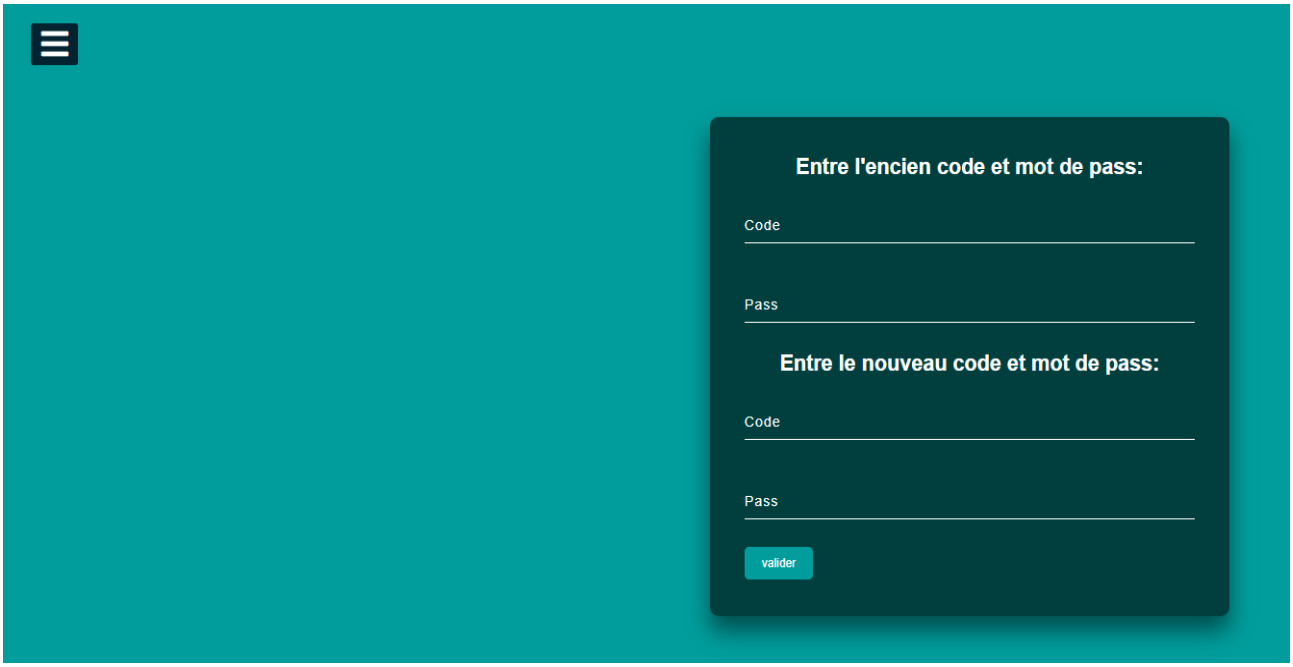


Figure 23: page de modification du code et mot de passe d'un responsable.

- **Pages de fiche journalière et l'historique d'un responsable du couvoir :**

Cette page ci-dessous représente la fiche journalière remplit chaque jour par le responsable du couvoir.

