**Université Saad DAHLAB - Blida 1**

**Faculté des sciences**

## Département d'Informatique

Mémoire présenté par :

M. BEHLOULI Zakaria

Pour l'obtention du diplôme de Master

**Domaine :** Mathématique et Informatique

**Filière :** Informatique

**Spécialité :** *Sécurité des systèmes d'information*

**Sujet :**

# *Planification d'un Système de Management de la Sécurité de l'Information selon la famille des normes ISO 2700X*

Soutenu le : **19 octobre 2019**

Devant le jury composé de :

| | | |
|---|---|---|
| Mme Ghebghoub | Présidente | Université de Blida 1 |
| Mme Bey | Examinatrice | Université de Blida 1 |
| Mme. MEZZI Melyara | Promotrice | Université de Blida 1 |

# Remerciements

Je voudrais exprimer mes sentiments les plus sincères envers les personnes qui ont fait tout leur possible pour que ce travail puisse voir le jour.

Tout d'abord, je tiens à remercier, Mme MEZZI pour son aide et ses conseils, son soutien et ses encouragements qui ont été déterminants pour que ce projet voit le jour.

Je tiens à exprimer ma gratitude à Mme BOUSTIA, enseignant chercheur et responsable de notre spécialité, qui nous a encadré efficacement tout au long de notre cycle master.

Je remercie aussi, le Groupe SIM à sa tête monsieur Taib zghaimi Farid PDG du Groupe, qui nous ont bien accueille et qui ont tous fait pour que notre séjour dans leur établissement soit agréable.

Je tiens a remercié aussi madame Ameur Karima pour son aide et sa présence, son encadrement et pour sa proposition de se thème qui ma permet d'avoir des perspectifs par rapport à ma vie professionnelle dans l'avenir prochain.

Je remercie les membres du jury pour la grande attention qu'ils ont bien voulu porter à mon travail.

Pour conclure, je garde une place toute particulière à ma famille, et surtout mes parents. Pour leur encouragement et les sacrifices qu'ont fait pour moi et mes sœurs. Rien n'aurait été possible sans votre présence et votre soutien.

# Résumé

L’implantation d’un système d’information fiable, opérant avec un contrôle continu et une sécurité maximale, est devenue l’objectif à atteindre pour tous type d’organisation quelle que soit son contexte ou son domaine d’activité.

Compte tenu du niveau d'exposition aux risques et de la dépendance vitale des organisations vis-à-vis de leurs systèmes d'information, il est crucial de prêter attention aux exigences de sécurité. La réalisation d'un équilibre entre la sécurité et l'efficacité du système d’information est une tâche complexe qui exige au préalable une analyse approfondie du contexte organisationnel. Elle nécessite également l'identification, l'analyse, et la gestion des risques encourus par l’entreprise.

Dans le cadre de notre projet de mise en place d’un système de management de la sécurité d’information, nous avons réussie à aboutir de la phase la plus essentiel, celle de sa planification en auditant le système actuel, et en analysant les risques encourus par ce dernier, nous proposons, pour cela, une base de connaissance des menaces et des vulnérabilités en plus d’une politique de sécurité des systèmes d’information dériver des exigences de sécurité recommander par l’ISO,



Mots clés

Exigences de sécurité, Analyse des risques, Audit, Menaces, Vulnérabilités

Abstract

The implementation of a reliable information system, operating with continuous monitoring and maximum security, has become the objective to be achieved for all types of organizations whatever their context or field of activity.

Given the level of exposure to risk and the vital reliance of organizations on their information systems, it is crucial to pay attention to security requirements.

Achieving a balance between security and the effectiveness of the information system is a complex task that requires a thorough analysis of the organizational context. It also requires the identification, analysis, and management of the risks incurred by the company.

As part of our project to set up an information security management system, we have managed to reach the most essential phase, that of its planning by auditing the current system, and by analyzing the risks. incurred by the latter, we propose, for this, a knowledge base of threats and vulnerabilities in addition to an information system security policy derive from the security requirements recommended by the ISO,

Keywords

Security Requirements, Risk Analysis, Audit, Threats, Vulnerabilities.

ملخص

أصبح تطبيق نظام معلومات موثوق، يعمل على المراقبة المستمرة والأمن الأقصى الهدف المراد تحقيقه من طرق مختلف المؤسسات بغض النظر عن سياقها أو مجال نشاطها.

بالنظر إلى مستوى التعرض للمخاطر والاعتماد الحيوي للمنظمات على نظم المعلومات الخاصة بها. يعد تحقيق توازن بين الأمن وفعالية نظام المعلومات مهمة معقدة تتطلب تحليلًا شاملاً للسياق التنظيمي. كما يتطلب تحديد وتحليل وإدارة المخاطر التي تتكبدها الشركة.

كجزء من مشروعنا لإنشاء نظام لإدارة أمن المعلومات، تمكنا من الوصول إلى المرحلة الأكثر أهمية، وهي مرحلة التخطيط من خلال التدقيق ومراجعة النظام الحالي، وتحليل المخاطر. التي استخرجناها بفضل هذه المراجعة، حيث نقترح في هذا العمل، قاعدة معرفة للتهديدات ونقاط الضعف بالإضافة إلى سياسة أمن نظام المعلومات المستمدة من متطلبات الأمان التي أوصت بها المنظمة الدولية للمقاييس

كلمات محورية

متطلبات الأمان، تحليل المخاطر، التدقيق، التهديدات، نقاط الضعف.

# Table des matières

# Liste de figures



# Liste de tableaux

# Listes des acronymes

| Acronymes | Significations |
|---|---|
| SI | Système d'information |
| ISO/IEC | International Organization for Standardization / International Electrotechnical Commission |
| ERP | Entreprise ressource planning |
| SMSI | Système de management de sécurité d'information |
| BSI | British Standards Institution |
| IANOR | Institut algérien de normalisation |
| DSI | Direction des systèmes d'information |
| AD | Active Directory |

# Introduction générale

Aujourd'hui, 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, dans un organisme agroalimentaire, comme *tous types d'organismes* une claire répartition des rôles et des responsabilités dans la gestion des systèmes d'information constitue une étape nécessaire pour initier toute démarche de progrès.

Dans le cas de la SIM Agro les cadres dirigeants ont vu nécessaire d'attribuer la plus importante des responsabilités, qui représente un véritable défi, à la fois technologique et économique. Celle de mutualiser l'ensemble des systèmes d'informations et des processus opérationnels, au département développement qui a comme objectif premier la mise à disposition de toutes les décideuses et tous les décideurs de l'entreprise la gestion de l'ensemble des données. Toutes les informations disponibles sont actualisées en temps réel et chaque utilisateur peut en connaître l'origine, garantissant par cela la disponibilité, l'intégrité et la traçabilité de cette dernière en développant un logiciel ERP (Enterprise Resource Planning) propre à l'entreprise.

Si le service commercial enregistre un bon de commande, le stock est actualisé en temps réel et l'écriture comptable s'inscrit automatiquement, L'architecture d'un ERP se compose principalement d'un serveur ERP sur

lequel est présente une base de données unique et disponible pour tous les salariés.

Les dirigeants en prenant compte du risque infligé par la mise en place de l'ERP qui centralisera toutes données importantes et indispensable au bon fonctionnement de l'entreprise ont vu convenable de le bâtir sur une base valide, une structure agile et une architecture qui répond aux normes mondiales de la sécurité (SMSI : norme ISO 27001 : 2013 pour notre cas d'étude). Chose qui garantira, d'un côté, une conception perfectionniste de leur ERP et de l'autre côté, une image de marque qui sera protégée et mise en valeur par rapport aux clients. Cette tâche l'est attribuée à un comité de sécurité formé des départements SI et du département Management Qualité vue leur assurance et leur expérience avec le respect des objectifs de sécurité, sous-ensemble du Système de Management de la qualité (SMQ : Norme ISO 9001), donc, ils sont les mieux placés pour nous aider à assurer la mise en place d'un système de management de la sécurité de l'information.

Notre rôle consiste tout d'abord, à aider le Responsable Système d'information ainsi que la direction Management Qualité à comprendre les exigences et le contexte de la norme ISO/CEI 27001 version 2013, qui nous guidera à mettre en place ce fameux Système de Management de la Sécurité d'Information tous en définissant le périmètre de l'étude, afin de garantir la protection des actifs informationnels et de sécuriser les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion.

Par la suite nous opterons pour un audit interne qui aura comme principaux objectifs l'évaluation du niveau de maturité du Système d'information en place en termes de sécurité,

Nous entamerons par la suite la phase de planification de notre système de management qui aura comme but de garantir une meilleure gouvernance et une meilleure gestion des risques. Car le statut de l'entreprise comme entité économique évoluant dans un environnement caractérisé par une concurrence acharnée et une multitude de risques, que l'origine des dysfonctionnements soit malveillante ou accidentelle. Un simple accident de traitement peut engendrer des impacts critiques, sur l'intégrité de l'information.

Notre travail apportera les réponses aux questions suivantes :

- ✓ Quels sont les principaux risques pouvant altérer l'exploitation du Système d'information ?
- ✓ Comment traiter ces risques ?
- ✓ Quelle est la gravité des nouveaux risques environnementaux et informationnels engendrés par cette nouvelle démarche ?

# *Chapitre I*

# *État de l’a*

# 1 Les systèmes de management de sécurité des systèmes d'information

Dans le chapitre suivant, nous allons aborder les systèmes de management de la sécurité de l'information, l'ensemble des normes qui constituent des références dans le cadre de notre mission ainsi que les méthodes de gestion des risques.

## 1.1 Qu'est-ce qu'un système de management ?

Le principe de système de management concerne généralement le monde de la qualité, surtout dans le domaine des services et de l'industrie [5], qui n'a jamais vu un papier à entête avec un petit logo « certifié iso 9001 » ? qui n'as jamais croisé un produit affichant fièrement dans son emballage « société certifié iso 22000 »

Un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif et une fois celui-ci atteint, à s'y tenir voir à le dépasser.[1]

### 1.1.1 Principaux systèmes de management

Les systèmes de management ne se cantonnent pas uniquement à la qualité. Ils concernent des domaines très variés comme l'environnement, les services informatiques, la sécurité de l'information, la sécurité alimentaire ou encore la santé. Le tableau ci-après donne un aperçu des principaux référentiels de systèmes de management.

*Tableau 1: référentiels des systèmes de management*

| Référentiel | Domaine |
|---|---|
| ISO 9001 | Qualité |
| ISO 14001 | Environnement |
| ISO 27001 | Sécurité de l'information |
| ISO 20000-1 | Services informatiques |
| ISO 22000 | Sécurité alimentaire |

### 1.1.2 Apports des systèmes de management

La mise en place et l'exploitation d'un système de management ne sont pas faciles à mener. Il faut commencer par fixer des politiques, formaliser les procédures par écrit et mener à bien des audits réguliers. Ces opérations sont loin d'être transparentes. Souvent lourdes à implémenter, leur coût humain et financier n'est pas négligeable. Dans ces conditions, il est légitime de se demander ce qui justifie un tel investissement.[1]

Quels apports concrets pouvons-nous en espérer ?

#### 1.1.2.1 L’adoption de bonnes pratiques

Les systèmes de management se basent sur des guides de bonnes pratiques dans le domaine qui les concerne (qualité, sécurité, environnement, etc.). Ainsi, celui qui se lance dans la mise en place d'un système de management est quasiment obligé d'adopter ces bonnes pratiques

Se poser les bonnes questions concernant les systèmes de management de sécurité de l'information permettra d'adopter des mesures de sécurité appropriées aux besoins de l'entreprise. Quels sont les éléments les plus sensibles de l'entreprise ? Où déployer en priorité les mesures de sécurité ? Comment détecter les incidents ? Comment réagir rapidement aux anomalies ?

#### 1.1.2.2 L’augmentation de la fiabilité

L'adoption de bonnes pratiques a pour conséquence directe, à court ou moyen terme, l'augmentation de la fiabilité. Ceci est principalement due au fait que les systèmes de management imposent la mise en place de mécanismes d'amélioration continue.

#### 1.1.2.3 La confiance

Adopter de bonnes pratiques entraine à court et à moyen terme une augmentation de la fiabilité. Mais celle-ci n’apporte pas des avantages commerciaux. Pour cela, l’entreprise fait appel à des auditeurs indépendant qui certifieront qu'elle applique effectivement les référentiels qu'elles engagée à adopter (ISO 9001, ISO 27001 ou autre).

#### 1.1.2.4 **Les parties prenantes**

Nous touchons enfin à la raison d'être des systèmes de management : ils fournissent la confiance envers les parties prenantes. Donc qu'entendons-nous par parties prenantes ? Il s'agit de toute personne, groupe ou instance à laquelle l'entreprise doit rendre des comptes. Nous en avons répertorié sept.

- Les actionnaires : en tant que propriétaires, ils sont directement concernés par les résultats de l'entreprise.
- Les clients : ils sont la partie prenante par excellence, puisque l'entreprise ne peut vivre sans eux.
- Les fournisseurs : même si la relation client-fournisseur place souvent ceux-ci en situation d'infériorité, l'entreprise a des responsabilités envers eux
- Les partenaires : les relations de partenariat sont devenues indispensables pour le développement de l'entreprise. Si les partenaires n'ont pas confiance, ils ne collaboreront pas.
- Les banques et les assurances : l'entreprise ne peut pas vivre sans leur confiance
- Le personnel : son adhésion est capitale pour le bon fonctionnement de l'entreprise.
- L'opinion publique : elle a un pouvoir de sanction très important, dont les conséquences peuvent se révéler désastreuses pour l'entreprise.

Sans la pression des parties prenantes, les systèmes de management n'existeraient pas. Ils sont mis en place à cause et pour les parties prenantes, Pourquoi la confiance est-elle si importante ? Tout simplement parce que qui dit confiance dit gains économiques.

### 1.1.3 **Démarche d'auto-évaluation selon le modèle PDCA**

L'amélioration continue du système de management de sécurité d'information et le rendre plus performant aujourd'hui est un enjeu pour un meilleur avenir durable pour les entreprises. Le déploiement d'une auto-évaluation selon le modèle PDCA est formel pour notre cas d'étude, on l'a choisie même si la nouvelle version de la norme ISO 27001 :2013 ne l'exige pas comme sa prédécesseur ISO 27001 :2005.

Le modèle en quatre temps appelé « PDCA », pour Plan, Do, Check, Act.

1. Phase Plan : dire ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité, etc.).
2. Phase Do : faire ce que l'on a dit dans ce domaine.
3. Phase Check : vérifier qu'il n'y a pas d'écart entre ce que l'on a dit et ce que l'on a fait.
4. Phase Act : entreprendre des actions correctives pour régler tout écart qui aurait été constaté précédemment.

Ce modèle présente deux propriétés principales (cyclique et fractal).

- **Caractère cyclique** : C'est ce cycle Plan, Do, Check, Act qui permet d'atteindre les objectifs (de sécurité, de qualité, d'environnement ou autre) fixés par le management. En revanche, que se passe-t-il une fois que l'objectif a été atteint ? Un nouveau cycle doit être entrepris. Ce nouveau cycle permet à l'entreprise non seulement d'atteindre ses objectifs, mais aussi de s'y tenir dans la durée. Un système de management est donc un processus qui tourne indéfiniment. [1]
- **Caractère fractal** : Une fractale est une figure géométrique qui garde les mêmes propriétés, quelle que soit l'échelle à laquelle on l'observe. Le principe est le même avec les systèmes de management (quelle que soit l'échelle à laquelle on l'observe, on doit retrouver le modèle P,D,C,A)

Ainsi, non seulement le modèle PDCA s'applique à l'échelle globale du système de management, mais on le retrouve également au niveau de chacun des processus du système.[1]

## 1.2 Sécurité de l'information

Commençons par préciser qu'il est question ici de sécurité de l'information au sens large du terme, c'est-à-dire que nous ne parlons pas seulement de sécurité informatique. Nous nous intéressons à l'information sous toutes ses formes, indépendamment de son support logiciel, matériel, mais aussi humain, papier, etc... Naturellement, en tant que support privilégié de l'information, l'informatique occupera une part importante, mais réduire le SMSI à son côté strictement informatique serait une erreur.

Nous utiliserons le mot sécurité pour désigner tout ce qui peut avoir des conséquences (positives ou négatives) en matière de confidentialité, de disponibilité ou d'intégrité de l'information. La norme ISO 27000 précisent le vocabulaire employé dans la suite des normes ISO 2700X définit ces trois notions comme suite :

- 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. Cela veut dire que l'information doit être disponible dans des conditions convenues à l'avance (soit 24 h/24, soit aux heures ouvrables, etc.).

### 1.2.1 Objectif de la sécurité de l'information

Le principal objectif d'un SMSI est de faire en sorte de préserver ces trois propriétés (confidentialité, intégrité et disponibilité) pour les informations les plus sensibles de l'entreprise.[1]

Les trois notions présentées en dessous ne sont pas les seules. On parle aussi de traçabilité, d'authentification, d'imputabilité, de non-répudiation, et de bien d'autres mécanismes de sécurité. Le fait que ces principes ne soient pas au centre du SMSI ne signifie pas qu'ils ne soient pas importants. Ils seront déployés en fonction des besoins de sécurité de l'entreprise.

### 1.2.2 Terminologie relative à la sécurité informatique

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

**Les vulnérabilités** : ce sont les faiblesses et les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitées par un attaquant.

**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.

## 1.3 Historique des normes de sécurité d'information

Depuis 1995, plusieurs normes concernant directement ou indirectement les SMSI ont été publiées. C'est ainsi que l'on a vu apparaître successivement les normes BS 7799, BS 7799-2, ISO 17799, ISO 27001 et ISO 27002. Encore aujourd'hui, même si ces travaux publiés sont dans une dynamique ascendante du point de vue progressive des contenue des normes les idées ne sont pas toujours très claires dans ce domaine ce qui génère une certaine confusion pour les moins expérimenté.[1]

Une brève revue historique permettra de clarifier cette progression des normes

- 1995 – La BSI (British Standards Institution), qui est l'organisme de normalisation britannique (équivalent de l'IANOR en Algérie), publie la norme BS 7799. Il s'agit d'un document articulé autour de dix grands chapitres, énumérant les mesures qui peuvent être prises en matière de sécurité de l'information. C'est en fait un catalogue d'une centaine d'entrées. Notons qu'à aucun moment il n'est question de SMSI dans ce document.
- 1998 – La BSI ajoute une seconde partie à cette norme, et la nomme BS 7799-2. Le « -2 » ne signifie pas ici « version 2 », mais « deuxième partie ». Cet ajout

précise les exigences auxquelles doit répondre un organisme pour mettre en place un SMSI.

- 2000 - La norme BS 7799 de 1995 connaît un tel succès dans le monde que l'iso l'adopte officiellement sous la référence ISO 17799, en l'enrichissant de quelques mesures de sécurité supplémentaires. On remarque que le radical 7799 a été conservé pour ne pas dérouter les personnes qui s'étaient habituées à la BS 7799.

Il ne s'agit que de la première partie de la norme (BS 7799-1), et non de la BS 7799-2. L'ISO 17799 est donc un référentiel qui ne traite pas non plus la question des SMSI.