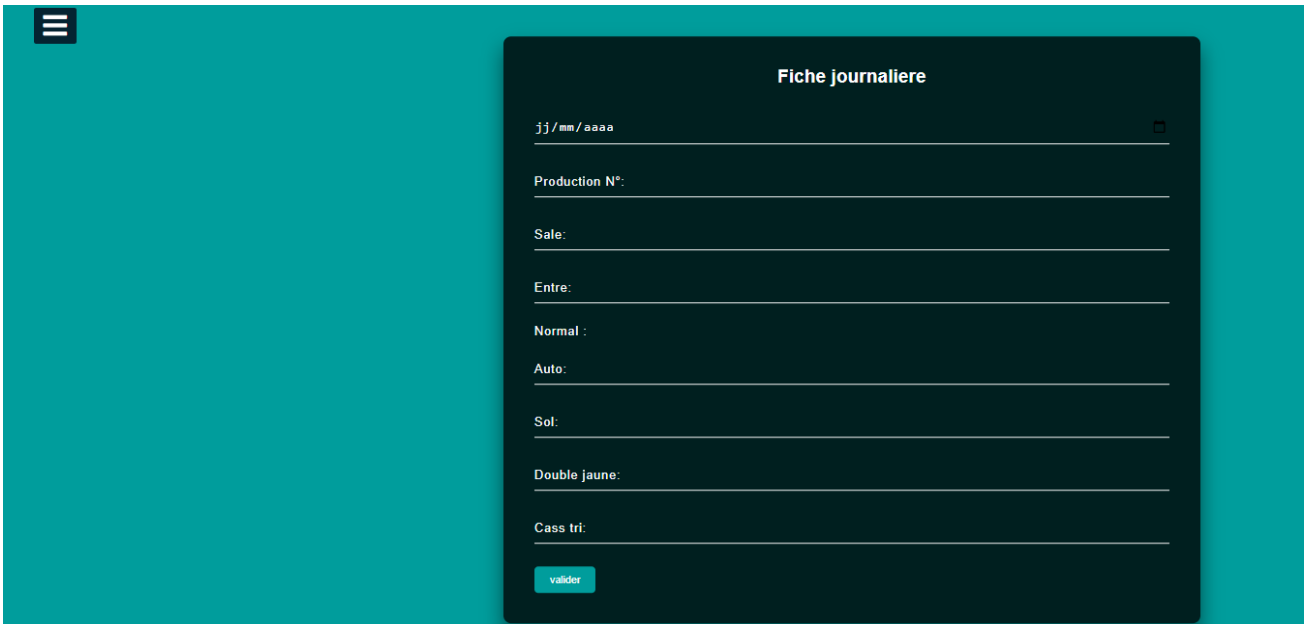


Figure 24 : Fiche journalière.

Cette page représente ci-dessous l'historique des fiches journalières du responsable de couvoir.

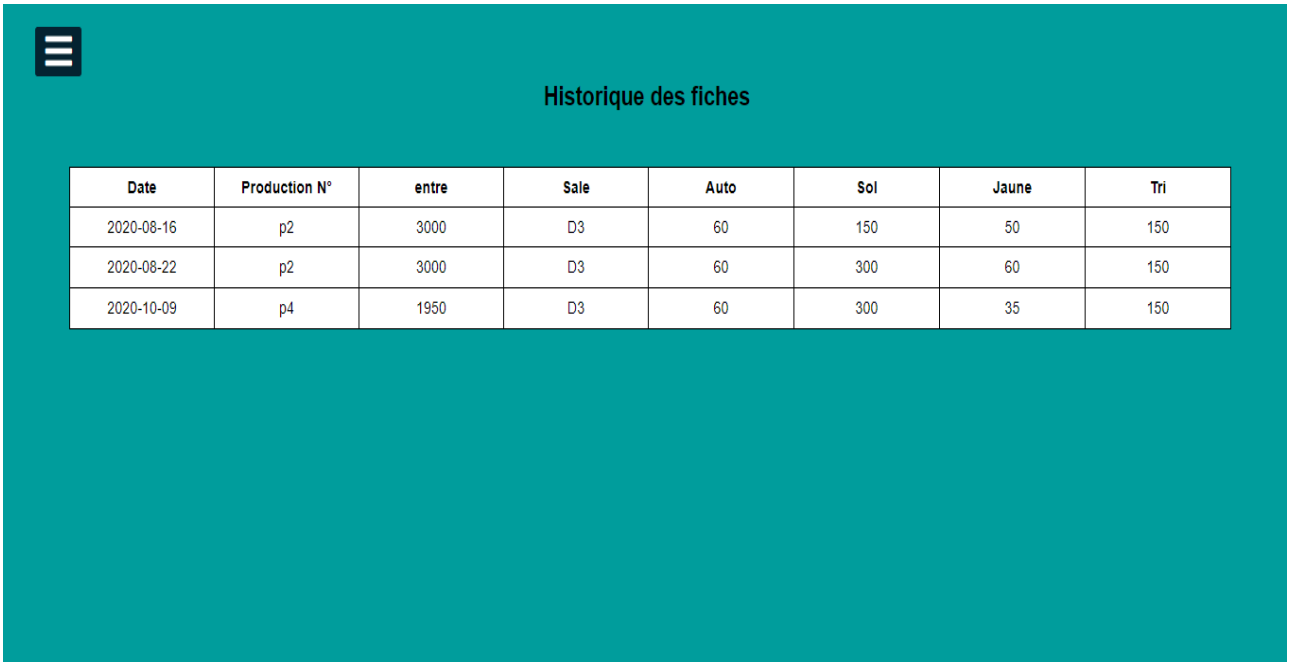


Figure 25 : Historique des fiches d'un responsable du couvoir.

- **Pages du bon de livraison et l'historique d'un responsable de production :**

Cette page ci-dessous représente le bon de livraison remplit chaque jour par le responsable de production.

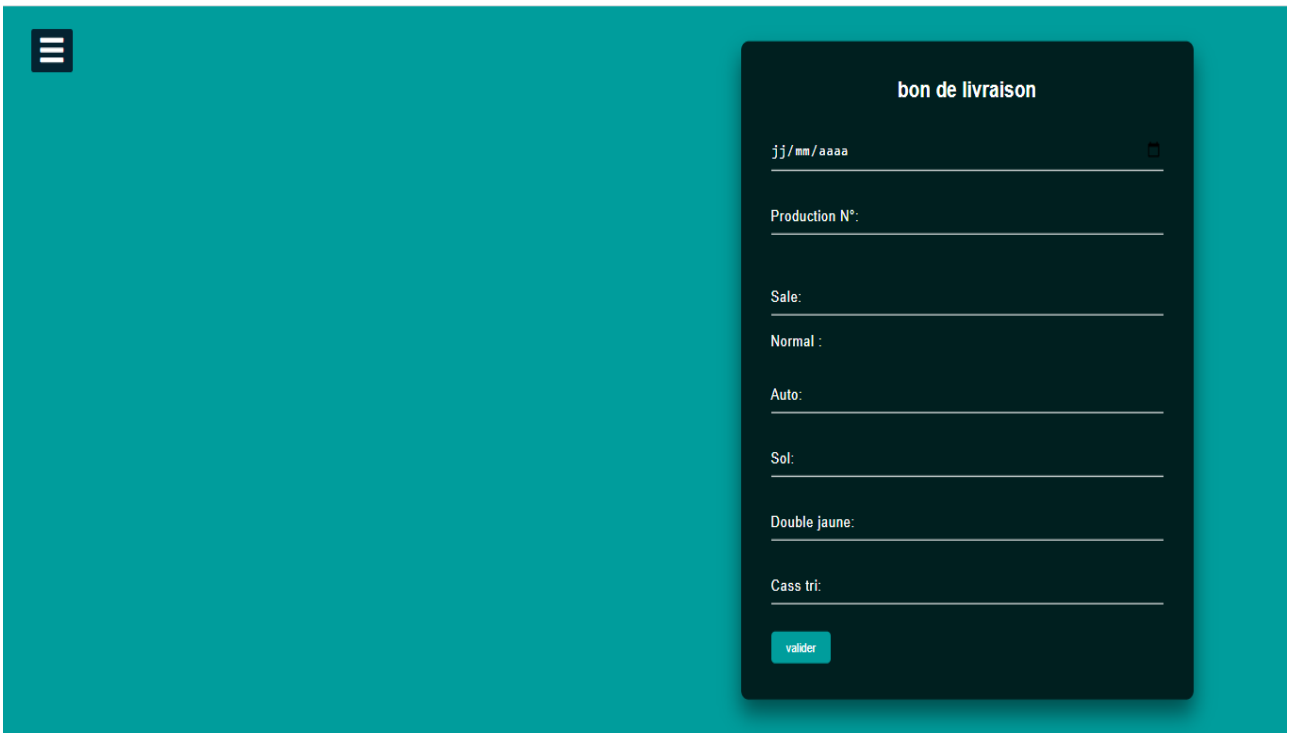


Figure 26 : bon de livraison.

Cette page ci-dessous représente l'historique des bons de livraison d'un responsable de production.

Figure 27 : Historique des bons de livraison d'un responsable de production.

- **page de contrôle du responsable technique de production :**

Cette page représente la page du contrôle du responsable technique qui lui facilite le contrôle et la comparaison des bons et fiches saisie.

Figue 28 : Contrôle des fiches du jour.

- **Pages d'historique des bons de livraison et fiches journalières de tous les responsables :**

Cette page ci-dessous représente l'historique de tous les bons de livraison saisie dans le syst ème avec le nom du responsable qui la remplit.