- 2002 – Parallèlement aux travaux de l'ISO, la BSI poursuit son travail sur la BS 7799-2 et en publie une deuxième version. C'est la BS 7799-2 :2002.
- Juin 2005 – L'ISO sort une nouvelle version de l'ISO 17799, légèrement remaniée et enrichie de nouvelles mesures de sécurité.
- Octobre 2005 – L'ISO adopte enfin la BS 7799-2 sous la référence ISO 27001 :2005. Il s'agit d'une adaptation de la norme britannique, modifiée pour se rapprocher le plus possible de l'ISO 9001. L'ISO 27001 spécifie donc les exigences auxquelles doit répondre un organisme pour mettre en place un SMSI.
- 2007 – Afin de rendre plus cohérentes les nomenclatures entre elles, l'ISO renomme l'ISO 17799 en ISO 27002.
- Fin 2013 – l'iso met à jour simultanément les normes ISO 27001 et ISO 27002.

Ce qu'on a retenu de cet historique est le fait qu'aujourd'hui, nous disposons de deux normes.

- L'ISO 27001 qui spécifie des exigences pour les SMSI.
- L'ISO 27002 qui recueille les bonnes pratiques en matière de sécurité de l'information, mais qui ne traite pas des SMSI.

Nous allons présenter ces deux normes, ainsi qu'une comparaison entre deux méthode référence dans la gestion des risques, pour qu'on puisse se positionner sur la méthodologie adéquate à notre domaine d'étude.

## 1.4 La norme ISO 27001

L'ISO 27001 s'est imposée comme référence en matière de systèmes de management de la sécurité de l'information (SMSI). Il est donc indispensable d'avoir une vision très claire de cette norme avant même de se lancer dans l'implémentation d'un tel système.

Malheureusement cette dernière n'est pas disponible dans l'institut algérien de normalisation (l'IANOR), en revanche on a pu la trouver sur les sites payant de l'ISO et sur celui de différents organismes de normalisation étranger tel que (AFNOR, BSI, etc.). Ce document compte 23 pages. Après un examen détaillé, on s'aperçoit que les trois premiers articles ne font que rappeler des notions de base. Ce n'est qu'à partir de l'article 4 que les exigences commencent vraiment à être spécifiées. Le dernier article se termine dès la page 10 et la norme se poursuit par une annexe (l'annexe A), qui occupe la moitié de la norme en volume.

### 1.4.1 Objectifs de la norme

La norme spécifie les exigences pour mettre en place, exploiter et améliorer un SMSI. On se focalisent dans ce travail sur la phase de planification d'une mise en place d'un SMSI, l'exploitation et à l'amélioration du système de management ne sera pas une nécessité vu qu'on n'aura pas le temp d'aboutir à tout un cycle PDCA pour Plan, Do, Check et Act faute de temp.

La norme spécifie, par ailleurs, les exigences pour la mise en place de mesures adaptées aux besoins de l'organisation. Les dispositions prises pour la mise en œuvre doivent ainsi être adéquates et proportionnées.[1] Ceci signifie que chaque cas est particulier. Une mesure de sécurité choisie pour un organisme ne sera pas déployée de la même façon, et avec la même profondeur, pour un autre.

### 1.4.2 Structure de la norme

Pour être conforme à l'ISO 27001, un SMSI doit impérativement répondre à toutes les exigences comprises entre les articles (ou chapitres) 4 et 10 de la norme, sans exception, Structurellement, la norme rédigée comme une grande roue Plan, Do, Check, Act comme démontré dans la figure suivante


*Figure 1: Structure de la norme ISO 27001 :2013* [5]

- **Plan** : les articles 4 à 7 spécifient toutes les fondations du SMSI qu'il faut mettre en place avant de l'exécuter (périmètre du SMSI, politique, objectifs de sécurité, appréciation des risques, répartition des responsabilités, gestion de la documentation, gestion des ressources, sensibilisation, communication, etc.)
- **Do :** l'article 8 concentre toutes les exigences relatives à la phase Do du SMSI. Il s'agit en fait de mettre en œuvre les dispositions qui ont été décidées dans les articles précédents.
- **Check :** tout ce que l'on peut faire pour contrôler l'efficacité et la conformité du SMSI est centralisé dans l'article 9 de la norme. Les trois grands leviers de contrôle sont la mise en place d'indicateurs, la conduite régulière d'audits internes ainsi que la tenue de revues de direction.
- **Act** : tous les incidents, anomalies, non-conformités et opportunités d'améliorations sont tenus de donner lieu à des actions d'amélioration. C'est l'article 10 qui traite ce sujet et qui clôture la norme. Les sections ci-dessous détaillent les exigences des articles 4 à 10 de la norme.

### 1.4.3 Annexe A

Il s'agit de la reprise des titres des chapitres de la norme ISO 27002. L'annexe A est une liste de 114 mesures de sécurité pouvant être implémentées. Elles sont classées en 14 catégories principales. En principe, tout ce qui peut être entrepris en matière de sécurité de l'information s'y trouve répertorié. L'annexe A ne donne aucun conseil et ne propose aucun exemple qui aiderait à l'implémentation, elle sert à s'assurer que l'on n'a oublié aucune mesure de sécurité dans l'appréciation des risques.

## 1.5 La norme ISO 27002

La norme ISO 27001 décrit les mesures nécessaires à la mise en place d'un SMSI. Si elle fixe l'objectif à atteindre, elle ne précise pourtant pas comment il convient de déployer ces mesures concrètement. Nous avons donc besoin d'un guide de bonnes pratiques pour les différentes actions qu'on va entreprendre. L'ISO 27002 répond à ce besoin par toute une série de préconisations concrètes, abordant des aspects tant techniques qu'organisationnels.

### 1.5.1 Présentation de la norme

Elle est structurée sur trois niveaux :

- Les chapitres (niveau 1).
- Les objectifs de sécurité (niveau 2).
- Les mesures de sécurité (niveau 3).

Les quatre premiers chapitres de l'ISO 27002 décrivent des généralités et rappellent quelques notions de base. C'est à partir du chapitre 5 que la norme devient intéressante.

### 1.5.2 Structure générale

La norme ISO 27002 peut être vue comme un dictionnaire comportant 114 entrées. Chacune de ces entrées décrit une mesure de sécurité, une mesure peut être un mécanisme que l'on met en place, ou l'action que l'on entreprend, pour assurer la sécurité dans un domaine particulier. Par exemple, les mots de passe sont une mesure de sécurité dont le but est de contrôler l'accès aux systèmes en identifiant et authentifiant les utilisateurs.

Chaque mesure de sécurité est décrite en trois parties.

- Une brève description de la mesure. Le but est de dire clairement de quoi il s'agit. Généralement, cette description ne prend que trois ou quatre lignes.
- Préconisations de mise en œuvre – Les préconisations sont développées et éventuellement accompagnées d'exemples pour les illustrer.
- Informations supplémentaires – Précisions jugées utiles, mais non abordées dans les préconisations.

Pour assurer une meilleure lisibilité, les 114 mesures de sécurité sont classées en 14 grands chapitres (de niveau 1) reprenant les principaux thèmes de la sécurité. Chacun des 14 chapitres est à son tour subdivisé en sous-chapitres (de niveau 2).

### 1.5.3 **Extrait de l'ISO 27002**

13.2.3 Messagerie électronique : Il convient de protéger de manière appropriée l'information transitant par la messagerie électronique.[6]

Préconisations de mise en œuvre : Pour la sécurité de l'information dans le cadre de la messagerie électronique, il convient de prendre en compte :

a) Une protection des messages contre tout accès non autorisé, toute modification ou tout déni de service.

b) La qualité de l'adressage et du transport du message.

c) La disponibilité et la fiabilité du service.

d) Les questions juridiques, comme les exigences en matière de signatures numériques.

e) L'obtention d'une autorisation avant d'utiliser des services externes publics comme une messagerie instantanée.

f) Des niveaux plus élevés d'authentification permettant de contrôler l'accès depuis les réseaux accessibles au public.

Informations supplémentaires : Il existe de nombreux types de messagerie électronique, tels que les courriers électroniques, l'échange de données informatisé (EDI) et le réseautage social, qui jouent un rôle important dans les communications professionnelles

Cette mesure appartient au chapitre 13, relatif à la sécurité des communications. Qui est subdivisé en deux sous-chapitres :

- 13.1 Gestion de la sécurité des réseaux
- 13.2 Transfert de l'information

La mesure 13.2.3 est donc une des mesures de sécurité concernant le sous-chapitre 13.2 Transfert de l'information ».

## 1.6 La norme ISO 27005

L'ISO 27005 répond point n'a point à toutes les exigences de l'ISO 27001 en matière d'appréciation des risques, sa création est fut exclusivement conçu pour permettre à un implémenter d'avoir une vision une analyse et une appréciation des risques souhaité. Les objectifs de cette norme ne sont pas de constituer une méthode complète de gestion de risque mais de fixer un cadre minimum et d'imposer des exigences, tant pour le processus à suivre, que pour l'identification des menaces et des vulnérabilités permettant d'estimer les risques et d'en évaluer le niveau puis de pouvoir sélectionner le mode de traitement ainsi que les plans et les éléments (dont les mesures de sécurité et les indicateurs) destinés à améliorer la situation.[1] Il ne s'agit donc pas d'un ensemble méthodologique complet et autosuffisant – il est même précisé que le choix d'une méthode doit être fait.

Pour cela nous avons deux méthodes qui couvrent différentes perspectives dans la gestion des risques

## 1.7 Méthodologies de gestion des risques

Une étude du CLUSIF (Club de la Sécurité de l'Information Français) dénombrait plus de deux cents méthodes d'appréciation des risques. Nous en avons retenu trois, EBIOS, MEHARI qui pour l'ENISA (Européen Network and Information Security Agency) figurent parmi les plus utilisées

### 1.7.1 **EBIOS RM**

(Pour expression des besoins et identification de objectifs de sécurité) est une méthode assez reconnue et fait référence dans le domaine de la gestion des risques des systèmes d'information, sa dernière version de 2018 publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI française) avec le soutien du Club EBIOS, cette dernière permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser. Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue.

Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.

### 1.7.2 **MEHARI**

(Pour méthode harmonisée d'analyse des risques) est une méthode de gestion de risque associée à la sécurité de l'information d'une entreprise de petite ou moyenne envergure. Elle a été développée initialement par le CLUSIF en France. L'objectif premier de MEHARI est de fournir une méthode d'analyse et de gestion des risques affectant la sécurité de l'information, une méthode conforme aux exigences de la norme ISO/IEC 27005 :2011, avec l'ensemble des outils et moyens requis pour sa mise en œuvre.

A cet objectif premier s'ajoutent deux objectifs complémentaires : Permettre une analyse directe et individualisée de situations de risque décrites par des scénarios de risque. Fournir une gamme complète d'outils adaptée à la gestion à court, moyen et long

terme, de la sécurité, quelle que soit la maturité de l'organisme en matière de sécurité et quelques soient les types d'actions envisagés.

### 1.7.3 Comparaison des deux méthodes

Le tableau suivant résume quelques aspects des méthodes observées sur lesquels le choix peut s'appuyer :

*Tableau 2: comparaison entre EBIOS RM et MEHARI*

| | **Ebios RM** | **Mehari** |
|---|---|---|
| **Caractéristiques** | | |
| Analyse des risques | Oui | Oui |
| Analyse des vulnérabilités | Oui | Oui |
| **Périmètre** | | |
| Adapté à toutes les tailles d'entreprises | Oui | Oui |
| **Outils** | | |
| Questionnaires | Oui | Oui |
| Modèles (formulaires, grilles...) | Non | Oui |
| Logiciel disponible | Non | Oui |
| **Divers** | | |
| Licence gratuite (concernant le logiciel) | Non | Non |
| Subit encore des mises à jour | Oui | Oui |

### 1.7.4 Choix de la méthodologie

Le choix d'une méthode à suivre n'était pas chose facile, car nous étions tenté par la première méthode, la nouvelle version d'EBIOS RM de 2018 malgré sa flexibilité en s'appliquant aussi bien à tous types organisations, quels que soient leur taille, leur secteur

d'activité et que leurs systèmes d'information soient en cours d'élaboration ou déjà existants, toutes les ateliers proposé par cette méthode soit d'analyse, de gestion ou d'appréciation des risques se focalise sur l'aspect numérique, contrairement à MEHARI qui présente une base de connaissance des scénarios pratiquement identique au contexte de l'organisme d'accueil et au périmètre d'étude, Les deux méthodes sont conforme aux exigences techniques, environnementales et légales auxquels se réfère notre travail. Le choix des ateliers proposé par EBIOS RM avec des bases de connaissance de MEHARI sera une bonne base pour le déroulement de la phase d'analyse. Le seul inconvénient est que leur logiciel est payant, ce qui va nous laisser opérer « manuellement » lors des différentes étapes d'analyse.

## 1.8 Conclusion

Cette partie de notre travail nous a permis de présenter le cadre général du projet. Nous venons aussi d'exposer, un ensemble de normes qui constituent des références dans le cadre de notre mission ainsi que les procédures de réalisation d'un audit de systèmes d'information, l'analyse et le traitement des risques La suite de ce document consistera à mettre en pratique les précédents aspects pour mettre en place le système de management de sécurité des systèmes d'information, par l'entame de la phase PLAN de notre modèle PDCA.

# *Chapitre II*

# *Contexte et Périmètre d'étude*

# 2 Introduction

La première étape de notre phase de planification commence par la définition du contexte et du périmètre du SMSI. Ces deux critères Permettent de cadrer le projet, et c'est sur eux que s'articulera notre système de management.

## 2.1 Contexte de l'organisme

### 2.1.1 Introduction

Pour mieux connaître et comprendre l'état actuel de la sécurité au niveau de SIM Agro l'étude de l'existant est une étape fondamentale et nécessaire.

Ce chapitre présente une étude sur le système informatique et les composants qui le constituent.

Pour cela il est recommandé de réaliser des interviews avec le responsable pour :

- Avoir une vision globale du domaine d'étude.
- Cerner les objectifs à atteindre.

### 2.1.2 **Présentation de l'organisme d'accueil**

#### 2.1.2.1 **Présentation générale**

| Fiche d'identité | |
|---|---|
| | **Le président directeur général :** Mr.Taieb ezzraimi Farid |
| | **Secteur d'activité :** Agroalimentaire |
| | **Date de création :** 1994 |
| | **Adresse :** Zone industrielle de Ain Romana, BP51, Bis 09210 Mouzaia, Algérie |
| | **Site internet :** www.groupesim.com |
| | **E-mail :** contact@groupesim.com |
| | **Téléphone :**025 24 79 79 |

*Figure 2:Fiche d'identité de Sim Agro SPA.*

#### 2.1.2.2 **Historique**

L'Entreprise a été fondée en 1990 par Monsieur TAIEB EZZRAIMI Abdelkader en tant que petite société familiale dans le domaine de la Minoterie-Semoulerie où elle a fait office de pionnière en sa qualité de première société privée dans cette filière d'activité en Algérie.

#### 2.1.2.3 **Domaine d'activité**

La filiale SIM Agro est chargée de l'approvisionnent et la transformation des céréales pour les besoins propres du groupe et ceux du marché algérien, Ça production est assurée par :

3 semouleries, 3 minoteries, 4 lignes de production de pâtes courtes, 3 lignes de production de pâtes longues, 6 lignes de production de couscous ,1 unité d'aliments du bétail et un ensemble de silos de stockage de 85.000 tonnes.

Les produits SIM sont conformes aux normes ISO 9001-2015 et à ceux de HACCP

### 2.1.3 **Présentation du département (SI) système d'information**

Le département système d'information de Sim Agro SPA a pour mission de :

- Piloter le système d'information de l'établissement (applications et infrastructures).
- Assister la direction et les services de l'établissement dans la définition de leurs besoins et dans la conduite des projets SI (fonction d'assistance à maîtrise d'ouvrage).
- Conduire la mise en œuvre des applications et des infrastructures informatiques.
- Maintenir en condition opérationnelle et faire évoluer les infrastructures et les applications informatiques.
- Fournir et maintenir en condition opérationnelle l'ensemble des postes informatiques ainsi que les moyens d'impression associés.
- Accompagner les usages du numérique par l'assistance et la formation
- Tenir à jour l'inventaire physique de l'ensemble des matériels informatiques de l'établissement.
- Mettre tous les moyens en œuvre pour garantir la sécurité du système d'information (SSI)

### 2.1.4 **Organigramme de la DSI**

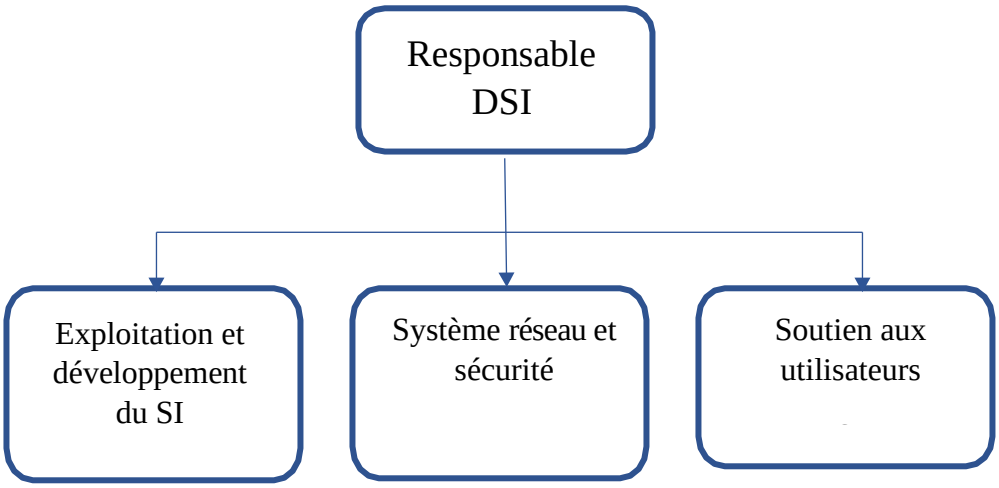


*Figure 3:Organigramme de la DSI.*

### 2.1.5 Description du système d'information

Dans cette partie nous allons identifier les éléments et les entités qui participent au fonctionnement du système d'information :

#### 2.1.5.1 Les postes de travail

Il existe 176 postes de travail de type PC équipés du système d'exploitation WINDOWS 8.1.