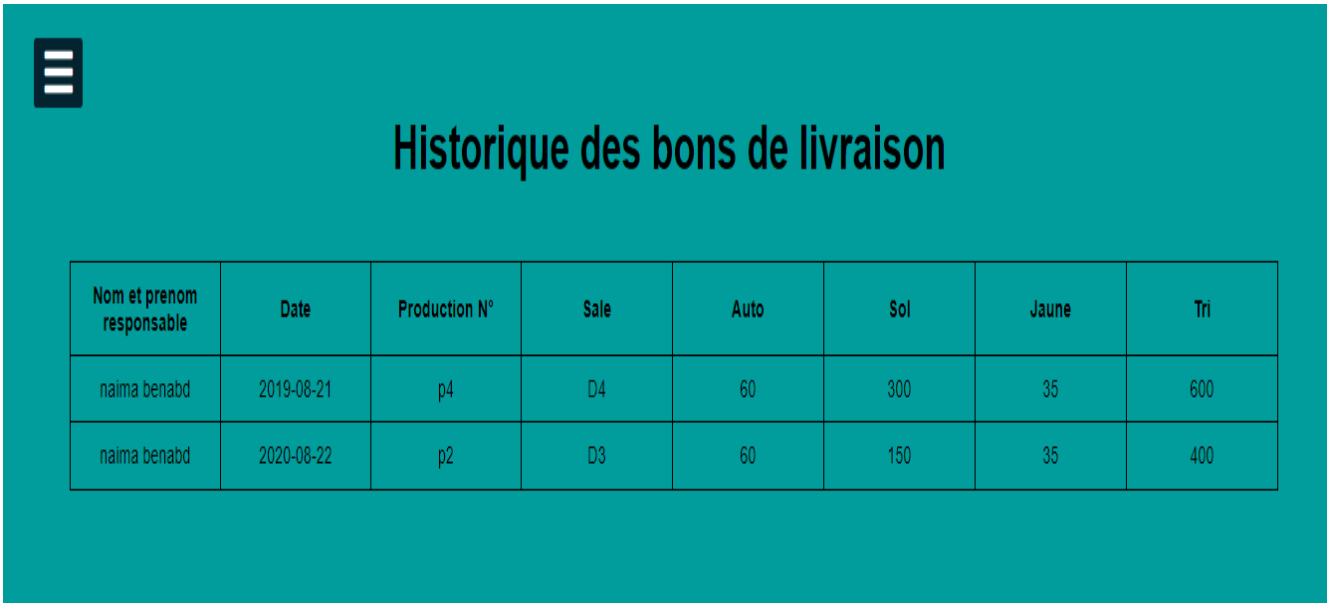


Figure 29: Historique des bons de livraison de tous les responsables de production.

Cette page ci-dessous représente l'historique de toutes les fiches journalières saisies dans le syst ème avec le nom du responsable qui la remplit.

Figure 30 : Historique des fiches journali ères de tous les responsables du couvoir.

6. conclusion

Dans ce chapitre, nous avons effectuant une présentation générale du site ; les acteurs avec leurs fonctions de plus les diagrammes nécessaires à la modélisation du site.

Nous avons aussi présenté notre implémentation du site avec des exemples d'interfaces plus important.

Conclusion générale et Perspective

La gestion du système d'information d'un organisme est devenue un élément essentiel pour le fonctionnement de celui-ci. Grâce aux nouvelles technologies, les entreprises produisent et exploitent de plus en plus de données qui doivent être sécurisées en précisant les propriétés de la sécurité, qui sont la confidentialité, l'intégrité et la disponibilité de l'information.

Notre travail s'est réalisée sur trois parties, dans la première partie qui se compose de deux chapitre nous avons présentés le concept de sécurité dans les systèmes d'informations en générale dans le premier chapitre et dans le deuxième nous avons parlés de la politique de sécurité , la deuxième partie été l'étude et la mise en place de la politique de sécurité du système d'information ,et enfin nous avons proposé dans la troisième partie un site web pour contrôler la transmission de données d'une manière sécurisée afin de déterminer où est le problème maintenant et d'on profiter dans l'avenir pour leur faciliter le travail.

La mise en place d'une Politique de sécurité d'un système d'information est un vrai plus pour le futur car dans le cas de départ de collaborateurs, la méthodologie est bien écrite. Ceci améliore le passage d'information car l'ensemble de nos éléments à risques sont détaillés.

Enfin comme perspectives nous suggérons :

-concernant le site web : Lors de l'installation du site sur le serveur on va leur propose d'acheter un certificat (pour que le site devient https) pour sécuriser la transmission de données et renforcé la sécurité. De plus nous les avant déjà conseil de mettre des parfeu pour sécuriser leur connexion.