#### 2.1.5.2 Les serveurs en exploitation

Il existe 5 serveurs :

- Deux serveurs Rackables
- Trois serveurs Tours

*Tableau 3 : Les serveurs en exploitation.*

| Serveur en exploitation | Services | Système d'exploitation |
|---|---|---|
| Rackable Dell PE R720 | Serveur principale AD Exchange | WIN2012R2 |
| Tour Dell PE T720 | Serveur secondaire (redondant) AD Exchange | WIN2012R2 |
| Tour Dell PE T610 | Serveur d'application (ERP) | WIN2008R2 |
| Rackable PE R320 | Serveur d'application (Commercial/Comptabilité) | WIN2016R2 |
| Tour PE T610 | Données | WIN2003 |

### 2.1.5.3 **Logiciels et applications**

*Tableau 4: Logiciels et applications.*

| **Application** | **Developpement (Externe / Interne)** |
|---|---|
| Gestion Commerciale / comptabilité | **Externe** |
| Système de pointage | **Externe / interne** |
| Gestion des ressources humaines | **Interne** |
| Gestion de la paie | **Interne** |
| Gestion de maintenance assistée par ordinateur | **Interne** |
| Gestion de la production assistée par ordinateur | **Interne** |
| Gestion de stocks | **Interne** |
| Gestion des pesés | **Interne** |

### 2.1.5.4 **Les équipements réseau**

*Tableau 5 : Les équipements réseau.*

| **Équipement** | **Marque et Modèle** |
|---|---|
| Firewall | Fortinet |
| Switch 48 Ports | Zyxel |
| Switch 24 ports | Zyxel / Fortinet |
| Switch 8 ports | Zyxel |

### 2.1.6 Aspects de sécurité existante

#### 2.1.6.1 Sécurité physique

D'après les visites et les entretiens, nous avons constaté les faits suivants :

- Existence des agents d'accueil qui contrôle l'accès au périmètre du site et l'enregistrement des informations relatives à chaque visiteur.
- Data center fermé avec serrure, seul les personnes autorisées peuvent y accéder.
- Absence d'un système d'extinction automatique de feu dans le datacenter.
- La climatisation est assurée dans le datacenter.
- Les serveurs sont protégés des coupures d'énergie par des onduleurs.
- Des issus de secours sont présents.

#### 2.1.6.2 Sécurité logique

- Acquisition d'une solution matérielle de sauvegarde qui comprend un robot de sauvegarde.
- Une redondance matérielle a été mise en place pour assurer la continuité des services et assurer la disponibilité nécessaire.

#### 2.1.6.3 Sécurité réseau

- Le réseau local et segmenté logiquement en plusieurs sous réseau au tour d'un Firewall.
- Le filtrage depuis et vers le réseau externe est assuré par le firewall.
- La gestion des accès à internet est assurée par le firewall.

#### 2.1.6.4 Sécurité système

- Existence d'une solution antivirale « Kaspersky Endpoint Security 2010 » avec une architecture client/serveur.

## 2.2 Périmètre d'étude

Après l'étude du contexte de l'entreprise et afin de définir un périmètre où la mise en place d'un SMSI sera simple et efficace, l'ERP en cours de développement sera le processus métier.

Cette décision a découlé d'une réunion ou le contexte, les objectif, le domaine d'application du projet ont été discuté.

### 2.2.1 Qu'est-ce qu'un ERP ?

Un ERP (Enterprise ressource planning) est un logiciel qui permet aux salariés d'une entreprise de travailler à partir d'une même base de données, tout en profitant de ses modules.

Les dirigeants de la SIM agro ont vu nécessaire d'avoir leur ERP de gestion intégrée adapté à leurs moyens, à la taille de l'entreprise et à son activité.

On peut résumer la volanté des dirigeants de bâtir un ERP dans leurs souhaits d'évoluer, être plus compétitifs et de revoir son organisation. Cela permet de :

- Travailler à partir d'une même base de données,
- Donner à chaque métier un module avec des fonctionnalités adaptées à son activité,
- Améliorer la gestion de chaque processus,
- Assurer la traçabilité des informations,
- Gagner en temps et en efficacité,
- Optimiser le travail d'équipe,
- Augmenter le potentiel managérial et économique du groupe.

### 2.2.2 Architecture de l'ERP

L'architecture de l'ERP se compose d'un serveur ERP sur lequel est présente une base de données unique. Il est constitué d'un ensemble de modules qui fonctionnent les uns avec les autres. Nous pouvons citer les modules suivants :

- Gestion des ressources humaines.
- Calcule des paies.
- Production.

- Park roulant.
- Gestion des approvisionnements.
- Gestion du stock.

Qui sont en états de marche et où les salariés peuvent bénéficier des avantages fournis, et d'autres modules en cours de développement comme :

- Comptabilité.
- Commercial.

Dans notre cas d'étude, On a choisi deux modules Gestion des ressources humaines, calcule paie utilisé par un processus, Ressources humaines

### 2.2.3 **ERP et sécurité**

La principale faille dans un système d'information, n'est statistiquement pas constituée par l'infrastructure ni par le logiciel, mais plutôt par la négligence humaine, si les pirates parviennent à s'infiltrer dans les systèmes informatiques, et à mettre en danger l'activité de l'entreprises, ils le doivent souvent à de mauvaises pratiques, et au non-respect de certaines règles de sécurité.

Les études estiment que 80% des attaques surviennent par suite d'une « erreur » ou négligence humaine. Ce sont ces erreurs commises par les administrateurs réseau et les utilisateurs qui ouvrent la porte à l'immense majorité des attaques réussies. »[3]

Si cette information est ramenée à l'échelle de l'ERP, il faudra donc s'attacher lors de son implantation, et durant tout son cycle de vie, à mettre en place des règles simples mais strictes en matière de sécurité, et à veiller à leur respect par tous. Cela peut sembler relativement accessible, la difficulté ne provient pas de la solution ERP elle-même, ni de l'infrastructure qui l'héberge. Le cœur du problème réside dans les terminaux d'utilisation qui peuvent être les principales portes d'entrée. Il suffit donc qu'un terminal soit infecté par un malware pour, qu'un pirate ait la capacité de prendre connaissance des codes et de la procédure d'accès à l'ERP, Ou encore d'une opération de « phishing » menée pour que

l’un des utilisateurs se laisse prendre, donnant ainsi l’accès à sa machine. Les intrus pourraient alors y trouver là encore les codes, procédures, ou moyens d’accès aux serveurs et de les chiffrer en guise de rançon.

## 2.3 Conclusion

Ce chapitre nous a permis de cerner le contexte et le périmètre de notre mission, Dans le chapitre suivant, nous allons auditer l’organisme pour définir les principales défaillances ou mauvaise pratique de sécurité pouvant affecter l’entreprise ou au moins le périmètre choisi pour l’étude.

# *Chapitre III*

# *Audit organisationnel et physique*

# 3 Introduction

L'audit organisationnel est une méthode d'analyse des forces et des faiblesses d'une entreprise, dans toutes leurs dimensions : taille, répartition du travail, circuit d'information et de communication, nombre de niveaux hiérarchiques, procédures et règles pour faire fonctionner les activités, etc.[7]

L'audit organisationnel met en avant les points forts et les points qui demandent à être améliorer au sein d'une entreprise.

## 3.1 Objectif de l'audit organisationnel et physique

L'objectif de cet audit est de mesurer la maturité de l'organisation de la sécurité des systèmes d'information sur la base de référentiels techniques et réglementaires et en accord avec les réglementations et méthodes applicables dans le domaine d'activité de l'entreprise (industriel). Cet audit permet avec un regard extérieur d'identifier les écarts présentant les vulnérabilités majeures du système audité.

## 3.2 Analyse des résultats de l'Audit organisationnel et physique

### 3.2.1 Paramètre d'analyse de l'audit

Dans la phase d'audit organisationnel et physique de la sécurité de la SIM Agro nous avons préparé une pile de question en s'inspirant des mesures citées dans la norme ISO 27002 :2013 Pour chaque question, après l'annonce de la mesure et de la question qui la concerne, le responsable devait répondre par « oui » ou par « non ». Onze questions ont été exclues de ce questionnaire car les mesures ne concernaient par notre périmètre d'étude. A titre d'Exemple, la mesure « 6.2.2 », qui définit les mesures de sécurité liée au télétravail a été exclue car les salariés n'ont pas le droit de quitté les lieus munis de leurs équipements [6]

Ce questionnaire va nous permettre d'évaluer le niveau de conformité de chaque clause par rapport aux différents chapitres définis dans la norme.

Une synthèse claire des résultats obtenus sur la maturité par chapitre est représentée dans le l' [Annexe A].

Le tableau suivant décrit les niveaux de maturités des chapitres selon leur moyenne de conformité

*Tableau 6: niveaux de maturité*

| **Niveau de maturité** | **Description** |
|---|---|
| Plus que 75% | Niveau de maturité élevé |
| 50%->75% | Niveau de maturité moyen |
| Moins de 50% | Niveau de maturité faible |
| 0% | Niveau de maturité nul |

### 3.2.2 Analyse des résultats de l'Audit

A l'issu de notre questionnaire, l'organisme enregistre une conformité globale de 42.27%, par rapport à la norme ISO/IEC 27002 :2013 preuves que des efforts sont à faire pour ce qui est de la sécurité et la documentation des procédures et les politiques, pour être le plus neutre possible beaucoup de ces mesures ont été déclaré non-conforme car même si elles sont mises en place leur documentation sous des procédures rédigé dévoilé et mise à jour ne l'est pas.

Nous abordons à présent l'analyse des résultats obtenus. Les points seront abordés suivant les clauses (ou chapitres) définis dans la norme ISO 27002 :2013 selon l'ordre dans lequel elles ont été évoquées.

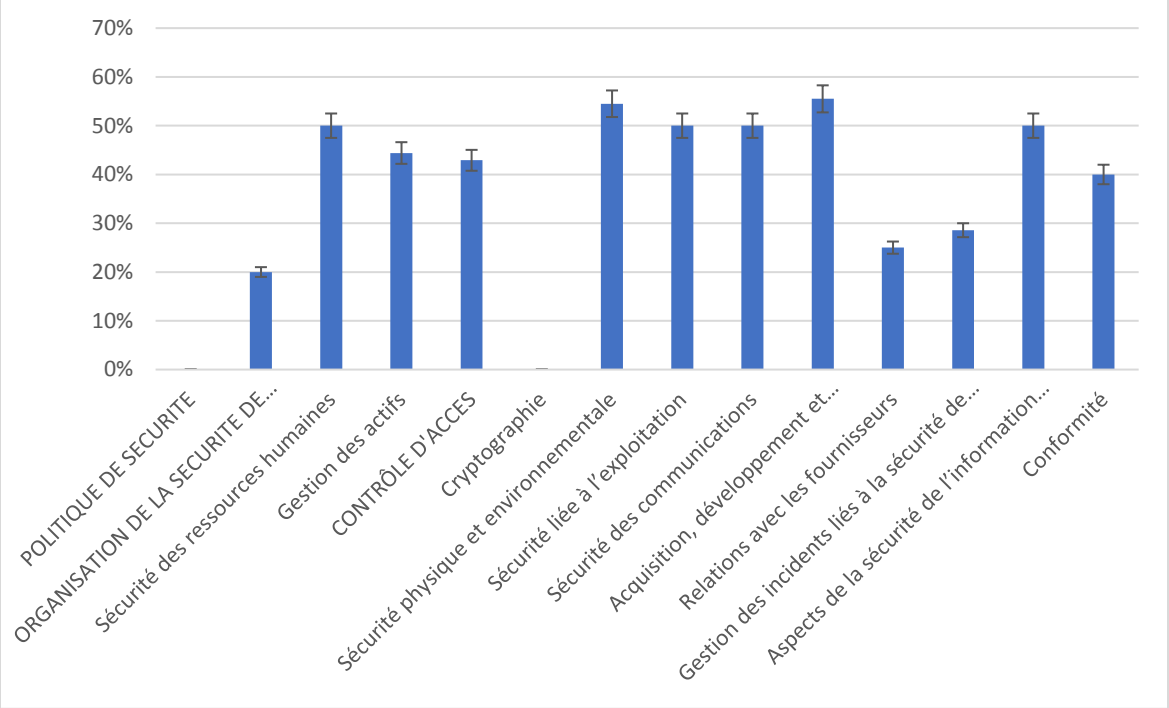


*Figure 4:histogramme du niveau de maturité de la Sim Agro par chapitre*

Ci-dessous, nous présentons l'analyse point à point de cet histogramme qui présente le niveau de conformité de la SIM Agro par rapport à notre questionnaire élaboré en se basant sur la norme ISO 27002 :2013.

#### 3.2.2.1 **Politique de sécurité**

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **0%**.

Cela s'explique par l'absence de documents de synthèse représentant le document de la politique de sécurité. Il existe certes une charte d'utilisation des systèmes d'information établie par les départements SI et SMQ dans le cadre de la mise en place de la norme ISO 14000 (Qualité) qui spécifie partiellement les bonnes pratiques mais cette dernière n'est ni diffusée auprès de l'ensemble des salariés et des tiers concernés ni revues à intervalles programmés. Ainsi en plus de la reconstruction de cette charte en une politique de sécurité, il faut prévoir également des mesures pour permettre à cette dernière d'être revue périodiquement.

Le niveau de maturité accordé à cette clause est donc **nul**.

#### 3.2.2.2 Organisation de la sécurité

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **20%.**

Ce niveau de conformité est le résultat des travaux du département SI au sein de l'organisme. Cependant les fonctions des responsables de sécurité ne sont pas formellement définies. Le département informatique n'a pas élaboré un plan permettant une visibilité et prévision de l'évolution du système dans les années à venir.

Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.3 Sécurité liée aux ressources humaines

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **50%**.

Les nouveaux employés sont informés de leurs droits et devoirs vis-à-vis de la sécurité de l'organisme également, mais cet engagement est formalisé avec la signature de la charte, mais cela n'est pas indiqué dans les contrats de recrutement. Ainsi il n'est pas défini de procédure visant à rappeler à l'ensemble du personnel son rôle dans la sécurité de l'organisme. Les salariés ne bénéficient pas d'une sensibilisation ou une formation périodique qui les incite à respecter les directifs de la charte.

Le niveau de maturité accordé à cette clause est donc **moyen**.

#### 3.2.2.4 Gestion des actifs

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **44%.**

L'ensemble des principaux actifs est identifié et inventorié, cet inventaire est tenu à jour. Pour chaque actif les règles d'utilisation sont définies et documentées par le bais de la charte de bonne utilisation. Cependant, les procédures de classification ne se basent pas sur une documentation précise qui définit les critères de classification, de sorte à pouvoir évaluer les conséquences d'une altération de cet actif sur l'organisme. De plus, il n'existe

pas de procédure d'étiquetage pour la classification ; simplement, les dossiers considérés sensibles sont astreints à rester dans le bureau du responsable en question.

Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.5 **Contrôle d'accès**

La clause enregistre une moyenne de 42,9% par rapport à la norme ISO/IEC 27002.

Une politique de mot de passe est instaurée au sein de l'organisme, pour l'accès à certaines applications. Cependant les bonnes pratiques en matière de choix et de l'utilisation de mot de passe ne sont pas centralisées pour les postes de travail des utilisateurs.

La permanence de ces mots de passe ne permet pas de réduire les risques d'usurpation de mots de passe ou de vol. De même on remarque l'absence d'un dispositif de revue des droits d'accès à des intervalles réguliers. Cependant, il y a un certain contrôle partiel ciblant les téléchargements pour en limiter les effets négatifs, de même pour empêcher tout abus tel que les outils de téléchargement Peer to Peer, par exemple, qui exposent le réseau aux risques d'infiltration et d'infection par les spywares et les virus. Également, l'accès aux locaux sensibles tel que la salle serveur reste protégé par des clefs. Seules les personnes qui en possèdent, sont habilitées à y accéder. L'accès distant, à partir de l'Internet est protégé par les règles d'accès gérées par le Firewall. Etant donné qu'on ne peut garantir qu'un accès illicite et qui ne peut se réaliser qu'à 100%, il n'y a pas de système de détection ou de prévention d'intrusion (IDS/IPS) pour contrer et réagir contre les actions malveillantes qui peuvent être des intrus interne/externe.

Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.6 **Cryptographie**

Le niveau de conformité de cette clause est de **0%.**

Cela s'explique par l'absence d'une politique d'utilisation des mesures cryptographiques pour la protection de l'information.

Le niveau de maturité accordé à cette clause est donc **Nul.**

#### 3.2.2.7 **Sécurité physique et environnementale**

La moyenne de cette clause est de 54,5% par rapport à la norme ISO/IEC 27002.

L'environnement de localisation ne présente pas d'exposition à des dangers naturels apparents dans l'ensemble appart la salle serveur qui ne suit pas à la lettre la recommandation de sécurité. En ce qui concerne la sécurité physique des locaux elle est assurée par une clôture qui les entoure, ainsi que des postes de gardiennage qui surveillent les principales entrées. Un mécanisme d'enregistrement des visiteurs a été instauré. Il permet de relever les identités des visiteurs ainsi que les dates et heures d'entrée et sortie. La zone sensible qu'est la salle serveur bénéficie d'une sécurité toute particulière, et ce à travers l'accès qui y est très réservé. En effet pour protéger cette salle de toute malveillance physique l'accès est limité aux personnes concernées possédant les clefs. La salle des serveurs. Concernant les actifs critiques (Firewall, switch…), utilisent la technologie de clustering, afin d'assurer la répartition de charge et la disponibilité et éviter l'arrêt des services. Les bureaux des employés sont dotés de serrures, offrant la possibilité de les verrouiller pendant leur absence.

Le niveau de maturité accordé à cette clause est donc **moyen**.

#### 3.2.2.8 **Sécurité liée à l'exploitation**

La moyenne de cette clause est de 50% par rapport à la norme ISO/IEC 27002.

Les mesures de continuité de services sont en parties assurées. Il s'agit des sauvegardes des bases de données des serveurs, effectuées une seule fois par jour. Ces sauvegardes ainsi que tous les évènements enregistrés sur les moyens de traitement de l'information sont conservées. Nous notons également qu'il existe de redondances des serveurs pour permettre une reprise presque instantanée en cas de panne de l'un des serveurs. On a constaté aussi que le système ne dispose pas d'une fonction automatique de surveillance en temps réel en cas d'accumulation d'événements anormaux, pour le moment il n'existe pas un système de détection d'intrusion et d'anomalies sur le réseau de l'organisme. Le niveau de maturité accordé à cette clause est donc moyen.

#### 3.2.2.9 **Sécurité des communications**

La moyenne de cette clause est de **50%** par rapport à la norme ISO/IEC 27002.

L'ensemble des serveurs est protégé d'intrusions externes (provenant de l'Internet) malveillantes par un firewall, Il n'existe cependant pas de DMZ pour l'instant au sein de cet organisme. Le réseau LAN de l'organisation est de type Ethernet. Une politique d'adressage par sous réseau existe pour permettre une segmentation, à un niveau plus élevé.

Le niveau de maturité accordé à cette clause est donc **moyen**.

#### 3.2.2.10**Acquisition, développement et maintenance des Systèmes d'information**

La clause enregistre une moyenne de **55,5%** par rapport à la norme ISO/IEC 27002.

L'acquisition de nouveaux systèmes porte l'attention particulière des dirigeants afin de s'assurer que le système à acquérir correspond aux besoins de l'organisme et ne mettra pas à mal la sécurité. Loin de là un groupe de développeurs est mis en place pour au lieu d'acquérir des nouveaux systèmes d'information ils les développent selon le besoin de l'organisme tous en s'assurant que les questions de sécurité de l'information sont étudiées et mises en œuvre. Également des tests sont effectués pour s'assurer qu'un nouvel équipement ne sera pas source de régression. Le niveau de maturité accordé à cette clause est donc **moyen**.

#### 3.2.2.11 **Relations avec les fournisseurs**

La moyenne de cette clause est de **25%** par rapport à la norme ISO/IEC 27002.

On a constaté l'absence de tous types d'exigences de sécurité de l'information documenté dans les contrats de prestation de services pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation. Cert L'organisation surveille et vérifie la prestation des services assurés par les fournisseurs, mais les accords conclus avec ces derniers n'inclure aussi pas d'exigences sur le traitement des risques liés à la

sécurité de l'information associé à aux produits et aux services informatiques fourni. Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.12 Gestion des incidents liés à la sécurité de l'information

La clause enregistre une moyenne de **28,57%** par rapport à la norme ISO/IEC 27002.

Le personnel a été sensibilisé sur la nécessité de déclarer les incidents ou failles de sécurité rencontrée. Cependant, pour l'instant il n'y a pas une planification d'instauration de procédures pour la gestion des incidents de sécurité ni l'Edition de rapports détaillés de ces derniers qui surviennent. Il n'est donc pas possible de s'informer des incidents déjà survenus.

Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.13 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **50%**.

Le plan de continuité d'activité ou de reprise d'activité se base essentiellement sur les sauvegardes de bases de données. Les actions à entreprendre en cas de reprise à la suite d'une catastrophe ne sont pas documenté, c'est suivant l'appréciation du responsable SI ou l'un de ses subordonnés que ces actions sont menées. Concernant la protection électrique, seuls les serveurs et les composants réseaux sont protégés par des onduleurs pour éliminer les problèmes d'alimentation électrique de courte durée, les prises de courant électriques sont non-ondulés. Le niveau de maturité accordé à cette clause est donc **moyen.**

#### 3.2.2.14 Conformité

Le niveau de conformité de cette clause par rapport à la norme ISO/IEC 27002 est de **40%**. Les responsables s'assurent de l'exécution correcte de l'ensemble de procédures de sécurité interne (chartre informatique, procédure IT) placées sous leur responsabilité. En vue de garantir leur conformité avec les normes de sécurité les dirigeants envisagent

de continuer le projet de mise en place d'un système de management de la sécurité de l'information. Le niveau de maturité accordé à cette clause est donc **faible**.

#### 3.2.2.15 **Conclusion**

L'audit a mis l'accent sur les vulnérabilités d'ordre organisationnel et physique existantes au niveau du système de l'information du SIM Agro. L'étape suivante consiste à quantifier les risques présents en estimant leurs impacts, leurs potentialités et leurs gravités.

# *Chapitre IV*

# *Analyse des risque*

# 4 Analyse des risques

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 et en estimant leurs impacts, leurs potentialités et leurs gravités.

## 4.1 Approche d'analyse des risques

Notre méthode basée sur la méthode MEHARI consiste à mettre en place une base de connaissance ou nous allons aborder successivement :

- L'active qui doit être le sujet de l'estimation
- Quelle vulnérabilité
- Quelle menace
- Analyse des menaces : événements déclencheurs
- Analyse des facteurs de réduction des risques

La démarche d'analyse de risques expliquée dans la figure ci-dessous aboutira à une base de connaissance propre à l'entreprise.

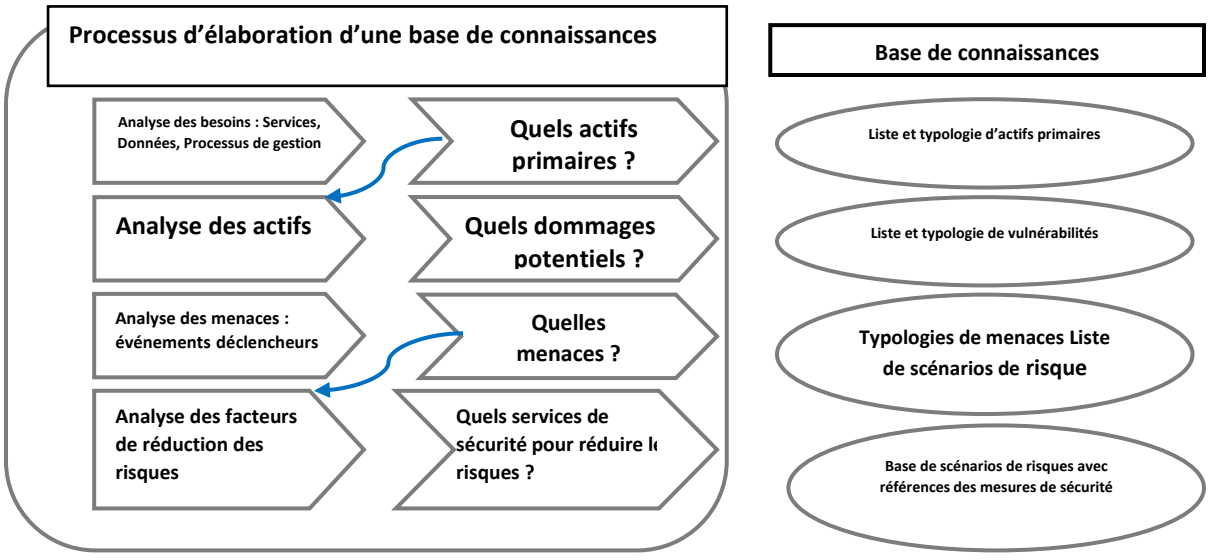


*Figure 5: démarche d'analyse de risque*

L'estimation de risque que nous proposons de réaliser aura pour objectif de déterminer les risques les plus graves sur le périmètre d'étude. Le risque peut être défini comme la conséquence de l'exploitation d'une faille en tenant compte de son impact et de sa potentialité.

## 4.2 Paramètre d'évaluation du risque

L'analyse des risques est l'utilisation systématique d'informations pour estimer le risque. Elle fournit une base à l'évaluation, au traitement et à l'acceptation du risque.[5] L'objectif de cette analyse est d'évaluer deux paramètres caractéristiques du risque encouru par l'entreprise ou l'organisme dans l'hypothèse d'occurrence d'un tel scenario. Ces paramètres sont :

- La potentialité : la potentialité du risque qui représente, en quelque sorte, sa probabilité d'occurrence, cette potentialité est en fonction du contexte et des mesures de sécurité en place.
- L'impact : l'impact du risque sur l'entreprise, qui présente la gravité des conséquences directes et indirectes qui découleraient de l'occurrence du risque. Il est éventuellement réduit par la mise en œuvre de mesures de sécurité adaptées.
- La gravité : la gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact.

Afin de quantifier le risque correspondant au scénario analysé, les évaluations de la potentialité et de l'impact seront faites sur une échelle ayant 4 niveaux.

### 4.2.1 L'impact

L'impact devrait être considéré comme un nombre entre 1 et 4.

- 1/ MINEURE : Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens.
- 2/ SIGNIFICATIVE : Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés.

- 3/GRAVE : Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés.
- 4/CRITIQUE : Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation.

### 4.2.2 La potentialité

La potentialité de la survenance d'un scénario de risque, devrait être considérée comme un nombre entre 1 et 4.

- 1/peu Vraisemblable : Le risque est non envisagé
- 2/ Vraisemblable : Le risque est improbable, mais sa survenance demeure possible
- 3/ Très vraisemblable : Il est probable que le risque se produise à plus ou moins court terme
- 4/ quasi certain **:** Il est très probable que le risque se produise très certainement et à court terme

## 4.3 Evaluation de la potentialité et de l'impact

L'objectif de cette étape est de calculer la gravité de chaque menace en calculant son impact et sa potentialité et nous nous basons pour le faire sur MEHARI, cette méthode s'appuie sur un modèle de risque qui distingue :

- Deux facteurs structurels, indépendants de toutes mesures de sécurité qui sont l'exposition naturelle et l'impact intrinsèque.
- Deux facteurs de réduction de la potentialité : Dissuasion et prévention.
- Trois facteurs de réduction de l'impact : confinement (ou protection), mesures palliatives et transfert du risque.[8]

La figure ci-dessous explique mieux le concept de mesure de la potentialité et de l'impact par la méthode MEHARI.

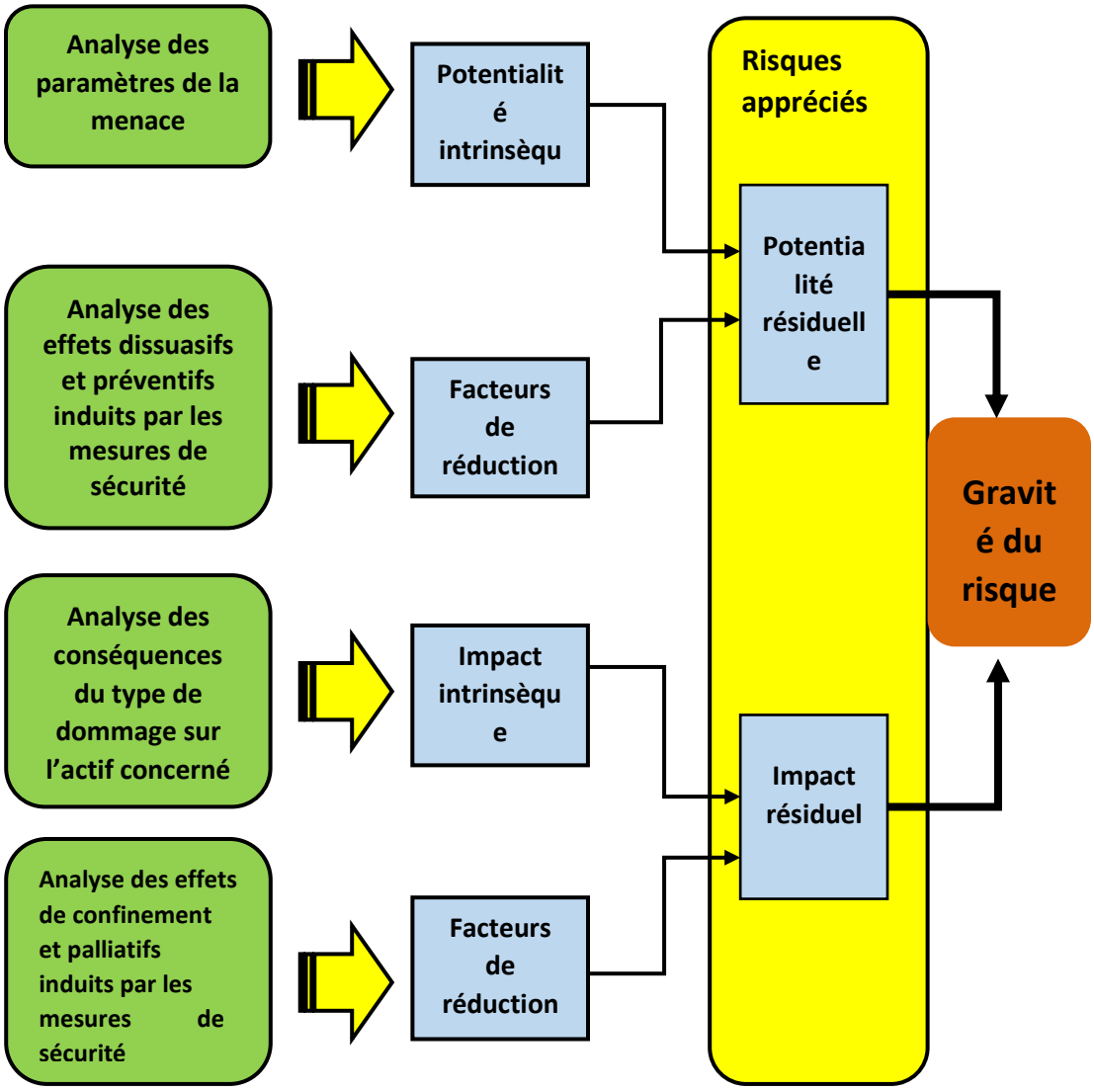


*Figure 6: processus d'estimation des risques MEHARI* [4]

### 4.3.1 **Evaluation de potentialité**

MEHARI propose une évaluation de la potentialité en partant de l'évaluation de L'exposition naturelle et du niveau de mesure entre dissuasif et préventif.[8]

➢ L'exposition naturelle à un risque donné peut dépendre de :

- Sa localisation et de son environnement, pour les risques naturels.
- L'enjeu potentiel d'un acte volontaire, pour son auteur (vol, détournement, satisfaction intellectuelle, etc.).

➢ Les mesures dissuasives qui permettent d'éviter la mise en œuvre des menaces potentielles.

➢ Les mesures préventives qui empêchent qu'une menace se réalise.

### 4.3.2 **Evaluation de l'impact**

L'évaluation de l'impact se fait par l'analyse préalable de plusieurs facteurs [8] :

➢ L'impact intrinsèque : L'impact intrinsèque d'un scénario est l'évaluation des conséquences de l'occurrence du risque, indépendamment de toute mesure de sécurité.

➢ Les mesures de protection qui limitent l'impact d'une menace. Ces mesures de protection sont :

- Mesures d'isolement et de compartimentage physique.
- Mesures de détection (intrusion, accidents, erreurs, etc.).
- Contrôle a posteriori incorporés aux processus et applications informatique.
- Capacité d'investigation sur détection d'anomalies.
- Capacité d'intervention rapide.

➢ Les mesures palliatives qui permettent de limiter les conséquences de la mise en œuvre d'une menace. Ces mesures concernent :

- L'étude préalable des modes dégradés acceptable, des fonctions minimales à remplir et des services indispensables.
- L'anticipation et de la préparation des solutions palliatives adéquates.
- La préparation et de la formation des hommes et des structures en préavisant des situations de crise (gestion de la crise, communication de crise, etc.).

➢ Les mesures de récupération qui visent à récupérer une partie du préjudice par transfert du risque se basent sur :

- Analyse spécifique des risques à couvrir par l'assurance.

- Couverture des risques insoutenables par l'assurance.

### 4.3.3 Evaluation de la gravité de risque

La mesure globale du risque, sa gravité, résulte d'une décision stratégique de l'organisation fondée sur les valeurs d'impact et de potentialité. La gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact. La grille d'acceptabilité des risques suivante définie, en fonction de l'impact et de la potentialité estimés si le risque est acceptable ou non [9].

*Tableau 7: grille d'acceptabilité des risques*

| IMPACT | | | | | |
|---|---|---|---|---|---|
| | 4 | 2 | 3 | 4 | 4 |
| | 3 | 2 | 3 | 3 | 4 |
| | 2 | 1 | 2 | 2 | 3 |
| | 1 | 1 | 1 | 1 | 2 |
| | | 1 | 2 | 3 | 4 |
| | | Potentialité | | | |

*Tableau 8:niveau de risque*

| Gravité du risque | Description |
|---|---|
| $3 < R \leq 4$ | Risques insupportable |
| $2 < R \leq 3$ | Risques inadmissibles |
| $0 < R \leq 2$ | Risques tolérés |

## 4.4 Application de la démarche :

Après la définition du périmètre et de la méthode de gestion des risques, Nous allons dans la suite dégager les ressources les plus critiques interagissant avec notre processus métier et qui une défaillance de leur côté suite a une menace exploitée affectera directement ce dernier, cela en se basant sur une discussion approfondie avec les

responsables du département SI de la SIM Agro et par la suite dégager une base de scénarios spécifiques qui servira comme point de départ dans l'estimation et la classification des risques majeurs.

### 4.4.1 Identification et classification des ressources :

Le tableau suivant est le résultat de recensement effectué dans le périmètre de notre projet, toujours avec la présence du responsable SI.

*Tableau 9:Ressources Matérielles et Humaines*

| Ressources | Type |
|---|---|
| Serveur AD Exchange | Serveur |
| Serveur d'application | Serveur |
| Serveur de données | Serveur |
| Onduleur | Equipement électricité |
| Routeur / switch | Equipement réseau |
| Personnel informatique | Ressource humaine |
| Réseau local | Réseau |

Apres l'identification des ressources matérielles et humaines liées au périmètre et après discussion avec le responsable SI pour choisir les ressources les plus critiques sur lesquels l'estimation doit être focalisée. Nous avons décidé d'étudier les risques liés aux :

- Serveur ERP
- Serveur de données

On a choisi deux serveurs qui ne bénéficie pas du même déploiement de mesure de sécurité

### 4.4.2 Création d'une base spécifique de scénarios :

À partir de la base de scénarios types proposés par la méthode MEHARI, On a bâti une base de scénarios adaptée au domaine étudié et les vulnérabilités qui faciliteront l'exploitation de ces scénarios. Le choix des scénarios est basé sur les discussions avec le responsable.

Les menaces qui découlent sont des grandes lignes qui regroupent les scénarios de notre base de connaissances regroupés en familles correspondant au même type d'actif et au même type de dommage comme suite :

#### 4.4.2.1 Dégâts des eaux et incendie :

- Incendie.
  - Incendie : accident interne endommageant gravement des équipements informatiques critiques.
- Inondation.
  - Inondation due à une canalisation percée ou crevée et rendant indisponibles des équipements informatiques critiques.

#### 4.4.2.2 Indisponibilité des ressources :

- Accident ou panne mettant hors service une ou plusieurs ressources matérielles :
  - Accident de nature électrique (court-circuit), mettant hors service un équipement informatique critique.
  - Panne rendant indisponible un équipement informatique critique.
  - Panne rendant indisponible un système terminal mis à la disposition des utilisateurs (PC, périphérique spécifique, etc.)
- Impossibilité de maintenance :
  - Défaillance matérielle d'un équipement critique impossible à résoudre par la maintenance, ou indisponibilité du prestataire.
- Modification du matériel :
  - Dégradation involontaire de performances, à l'occasion d'une opération de maintenance matérielle à la suite d'une panne d'un système.
- Surutilisation accidentelle de ressources informatiques ou réseau :

- Dégradation des performances du réseau local due à une saturation accidentelle de ressources résultant d'un incident ou d'une panne sur un équipement du réseau.

#### 4.4.2.3 **Dysfonctionnement logiciel :**

- Modification du logiciel :
  - Dégradation involontaire des performances applicatives, à l'occasion d'une opération de maintenance corrective ou évolutive de logiciel.
- Effacement de code exécutable ou de configurations :
  - Effacement direct de code exécutable par une personne autorisée (exploitation, support informatique, maintenance, etc.)
- Altération malveillante des fonctionnalités prévues d'une application :
  - Altération malveillante des fonctionnalités prévues d'une application via une bombe logique ou une porte dérobée.
- Modification volontaire des fonctionnalités prévues d'une application informatique :
  - Modification volontaire des fonctionnalités prévues d'une application par les équipes de développement, par la maintenance ou par le personnel d'exploitation.
- Accident d'exploitation :
  - Altération accidentelle des données pendant la maintenance.
- Effacement par bombe logique :
  - Effacement de fichiers de données applicatives par bombe logique introduite par un administrateur ou un ingénieur système (sabotage).
- Effacement de supports par virus :
  - Effacement des fichiers de données partagés, par un virus.
- Effacement de fichiers par bombe logique :
  - Destruction ou pollution massive de fichiers de données applicatives et de leurs sauvegardes, par voie logique par un ingénieur système de l'équipe d'exploitation.
  - Destruction ou pollution massive de fichiers programmes (codes sources) et de leurs sauvegardes, par voie logique par un ingénieur système de l'équipe d'exploitation.

#### 4.4.2.4 **Abus ou usurpation des droits :**

▪ Données applicatives faussées pendant la transmission :

- Données applicatives faussées pendant la transmission par un membre du personnel manipulant un équipement de réseau local.
- Données applicatives faussées pendant la transmission par un membre du personnel branchant un équipement parasite en coupure sur le réseau local (man in the middle).

▪ Saisie faussée de données :

- Saisie de fausses données par un membre du personnel usurpant l'identité d'un utilisateur autorisé.