Bibliographie

[1] Margaret Rouse , « Sécurité de l'information (infosécurité, infosec) », Consulté le 09/04/2020, sur https://www.lemagit.fr/definition/Securite-de-linformation-infosecurite-infosec

[2] riadh hajji, « les principes de la sécurité informatique », Consulté le 09/04/2020, sur https://apcpedagogie.com/les-principes-de-securite-informatique/definition

[3] Jean-François Pillou, « introduction à la sécurité informatique : objectif de la sécurité d'information », Consulté le 08/06/2020, sur https://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique

[4] WatchGuard Technologies, « guide des bonnes pratiques », Consulté le 19/04/2020, sur https://www.watchguard.com/docs/whitepaper/wg_charte-informatique_wp_fr.pdf

[5] Jacass, « Système Informatique », Consulté le 20/08/2020, sur https://adnethique.org/Glossaire/systeme-informatique

[6] Laurent GRANGER, « système d'information : l'essentiel à savoir - Manager GO ! », Consulté le 09 04,2020, sur https://www.manager-go.com/organisation-entreprise/systeme-information.htm

[7] N. BOUSTIA, « modélisation des politiques de sécurité des systèmes d'information multi-niveaux », diplôme de magister informatique, Université Des Sciences Et De La Technologie Houari Boumediene, pp. 12-15,2004

[8] Ali Ben Mouloud, « Mise en œuvre d'un système de management de la sécurité

de l'information (SMSI) au sein de l'Ambassade du Royaume du Maroc à Tunis »,pp 20, Université Virtuelle de Tunis,2010

[9] Linlaud Daniel, « Sécurité de l'information – La norme ISO/CEI 27002 », Consulté le 01/08/2020 sur https://bivi.afnor.org/notice-details/securite-de-linformation-la-norme-iso-cei-27002/1294542

[10] ISO/IEC 27002 Sécurité de l'information - Code de bonne pratique. Consulté le 09 01,2020, sur https://pecb.com/fr/education-and-certification-for-individuals/iso-iec-27002

[11] N. BOUSTIA, « cour de méthodologie sécurité », Universite Saad Dehleb Blida 1,2019

[12] G.MOISIO, « méthodologies appliquées », Livre, pp 7, disponible sur https://methodes.pressbooks.com/chapter/analyses-de-risques-ssi/

[13] Ivision. « Mettre en place une politique de sécurité informatique : les bonnes pratiques », Consulter le 14/02/2020, sur https://www.ivision.fr/mettre-en-place-une-politique-de-securite-informatique-les-bonnes-pratiques/

[14] ANSSI, « Guide d'élaboration de politiques de la sécurité des systèmes d'information »,Consulté le 14/02/2020 , pp 10-sur https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

[15] Nomios, « Politique de securité des systemes d'information », Consulté le 14/06/2020, sur https://www.nomios.fr/pssi-politique-de-securite-du-systeme-dinformation

[16] Francis B, « Identifiez les enjeux et objectifs d'une PSSI», Consulté le 10/08/2020, sur

https://openclassrooms.com/fr/courses/1734201-definissez-la-politique-de-securite-de-votre-entreprise/6206013-identifiez-les-enjeux-et-objectifs-dune-pssi

[17] Malia, « *DÉFINITION : ORGANIGRAMME»*, Consulté le 10/11/2020, sur https://www.7-dragons.com/lexique-business-et-marketing/definition-organigramme/

[18] roels.C, «UML, c'est quoi ?-débuter l'analyse logicielle avec UML », Consulté le 14/02/2020, sur https://openclassrooms.com/courses/debutez-l-analyse-logicielle-avec-uml/uml-c-est-quoi

[19] IBM, « Diagrammes de séquence », Consulté le 20/05/2020, sur https://www.ibm.com/support/knowledgecenter/fr/SSRTLW_9.6.1/com.ibm.xtools.sequence.doc/topics/cseqd_v.html

[20] Margaret rouse, « Maria DB », Consulté le 20/05/2020, sur https://searchdatamanagement.techtarget.com/definition/MariaDB#

[21] El Haouat.B, Chouef.W, «Conception et Réalisation d'un site web », projet fin D'étude, informatique, Universite Sidi Mohamed Ben Abdellah, 2017

[22] Deherve, «SUBLIME TEXT 2, UN ÉDITEUR DE TEXTE COMPLET ET MULTI-PLATEFORMES », Consulté le 15/11/2020, sur https://www.winmacsofts.com/sublime-text-2-un-editeur-de-texte-complet-et-multi-plateformes/

Annexe A : questionnaire de la structuration de l'entreprise

Questionnaire

Q1 : quelle est votre fonction dans l'entreprise ?