▪ Manipulation de fichiers :

- Manipulation de fichiers de données par un tiers non autorisé usurpant l'autorité d'un utilisateur autorisé.
- Manipulation de fichiers de données par un membre du personnel autorisé illégitime.

#### 4.4.2.5 **Espionnage et malveillance à distance :**

▪ Accès au système et consultation :

- Accès au système et consultation en ligne, par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu.
- Accès au système et consultation en ligne, par un tiers autorisé à pénétrer dans les locaux et ayant accès (physique) au réseau local interne (prise LAN dans une salle de réunion).

▪ Captation d'informations fugitives :

- Captation d'informations fugitives : branchement d'un équipement parasite sur le réseau local, dans les locaux de l'entreprise, par une personne autorisée à y pénétrer.
- Captation d'informations fugitives : modification distante d'un équipement de réseau, pour piéger les messages échangés, par un utilisateur autorisé à se connecter sur le réseau interne.
- Transfert de données sensibles détourné par un pirate ayant connecté un équipement usurpant l'identité d'une entité connectée au réseau étendu.

▪ Falsification de message :

- Message faussé pendant la transmission entre un utilisateur et le réseau interne.

▪ Accès au système et copie de fichiers de données applicatives :

- Copie de fichiers de données applicatives par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu.
- Copie de fichiers de données applicatives par une personne non-membre du personnel ayant accès aux locaux et la possibilité de se connecter sur le LAN.
- Accès au système et copie de fichiers de données applicatives par un agent autorisé illégitime.
- Accès au système et copie de fichiers de données applicatives par une personne du développement via une porte dérobée placée dans une application.

▪ Accès aux serveurs et copie de fichiers partagés :

- Copie de fichiers partagés (serveur de données partagées) par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu.
- Copie répétée de fichiers par une personne membre du personnel non autorisé sur le poste de travail.

▪ Détournement de code source :

- Détournement du code source d'une application stratégique par un pirate se connectant depuis l'extérieur sur un port ouvert du réseau étendu.

▪ Effacement ou destruction de configurations logicielles utilisateurs :

- Effacement de configurations utilisateurs par un tiers.

#### 4.4.2.6 Saturation du système

▪ Surutilisation malveillante de ressources informatiques ou réseau

- Dégradation des performances applicatives due à la saturation répétitive malveillante de moyens informatiques par un groupe d'utilisateurs.
- Dégradation de performances du réseau local due à la saturation du réseau par un ver.

#### 4.4.2.7 Non-conformité à la législation et à la réglementation

▪ Violation des droits de propriété industrielle :

- Utilisation de logiciels sans licences.

## 4.5 L'impact des scénarios recensé

Après avoir abouti à une base de scénarios, nous avons discuté l'impact de ces derniers sur les actifs à base des paramètres que nous avons cité en de-sous

### 4.5.1 Pour le Serveur ERP :

La discussion est faite en présence de la Responsable de DSI, ou pour chaque famille de scénario, nous avons et selon les critères d'évaluation de l'impact intrinsèque et l'existence des mesures de sécurité qui permet la réduction de ces derniers estimé une valeur pour définir l'impact qu'aura le scénario si ce dernier se produira.

*Tableau 10:Base des scénarios et leur impact sur le Serveur d'application*

| Ressources | Scénario | | Impact |
|---|---|---|---|
| Serveur ERP | 1 | Dégâts des eaux et incendie | 4 |
| | 2 | Indisponibilité des ressources | 4 |
| | 3 | Dysfonctionnement logiciel | 4 |
| | 4 | Abus ou usurpation des droits | 3 |
| | 5 | Espionnage a distance | 4 |
| | 6 | Saturation du système | 4 |

A titre d'exemple, lors de la discussion, la famille des scénarios « Dégâts des eaux et incendie » s'est vu attribué la valeur de **4** car pour l'emplacement du serveur ERP aucune mesure de sécurité est prise, il est localisé dans le bureau des développeurs, loin du DATA Center ou les critères de sécurité sont plus fiable.

### 4.5.2 Pour le Serveur de données :

*Tableau 11: Base des scénarios et leur impact sur le Serveur de données*

| Ressources | Scénario | | Impact |
|---|---|---|---|
| **Serveur de donnés** | **1** | **Dégât des eaux et incendie** | **4** |
| | **2** | **Indisponibilité des ressources** | **4** |
| | **3** | **Dysfonctionnement logiciel** | **4** |
| | **4** | **Abus ou usurpation des droits** | **3** |
| | **5** | **Espionnage à distance** | **3** |
| | **6** | **Saturation du système** | **3** |

A titre d'exemple, lors de la discussion, et toujours pour le cas de la famille des scénarios « Dégâts des eaux et incendie », On a attribué la valeur de **4** car pour l'emplacement du serveur de données et même si ce dernier est localisé dans le DATA Center, ce dernier ne respecte pas les normes de sécurité exigée pour construire un DC, rendant l'impact d'inondation ou d'incendie Critique.

## 4.6 Evaluation quantitative des scénarios

La gravité du scénario ou de la situation de risque résulte à la fois de sa potentialité et de son impact en se basant sur la grille d'aversion du risque.

Partant de la base spécifique de scénarios et de l'évaluation automatique de leur gravité, il devient aisé de calculer le niveau de gravité de chaque scénario comme le montrent les tableaux ci-après.

### 4.6.1 Pour le Serveur ERP :

*Tableau 12: évaluation quantitative des risque pout le serveur d'application ERP*

| Ressources | Scénario | | Potentialité | Impact | Gravité |
|---|---|---|---|---|---|
| Serveur ERP | 1 | Dégâts des eaux et incendie | 2 | 4 | 3 |
| | 2 | Indisponibilité des ressources | 2 | 4 | 3 |
| | 3 | Dysfonctionnement logiciel | 3 | 4 | 4 |
| | 4 | Abus ou usurpation des droits | 3 | 3 | 3 |
| | 5 | Espionnage a distance | 3 | 4 | 4 |
| | 6 | Saturation du système | 3 | 4 | 4 |

### 4.6.2 Pour le Serveur de données :

*Tableau 13:évaluation quantitative des scénarios pour le serveur de donnée*

| Ressources | Scénario | | Potentialité | Impact | Gravité |
|---|---|---|---|---|---|
| Serveur de donnés | 1 | Dégât des eaux et incendie | 2 | 4 | 3 |
| | 2 | Indisponibilité des ressources | 1 | 4 | 2 |
| | 3 | Dysfonctionnement logiciel | 2 | 4 | 3 |
| | 4 | Abus ou usurpation des droits | 2 | 3 | 3 |
| | 5 | Espionnage à distance | 1 | 3 | 2 |
| | 6 | Saturation du système | 2 | 3 | 3 |

## 4.7 Le traitement des risques

Le traitement des risques consiste théoriquement à analyser chaque scénario de risque et à prendre des décisions spécifiques qui peuvent être :

- Accepter le risque tel quel.
- Réduire le risque c'est-à-dire prendre des mesures pour que l'impact ou la potentialité ou les deux soient réduits et diminuent la gravité résiduelle en conséquence.
- Décider d'éviter le risque en supprimant la situation de risque par des mesures structurelles ou organisationnelles
- Transférer le risque, essentiellement par l'assurance

En pratique, nous avons travaillé en adoptons l'approche de MEHARI qui consiste à ce que le traitement soit par familles de scénarios visant le même type d'actif et ayant donc le même impact intrinsèque et sélectionner des plans d'action par famille [5]

### 4.7.1 Sélection de plans d'action par famille de scénarios

Les scénarios de notre base de connaissances ont été regroupés en familles correspondant au même type d'actif et au même type de dommage.

Pour chaque couplé (famille de scénario /vulnérabilité), des mesures de la norme ISO 27002 ont été référé pour permettre au responsable de la DSI de dissuader, confiner ou pâlir ces menaces et un chapitre de la politique de la SSI proposé est dédié (Annexe), des recommandations par rapport aux différentes clauses des normes de sécurité, sont proposés dans le dernier chapitre visant le renforcement de la sécurité selon les résultats de l'analyse des risques encourut.

Comme le tableau l'exprime nous avons recensé quatre vulnérabilités pour la famille des scénarios (Abus ou usurpation de droit)

- Absence de dispositif de contrôle d'accès robuste
- Absence de journalisation des événements
- La base de mots de passe du système d'exploitation est déchiffrable
- Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés

Ces vulnérabilités ont été associé aux mesures de sécurité adéquat qui seront documenté dans le chapitre **contrôle d'accès** de la politique de la sécurité des systèmes d'information proposé.

| Menaces | Vulnérabilités | Objectifs de sécurité (classé selon l'ISO 27002 :2013) | Mesures 1 | Mesures 2 | Mesures 3 | Politique de Sécurité (Chapitre de la PSSI) |
|---|---|---|---|---|---|---|
| Abus ou usurpation de droit | **Absence de dispositif de contrôle d'accès robuste** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.1(Restriction d'accès à l'information) L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès. | A.9.4.2(Sécuriser les procédures de connexion) Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée. | A.9.4.4(Utilisation de programmes utilitaires à privilèges) L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée. | **Contrôle d'accès** |
| | **Absence de journalisation des événements** | A.12.4(Journalisation et surveillance) | A.12.4.1(Journalisation des événements) Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement. | A.12.4.3(Journaux administrateur et opérateur) Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement. | | **Contrôle d'accès** |
| | **La base de mots de passe du système d'exploitation est déchiffrable** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.3(Système de gestion des mots de passe) Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe. | A.9.4.2(Sécuriser les procédures de connexion) Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée. | | **Contrôle d'accès** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés** | A.10.1(Mesures cryptographiques) | A.10.1.1(Politique d'utilisation des mesures cryptographiques) Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre. | A.10.1.2(Gestion des clés) Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie. | | **Contrôle d'accès** |

*Tableau 14:Base de scénarios de risques avec références des mesures de sécurité*

### 4.7.2 **Conclusion :**

Dans ce chapitre nous avons essayé de faire une estimation de risques focalisée sur deux actifs critiques afin de déterminer la gravité des différents scénarios de risque possibles, les vulnérabilités facilitant l'exploitation de ces derniers, et les mesures de sécurité à mettre en place afin de neutraliser ces risques ou réduire leurs impacts.

Les résultats de cette étape de la mission seront utiles lors de l'élaboration de la politique de sécurité et les recommandations d'ordre organisationnel et physique détaillées dans le dernier chapitre.

# *Chapitre V*

# *Politique de sécurité des systèmes d'information et recommandations*

# 5 Politique de sécurité des systèmes d'information et recommandations

Dans ce dernier chapitre nous allons nous consacrer aux revendication fournis et aux bonnes pratiques choisis après l'analyse des différents risques encoururent par notre périmètre d'étude.

## 5.1 Politique de sécurité des systèmes d'information

En analysant les risques, on peut construire une politique de sécurité du SI, qui permet de définir et de cadrer les bonnes pratiques d'utilisation des moyens informatiques et de télécommunications constituant l'ensemble du système d'information de la SIM Agro.

### 5.1.1 But de la politique de sécurité

La politique de sécurité informatique fixe les principes visant à garantir la protection des ressources informatiques et de télécommunications en tenant compte des intérêts de l'organisation et de la protection des utilisateurs. Elle sera la référence pour toute démarche future de conformité avec les normes de sécurité, ou pour établir un deuxième cycle PDCA de ce présent travail.

### 5.1.2 Périmètre de la politique de sécurité et domaine d'application

En prenant compte du présent travail, les recommandations et les directifs regroupés dans ce chapitre couvrent non seulement le périmètre réduit de l'étude, mais aussi l'ensemble de l'organisme, les bonnes pratiques d'utilisation s'appliquent à tous les utilisateurs et les contributeurs du System d'information.

### 5.1.3 Structure du document

#### 5.1.3.1 Organisation de la sécurité

Cette clause de la politique couvre l'ensemble des besoins de l'organisme en sécurité de l'information du point de vu organisationnel.

Nous avons essayé de réduire les risques des non-conformités liées au chapitre 6,7 et 8 de la norme ISO 27002, détectés dans la phase d'analyse.

Cette clause mettra le point sur des essentialité délaissé par les responsables du département SI tel que la répartition des tâches liée à la sécurité, l'importance de la sensibilisation des utilisateurs de leurs contribution dans la sécurité et le bon fonctionnement des mécanismes mis à leur disposition, et l'utilité de la classification de ces derniers, La clause comportera une procédure nommé « Politique du bureau propre et de l'écran vide » visant la documentation des différentes directives assurant la confidentialité et l'intégrité de l'ensemble des informations sensibles.

#### 5.1.3.2 **Protection physique**

Cette clause de la politique couvre l'ensemble des besoins de l'organisme en sécurité de l'information du point de vu environnementale et physique.

Nous avons essayé de réduire les risques des non-conformités liées au chapitre 11 de la norme ISO 27002, détectées dans la phase d'analyse.

Cette clause vise à cadrer les procédures d'entretien, de maintenance et d'installation des équipements dans le but d'éliminer toutes possibilité de défaillance due au vieillissement du matériel ou des pannes susceptibles.

#### 5.1.3.3 **Suivi de l'Exploitation**

Cette clause de la politique couvre l'ensemble des besoins de l'organisme en sécurité de l'information du point de vu de l'exploitation et du développement des systèmes d'information de l'organisme.

Nous avons essayé de réduire les risques des non-conformités liées au chapitre 12 de la norme ISO 27002, détectées dans la phase d'analyse.

Cette clause mettra le point sur des essentialités délaissées ou sous-estimées par les responsables du département SI telles que la séparation de l'environnement de développement de celui du traitement de l'information, du besoin essentiel des sauvegardes et de la redondance et de la protection des systèmes d'exploitation.

Elle vise aussi à sensibiliser l'ensemble de l'équipe de développement sur l'importance de la sécurité tous au long du cycle de vie du projet, en les incitant à documenter leur travail (Architecture Techniques, Spécifications fonctionnelles, rapport de tests, etc.) pour permettre aux auditeurs une fois sur place de s'assurer que les mécanismes de sécurité sont bien mis en œuvre.

#### 5.1.3.4 **Continuité de l'activité**

Cette clause de la politique couvre l'ensemble des besoins de l'organisme en sécurité de l'information du point de vu de la gestion de la continuité de l'activité des différent composant du Système d'information de l'organisme.

Nous avons essayé de réduire les risques des non-conformités liées au chapitre 17 de la norme ISO 27002, détectées dans la phase d'analyse.

Cette clause mettra le point sur le besoin de l'entreprise par rapport à la haute disponibilité essentielle à l'aspect fonctionnel et la continuité des services vitaux aux traitements de l'information, pour cela une procédure de continuité et de reprise d'activité documenté, revue et mise a jours à intervalle définit est mise en place indiquant les directifs de la redondance.

#### 5.1.3.5 **Sauvegardes et journalisation**

Cette clause de la politique couvre la une partie du chapitre 12 de la norme ISO 27002, elle est donc complémentaire de la clause précédente, son importance nous a motivé pour l'aborder indépendamment,

Nous avons essayé de réduire les risques des non-conformités liées à cette partie du chapitre 12 de la norme ISO 27002, détectées dans la phase d'analyse.

Cette clause mettra le point sur l'ERP en cour de développement, la politique mise en œuvre permettant sa surveillance toute en précisant les modalités et les durées de conservation des différents journaux ainsi que les méthodes d'analyse des données produites.

La clause reprend la notion si importante de traçabilité des opérations effectuées sur l'ERP, pour garantir la supervision des actifs, afin de détecter le moindre dysfonctionnement qui pourrait remettre en cause l'intégrité de l'information.

Le dispositif de sauvegarde destinées à permettre la conservation des données importants et à assurer la continuité et la reprise d'activité est testé fréquemment, pour valider sa fiabilité.

#### 5.1.3.6 **Contrôle d'accès**

Cette clause de la politique couvre le besoin de l'organisme en termes de contrôle d'accès et la gestion du dispositif mis en œuvre pour garantir l'efficacité de ce dernier.

Nous avons essayé de réduire les risques des non-conformités liés au chapitre 9 de la norme ISO 27002, détectées dans la phase d'analyse.

Cette clause mettra le point sur le principe de manquement des responsables en matière de contrôle d'accès, celui de l'exploitation moyenne du dispositif mis en place soit l'Active directory en l'associant à une politique de contrôle d'accès documentée et tenue à jour fréquemment, visant l'optimisation des prestations du dispositif.

L'adoption d'une politique telle que le RBAC[1] nous est paru chose primordiale pour l'élimination des accords d'accès individuel nocive et non instantanément contrôle, et la supervision des fonctions nécessitant l'accès privilégié.

## 5.2 Recommandation d'ordre organisationnel et physique

Les recommandations proposées visent à améliorer l'aspect organisationnel et physique de la sécurité de la SIM Agro.

### 5.2.1 **Séparation et réorganisation des tâches liées à la sécurité**

Organiser et attribuer les responsabilités liées à la sécurité permet d'assurer une implémentation appropriée des mesures de sécurité en rapport avec les objectifs de la société, et de pouvoir prévenir et anticiper les risques éventuels sur les systèmes de la société avec rapidité et efficacité, parmi les étapes à considérer pour garantir ceci :

- Consacrer un poste de responsable de sécurité des systèmes d'information, et mettre à sa disposition tous les manuels, guides de procédures, de politiques et des chartes d'utilisation.
- Désigner un comité de soutien qui aura pour mission le suivi de l'état de sécurité et d'aider le RSSI dans les prises de décisions nécessaires.

[1] RBAC : role-based Access control est une méthode de sécurité d'accès basée sur le rôle d'une personne au sein d'une entreprise.

- Définir les responsabilités (en termes de sécurité) de chaque utilisateur du SI et diffuser le document correspondant.

### 5.2.2 Formation et sensibilisation des utilisateurs

Les mesures prises pour sécuriser le Système d'information ne peuvent être efficaces que si l'ensemble du personnel soit conscient de l'importance de son adhésion au projet et capable de distinguer les bonnes pratiques qui mettent le SI à l'abri de tout danger :

- Planifier des cycles de formation spécifiques et approfondis en sécurité pour tout le service informatique. Une fois formés, les informaticiens seront capables d'organiser des journées de sensibilisation pour le reste des utilisateurs du SI,
- Sensibiliser et former le personnel aux menaces dues aux éventuelles intrusions causées par leur négligence.

### 5.2.3 Classification des ressources

Pour faciliter la gestion des ressources et des dangers qui menacent leur utilisation, il est fortement recommandé de :

- Définir une classification des informations sensibles de l'organisation. Cette classification doit être basée sur les 3 axes correspondant aux besoins en termes de Disponibilité, Intégrité et Confidentialité pour pouvoir lui attribuer le niveau de protection nécessaire.
- Rédiger pour chaque équipement réseau une charte d'utilisation qui décrit comment exploiter cet équipement d'une manière sécurisée, que faut-il faire en cas de panne, et à qui faut-il s'adresser en cas de problème.

### 5.2.4 Protection des ressources et des actifs

La protection physique des ressources est un des principaux enjeux de la sécurité nous recommandons de :

- S'assurer que les actifs les plus critiques sont à l'abri de tout danger : vol, inondation, incendie et chocs électriques…

- Les supports contenant les sauvegardes de secours doivent être fortement protégées dans des armoires anti-feu par exemple et ne doivent pas être dans le même endroit qui abrite les supports en activité.

### 5.2.5 Valorisation des audits

Les missions d'audit internes et externes permettent de savoir à quel niveau le SI est-il conforme aux exigences de la sécurité et quelles sont les mesures à prendre pour le sécuriser d'une façon efficace.

Nous recommandons de planifier des audits internes et externes d'une manière régulière (au moins une fois par an), et ceci pour évaluer le niveau de sécurité de l'organisme et des procédures efficaces de traitement des risques, en s'appuyant sur l'avis d'un expert externe en sécurité dans les décisions importantes.

### 5.2.6 Mettre en place une procédure formalisée pour la gestion des utilisateurs

La procédure de contrôle d'accès déjà évoquée doit être documentée et installée sur les différents systèmes de la société pour formaliser les procédures suivantes :

- La création d'un nouvel utilisateur sur les systèmes d'exploitation et les applications,
- La modification d'un profil utilisateur (à la suite d'un changement d'affectation).
- La gestion de l'identification de l'utilisateur.
- Le départ d'un utilisateur (démission, départ en congé ou à la retraite).
- La revue ou l'audit de la sécurité logique (systèmes et applications).

## 5.3 Conclusion

Dans ce chapitre, en premier lieu, nous avons détaillé les six clauses de la politique de sécurité que nous avons proposé en se basant sur les résultats de la « Base de scénarios de risques avec références des mesures de sécurité »

En deuxième lieu nous avons proposé des recommandations que nous jugeons nécessaires à mettre en œuvre pour améliorer la sécurité du point de vue organisationnel et physique de la SIM Agro en se basant sur les exigences et les bonnes pratiques de la

norme ISO 27002 : 2013 afin de minimiser le risque d'exploitation des vulnérabilités détecté et de protéger les différents équipements pour assurer la continuité et la disponibilité du système d'information.

# Conclusion Générale

Les systèmes de management de la sécurité d'information occupent une place de plus en plus importante dans le domaine de la sécurité entrepreneuriale en Algérie. Beaucoup d'organismes optent pour cette solution en prenant compte des avantages commerciaux acquis par la certification ISO, et des avantages organisationnels bénéfiques adoptés en suivant les exigences et les bonnes pratiques de ces normes. C'était dans ce contexte que notre projet a pris lieu visant une planification adéquate d'un Système de gestion de la sécurité de l'information dans un périmètre réduit de la SIM Agro.

Notre mission s'est réalisée sur trois parties, la première était d'effectuer un audit organisationnel et physique basé sur les exigences de la norme ISO 27002 : 2013 qui est notre référentiel, la deuxième partie était l'analyse et l'estimation du risque inspirée de la méthodologie MEHARI et après avoir essayé de discerner les points forts et points faibles des deux méthodes d'analyse de risque, nous avons opté pour l'approche de MEHARI qui nous a paru le choix le plus convenable à notre étude, et enfin nous avons proposé dans la troisième partie une politique jugée nécessaire à mettre en œuvre pour améliorer la sécurité de notre domaine d'étude.

A travers ce projet, nous avons pu avoir une idée claire sur le monde de la sécurité entrepreneuriale et les différents risques qui menacent le bon fonctionnement et même la survie des entreprises. Après avoir déroulé et appliqué les directives de la méthodologie d'analyse des risques choisie, ensuite, tout au long du reste de ce mémoire, nous avons tenté d'apporter des solutions organisationnelles et physiques, afin de résoudre les problèmes suscités.

Notre travail constitue la première et la plus essentielle phase de la mise en place du système de management de la sécurité de l'information, les responsables de la SIM Agro se sont engagés à compléter ce cycle en mettant en œuvre les différentes directives et recommandations dans un premier temps, de s'offrir les services externes d'audit pour remettre le point sur l'état de la sécurité de leur organisme, de procéder annuellement à

un autre cycle PDCA suite à l'envie du comité de sécurité récemment formé de continuer notre initiative, et enfin de faire de la sécurité une nécessité dans tous types de projet.

Notre passage dans l'établissement même si nous avons réussi à avoir l'essentiel d'information voulu, avoir le soutien total des dirigeants était très difficile, ce chapitre de soutien qu'on a régulièrement rencontré lors de nos recherches concernant les documents lié à la norme ISO 27001 : 2013, et que toutes les sources le considérer comme acquis essentiel pour toutes démarche de mise en place d'un SMSI n'était malheureusement pas en notre faveur.

De plus, la répartition et la séparation des taches du département SI est faite selon l'appréciation des hauts dirigeants qui voyaient dans l'isolation du département de développement de l'ensemble du réseau une solution de sécurité, nous a causé beaucoup d'empêchements et a réduit notre vision de notre projet à ce travail présenté.

# Bibliographie

[1] : Alexandre FERNANDEZ TORO « Management de la sécurité de l'information ».4eme édition. EYROLLES. Septembre 2018.

[5] : Laurent Note. Détermination et évaluation des systèmes de management combinés. QUALITA' 2015, Mar 2015, Nancy, France. ffhal-01149773f

[6] : Agence française de normalisation « NF ISO 27002 version 2013 » janvier 2014.

[8] : Nabil Laoufi. Processus guidé pour l'identification des exigences de sécurité à partir de l'analyse des risques. Cryptographie et sécurité [cs.CR]. Conservatoire national des arts et metiers - CNAM, 2017.

[9] : Mohamed Habib Mazouni. Pour une meilleure approche du management des risques : de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision. Automatique /Robotique. Institut National Polytechnique de Lorraine - INPL, 2008.

# Webographie

[2] : <https://www.isms.online/iso-27001>

[3] : < https://www.silog.fr/blog/logiciel-erp-et-securite-informatique-quel-impact>

[4] : <https://clusif.fr/publications/guide-de-developpement-dune-base-de connaissance-danalyse-de-risque-mehari/>

[7] : audit organisationnel disponible sur < https://qualite.ooreka.fr>

**Annexe A** : Questionnaire d'audit organisationnel et physique

| | Thème | Article | Exigence | Questions à poser | Reponse/Constat | cote |
|---|---|---|---|---|---|---|
| | **5 POLITIQUE DE SECURITE** | | | | | |
| | | **5.1 Politique de sécurité de l'information** | **Objectif :**Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. | | | |
| 1 | | 5.1.1Politiques de sécurité de l'information | | | | |
| | | | **Mesure :** Un document de politique de sécurité de l'information doit être approuvé par la direction , puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés. | L'organisation et la gestion de la sécurité sont-elles formalisées dans un document chapeau couvrant l'ensemble du périmetre visé par la mise en place ? | **non** | **0%** |
| 2 | | 5.1.2 Revue des politiques de sécurité de l'information | | | | |
| | | | **Mesure :** Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps. | Cette politique de sécurité est-elle revue à intervalles réguliers afin d'assurer sa pertinence et son efficacité ? | **Non** | |
| | **6 ORGANISATION DE LA SECURITE DE L'INFORMATION** | | | | | |
| | | **6.1 Organisation interne** | **Objectif :** Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation. | | | |
| 3 | | 6.1.1 Rôles et responsabilités en matière de sécurité de l'information | | | | |
| | | | **Mesure :** Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées. | Les rôles et actions des différents acteurs de la SSI ont-ils été définis et ont-ils fait l'objet d'une communication ? | **Non** | **25%** |
| 4 | | 6.1.2 Séparation des tâches | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation. | Les tâches des différents acteurs de la SSI sont-elles séparées et documentées ? | **Non** | |
| **5** | 6.1.3 Relations avec les autorités | | | | |
| | | **Mesure :** Des relations appropriées avec les autorités compétentes doivent être entretenues. | | **Exclu** | |
| **6** | 6.1.4 Relations avec des groupes de travail spécialisés | | | | |
| | | **Mesure :** Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues. | Des contacts appropriés avec des groupes ou des associations professionnelles en sécurité sont-ils maintenus ? | **Oui** | |
| **7** | 6.1.5La sécurité de l'information dans la gestion de projet | | | | |
| | | **Mesure :** La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné. | La sécurité de l'information est-elle abordée dans la gestion de projet (quel que soit le type de projet) ? | **Non** | |
| | **6.2 Appareils mobiles et télétravail** | **Objectif :** Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles. | | | |
| **8** | 6.2.1 Politique en matière d'appareils mobiles | | | | **0%** |
| | | **Mesure :** Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles. | La procédure d'utilisation des appareils mobiles exige-t-elle ?-L'enregistrement de tous les appareils mobiles.-Une protection physique.-Une restriction des logiciels à installer.-Obligation de mise à niveau des logiciels et application,-Une protection contre les logiciels malveillants-La possibilité de désactivation ou effacement de données à distance.-Un système de sauvegarde. | **non** | |
| **9** | 6.2.2 Télétravail | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail. | | **Exlcu** | |
| | **7 Sécurité des ressources humaines** | | | | |
| | **7.1 Avant l'embauche** | **Objectifs :**<br>- Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées<br>- Réduire le risque de vol, de fraude ou de mauvais usage des équipements. | | | |
| **10** | 7.1.1 Sélection des candidats | | | | **50%** |
| | | **Mesure :** Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés. | Des critères spécifiques par rapport à la sensibilité des missions ont-ils été pris en compte lors du recrutement d'une personne? Sont-ils spécifiés dans les fiches de postes? | **oui** | |
| **11** | 7.1.2 Termes et conditions d'embauche | | | | |
| | | **Mesure :** Les accords contractuels avec les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information. | Les obligations contractuelles pour les entrepreneurs reflètent-elles la politique de l'organisation en matière de sécurité de l'information ? | **non** | |
| | **7.2 Pendant la durée du contrat** | | **Objectifs :** S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités. | | |
| **12** | 7.2.1 Responsabilités de la direction | | | | **67%** |
| | | **Mesure :** La direction doit demander à tous les salariés et sous-traitants d'appliquer les règles de sécurité de l'information conformément aux politiques et aux procédures en vigueur dans l'organisation. | Les employées et entrepreneurs sont-ils correctement informés de leurs rôles et responsabilités envers la sécurité de l'information ? | **oui** | |
| **13** | 7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**L'ensemble des salariés de l'organisation et, quand cela est pertinent, des sous-traitants, doit bénéficier d'une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions. | Les employées reçoivent-ils des formations et des programmes de sensibilisation envers la sécurité de l'information ? | **Non** | |
| **14** | 7.2.3 Processus disciplinaire | | | | |
| | | **Mesure :**Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information. | Existe-t-il un processus disciplinaire formel et communiqué en place pour agir contre les employés qui ont commis une violation de la sécurité de l'information ? | **Oui** | |
| | **7.3 Rupture, terme ou modification du contrat de travail** | | **Objectifs :**Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail. | | |
| **15** | 7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail | | | | **0%** |
| | | **Mesure :** Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, doivent être définies, communiquées au salarié ou au sous-traitant, et appliquées. | Les responsabilités et les devoirs qui restent valides après la terminaison ou le changement de l'emploi sont-ils bien définis et communiqués aux employées ? | **non** | |
| | **8 Gestion des actifs** | | | | |
| | **8.1 Responsabilités relatives aux actifs** | | **Objectif :** Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée. | | |
| **16** | 8.1.1Inventaire des actifs | | | | **75%** |
| | | **Mesure :**Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour. | Les actifs contenant de l'information sont-ils identifiés et inventoriés ? | **oui** | |
| **17** | 8.1.2 Propriété des actifs | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**Les actifs figurant à l'inventaire doivent être attribués à un propriétaire. | Les actifs maintenus dans l'inventaire ont-ils tous un propriétaire ?<br>Le propriétaire d'un actif est-il responsable de :<br>•S'assurer que l'actif est inventorié.<br>•S'assurer de la manipulation correcte de l'actif ainsi que la destruction appropriée. | **Non** | |
| **18** | 8.1.3 Utilisation correcte des actifs | | | | |
| | | **Mesure :**Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre. | Existe-t-il une « politique d'utilisation acceptable » qui prenne en compte l'ensemble des actifs informationnels auxquels ils ont accès ? | **Oui** | |
| **19** | 8.1.4 Restitution des actifs | | | | |
| | | **Mesure :**Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord. | Y a t il dans les contrats du personnel ou de la soutraitance des clause obligeant la restitutions des actifs informationnelle ? | **Oui** | |
| | **8.2 Classification de l'information** | **Objectif :** S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation. | | | |
| **20** | 8.2.1 Classification des informations | | | | **0%** |
| | | **Mesure :** Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée. | Les propriétaires de l'information sont-ils responsables de sa classification ?<br>La classification d'un actif indique-t-elle sa valeur et son niveau de critique ? | **non** | |
| **21** | 8.2.2 Marquage des informations | | | | |
| | | **Mesure :** Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation. | Existe t-il une procédure d'étiquetage qui refléter le système de classification établi en 8.2.1. | **non** | |
| **22** | 8.2.3 Manipulation des actifs | | | | |
| | | **Mesure :** Des procédures de traitement de l'information doivent être élaborées et mises en œuvre conformément au plan de classification de l'information adopté par l'organisation. | Le schéma de classification est-il aligné avec la Les procédures de traitement des actifs ? | **non** | |
| | **8.3 Manipulation des supports** | **Objectif :**Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports. | | | |
| **23** | 8.3.1 Gestions des supports amovibles | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l'organisation. | Des exigences de sécurité ont-elles été définies pour la gestion des supports amovibles (comment réagir en cas de perte, de vol, etc.)? Si oui, ont-elles fait l'objet d'une communication? | **Oui** | **50,00 %** |
| **24** | 8.3.2 Mise au rebut des supports | | | | |
| | | **Mesure :** Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles. | Existe-t-il des procédures formelles pour éliminer les médias en toute sécurité ? | **Non** | |
| **25** | 8.3.3 Transfert physique des supports | | | | |
| | | **Mesure :** Les supports contenant de l'information doivent être protégés contre les accès non autorisés, les erreurs d'utilisation et l'altération lors du transport. | Les médias contenant des informations confidentielles sont-elles protégées contre l'accès non autorisé ou la corruption durant leur transportation ? | **Exclu** | |
| | **9 CONTRÔLE D'ACCES** | | | | |
| | **9.1 Exigences métier relatives au contrôle d'accès** | | **Objectif :** Limiter l'accès à l'information et aux moyens de traitement de l'information. | | |
| **26** | 9.1.1 Politique de contrôle d'accès | | | | |
| | | **Mesure :** Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information. | Avez-vous élaboré une politique de contrôle d'accès? | **non** | **50%** |
| **27** | 9.1.2 Accès aux réseaux et aux services réseau | | | | |
| | | **Mesure :** Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation. | L'utilisation des services réseau est-elle monitorée et surveillée ? | **oui** | |
| | **9.2 Gestion de l'accès utilisateur** | | **Objectif :** Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information. | | |
| **28** | 9.2.1 Enregistrement et désinscription des utilisateurs | | | | |
| | | **Mesure :** Une procédure formelle d'enregistrement de désinscription des utilisateurs, destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie. | Avez-vous mis en place une procédure d'enregistrement d'un nouvel utilisateur ? | **oui** | **50,00 %** |
| **29** | 9.2.2 Distribution des accès aux utilisateurs | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes. | Un processus simple et documenté d'attribution ou révocation des droits d'accès de tous les types d'utilisateurs à tous les systèmes et services est -il mis en place ? | **Oui** | |
| **30** | 9.2.3 Gestion des droits d'accès à privilèges | | | | |
| | | **Mesure :**L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées. | L'attribution de droits d'accès privilégiés est-il vérifiée et approuver par un processus d'autorisation ? | **Oui** | |
| **31** | 9.2.4 Gestion des informations secrètes d'authentification des utilisateurs | | | | |
| | | **Mesure :**L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel. | Des processus de vérification d'identité avant l'attribution des informations classé secrètes est t-il mis en place ? | **Non** | |
| **32** | 9.2.5 Revue des droits d'accès utilisateurs | | | | |
| | | **Mesure :** Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers. | Les conditions d'expiration des droits d'accès privilégiés sont-elles définies ? | **Non** | |
| **33** | 9.2.6 Suppression ou adaptation des droits d'accès | | | | |
| | | **Mesure :**Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord. | Les droits d'accès des employés et les parties externes sont-ils supprimés à la fin de l'emploi ou contrat, ou ajustés lors de la modification ? | **Non** | |
| | **9.3 Responsabilités utilisateurs** | | **Objectif :** Rendre les utilisateurs responsables de la protection de leurs informations d'authentification. | | |
| **34** | 9.3.1 Utilisation d'informations secrètes d'authentification | | | | |
| | | **Mesure :**Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification. | Les bonnes pratiques d'utilisation des informations secrètes d'authentification ont-elles fait l'objet d'une sensibilisation des utilisateurs? | **oui** | **100%** |
| | **9.4 Contrôle de l'accès au système et à l'information** | | **Objectif :** Empêcher les accès non autorisés aux systèmes et aux applications. | | |
| **35** | 9.4.1 Restriction d'accès à l'information | | | | |
| | | **Mesure :**L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès. | Les accès au SI sont-ils soumis à des procédures sécurisées?<br>Les exploitants sont-ils authentifiés par des mécanismes d'authentification forte ? | **non** | **20%** |
| **36** | 9.4.2 Sécuriser les procédures de connexion | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée. | Les procédures de connexion vérifient-elles les points suivants ?<br>Ne pas afficher d'information tant que la procédure de connexion n'a pas complètement terminé.<br>Enregistrer toutes les tentatives de connexion (échoué ou réussi)<br>Afficher le temps et la date de la dernière connexion.<br>Afficher les détails des tentatives de connexions échoués.<br>Ne pas transmettre les mots de passe en claire sur le réseau. | **Non** | |
| **37** | 9.4.3 Système de gestion des mots de passe | | | | |
| | | **Mesure :**Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe. | Existe-t-il un système de génération et de gestion de mots de passe centralisé ? | **Non** | |
| **38** | 9.4.4 Utilisation de programmes utilitaires à privilèges | | | | |
| | | **Mesure :** L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée. | L'utilisation des programmes utilitaire permettant de contourner les mesures de sécurité d'un système ou d'une application est-elle restreinte et contrôlée ? | **Non** | |
| **39** | 9.4.5 Contrôle d'accès au code source des programmes | | | | |
| | | **Mesure :**L'accès au code source des programmes doit être restreint. | L'accès au code source des programmes est-il limité et contrôlé ? | **Oui** | |
| | **10 Cryptographie** | | | | |
| | **10.1 Mesures cryptographiques** | | **Objectif :** Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information. | | |
| **40** | 10.1.1 Politique d'utilisation des mesures cryptographiques | | | | |
| | | **Mesure :** Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre. | Des méthodes cryptographiques sont-elles développées et mises en œuvre afin de protéger l'information et les données stockées ?<br>Existe-t-il une politique formelle sur l'utilisation des contrôles cryptographique et pour la gestion des clés ? | **non** | **0%** |
| **41** | 10.1.2 Gestion des clés | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie. | Un contrôle qui gere la création, la distribution, les modifications, la sauvegarde et le stockage des clés cryptographiques existe-t-il ? | **Non** | |
| | **11 Sécurité physique et environnementale** | | | | |
| | **11.1 Zones sécurisées** | | **Objectif :** Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation. | | |
| **42** | 11.1.1 Périmètre de sécurité physique | | | | **60%** |
| | | **Mesure :** Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information. | L'organisation a-t-elle définis les zones de sécurités contenant l'information sensible ou critique ? | **oui** | |
| **43** | 11.1.2 Contrôle d'accès physique | | | | |
| | | **Mesure :** Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis. | Les zones sécurisées sont-elles protégées par les contrôles d'entrée appropriés afin de garantir que seul le personnel autorisé peut y accéder ? | **oui** | |
| **44** | 11.1.3 Sécurisation des bureaux, des salles et des équipements | | | | |
| | | **Mesure :** Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées. | Existe-t-il des règles et des contrôles physique appropriés qui assure la protections des biens de valeur ? | **oui** | |
| **45** | 11.1.4 Protection contre les menaces extérieures et environnementales | | | | |
| | | **Mesure :**Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées. | Des procédures de protection physique contre les catastrophes naturelles ou les accidents sont-elles conçues et appliquées ? | **non** | |
| **46** | 11.1.5 Travail dans les zones sécurisées | | | | |
| | | **Mesure :** Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées. | Existe-t-il des règles et des contrôles consernant le travail dans les zones sécurisées | **non** | |
| **47** | 11.1.6 Zones de livraison et de chargement | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés. | | **Exclu** | |
| | **11.2 Matériels** | | **Objectif** : Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation. | | |
| **48** | 11.2.1 Emplacement et protection des matériels | | | | **50,00 %** |
| | | **Mesure :** Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé. | L'équipement est-il protégé contre les pannes d'alimentation et autres interruptions ? | **non** | |
| **49** | 11.2.2 Services généraux | | | | |
| | | **Mesure :** Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux. | avez-vous mis en place des solution pour les coupures de longue durée ? | **non** | |
| **50** | 11.2.3 Sécurité du câblage | | | | |
| | | **Mesure :** Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage. | Le câblage électrique et de télécommunications est-il protégé contre l'interception, les interférences ou les dommages ? | **oui** | |
| **51** | 11.2.4 Maintenance des matériels | | | | |
| | | **Mesure :** Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité. | L'équipement informationnels est-il fréquemment entretenu ? | **oui** | |
| **52** | 11.2.5 Sortie des actifs | | | | |
| | | **Mesure :** Les matériels, les informations ou les logiciels des locaux de l'organisation ne doivent pas sortir sans autorisation préalable. | Y a-t-il un processus qui gère la restitution des actifs informationnel ? | **oui** | |
| **53** | 11.2.6 Sécurité des matériels et des actifs hors des locaux | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site. | | **Exclu** | |
| **54** | 11.2.7 Mise au rebut ou recyclage sécurisé(e) des matériels | | | | |
| | | **Mesure :**Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation. | y a-t-il une politique qui assure la réutilisation des équipement en toute sécurité ? | **Non** | |
| **55** | 11.2.8 Matériels utilisateur laissés sans surveillance | | | | |
| | | **Mesure :** Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée. | L'équipement non surveillé bénéficie-t-il de la protection appropriée ? | **Oui** | |
| **56** | 11.2.9 Politique du bureau propre et de l'écran verrouillé | | | | |
| | | **Mesure :** Une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran verrouillé pour les moyens de traitement de l'information doivent être adoptées. | Adopter-vous une politique qui incite les utilisateurs de votre système a protéger tous type de moyens de traitement d'information | **Non** | |
| | **12 Sécurité liée à l'exploitation** | | | | |
| | **12.1 Procédures et responsabilités liées à l'exploitation** | | **Objectif :** Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information. | | |
| **57** | 12.1.1 Procédures d'exploitation documentées | | | | **75%** |
| | | **Mesure :** Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés. | Les procédures d'exploitation sont-elles documentées et mises à la disposition de tous les utilisateurs qui en ont besoin ? | **oui** | |
| **58** | 12.1.2 Gestion des changements | | | | |
| | | **Mesure :** Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés. | Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information affectant la sécurité de l'information sont-ils contrôlés ? | **oui** | |
| **59** | 12.1.3 Dimensionnement | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système. | des prévisions des besoins en capacité ( de stockage de données , de puissance de traitement , de communication ) sont-t-ils élaboré ? | **Non** | |
| **60** | 12.1.4 Séparation des environnements de développement, de test et d'exploitation | | | | |
| | | **Mesure :** Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation. | Les environnements de développement, de test et d'exploitation sont-ils séparés ? | **Oui** | |
| | **12.2 Protection contre les logiciels malveillants** | | **Objectif :** S'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants. | | |
| **61** | 12.2.1 Mesures contre les logiciels malveillants | | | | |
| | | **Mesure :** Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants. | Existe-t-il des contrôle (détection, prévention ) pour se protéger contre les logiciels malveillants ? | **non** | **0%** |
| | **12.3 Sauvegarde** | | **Objectif :** Se protéger de la perte de données. | | |
| **62** | 12.3.1 Sauvegarde des informations | | | | |
| | | **Mesure :**Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue. | Des copies des informations et des images du système sont-elles prises régulièrement conformément à une politique de sauvegarde définie ?<br>Les sauvegardes sont-ils stockés à un emplacement distant suffisamment pour échapper à un dommage causé par une catastrophe sur le site principal ? | **non** | **0%** |
| | **12.4 Journalisation et surveillance** | | **Objectif :** Enregistrer les événements et générer des preuves. | | |
| **63** | 12.4.1 Journalisation des événements | | | | **50%** |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement. | Les journaux d'événements enregistrant les activités des utilisateurs, les exceptions, les défauts et les événements sont-ils produits, conservés et revus régulièrement ? | **Oui** | |
| **64** | 12.4.2 Protection de l'information journalisée | | | | |
| | | **Mesure :**Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé. | Veillez-vous à ce que les journaux générer et les moyens de journalisation soient stockés de manière sécurisée et inviolable ? | **Non** | |
| **65** | 12.4.3 journaux administrateur et opérateur | | | | |
| | | **Mesure :**Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement. | les comptes privilégiés tels que les administrateurs système et les opérateurs système bénifissent-ils d' un niveaux de journalisation plus élevés ? | **Oui** | |
| **66** | 12.4.4 Synchronisation des horloges | | | | |
| | | **Mesure :** Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique. | Les horloges de tous les systèmes de traitement d'information sont-elles synchronisées avec une seule source de temps de référence ? | **Non** | |
| | **12.5 Maîtrise des logiciels en exploitation** | | **Objectif :** Garantir l'intégrité des systèmes en exploitation. | | |
| **67** | 12.5.1 Installation de logiciels sur des systèmes en exploitation | | | | **100%** |
| | | **Mesure :**Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur des systèmes en exploitation. | Des procédures qui contrôle l'installation de logiciels sur des systèmes opérationnels sont-ils mises en place ? | **Oui** | |
| | **12.6 Gestion des vulnérabilités techniques** | | **Objectif :** Empêcher toute exploitation des vulnérabilités techniques. | | |
| **68** | 12.6.1 Gestion des vulnérabilités techniques | | | | **50%** |
| | | **Mesure :**Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé. | Les rôles et les responsabilités associés à la gestion technique des vulnérabilités y compris le suivi, l'évaluation des risques et l'application des correctifs sont-ils identifiés ? | **non** | |
| **69** | 12.6.2 Restrictions liées à l'installation de logiciels | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre. | Les règles régissant l'installation de logiciels par les utilisateurs existe t'-ils ? | **oui** | |
| | **12.7 Considérations sur l'audit des systèmes d'information** | | **Objectif :** Réduire au minimum l'impact des activités d'audit sur les systèmes en exploitation. | | |
| **70** | 12.7.1 Mesures relatives à l'audit des systèmes d'information | | | | |
| | | **Mesure :**Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier. | Des audits et des activités impliquant la vérification des systèmes opérationnels sont-ils programmés ? | **non** | **0%** |
| | **13 Sécurité des communications** | | | | |
| | **13.1 Signalement des événements et des failles liés à la sécurité de l'information** | | **Objectif :** Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie. | | |
| **71** | 13.1.1 Contrôle des réseaux | | | | |
| | | **Mesure :** Les équipements réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications. | Les responsabilités et les procédures de gestion des équipements réseau sont-elles établies ? | **oui** | **66,60 %** |
| **72** | 13.1.2 Sécurité des services de réseau | | | | |
| | | **Mesure :** Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés. | Existe-t-ils des contrats ou les exigences de gestion de tous les services réseau sont identifiés et inclus ? | **non** | |
| **73** | 13.1.3 Cloisonnement des réseaux | | | | |
| | | **Mesure :** Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux. | Les groupes de services et groupes utilisateurs sont-ils séparés sur le réseau ? | **Oui** | |
| | **13.2 Transfert de l'information** | | **Objectif :** Maintenir la sécurité de l'information transférée au sein de l'organisme et vers une entité extérieure. | | |
| **74** | 13.2.1 Politiques et procédures de transfert de l'information | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication. | Existe-t-il des contrôles spéciaux pour protéger la confidentialité et l'intégrité des données qui circule dans les réseaux de l'organisme ? | **non** | **33,30 %** |
| **75** | 13.2.2 Accords en matière de transfert d'information | | | | |
| | | **Mesure :**Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers. | Les accords entre l'organisation et les parties externes traitent-ils le transfert sécurisé des informations ? | **Exclu** | |
| **76** | 13.2.3 Messagerie électronique | | | | |
| | | **Mesure :** L'information transitant par la messagerie électronique doit être protégée de manière appropriée. | Existe-t-il une mesure concernant l'utilisation de la messagerie et la protection des informations ? | **Oui** | |
| **77** | 13.2.4 Engagements de confidentialité ou de non-divulgation | | | | |
| | | **Mesure :** Les exigences en matière d'engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation. | Est-ce que toutes informations est protégée par un accord de confidentialité et de non-divulgation régulièrement revues et documentées reflétant les besoins de l'organisation en matière de protection des informations ? | **Non** | |
| | **14 Acquisition, développement et maintenance des systèmes d'information** | | | | |
| | **14.1 Exigences de sécurité applicables aux systèmes d'information** | | **Objectif :** Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d'information fournissant des services sur les réseaux publics. | | |
| **78** | 14.1.1 Analyse et spécification des exigences de sécurité de l'information | | | | **100%** |
| | | **Mesure :** Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants. | Les exigences relatives à la sécurité de l'information sont-elles incluses dans les exigences relatives aux nouveaux systèmes d'information ou aux améliorations apportées aux systèmes existants ? | **oui** | |
| **79** | 14.1.2 Sécurisation des services d'application sur les réseaux publics | | | | |
| | | **Mesure :** Les informations liées aux services d'application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents contractuels, ainsi que la | Les informations passant sur des réseaux publics sont-elles protégées contre les activités frauduleuses, les litiges contractuels, les divulgations et modifications non autorisées ? | **exclu** | |