- Chef d'entreprise (gérant)
- Secrétariat
- Chef de cite
- Responsable des achats
- Ouvriers
- Responsable de service
    - Responsable technique de production
    - Responsable d'usine d'aliment
    - Responsable couvoir

Q2 : quelle est la composition de votre parc informatique ?

Ordinateurs de bureau	
Ordinateurs portables	
Serveurs	

Q3 : vos ordinateurs et imprimantes sont-ils en réseau, c'est-à-dire connectéentre eux ?

- Oui
- Non

Q4 : tous les ordinateurs de votre entreprise ont-ils accès à l'internet ?

- Oui

- Non

Q5 : ou sont enregistrer vos données informatiques ?

- Sur chaque ordinateur
- Centralisées sur un ordinateur, un serveur
- Sur papiers
- Chez un prestataire de services
- Autre, précisez

Q6 : De quelle manière sauvegarder vous les données informatiques de votre entreprise ?

- Un support amovible type clé USB, CDROM ou DVD
- Sur disque dur externe
- Sur papiers
- Sur bande magnétique
- Autre, précisez

Q7 : Quel degré d'importance attachez-vous à la Sécurité de l'Information (disponibilité – intégrité – confidentialité) dans votre entreprise ?

- très importante
- Importante
- peu importante

Q8 : sur une échelle de 1 à 5 pourriez-vous noter l'importance que vous attachez a la formation règlementaire

	1 = pas du tout important	2	3	4	5= très important
L'existence d'une Politique de mesure de sécurité	○	○	○	○	○
La sécurisation de la communication	○	○	○	○	○
Prévention des risques liés à l'activité physique	○	○	○	○	○
La sécurité physique des équipements, du document et stockages	○	○	○	○	○
L'existence de La sécurité du personnel	○	○	○	○	○
L'existence de La sécurité des périmètres et zones	○	○	○	○	○
La protection des risques résultant par internet	○	○	○	○	○
La disponibilité des équipements de communications et de sauvegarde	○	○	○	○	○

Q9 : Si un jour il y a un incendie ou un problème dans l'entreprise, qu'elle sera votre réaction ?

- Appeler la protection civile
- Aller au patron

Autre réaction :

Q10 : si voulez-vous détruire une donnée comment le faites ?

Q11 : Comment gérer les ventes avec l'acheteur ?

- La société s'assure de la livraison
- Le client s'on occupe

Merci de votre contribution

Annexe B : études des postes de travail et des documents

4-1-1Directeur général

Désignation : Poste directeur général
Effectif : 1

Taches accomplis par ce poste	**Fréquence**
Demende des poussins GP	Chaque 3 mois
Programme de vacctinations (occupe poste de vetérinaire)	Aléatoire
Gestion de la caisse	Aléatoire
Recrutements des employées	Aléatoire

Documents diffusés par ce poste :

Désigniation	**Fréquence**	**Destination**
Certificat veterinaire	Pour chaque vente	Clients
Papiers administratifs	Aléatoire	DSA
Papiers pour la banque	Aléatoire	Banque

Documents provenant a ce poste :

Désigniation	**Fréquence**	**Provenance**
Relevébancaire	Aléatoire	Banque
Les impots	Chaque mois	Comptable
Fiche d'éclosion	Chaque éclosion	Responsable couvoir

4-1-2 Administration pricncipale :

Désigniation :Administration pricncipale
Dépend hiérarchiquement de :Directeur générale
Effectif : 01

Taches accomplis par ce poste	Fréquence
Gestion de la caisse	Aléatoire
Rédiger les achats	Aléatoire
Les prévision	Aléatoire
Gestion des personnels	Aléatoire
Pointage	Quatidien
Les charges	Aléatoire

Documents diffusés par ce poste :

Désigniation	Fréquence	Destination
Fiche de pointage par moi	Chaque moi	Comptable
Facture d'achat	Chaque moi	Comptable
Facture de vente	Chaque moi	Comptable

Documents provenant a ce poste :

Désigniation	Fréquance	Provenance
Fiche pointage couvoir	Par semaine	Couvoir
Fiche pointage administration02	Par semaine	Administration02
Fiche de paie	Chaque moi	Comptable
Facture d'achat	Aléatoire	Vendeur
Facture de vente	Aléatoire	Vendeur

4-1-3 poste d'administration 02 :