| | | | | | |
|---|---|---|---|---|---|
| | | divulgation et la modification non autorisées. | | | |
| **80** | 14.1.3 Protection des transactions liées aux services d'application | | | | |
| | | **Mesure :** Les informations impliquées dans les transactions liées aux services d'application doivent être protégées pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission. | Les informations impliquées dans les transactions de service d'application sont-elles protégées ? | **Exclu** | |
| | **14.2 Sécurité des processus de développement et d'assistance technique** | | **Objectif :** S'assurer que les questions de sécurité de l'information sont étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information. | | |
| **81** | 14.2.1 Politique de développement sécurisé | | | | **50%** |
| | | **Mesure :** Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation. | Y a-t-il des règles indiquant comment la sécurité doit être prise pour le développement de logiciels et de systèmes ? | **oui** | |
| **82** | 14.2.2 Procédures de contrôle des changements de système | | | | |
| | | **Mesure :** Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles. | Les modifications apportées aux systèmes pendant le développement sont-elles contrôlées par l'utilisation de procédures de contrôle des modifications ? | **non** | |
| **83** | 14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation | | | | |
| | | **Mesure :** Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité. | Lorsque les plates-formes d'exploitation sont modifiées, les applications sont-elles examinées et testées afin de s'assurer qu'il n'y a pas d'impact négatif sur les opérations de l'organisation ou la sécurité ? | **oui** | |
| **84** | 14.2.4 Restrictions relatives aux changements apportés aux progiciels | | | | |
| | | **Mesure :** Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé. | Les modifications apportées aux progiciels sont-elles limitées aux modifications nécessaires.<br>Est-ce que les modifications sont strictement contrôlées ? | **oui** | |
| **85** | 14.2.5 Principes d'ingénierie de la sécurité des systèmes | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information. | les travaux de mise en œuvre des systèmes d'information tient-ils en compte les principes d'ingenierie de la sécurité des systemes ? | **non** | |
| **86** | 14.2.6 Environnement de développement sécurisé | | | | |
| | | **Mesure :**Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée. | Les environment de development sont-ils protégés ? | **Non** | |
| **87** | 14.2.7 Développement externalisé | | | | |
| | | **Mesure :** L'organisation doit superviser et contrôler l'activité de développement du système externalisée. | L'organisation supervise-t-elle l'activité de développement des systèmes externalisé ? | **Exlcu** | |
| **88** | 14.2.8 Test de la sécurité du système | | | | |
| | | **Mesure :**Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement. | Les tests des fonctionnalités de sécurité sont-ils effectués au cours du développement ? | **Oui** | |
| **89** | 14.2.9 Test de conformité du système | | | | |
| | | **Mesure :** Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions. | les nouveaux systèmes d'information, les mises à jour et les nouvelles versions des systemes existant ont-elles des programmes de test de conformité bien déterminés | **Non** | |
| | **14.3 Données de test** | | **Objectif :** Garantir la protection des données utilisées pour les tests. | | |
| **90** | 14.3.1 Protection des données de test | | | | **100%** |
| | | **Mesure :** Les données de test doivent être sélectionnées avec soin, protégées et contrôlées. | Les données de test sont-elles contrôlées et sélectionnées à ce qu'il n'y a pas de divulgation d'information critique ou confidentielle ? | **oui** | |
| | **15 Relations avec les fournisseurs** | | | | |
| | **15.1 Sécurité dans les relations avec les fournisseurs** | | **Objectif :** Garantir la protection des actifs de l'organisation accessible aux fournisseurs. | | |
| **91** | 15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs | | | | **0,00%** |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être acceptées par le fournisseur et documentées. | une approche plus prospective de la sécurité de l'information avec les fournisseurs les plus stratégiques (risque élevé) existe-t-elle ? | **non** | |
| **92** | 15.1.2 La sécurité dans les accords conclus avec les fournisseurs | | | | |
| | | **Mesure :** Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation. | Les exigences en matière de sécurité de l'information pour atténuer les risques associés à l'accès des fournisseurs aux actifs de l'organisation et autre information sont-elles définies et documentées ? | **Non** | |
| **93** | 15.1.3 Chaîne d'approvisionnement des produits et des services informatiques | | | | |
| | | **Mesure :** Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques. | | **Non** | |
| | **15.2 Gestion de la prestation du service** | | **Objectif :** Maintenir le niveau convenu de sécurité de l'information et de service conforme aux accords conclus avec les fournisseurs. | | |
| **94** | 15.2.1 Surveillance et revue des services des fournisseurs | | | | |
| | | **Mesure :** Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs. | L'organisation vérifie, contrôle et surveille-t-elle les services des fournisseurs ? | **oui** | |
| **95** | 15.2.2 Gestion des changements apportés dans les services des fournisseurs | | | | |
| | | **Mesure :** Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques. | les changements effectués lors d'une prestation de service sont-elles gérés selon la criticité de l'information ? | **non** | **50%** |
| | **16 Gestion des incidents liés à la sécurité de l'information** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | **16.1** | **Gestion des incidents liés à la sécurité de l'information et améliorations** | **Objectif :** Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité | | |
| **96** | 16.1.1 Responsabilités et procédures | | | | **28,57 %** |
| | | **Mesure :** Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information. | Les responsabilités et des procédures de gestion sont- elles établies pour assurer une réponse rapide, efficace et ordonnée aux incidents de sécurité de l'information ? | **Non** | |
| **97** | 16.1.2 Signalement des événements liés à la sécurité de l'information | | | | |
| | | **Mesure :** Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées. | Les employés et les parties intéressées associées sont-ils informés de leur obligation de signaler les incidents de sécurit | **Oui** | |
| **98** | 16.1.3 Signalement des failles liées à la sécurité de l'information | | | | |
| | | **Mesure :** Les salariés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services. | Les salariés et les sous-traitants comuniquent t-ils les failles de sécurité observée dans les systèmes d'information ou les services qu'ils utilisent ? | **Oui** | |
| **99** | 16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision | | | | |
| | | **Mesure :**Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information. | Les événements de sécurité de l'information sont-ils évalués pour décider s'ils doivent être classés comme incidents de sécurité ? | **Non** | |
| **100** | 16.1.5 Réponse aux incidents liés à la sécurité de l'information | | | | |
| | | **Mesure :** Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées. | Les taches de rassemblement des preuves, communication des incidents et le traitement des faiblaisses ont-elles un propriétaire chargé de les gérer ? | **Non** | |
| **101** | 16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information | | | | |
| | | **Mesure :**Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs. | Les connaissances acquises lors de l'analyse et de la résolution des incidents de sécurité des informations seront-ils utilisées au futur ? | **Non** | |
| **102** | 16.1.7 Collecte de preuves | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :** L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve. | Existe-t-il des procédures pour l'identification, la collecte, l'acquisition et la préservation de l'information, qui peuvent servir de preuve ? | **Non** | |
| | **17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité** | | | | |
| | **17.1 Continuité de la sécurité de l'information** | | **Objectif :** La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité. | | |
| **103** | 17.1.1 Organisation de la continuité de la sécurité de l'information | | | | **33,30 %** |
| | | **Mesure :** L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre | L'organisation a-t-elle déterminé ses exigences en matière de sécurité de l'information et la continuité de la gestion de la sécurité dans des différentes situations défavorables, par exemple lors d'une crise ou d'un désastre ? | **oui** | |
| **104** | 17.1.2 Mise en œuvre de la continuité de la sécurité de l'information | | | | |
| | | **Mesure :**L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable. | le niveau de continuité requis pour la sécurité des informations est-il garantis par des contrôles et des processus documente et mise en œuvre par l'organisation ? | **non** | |
| **105** | 17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information | | | | |
| | | **Mesure :**L'organisation doit vérifier les mesures de continuité de la sécurité de l'information mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables. | les contrôles de continuité de la sécurité de l'information sont-ils établis et mis en œuvre et tester à intervalles réguliers afin de s'assurer de leur validité et de leur efficacité ? | **non** | |
| | **17.2 Redondances** | | **Objectif :** Garantir la disponibilité des moyens de traitement de l'information | | |
| **106** | 17.2.1 Disponibilité des moyens de traitement de l'information | | | | **100%** |
| | | **Mesure :**Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité. | Les installations de traitement de l'information sont-elles mises en œuvre avec une redondance suffisante pour répondre aux exigences de disponibilité ? | **oui** | |

| | | | | | |
|---|---|---|---|---|---|
| | **18 Conformité** | | | | |
| | **18.1** | **Conformité aux obligations légales et réglementaires** | **Objectif :** Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité. | | |
| **107** | 18.1.1 Identification de la législation et des exigences contractuelles applicables | | | | **100%** |
| | | **Mesure :** Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisation elle-même. | les exigences légales, réglementaires, contractuelles et législatives pertinentes sont-elles explicitement identifiées, documentées ? | **oui** | |
| **108** | 18.1.2 Droits de propriété intellectuelle | | | | |
| | | **Mesure :**Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires. | Des procédures sont-elles mises en place pour assurer le respect des droits de propriété intellectuelle et à l'utilisation de produits logiciels légale ? | **oui** | |
| **109** | 18.1.3 Protection des enregistrements | | | | |
| | | **Mesure :**Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier. | | **exclu** | |
| **110** | 18.1.4 Protection de la vie privée et protection des données à caractère personnel | | | | |
| | | **Mesure :** La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant. | | **exclu** | |
| **111** | 18.1.5 Réglementation relative aux mesures cryptographiques | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | **Mesure :**Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables. | | **exclu** | |
| | **18.2 Revue de la sécurité de l'information** | | **Objectif :** Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles. | | |
| **112** | 18.2.1 Revue indépendante de la sécurité de l'information | | | | |
| | | **Mesure :**Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus. | les examens de conformité des systemes d'information avec la politiques de sécurité sont-elles planifié ? | **non** | **0,00%** |
| **113** | 18.2.2 Conformité avec les politiques et les normes de sécurité | | | | |
| | | **Mesure :**Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité. | Les systèmes d'information sont-ils régulièrement examinés pour se conformer aux politiques et aux normes de sécurité de l'information ? | **non** | |
| **114** | 18.2.3 Vérification de la conformité technique | | | | |
| | | **Mesure :** Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation. | La conformité technique des systèmes et des réseaux est-elle vérifiée par le bais des outils automatisés a intervalle régulier ? | **non** | |