Désigniation :administration 02
Dépend hiérarchiquement de :administration principale
Effectif : 01

Taches accomplis par ce poste	**Fréquence**
Pointage des employées	Par jour
Magasin	Aléatoir
Gestion du personnel	Aléatoir

Documents diffusés par ce poste :

Désigniation	**Fréquence**	**Destination**
Fiche de pointage	Par semain	Administration principale
Bon de commande	Aléatoir	Administration principale

Documents provenant a ce poste :

Désigniation	**Fréquence**	**Destination**
Bon de livraison	Aléatoir	vendeur

4-1-4 poste du responsable technique de production :

Désignation : responsable technique de production
Dépend hiérarchiquement de : directeur générale
Effectif : 01

Taches accomplis par ce poste	**Fréquence**
Contrôler les bons de livaison et les fiches journalière	Par jour
Remplir les fiches techniques	Par semaine
Visiter les sites	Aléatoire

Documents diffusés par ce poste :

Désignation	**Fréquence**	**Destination**
Fichiers techniques	Par semaine	Directeur générale

Documents provenant a ce poste :

Désignation	**Fréquence**	**Destination**
Les fiches techniques	Par semaine	Tout les responsables des sites
Bons de livraison d'aliment	Par semaine	Responsable d'usine d'aliment

Etude des documents :

Document1 : Fiche de transfert

Désignation : Fiche de transfert

Emetteur : poussinière

Récepteur : production

Nature : interne

Rôle : cette fiche contient les informations de transfert des poules du site d'élevage vers la production.

Nombre d'exemplaire : 1.

Description du document

Désignation	Type	Taille	Observation
Site d'élevage	A	20	_
Site de production	A	20	_
Date	D	08	JJ/MM/AAAA
Lot n°	N	10	_
Lignée	A	03	_
Box	N	02	_
Eff. Elevage	N	05	_
TOTAL	N	05	Calculable
Eff. Production	N	05	_
Différence	N	05	Calculable
Date dutransfert	D	08	JJ/MM/AAAA
Observations	A	100	_

Document 2 :fiche journalière

Désignation :fiche journalière

Emetteur : responsable de production

Récepteur : Responsable technique de production

Nature : interne

Rôle : cette fiche contient les informations détaille de la production par jour.

Nombre d'exemplaire : 1.

Description du document

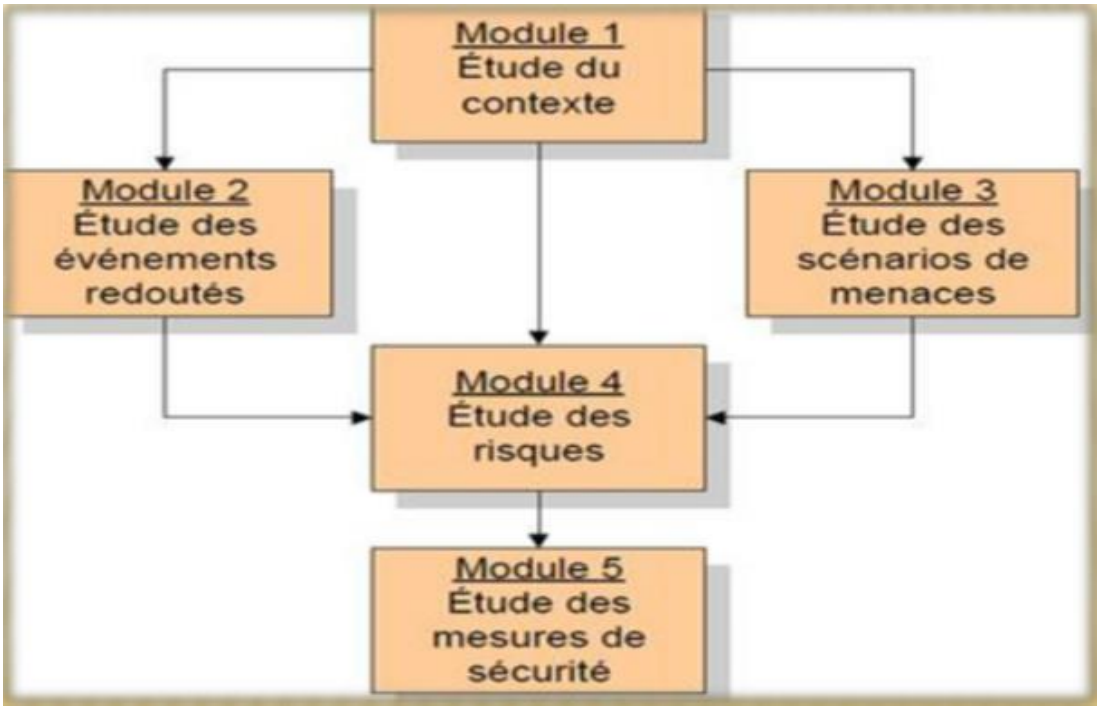
Désignation	Type	Taille	Observation
Date	D	08	JJ/MM/AAAA
Désignation	A	03	_
Mortalité	N	05	_
Effectif présent	N	05	_
Normal	N	06	_
Casse	N	04	_
Double jaune	N	04	_
Tri	N	05	_
Total œufs	N	06	Calculable
% de ponte	N	04	Calculable
% de ponte au sol	N	04	Calculable
Poids d'œuf	N	04	_
Ration	N	04	_
Temps de consommation	N	04	_
Insémination artificielle	N	-	_
Œuf entrée	N	06	_
Œuf sortie	N	06	_
Œuf stock	N	04	_
aliment entrée	N	05	_
aliment sortie	N	-	_
aliment en stock	N	-	_