*Tableau 1:questionnaire d'audit selon les exigences de la norme ISO 27002 :2013*

**Annexe B** : Base de scénarios de risques avec références des mesures de sécurité

| Menaces | Vulnérabilités | Objectifs de sécurité (classé selon l'ISO 27002:2013) | Mesures 1 | Mesures 2 | Mesures 3 | Politique de Sécurité (Chapitre de la PSSI) |
|---|---|---|---|---|---|---|
| Dégât des eaux et Incendie | **Absence de matériels de remplacement** | A.17.1 (Continuité de la sécurité de l'information) | A.17.1.2 (Mise en œuvre de la continuité de la sécurité de l'information) | | | **Continuité de l'activité** |
| | **Absence de plan de reprise des activités essentielles de l'organisme** | A.17.2 (Redondances) | A.17.2.1 (Disponibilité des moyens de traitement de l'information) | | | **Continuité de l'activité** |
| | **Canalisation d'eau à proximité des équipements de terminaison** | A.11.2 (Matériels) | A.11.2.1(Emplacement et protection des matériels) | | | **Protection physique** |
| | **Absence de sauvegarde des données contenues sur les supports** | A.12.3(Sauvegarde) | A.12.3.1(Sauvegarde des informations) | | | **Sauvegardes et journalisation** |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Indisponibilité des ressources | **Matériel sensible aux perturbations électrique (chutes de tension)** | A.11.2 (matériel) | A.11.2.3(Sécurité du câblage) | | | **Protection physique** |
| | **Mauvais dimensionnement des dispositifs de secours énergie (onduleur)** | A.11.2 (matériel) | A.11.2.2 (Services généraux) | | | **Protection physique** |
| | **Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques** | A.11.2 (matériel) | A.11.2.1(Emplacement et protection des matériels) | | | **Protection physique** |
| | **Vieillissement du matériel** | A.11.2(matériel) | A.11.2.4(Maintenance des matériels) | | | **Protection physique** |
| | **Absence de plan de reprise des activités essentielles de l'organisme** | A.17.1 (Continuité de la sécurité de l'information) | A.17.1.2 (Mise en œuvre de la continuité de la sécurité de l'information). | | | **Continuité de l'activité** |
| | **Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication** | A.11.2(Matériel) | A.11.2.1(Emplacement et protection des matériels) | | | **Protection physique** |
| | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Dysfonctionnement logiciel (atteinte à la maintenabilité) | **Absence de procédure de maintenance** | A.12.1(Procédures et responsabilités liées à l'exploitation) | A.12.1.2(Gestion des changements). | | | **Suivi de l'Exploitation** |
| | **Utilisation d'une version obsolète du système d'exploitation ou des applicatifs** | A.14.2 (Sécurité des processus de développement et d'assistance technique) | A.14.2.9(Test de conformité du système) | | | **Suivi de l'Exploitation** |
| | **Absence de conservation des traces des traitements** | A.12.3 (Sauvegarde) | A.12.3.1(Sauvegarde des informations) | A.12.4.1(Journalisation des événements) | A.12.4.3(Journaux administrateur et opérateur) | **Sauvegardes et journalisation** |
| | | A.12.4(Journalisation et surveillance) | | | | |
| | **La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau** | A.12.1(Procédures et responsabilités liées à l'exploitation) | A.12.1.4(Séparation des environnements de développement, de test et d'exploitation) | | | **Suivi de l'Exploitation** |
| | | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.5(Contrôle d'accès au code source des programmes) | A.9.4.4 (Utilisation de programmes utilitaires à privilèges) | | **Contrôle d'accès** |
| | **Non utilisation de normes ou standard dans le cadre du développement du système d'information** | A.14.2 (Sécurité des processus de développement et d'assistance technique) | A.14.2.1(Politique de développement sécurisé) | | | **Suivi de l'Exploitation** |
| | **Aucune vérification des applicatifs n'est faite avant l'installation** | A.12.5(Maîtrise des logiciels en exploitation) | A.12.5.1(Installation de logiciels sur des systèmes en exploitation) | | | **Suivi de l'Exploitation** |

| | | | | | | |
|---|---|---|---|---|---|---|
| Abus ou usurpation de droit | **Absence de dispositif de contrôle d'accès robuste** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.1(Restriction d'accès à l'information) | A.9.4.2(Sécuriser les procédures de connexion) | A.9.4.4(Utilisation de programmes utilitaires à privilèges) | **contrôle d'accès** |
| | **Absence de journalisation des événements** | A.12.4(Journalisation et surveillance) | A.12.4.1(Journalisation des événements) | A.12.4.3(Journaux administrateur et opérateur | | **Contrôle d'accès** |
| | **La base de mots de passe du système d'exploitation est déchiffrable** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.3(Système de gestion des mots de passe) | A.9.4.2(Sécuriser les procédures de connexion) | | **Contrôle d'accès** |
| | **Possibilité d'administrer le système à distance avec des outils d'administration non chiffrés** | A.10.1(Mesures cryptographiques) | A.10.1.1(Politique d'utilisation des mesures cryptographiques) | A.10.1.2(Gestion des clés) | | **Contrôle d'accès** |
| | | | | | | |
| Espionnage à distance | **Pas ou peu de changement de mot de passe d'accès au système ou à l'application** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.2(Sécuriser les procédures de connexion) | | | **Contrôle d'accès** |
| | **Utilisation de mots de passe d'accès au système ou à l'application simples à observer (forme sur un clavier)** | A.9.4(Contrôle de l'accès au système et à l'information) | A.9.4.3(Système de gestion des mots de passe) | A.11.2.9(Politique du bureau propre et de l'écran verrouillé) | | **Contrôle d'accès** |
| | | A.11.2(Matériels) | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Faible sensibilisation à la protection de l'information** | A.7.2(Pendant la durée du contrat) | A.7.2.2(Sensibilisation, apprentissage et formation à la sécurité de l'information s'appliquant à leurs fonctions.) | | | **Organisation de la sécurité** |
| | | | | | | |
| Saturation du système informatique | **Mauvais dimensionnement (ex: trop de données par rapport à la bande passante maximale)** | A.12.1(Procédures et responsabilités liées à l'exploitation) | A.12.1.3(Dimensionnement) | | | **Suivi de l'Exploitation** |
| | **Possibilité de mal configurer** | A.14.2(Sécurité des processus de développement et d'assistance technique) | A.14.2.9(Test de conformité du système) | | | **Suivi de l'Exploitation** |
| | **Possibilité que les relais soient soumis à un nombre trop important de requêtes ou à un parasitage intense (ex: attaque de déni de service type "smurf")** | A.13.1(Signalement des événements et des failles liés à la sécurité de l'information)<br>A.12.1(Procédures et responsabilités liées à l'exploitation) | A.13.1.3 (Cloisonnement des réseaux) | A.12.1.2(Gestion des changements) | | **Suivi de l'Exploitation** |

*Tableau 2:Base de scénarios de risques avec références des mesures de sécurité*

Annexe C : politique de sécurité des systèmes d'information proposé

| |
|---|
| L'ensemble des chapitres du présent document, constitue notre proposition d'une politique de sécurité du système dans le cadre de notre projet de fin d'étude, élaborées à partir de l'organisation prévue par le département SI de la SIM Agro, des mesures de sécurité issues de l'analyse de risque réalisée en commun avec l'ensemble des entités impliquées qui nous aidera à répondre à la sécurité du système d'information du périmetre d'etude soit l'ERP en cours de développement. |

| | | |
|---|---|---|
| **1.Organisation de la sécurité** | | |
| | 6.1.1 Rôles et responsabilités en matière de sécurité de l'information | Le département SI s'engage à définir les responsabilités en matière de sécurité de l'information et les attribuées. Le responsable SI tache d'informer le RSSI de ces attributions et, des lignes directrices et des attentes en matière de sécurité de l'information qu'implique la collaboration à un tel projet. |
| | 7.2.1 Responsabilités de direction | Le département SI s'engage à informer les utilisateurs de l'ERP de leurs attributions et de leurs responsabilités, des lignes directrices et des attentes en matière de sécurité de l'information qu'implique la collaboration à un tel projet. |
| | | Le département SI s'engage à sensibiliser les utilisateurs de l'ERP à l'importance de la sécurité de l'information, à les inciter à respecter les principes et les règles et les procédures. |
| | | Le département SI s'engage à permettre aux utilisateurs de signaler à l'Administration, dans les délais les plus brefs tout fait susceptible de porter préjudice à la sécurité du périmètre du projet. |
| | 7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information | Le département SI s'engage à élaborer et mettre en œuvre un plan de sensibilisation et de formation sur la durée du projet et à préparer un support remis à chacune des personnes sensibilisées et formées. |
| | 8.2.1 Classification de l'information | Le département SI s'engage à élaborer une procédure de classification d'information. |
| | | la procédure utilise l'échelle de classification suivante :<br>• Public ou Non Protégé : les informations traitées par le système sont accessibles à tous<br>• DL - diffusion limitée : les informations traitées par le système ne doivent être accessibles qu'aux personnes ayant accès à l'ERP.<br>• DR - diffusion restreinte : les informations traitées par le système ne doivent être accessibles qu'aux personnes impliquées dans le traitement de ces données.<br>• Classifié - Secret inconditionnel : les informations traitées par le système ne doivent être accessibles qu'aux personnes désignées, habilitées pour les traiter. |

| | | |
|---|---|---|
| | 11.2.9 Politique du bureau propre et de l'écran vide | L'ensemble des informations sensible imprimées ou affichées sur les écrans n'ont pas vocation à être diffusés publiquement. Le département SI s'assure, grâce à une sensibilisation et à des contrôles de sécurité réguliers, que ses collaborateurs prennent les précautions nécessaires pour protéger ces informations, notamment en ne les laissant pas trainer sur les bureaux ou sur les imprimantes, en les stockant dans des meubles fermant à clef, en fermant leurs bureaux, en évitant que leur écran ne soit visible d'un tiers et en utilisant des écrans de protection lorsqu'ils se déplacent. |
| **2.Protection physique** | | |
| | 11.2.1 Emplacement et protection du matériel | Le département SI définit les mesures de gestion appropriées relatives au matériel, au câblage et aux équipements de support afin d'empêcher la perte, les dommages, le vol et la modification non souhaitée de données. |
| | 11.2.2 Services généraux | Pour permettre leur remplacement facile, le département SI s'engage à déployer des équipements et câbles normalisés. |
| | 11.2.4 Maintenance du matériel | Le département SI s'engage à élaborer une procédure d'analyse et de des pannes pour subvenir au besoin de disponibilité des matériels, une planification d'entretien avec les prestataires est mise en place en fonction de la gravité de l'incident. |
| | | Le département SI s'engage à élaborer et mettre en œuvre un plan d'entretien correcte des matériels pour garantir leur disponibilité permanente et leur intégrité. |
| | | Le département SI décrit, et fait valider, les principes de redondance qu'il met en œuvre et les tests réguliers qu'il pratique. |
| **3.Suivi de l'Exploitation** | | |
| | A.12.1(Procédures et responsabilités liées à l'exploitation) | Le département SI s'assure que les procédures d'exploitation des différents environnements sont définies et tenues à jour. |
| | | Le département SI s'assure que les changements due à l'évolutions du système d'information sont pris en compte et tenues à jour. |
| | | Le département SI s'engage à renforcer le système de sauvegarde. |
| | | Les environnements de développements, de tests, de traitements doivent être décrits et cloisonnés entre eux. |
| | | Les accès aux différents environnements de développements doivent être restreint aux employés hors service de développement et tracés pour les développeurs |

| | | |
|---|---|---|
| | A.12.6(Gestion des vulnérabilités techniques) | Le département SI s'engage à assurer le maintien en condition de sécurité des systèmes d'exploitation et des outils utilisés pour l'ensemble des environnements. |
| | A.14.2(Sécurité des processus de développement et d'assistance technique) | Les départements SI et développement s'engagent à prendre en compte la sécurité tout le long du cycle de vie du projet. Le développeur doit montrer qu'il a pris en compte les risques associés à la solution du traitements centralisé des données en décrivant comment il satisfait l'ensemble des prérequis de sécurité associés, et fournir aux auditeurs une documentation ( Architecture Techniques, Spécifications fonctionnelles , rapport de tests, etc.) permettant de comprendre comment les prérequis de sécurité sont atteints par la conception de l'application ainsi que par les mécanismes de sécurité mis en œuvre (par exemple algorithme de chiffrement). |
| | | Le responsable du département de développement doit fournir les recommandations et bonnes pratiques de sécurité suivies par les développeurs lors de l'implémentation de l'application, les outils utilisés permettant leur mise en œuvre ainsi que les recommandations concernant l'écriture, la structure et les commentaires du code. Afin de permettre un audit du code. |
| **4.Continuité de l'activité** | | |
| | 17.1.1 Organisation de la continuité de la sécurité de l'information | Le département SI définit et fait valider une procédure de continuité ou de reprise d'activité pour garantir la disponibilité des moyens de traitement dans le périmètre du projet. |
| | 17.1.2 Mise en œuvre de la continuité de la sécurité de l'information | Le département SI est responsable de la conduite des opérations de continuité ou de reprise d'activité selon la procédure de conduite d'activité |
| | 17.2.1 Disponibilité des moyens de traitement de l'information | Le département SI prévoit et fait valider les dispositifs qu'il met en œuvre (dimensionnement, configuration, redondance, …) selon les normes, pour permettre la disponibilité des moyens de traitement. |
| | A.12.1(Procédures et responsabilités liées à l'exploitation) | Les dispositifs mis en œuvre garantissant la haute disponibilité doivent être situées dans deux locaux différent bâtis sur les standards. |
| **5.Sauvegardes et journalisation** | | |
| | 12.3.1 Sauvegarde des informations | L'ERP en cour de développement fait l'objet de mesures de sauvegarde destinées à permettre de conserver les données importantes et à assurer la continuité et la reprise d'activité. |
| | | Le dispositif de sauvegarde est testé fréquemment, pour valider sa fiabilité. |

| | | |
|---|---|---|
| | 12.4.1 Journalisation des événements | Le département SI définit et fait valider une politique de surveillance précisant les modalités et les durées de conservation des différents journaux ainsi que les méthodes d'analyse des données produites. |
| | | La traçabilité des opérations effectuées sur l'ERP avant (installation, configuration), pendant (traitement de l'information) doit figurer dans la procédure de surveillance. En effet, le respect de cette procédure s'impose pour garantir la supervision des actifs, afin de détecter le moindre dysfonctionnement ou la moindre irrégularité qui pourrait remettre en cause l'intégrité de l'information. |
| | | Chaque élément du système d'information doit transmettre ses évènements vers le système de journalisation. Les accès, anomalies, incidents, attaques, et opérations de gestion et d'administration doivent être conservées en temps réel et un système d'alerte doit être mis en place pour informer immédiatement le Responsable SI de tous évènements suspects. |
| **6.Contrôle d'accès** | | |
| | 9.1 Exigence métier en termes de contrôle d'accès | Le département SI doit renforcer le dispositif de contrôle d'accès mis en place, en l'associant à une politique de contrôle d'accès documentée et revue sur la base des exigences métier et de sécurité de l'information. |
| | | Pour faciliter la gestion et la mise en œuvre du dispositif de contrôle d'accès, les mesures de gestion de contrôle d'accès (si elle doivent demeurer individuelles, imputables et journalisables), peuvent être catégorisées en profils accordés à des populations de personnes homogènes et disposant du même rôle (administrateurs systèmes, administrateurs de bases de données, surveillance de sécurité, gestionnaires de paie …). |
| | | Les mesures de contrôle du droit d'accès permettent une imputabilité individuelle doivent faire l'objet de mesures d'enregistrement d'événements (usage du droit d'accès, modification du droit d'accès) permettant d'identifier l'action, la personne qui a réalisé l'action et le résultat de l'action (succès ou échec). |
| | | Les fonctions nécessitant un privilège élevé (gestion des droits d'accès, configuration des systèmes et des applications, …) doivent pouvoir être isolées et journalisées spécifiquement afin de les intégrer dans un système de supervision et d'alerte. |
| | 9.2 Gestion de l'accès utilisateur | L'enregistrement, la gestion et la désinscription des utilisateurs du système doit figurer dans la politique de contrôle d'accès pour permettre la configuration des opérations de création, de modification ou de suppression d'identifiants et celles qui consistent à associer à ces identifiants des droits sur le système. |

| | | |
|---|---|---|
| | | Le département SI s'attache à élaborer une procédure formelle rattaché a la politique de contrôle d'accès pour la maitrise des privilèges d'accès et d'utilisation du système. |
| | | La revue des droits est annuelle avec une possibilité de revue exceptionnelle à la demande des supérieurs hiérarchique. |
| | | La suppression des droits d'accès ou l'adaptation des droits d'accès sont mises en œuvre au sein du dispositif de gestion des utilisateurs mis en place. |
| | | La suppression et l'adaptation interviennent lorsque les utilisateurs n'ont plus de raison d'accéder au système ou que leurs droits doivent être modifiés. |
| | 9.3 Responsabilité des utilisateurs | Chaque utilisateur du système est responsable des informations secrètes d'authentification qui lui sont confiées, il doit signaler toute anomalie lors de son authentification au système, de signaler une utilisation de ces informations secrètes en son absence et de procéder au renouvellement de ces informations. |
| | | Le département SI prévoit un module d'information et de sensibilisation de l'utilisateur à cette responsabilité, notamment pour la protection de son ordinateur contre les codes malveillants et pour les bonnes pratiques en matière d'usage de ces informations secrètes. |

*Tableau 3: politique de sécurité des systèmes d'information*