Annexe C : Approche d'analyse des risques

Notre méthode basée sur la méthode EBIOS consiste à formaliser les besoins de sécurité et

Les menaces, et permet de déterminer les risques pesant sur les périmètres à auditer.

Les étapes d'EBIOS



ETUDE DE CONTEXTE

Les objectifs de cette étude sont : d'identifier d'une façon globale le système-cible et de le situer dans son environnement et de réunir les informations nécessaires à la planification de l'étude.

Activité 1 : Définir le cadre de la gestion des risques :

Son objectif est de savoir ce qui est dans le champ de l'étude et ce qui ne l'est pas et de disposer des éléments contextuels susceptibles d'orienter les décisions.

Activité 2: Préparer les métriques :

Son objectif est de fixer les critères et les échelles de mesure et les règles de gestion qui devront être appliquées

Activité 3: Identifier les biens :

Son objectif est obtenir la liste des biens essentiels (immatériels),la liste des biens supports (physiques),la liste des mesures existantes.

ÉTUDES DES ÉVÉNEMENTS REDOUTÉS

L'objectif de cette étape est : d'obtenir une liste hiérarchisée de ce que craint l'organisme.

À la fin de cette étude, les événements redoutés sont identifiés, explicités et positionnés les uns par rapport aux autres, en termes de gravité et de vraisemblance.

Elle comprend une seule activité

Activité 1 : Appréciation des événements redoutés

Son objectif est de faire émerger et caractériser les événements liés à la sécurité de l'information que l'organisme redoute sans étudier la manière dont ceux-ci peuvent arriver.

ÉTUDE DES SCÉNARIOS DE MENACES

L'objectif de cette étape est : d'obtenir une liste hiérarchisée de tous les scénarios possibles, et comme résultat, les scénarios de menaces seront identifiés, explicités et positionnés les uns par rapport aux autres en termes de vraisemblance.

Elle a une seule activité

Activité 1: Appréciation des scénarios de menaces:

Son objectif est d'identifier les différentes possibilités d'actions sur les biens supports, afin de disposer d'une liste complète de scénarios de menaces.

ÉTUDE DES RISQUES

L'objectif de cette étude est de déterminer les risques qui doivent être couverts par les objectifs de sécurités de la cible de l'étude et choisir les options de traitement adéquates.

À la fin de cette étude, les risques sont appréciés et évalués, et les choix de traitement effectués.

Elle se divise en 2 activités

Activité 1: Apprécier les risques :

Elle a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.

Activité 2: Identifier les objectifs de sécurité:

Son objectif est de choisir la manière dont chaque risque devra être traité au regard de son évaluation.

ÉTUDE DES MESURES DE SÉCURITÉS

L'objectif de cette étude est de déterminer les moyens de traiter les risques et de suivre leur mise en œuvre, en cohérence avec le contexte de l'étude.

Elle se divise en 2 activités :

Activité 1: les mesures de sécurité à mettre en œuvre :

Son Objectif est d'obtenir la liste des mesures de sécurité destinées à traiter les risques conformément aux objectifs de sécurité et obtenir la liste des risques résiduels.

Activité 2: Mettre en œuvre les mesures de sécurité :

Son objectif est de disposer d'un plan d'action